Avaya CallPilot® High Availability: Installation and Configuration

5.0
NN44200-311, 01.26
April 2012

© 2012 Avaya Inc.

All Rights Reserved.

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/ 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 ... 7
- Getting technical documentation ... 7
- Getting product training ... 7
- Getting help from a distributor or reseller ... 7
- Getting technical support from the Avaya Web site ... 8

Chapter 2: Introduction ... 9
- In this chapter ... 9
- Overview of High Availability ... 9
- High Availability hardware ... 10
- Heartbeat signals ... 10
- Mirroring ... 10
- Managed TCP/IP settings ... 11
- Switch connectivity ... 12
- High Availability network ... 12
- AutoStart software ... 13
- Failovers ... 14
- Geographic Redundancy versus High Availability ... 14
- Limitations ... 15
- Reference documents ... 16

Chapter 3: Preparing for Installation ... 19
- In this chapter ... 19
- Introduction ... 19
- Management of the TCP/IP network ... 19
- Network planning ... 21
- Planning the High Availability configuration ... 22
- High Availability system checklist ... 22
- Facility planning ... 25
- Switch planning ... 25
- Meridian 1 planning ... 26
- CS 1000 planning ... 27
- Required hardware ... 27
- Hardware included ... 27
- Customer provided equipment ... 29
- Supported hardware configurations ... 29

Chapter 4: Failover overview ... 31
- In this chapter ... 31
- Introduction ... 31
- Automatic failovers ... 32
- Manual failovers ... 33

Chapter 5: Install and configure the High Availability pair ... 35
- In this chapter ... 35
- New system installation procedure ... 35
- Prepare the switch and install the 1005r or 1006r servers ... 38
- Prepare both 1005r or 1006r servers ... 39

Configure CP1 and CP2 using the CallPilot Configuration Wizard ... 42
Connect and verify LAN connections ... 52
Run Stage 1 of the High Availability Configuration Wizard to check CP1 and CP2 configuration ... 58
Install the AutoStart Agent and Console software ... 62
Install the AutoStart software on CP1 ... 62
Add the node 2 administrator account to the AutoStart Console on node 1 ... 70
Install the AutoStart software on CP2 ... 72
Configure the AutoStart software ... 81
Configure the AutoStart software on CP1 ... 81
Import the AutoStart definition file on CP1 ... 88
Add the Windows administrator password for the AutoStart Utility Processes ... 89
Add e-mail addresses to the Managed_ELAN_IP_Failure_Notif rule ... 90
Bring the Resource Groups online ... 92
Bring the CallPilot Resource Group online on CP1 ... 93
Bring the Resource Groups CallPilot_[CP1] and CallPilot_[CP2] online ... 95
Test your configuration ... 97
Create the CallPilot Reporter connections ... 98
Add the servers to a Windows domain ... 99
Chapter 6: Maintaining a High Availability system ... 105
In this chapter ... 105
Avaya CallPilot® Configuration Wizard ... 106
Change the Server Information ... 106
Computer name changes ... 109
Administrator account changes ... 111
Change the Media Allocation ... 113
Change the Switch Configuration ... 115
Install a new language ... 117
Change the Network Interface Card configuration and network settings ... 120
Local networking settings ... 121
Managed networking settings ... 126
Change the administrator account password for the Utility Processes ... 131
Increase software licenses ... 133
Increase CallPilot channel capacity by adding MPB96 boards ... 141
Working with domains and workgroups ... 147
Moving from a domain to a workgroup ... 147
Manually change the administrator password ... 151
EMC AutoStart Agent and Console ... 153
AutoStart maintenance ... 153
Configure the AutoStart notification settings ... 154
Add e-mail addresses to the Managed_ELAN_IP_Failure_Notif rule ... 156
Configure failover on the Path Test failures of the Managed ELAN IP address ... 158
License administration ... 160
Check the status of the servers and failovers using AutoStart ... 161
Import and export of the AutoStart Definition file ... 164
Recreate the AutoStart definition file ... 167
Change the Switch IP address in AutoStart Console ... 172
Work with resource groups ... 175

Bring a resource group online ... 176
Take a resource group offline ... 177
Perform failovers and monitoring ... 179
Automatic failovers ... 179
Manual failovers ... 181
Software operations ... 183
Install the AutoStart Console on a stand-alone PC ... 183
Uninstall the AutoStart software ... 192
Reinstall the AutoStart software ... 195
EMC software updates (AutoStart Agent/Console) ... 195
Support ... 195
Install PEPs ... 195
Uninstall PEPs ... 198
Uninstalling PEPs ... 198
Microsoft Hotfixes ... 200
Remote support ... 200
USB modem dial-in ... 200
Remote Access tools ... 203
Backup and restore ... 203
Restoring the High Availability system ... 208
Reimage or replace a server in the High Availability pair ... 209
Installing the AutoStart software on the replacement server ... 216
RAID splitting for HA systems ... 226
Splitting the RAID on a 1005r server ... 226
Splitting the RAID on a 1006r server ... 229
CallPilot Manager, Channel Monitor ... 231
Chapter 7: Upgrades, migrations, and feature expansion ... 233
In this chapter ... 233
Introduction ... 233
Guidelines ... 235
Feature Expansion: Adding the High Availability feature to an existing CallPilot 5.0 1005r or 1006r server 237
Feature expansion task list ... 238
Prepare the switch ... 238
Install the new 1005r or 1006r server (CP2) ... 239
Record the current 1005r or 1006r server configuration (CP1) ... 240
Run the Upgrade Wizard on the existing server (CP1) ... 241
Prepare the new 1005r or 1006r server (CP2) ... 244
Run the Setup Wizard on CP2 ... 244
Configure CP1 using the Configuration Wizard ... 249
Configuring the replacement server using the Configuration Wizard ... 252
Complete the High Availability configuration process ... 257
Index ... 261

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 7
- Getting product training on page 7
- Getting help from a distributor or reseller on page 7
- Getting technical support from the Avaya Web site on page 8

Getting technical documentation

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

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: Introduction

In this chapter

Overview of High Availability on page 9

High Availability hardware on page 10

High Availability network on page 12

AutoStart software on page 13

Failovers on page 14

Limitations on page 15

Reference documents on page 16

Overview of High Availability

In a High Availability configuration, a pair of peer Avaya CallPilot® servers are used in the place of a single server. Both servers are connected to the same switch (Meridian 1 or Communication Server 1000 [CS 1000]) and they are configured so that one Avaya CallPilot server is active (that is, processing calls) and the other server is in standby mode.

The standby server takes over if the active server fails (due to predefined failure conditions), or if the administrator decides to manually switch over to the standby server. This process is known as a failover. For more information, see Failovers on page 14.

To support a High Availability configuration for CallPilot, a combination of hardware and third-party software is required, as follows:

- There is an entry in the CallPilot 5.0 keycode for the High Availability feature.
- High Availability is supported only on the 1005r and 1006r platforms. For more information about the hardware, see High Availability hardware on page 10.
- System control and monitoring and disk mirroring of the High Availability system is provided by the EMC AutoStart software. For more information, see AutoStart software on page 13.

High Availability hardware

High Availability is supported on the 1005r and 1006r platforms only. Two servers, either a 1005r pair or 1006r pair, are required for the High Availability configuration.

The 1005r and 1006r servers are equipped with two extra dual-Ethernet interface cards that provide the following three connections between the two High Availability servers:

- The Heartbeat signal (HB1) connection is used to monitor the state of the active server.
- The Heartbeat backup signal (HB2) connection is a backup of HB1 in case the IP interface for HB1 fails.
- The Mirroring connection is used for mirroring data between the two servers.

Important:

These three connections are critical to High Availability operation. Avaya recommends that these three connections be made directly, using crossover cables instead of a hub or switch. Failure of any device such as a hub or switch in the signal path can create an unwanted results.

Heartbeat signals

The standby server needs a way to tell if the active server is running to know when to take control if the active serves ceases to run. This is accomplished through the use of a heartbeat signal that is communicated between the active and standby server.

Due to the importance of the heartbeat signal, a pair of physical links (Heartbeat 1 and Heartbeat 2) between the active and the standby servers are used to transport the signal. This way, if either of the links fail, the heartbeat signal still has a path between the two servers.

Mirroring

In order for the standby server to take over call processing, the server must have the same configuration as the failed active server and have access to all of the data (such as the users and the Application Builder applications) on the failed server. This task is accomplished by mirroring data between the two servers. This way, if an active server fails, the standby server of the pair has an up-to-date copy of all of the data from the active server so it can take over the role of the failed active server.

Managed TCP/IP settings

To the external IP network (including the end users, the switch, and the CallPilot Web applications) the pair of servers must look like one server. To accomplish this, Managed IP (also called virtual IP) addresses and host name settings are used. The Managed IP addresses and host name settings allow the pair of CallPilot High Availability servers to appear as one IP address to the outside IP network.

The following figure shows two CallPilot servers and the connections between them.

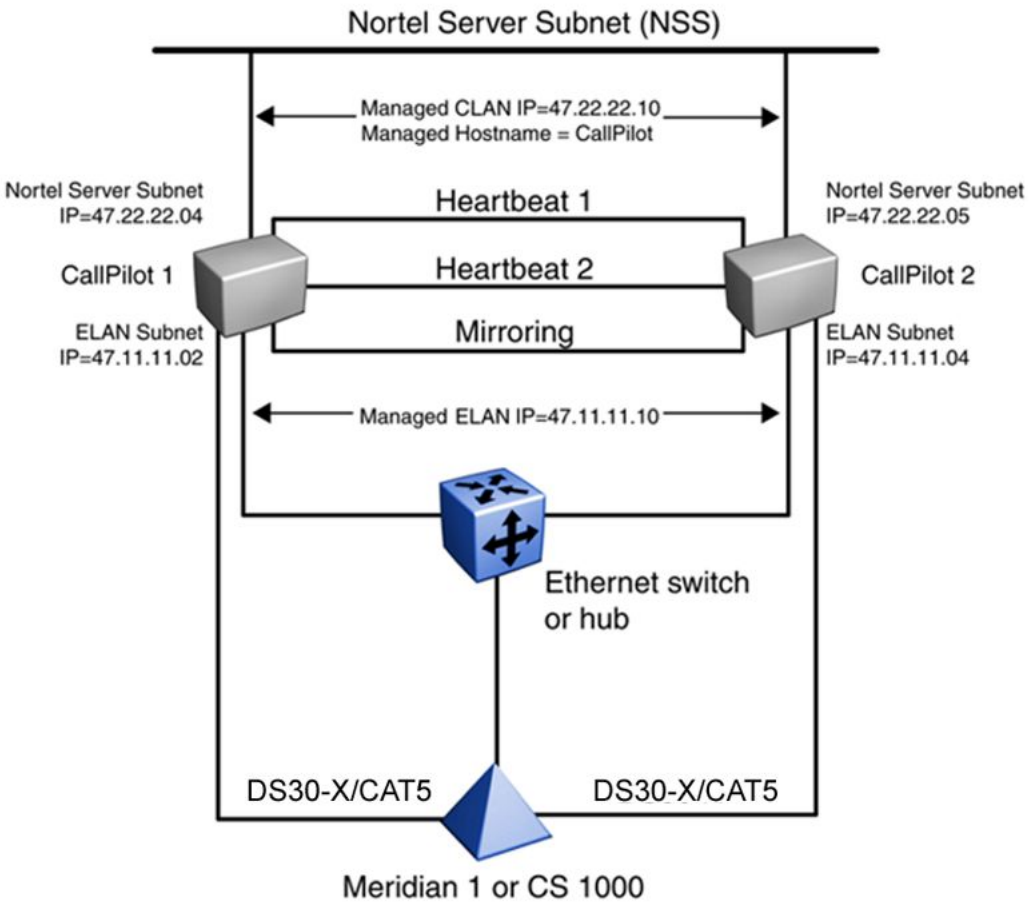


Figure 1: Example of a High Availability system

Switch connectivity

Both CallPilot servers in a High Availability pair are connected to the switch by cables. The 1005r servers can be connected to the switch by either DS30X or CAT5 cables. The 1006r servers can only be connected to the switch by CAT5 cables. The number of MGate cards required in the switch is double the number required for a single CallPilot server. For a pair of servers providing 192 channels, the switch must have a total of 12 MGate cards installed (six MGate cards per 192 channels times two servers). At any one time only one of the two CallPilot servers is up and running. Therefore, even though there are 384 channels configured on the switch, a maximum of 192 channels are available for call processing at any one time.

High Availability network

The following figure shows the network containing the two High Availability servers (CallPilot 1 and CallPilot 2).

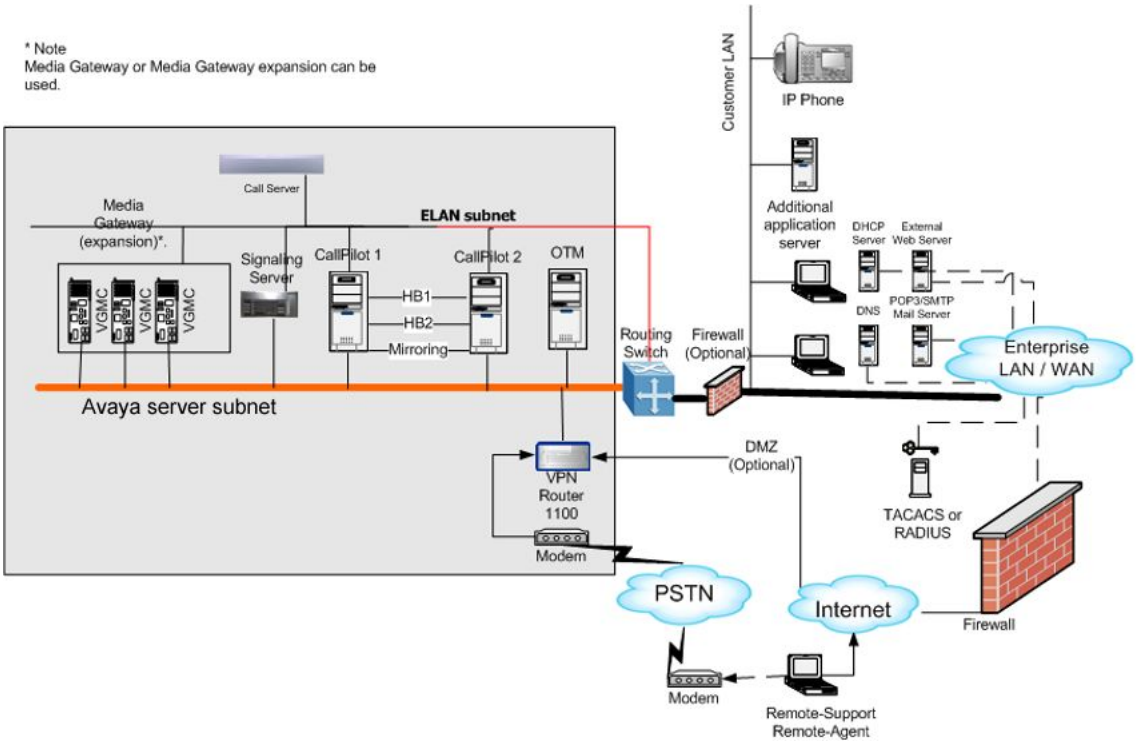


Figure 2: High Availability network

AutoStart software

The AutoStart software is installed on each server and performs the following functions:

- Monitors the status of both servers in the High Availability pair.
- Performs an automatic failover when a failure condition is detected.
- Keeps the hard drives on both servers synchronized through a mirroring process.
- Manages the IP addresses of the ELAN subnet and Avaya Server subnet, making the server pair appear as a single server to the network.
- Provides a mechanism for administrator-initiated (manual) failovers.

The CallPilot High Availability system uses the following components of the AutoStart software:

- AutoStart Agent—The Agent software resides on both CallPilot servers and provides the disk mirroring and managed IP services. The AutoStart Agent includes the set of processes that performs the AutoStart monitoring and management functionality.
- AutoStart Backbone—The AutoStart Backbone includes the processes running on the AutoStart Agent that provide messaging services.
- AutoStart Console—The Console software provides a visual interface to the High Availability server pair and is used to administer the Agent software installed on the CallPilot servers. By default, the Console software is installed on both CallPilot servers so administration of the pair can be done when the administrator is logged on to either server; however, the Console software can also be installed on a PC on the Avaya Server subnet for remote administration.

  The AutoStart Console provides the following:

  - A centralized monitoring and administration tool for taking managed resources and resource groups online and offline, which reduces administrative overhead.
  - A real-time reflection of object states. As soon as AutoStart detects a state change for an object, the graphical interface updates its display to reflect that change. See Checking the status of the servers and failovers on page 162.
  - An interface to define and configure all the managed resources from a single local or remote location.

The AutoStart software is manually installed when you configure the pair of CallPilot servers with the High Availability feature. The required AutoStart software is included on the CallPilot 5.0 Applications CD.

Important:

This version of the software is tested and verified to work correctly with the CallPilot 5.0 High Availability feature. The AutoStart software on the CallPilot server must not be updated or patched unless the new software or patch is tested and validated by Avaya.

Failovers

In a High Availability system, one server is active while the other is in the standby mode. If a predefined failure occurs on the active server, the standby server comes into service, becoming the active server. The process of the standby server becoming the active server is called a failover.

For more information, see Failover overview on page 31.

Geographic Redundancy versus High Availability

CallPilot provides two features that increase server availability: Geographic Redundancy (GR) and High Availability (HA). Each feature has different characteristics due to underlying architecture. The following table provides a high level comparison between GR and HA.

	Geographic Redundancy	High Availability
Location of servers relative to one another	No restrictions	Co-located
Supported Platforms	202i, 600r, 1005r, 1006r, 703t	1005r and 1006r
Configuration	Active-active	Active-standby only
Replication	VPIM (only users, messages and some system settings are replicated)	Disk mirroring (only active server can access mirrored disks)
Dongle and keycode	Each server has its own dongle and keycode.	One shared between the HA pair.
CS 1000	Each server can be connected to either the same or a different CS 1000.	Each server must be connected to the same CS 1000.

Note:
GR and High Availability can not coexist on the same server. For more information about GR, refer to the *Geographic Redundancy Application Guide*, (NN44200-322).

Limitations

The limitations of the High Availability system include the following:

- The High Availability pair must consist of the same server type. A mixture of server types is not supported. For example, a High Availability pair can not consist of a 1005r and a 1006r.
- The two High Availability servers must be collocated. The locations of the servers are limited by the length of the cables that connect the High Availability servers to the Meridian 1 or CS 1000 switch. The 1005r High Availability pair can use either DS30X or CAT5 cables while the 1006r High Availability pair can only use CAT5 cables. The maximum length of the DS30X cables is 60 feet or 18.29 meters long. The maximum length of the CAT5 cables is 1968.50 feet or 600 meters long.
- Failover limitations include the following:
  - Any connections (that is, calls in progress) to the active CallPilot server are lost after a automatic or manual failover occurs.
  - There is a window during the failover when neither the active nor standby server is available; therefore, the CallPilot system is inaccessible. In the default configuration, voice processing is not available for approximately 10 minutes after the failover is started. This time can be decreased by disabling the DSP diagnostics. Other services, such as Internet Message Access Protocol (IMAP) connections, may be available in a shorter window.
  - Only a limited number of automatic failover cases are supported, as follows:
    - A reboot or shut down of the active server.
    - Loss of connection on the ELAN at the TCP/IP level (for example, failure of the server to respond to the ping command for a specified period of time).
    - Failure of one or more of the critical CallPilot services. The system attempts to restart a failed critical CallPilot service three times before resorting to a failover.
- Mirroring limitations include the following:
  - Due to the way the AutoStart software does disk mirroring, the mirrored drives cannot be accessed on the standby server while in use on the active server. This means that the multimedia file system (MMFS), database, and Application Builder applications cannot be accessed on the standby server while the active server is up and running.
  - There is no way to break the mirroring between the active and standby servers (to make the mirrored drives visible on the standby server while the active server is running) without also temporarily taking down the active server.

- Performance Enhancement Packages (PEPs) must be applied individually to each server in the High Availability pair.
- The CallPilot 5.0 High Availability feature does not support geographic redundancy.
- The Voice Profile for Internet Mail (VPIM) prefix on both servers in a High Availability server must be the same.
- If the High Availability system is part of a Windows Domain, both servers (CP1 and CP2) must belong to the same Windows domain.
- The CallPilot system monitor cannot run on the standby server as there are no database, MMFS access, or CallPilot services running.
- If scheduled backups are performed to a local tape drive on the active server, the backup fails after a switchover unless the tape drive is physically moved and connected to the standby server or a second tape drive is connected to the standby server.
- If scheduled backups are performed to a remote backup device (that is, a network share), the same backup device must be configured through CallPilot Manager on both servers in the pair. If the device is only defined on the active server, any scheduled backups to that device fail on the standby server.
- The computer names of the High Availability servers must contain only alphanumeric characters. Nonalphanumeric characters (such as a hyphen [-]) are not allowed.
- In CallPilot 5.0, you can use the High Availability feature with CallPilot and Contact Center 6 and 7 integration, but it requires supplemental PEP updates to CS 1000, Contact Center, and CallPilot. For more information about CallPilot High Availability and Contact Center Inter-working, see DTR-2007-0069-Global-Rev12 – CallPilot Release 5.0 (see appendices specific for High Availability and Contact Center inter-working)

Reference documents

For a list of all CallPilot documents, see the following CallPilot Customer Documentation Map.

Table 1: Call Pilot Customer Documentation Map

Fundamentals
Fundamentals Guide (NN44200-100)
Library Listing (NN44200-117)
Planning and Engineering
Planning and Engineering Guide (NN44200-200)
Network Planning Guide (NN44200-201)
Converging the Data Network with VoIP Guide (NN43001-260)

- Solution Integration Guide for Communication Server 1000/Call Pilot/Contact Center/Telephony Manager (NN49000-300)

Installation and Configuration

- Upgrade and Platform Migration Guide (NN44200-400)
- High Availability: Installation and Configuration (NN44200-311)
- Geographic Redundancy Application Guide (NN44200-322)
- Installation and Configuration Task List Guide (NN44200-306)
- Quickstart Guide (NN44200-313)
- Installer Roadmap (NN44200-314)
- Server Installation Guides
  - 201i Server Hardware Installation Guide (NN44200-301)
  - 202i Server Hardware Installation Guide (NN44200-317)
  - 202i Installer Roadmap (NN44200-319)
  - 703t Server Hardware Installation Guide (NN44200-304)
  - 1002rp Server Hardware Installation Guide (NN44200-300)
  - 1002rp System Evaluation (NN44200-318)
  - 1005r Server Hardware Installation Guide (NN44200-308)
  - 1005r System Evaluation (NN44200-316)
  - 1006r Server Hardware Installation Guide (NN44200-320)
  - 600r Server Hardware Installation Guide (NN44200-307)
  - 600r System Evaluation (NN44200-315)
- Configuration and Testing Guides
  - Meridian 1 and CallPilot Server Configuration Guide (NN44200-302)
  - T1/SMDI and CallPilot Server Configuration Guide (NN44200-303)
  - Communication Server 1000 System and CallPilot Server Configuration Guide (NN44200-312)
- Unified Messaging Software Installation
  - Desktop Messaging and My CallPilot Installation and Administration Guide (NN44200-305)

Administration

- Administrator Guide (NN44200-601)
- Software Administration and Maintenance Guide (NN44200-600)
- Meridian Mail to CallPilot Migration Utility Guide (NN44200-502)

- Application Builder Guide (NN44200-102)
- Reporter Guide (NN44200-603)

Maintenance

- Troubleshooting Reference Guide (NN44200-700)
- Preventative Maintenance Guide (NN44200-505)
- Server Maintenance and Diagnostics
  - 201i Server Maintenance and Diagnostics Guide (NN44200-705)
  - 202i Server Maintenance and Diagnostics Guide (NN44200-708)
  - 703t Server Maintenance and Diagnostics Guide (NN44200-702)
  - 1002rp Server Maintenance and Diagnostics Guide (NN44200-701)
  - 1005r Server Maintenance and Diagnostics Guide (NN44200-704)
  - 1006r Server Maintenance and Diagnostics Guide (NN44200-709)
  - 600r Server Maintenance and Diagnostics Guide (NN44200-703)
  - Contact Center Manager Communication Server 1000/Meridian 1 & Voice Processing Guide (297-2183-931)

End User Information

- End User Cards
  - Unified Messaging Quick Reference Card (NN44200-111)
  - Unified Messaging Wallet Card (NN44200-112)
  - A-Style Command Comparison Card (NN44200-113)
  - S-Style Command Comparison Card (NN44200-114)
  - Menu Interface Quick Reference Card (NN44200-115)
  - Alternate Command Interface Quick Reference Card (NN44200-116)
  - Multimedia Messaging User Guide (NN44200-106)
  - Speech Activated Messaging User Guide (NN44200-107)
  - Desktop Messaging User Guide for Microsoft Outlook (NN44200-103)
  - Desktop Messaging User Guide for Lotus Notes (NN44200-104)
  - Desktop Messaging User Guide for Novell Groupwise (NN44200-105)
  - Desktop Messaging User Guide for Internet Clients (NN44200-108)
  - Desktop Messaging User Guide for My CallPilot (NN44200-109)
  - Voice Forms Transcriber User Guide (NN44200-110)

Chapter 3: Preparing for Installation

In this chapter

Introduction on page 19

Management of the TCP/IP network on page 19

Network planning on page 21

Planning the High Availability configuration on page 22

High Availability system checklist on page 22

Facility planning on page 25

Switch planning on page 25

Required hardware on page 27

Introduction

For detailed Avaya CallPilot® 5.0 and 1005r or 1006r server information, see the *Planning and Engineering Guide* (NN44200-200).

Planning and engineering information specific to High Availability is covered in this chapter.

Important:

The High Availability pair must consist of the same type of servers. A mixture of server types is not supported. For example, you can not have a 1005r and a 1006r in a High Availbility pair.

Management of the TCP/IP network

Each server in the pair of High Availability servers requires its own unique host name, ELAN IP address, and CLAN IP address. In addition, the pair of servers are assigned a Managed (or virtual) host name, Managed ELAN IP address, and Managed CLAN IP address to make the

pair of servers look like a single Avaya CallPilot server to the end clients. The end clients include the following:

- CallPilot Reporter
- My CallPilot
- Desktop Client
- Application Builder
- CallPilot Manager
- the switch

The managed network settings must be used by all clients. The clients do not need to access either server directly. All access must be done using the managed networking parameters. The EMC AutoStart software ensures that the currently active server responds to any requests made to either the Managed host name or IP addresses.

The CallPilot High Availability system uses managed networking settings so that common settings are used by the CallPilot clients, as follows:

- CallPilot Reporter, My CallPilot, Desktop Client, Application Builder, and CallPilot Manager (accessed using the Web) use the Managed CLAN IP address and host name.
- The switch uses the Managed ELAN IP address.

When a switchover occurs from Node 1 (CP1) to Node 2 (CP2), the CallPilot applications and the switch do not change IP settings and the clients do not notice any changes. The Managed CLAN requires IP name resolution. This means that the manage CLAN must be manually added by a Domain Name Service (DNS) administrator if you are using a DNS server as the solution or the host file must be updated on both the CP1 and CP2 servers.

For servers that are receiving the High Availability feature expansion, it is important that the current host name, CLAN IP address, and ELAN IP address are reused as the Managed host name, Managed CLAN IP address, and Managed ELAN IP address for the new High Availability pair. Reusing the network settings as the managed network settings ensures that any existing clients (for example, desktop client installations) do not have to change their configuration to access the new High Availability pair. The clients are unaware that there is now a pair of High Availability servers where there used to be a single CallPilot server.

⚠ Warning:

If you do not reuse the existing host name, ELAN IP address, and CLAN IP address during an upgrade and you have an existing CallPilot Reporter installation with historical data, after the upgrade, all new data is recorded against the new Managed host name. Any older data collected in CallPilot Reporter does not appear.

If you do not reuse the existing host name, ELAN IP address, and CLAN IP address during an upgrade and you have existing Application Builder applications, then after the upgrade the applications must be recreated.

Network planning

In addition to the CLAN and ELAN connections, a pair of High Availability servers has three additional dedicated network interface ports for the following:

- HB1 (Heartbeat 1)
- HB2 (Heartbeat 2 backup)
- Mirror (Data mirroring between the two servers)

The NICs must be physically connected between the two servers using crossover LAN cables and must not be run through any type of switch or hub, as such a configuration is not supported.

Warning:

Crossover cables must be used to connect the NICs between the two High Availability servers.

Networking equipment (switch, hub, or router) is not supported in this configuration. The only supported configuration is the use of dedicated crossover LAN cables between the HB1, HB2, and Mirror NICs between the two High Availability servers.

The networking parameters (that is, IP address and subnet mask) for both nodes in the High Availability pair must be set before the EMC AutoStart software is installed or the High Availability pair does not work correctly (see Install the AutoStart Agent and Console software on page 62). Each network connection must be on a different subnet. Avaya recommends the following values be used for the dedicated network connections:

Table 2: Node 1

Network Interface Card (NIC)	IP address	Subnet mask
Heartbeat 1 (HB1)	192.0.0.10	255.255.255.0
Heartbeat 2 (HB2)	194.0.0.10	255.255.255.0
MIRROR	193.0.0.10	255.255.255.0

Table 3: Node 2

Network Interface Card (NIC)	IP address	Subnet mask
Heartbeat 1 (HB1)	192.0.0.11	255.255.255.0
Heartbeat 2 (HB2)	194.0.0.11	255.255.255.0
MIRROR	193.0.0.11	255.255.255.0

During the configuration of the High Availability servers, a CLAN Test IP address is required. The CLAN Test IP address can be any reliable working IP address on the CLAN subnet (Avaya

server subnet). As a result, the High Availability system can ping this IP address at any time. If the CLAN subnet (Avaya server subnet) is configured, Avaya recommends that the CLAN Gateway IP address be used as the CLAN Test IP address. If the gateway is configured such that it does not reply to the ping command, another CLAN address that responds to the ping command must be used. If there is no CLAN subnet (Avaya server subnet) at the your site, enter 127.0.0.1 as the CLAN Test IP address.

Planning the High Availability configuration

During the configuration of the High Availability servers, the following information is needed by the High Availability Configuration Wizard (see Figure 11: High Availability Configuration Wizard on page 59):

- User Name—This is the Windows administrator user name. Avaya recommends the use of the Windows default administrator user name (that is, administrator).

  If you use any other Windows user name, that user must have the full Windows administrative rights. Enter the name of a Windows account that is a member of the administrators group and that exists on both servers in the pair.

  Avaya recommends using the account called administrator. However, if the administrator account is renamed or another administrator account with a different name is created, use that renamed or new account.

- Server Workgroup / Domain Name—This is the Windows Workgroup / Domain name. Enter workgroup for the default Windows Workgroup or enter the real Windows Domain name if both servers in the High Availability pair have already joined the customer domain.

  However, Avaya recommends using the Windows default workgroup to first configure the High Availability system, and then join the customer domain after the High Availability system is working (if the system has to join the domain).

- EMC AutoStart Domain Name—This is the unique name for the EMC AutoStart domain. The EMC AutoStart domain name must be the same for the pair of High Availability servers. This name must contain only alphanumeric characters and must have a maximum length of eight characters.

High Availability system checklist

Use the following table to plan and track the system settings for your High Availability servers. These settings are configured using the CallPilot Configuration Wizard and the High Availability Configuration Wizard.

Important:

The High Availability pair must consist of the same type of servers. A mixture of server types is not supported. For example, you can not have a 1005r and a 1006r in a High Availability pair.

Table 4: High Availability system checklist

	CP Node 1 (CP1)	CP Node 2 (CP2)
Configuration Wizard: Serial Number and Keycode page		
Serial Number		
Keycode		
Configuration Wizard: Server Information page		
Computer Name **Note:** Must only include alphanumeric characters.		
Time Zone		
Area Code		
Country Code		
LDAP Search Base		
Configuration Wizard: Password Information page		
Administrator password **Note:** Both nodes must have the same password.		
Configuration Wizard: Switch Information page		
Switch Type		
Switch Customer Number		
Switch IP Address		
Link1 TN		
Link1 Key0		
Link1 Key1		
Link2 TN		
Link2 Key0		
Link2 Key1		
Link3 TN		

	CP Node 1 (CP1)	CP Node 2 (CP2)
Link3 Key0		
Link3 Key1		
CDN		
Configuration Wizard: Language Source Directory page		
Primary language		
Secondary language		
Configuration Wizard: CallPilot Local Area Network Interface page		
ELAN subnet IP address		
ELAN subnet mask		
Avaya server subnet (CLAN) IP address		
Avaya server subnet (CLAN) subnet mask		
Avaya server subnet (CLAN) gateway IP address		
Heartbeat 1 (HB1) IP address		
Heartbeat 1 (HB1) subnet mask		
Heartbeat 2 (HB2) IP address		
Heartbeat 2 (HB2) subnet mask		
Mirror IP address		
Mirror subnet mask		
High Availability Configuration Wizard		
Managed CLAN Host Name **Note:** The CLAN is the server subnet.		
Managed CLAN IP address		
Managed ELAN IP address **Note:** The ELAN is the ELAN subnet.		

	CP Node 1 (CP1)	CP Node 2 (CP2)
Node 1 Host Name		
Node 2 Host Name		
Number of MPB96 Boards		
User Name **Note:** This is the Administrator's user name.		
Server Workgroup/Domain Name		
EMC AutoStart Domain Name		
CLAN Test IP		

Facility planning

The two servers in the High Availability pair must be collocated, as they must be connected to the same switch. Having the servers collocated lets the servers take advantage of a common (customer-supplied) UPS if there is one available.

The physical distance that can separate the two servers is limited by the following:

- The length of the cables connecting the servers to the MGate cards in the Meridian 1 or Avaya CS 1000 switch: In the case of the 1005r, the DS30X cable length is up to 60 feet or 18.29 meters long. In the case of the 1005r or 1006r, the CAT5 cable length is up to 1968.50 feet or 600 meters long.
- The requirement that the HB1, HB2, and Mirror network connections between the two servers are connected using dedicated crossover LAN cables with no networking hardware (that is, switches, routers, or hubs) between the servers.
- The common grounding requirements for all hardware that is connected to the switch. For grounding requirements, see the *Planning and Engineering Guide* (NN44200-200).

Avaya recommends that the two servers be collocated to ensure that all of these requirements are met.

Switch planning

AML over Ethernet is the only switch integration that is supported.

Note:
T1 connectivity is not supported.

For detailed switch information, see the following:

- Meridian 1 and CallPilot Server Configuration (NN44200-302)
- Communication Server 1000 and CallPilot Server Configuration (NN44200-312)

Both servers must be connected to the same switch (using MGate cards and DS30X cables). Because both servers are connected to the same switch with their own dedicated DS30X cables, the switch must have twice as many MGate cards installed than it would for a single CallPilot server. For example, if a switch has a single 192-channel CallPilot server connected to it, the switch must have six MGate cards installed. For a 192-channel High Availability configuration, the switch must have 12 MGate cards installed because six are required for each CallPilot server in the High Availability pair.

Each 1005r server has a dedicated connection to the switch, and therefore, requires dedicated DS30X or CAT5 connections, MGate cards, and matching switch configuration. Each 1006r server has a similar dedicated connection to the switch but requires CAT5 connections, MGate cards, and matching switch configuration.

Two configuration are supported:

1. Two servers, either 1005r or 1006r, with one MPB96 each (up to 96 channels).

   For a 96-channel High Availability server, each server in the pair can support 96 channels, which means there could be three MGate cards per server for a total of 6 MGate cards.

2. Two servers, either 1005r or 1006r, with three MPB96 each (up to 192 channels).

   For a 192-channel High Availability server, each server in the pair can support 192 channels, which means there could be six MGate cards per server for a total of 12 MGate cards.

Both High Availability servers must share the same CDN so that users do not know which server in the pair is servicing requests.

Meridian 1 planning

For Meridian 1 Option 51/61/81 switches, the clock controller card (QPC775c) must have vintage NTRB53AA or higher. This is required to avoid a problem when the midnight audit runs on the switch and IP connectivity is temporarily lost, which in turn causes the AutoStart software to initiate a failover to the standby server.

CS 1000 planning

Media Gateway shelves in a CS 1000E do not share the same clock reference. Media Gateway Expansion shelves share the same clock reference as the Media Gateway shelf to which they are connected. In a CS 1000E, all MGate cards connected to the CallPilot server must reside in the same Media Gateway/Media Gateway Expansion shelf pair.

Important:

Each server in the High Availability pair must have all of its MGate connections in the same Media Gateway/Media Gateway Expansion shelf pair on a CS 1000E.

For the CS 1000M and CS 1000S, the MGate cards can reside on separate shelves.

Required hardware

The following checklists describe the contents required for a High Availability system. Most items are included when you order the High Availability feature; however, some items must be supplied by the customer. Ensure you have all of the applicable items prior to beginning the installation of the High Availability system.

Hardware included

When you order an High Availability system, the following hardware is included:

Table 5: 1005r High Availability system (up to 96 MPUs or 288 MPUs)

Included with system	Qty	PEC number
CallPilot 5.0 1005r Server 96 MPU Chassis Sub-Assembly Package or CallPilot 5.0 1005r Server 288 MPU Chassis Sub-Assembly Package	2	NTUB28CAE5 NTUB28DAE5
CallPilot 5.0 Rackmount 1005r Server CD Image Set	2	NTUB50RA
CallPilot 5.0 Common Software Components and Documentation BOM	2	NTUB63CA
CallPilot 5.0 Keycode	1	N0119677
CallPilot 5.0 HA Feature Activation	1	NTZE64AA
EMC Software RTU License Royalty - R	2	N0119699

Included with system	Qty	PEC number
EMC License Registration Card	2	N0129528
Ghost Solution Suite 1.1 with CallPilot 5.0	2	N0119681
RTU for Symantec PCAnywhere v12.0 for New CallPilot Applications	2	N0119700
RTU for Windows 2003 Document	2	P1013471
RTU for Crystal Decision (Report)	2	P0989628
RTU for DOS 6.20 Document	2	P0887449
RTU for SQL Anywhere	2	P0887451
CallPilot 1005r Storage Hours - 2400 Hours	1	NTZE08FA
CallPilot Prompt Languages - Activate Six	1	NTZE16AB
CallPilot Speech Activated Messaging Vocabulary - Activate Three	1	NTZE16BB
Avaya Standard Security Device [RoHS]	1	NTDK57AAE5
CABLE ASSY, TRIPLE DS30X InterConnect Cable for MPB96 2 (for 96 MPUs) or 4 (for 288 MPUs)	2 or 4	NTRH2014E6

Table 6: 1006r High Availability system (up to 96 MPUs or 288 MPUs)

Included with system	Qty	PEC number
CallPilot 5.0 1006r Server 96 MPU Chassis Sub-Assembly Package or CallPilot 5.0 1006r Server 288 MPU Chassis Sub-Assembly Package	2	NTUB37AAE5 NTUB74AAE5
CallPilot 5.0 Rackmount 1006r Server CD Image Set	2	NTUB50UA
CallPilot 5.0 Common Software Components and Documentation BOM	2	NTUB63CA
CallPilot 5.0 Keycode	1	N0119677
CallPilot 5.0 HA Feature Activation	1	NTZE64AA
EMC Software RTU License Royalty - R	2	N0119699
EMC License Registration Card	2	N0129528
Ghost Solution Suite 1.1 with CallPilot 5.0	2	N0119681
RTU for Symantec PCAnywhere v12.0 for New CallPilot Applications	2	N0119700
RTU for Windows 2003 Document	2	P1013471
RTU for Crystal Decision (Report)	2	P0989628

Included with system	Qty	PEC number
RTU for DOS 6.20 Document	2	P0887449
RTU for SQL Anywhere	2	P0887451
CallPilot 1006r Storage Hours - 2400 Hours	1	NTZE08FA
CallPilot Prompt Languages - Activate Six	1	NTZE16AB
CallPilot Speech Activated Messaging Vocabulary - Activate Three	1	NTZE16BB
Avaya Standard Security Device [RoHS]	1	NTDK57AAE5

Customer provided equipment

The following table provides the list of equipment that must be supplied by the customer.

Table 7: Customer provided equipment

Not included with system	Qty	PEC number	Notes
Crossover cable	3	n/a	Used to connect the HB1, HB2, and Mirror NICs.
1005r/1006r/600r/202i USB modem	2	NTRH9242E6	Used for remote support. Each server must have a dedicated modem.
ELAN cable	2	n/a	One for each 1005r server.
CLAN cable	2	n/a	One for each 1005r server.

Supported hardware configurations

The CallPilot 5.0 High Availability feature is only supported on the 1005r or 1006r platform. Two identical servers are required for the High Availability feature. A mixture of server types is not supported, therefore the High Availability pair can only include two 1005r servers or two 1006r servers. The pair of servers are required to provide the active and standby server configuration.

One dongle is shared between the pair of High Availability servers as they share the same keycode and serial number.

The two supported hardware configurations are:

- three MPB96 boards (up to 192 channels/288 MPU) with two dual-port NIC cards
- one MPB96 board (up to 96 channels/96 MPU) with two dual-port NIC cards

Note:

The hardware configuration must be identical on both servers making up the High Availability pair.

Chapter 4: Failover overview

In this chapter

Introduction on page 31

Automatic failovers on page 32

Manual failovers on page 33

Introduction

In a High Availability system, one server is active while the other is in standby mode. If a failure occurs on the active server, the standby server comes into service, becoming the active server. The process of the standby server becoming the active server is called a failover.

The standby server takes over from the active server when:

- A failure condition is detected on the active server and the software triggers a failover to the standby server. This is known as an automatic failover. For more information, see Automatic failovers on page 32.
- A manual failover is initiated by an administrator to perform maintenance activities, or when there is degradation of service that is not detected by the AutoStart software. For more information, see Manual failovers on page 33.

In normal day-to-day use, end users are not aware that two Avaya CallPilot® servers are configured in a High Availability pair. There is one Control Directory Number (CDN) configured on the switch that users call for any given service. Any calls to a given CDN are routed to the Avaya CallPilot server that is currently active.

Note:

The CDNs configured on both server must be the same.

If a failover occurs, the standby CallPilot server becomes the active server of the pair and the switch routes incoming calls to the active server.

In case of a failover, where the standby server becomes the active server, any calls or connections that were in process when the failover occurs are dropped. The CallPilot server is out-of-service from the time the active server fails to the time the standby server takes over.

During the failover process, when the standby server is coming into active service, neither server is available to accept or process connections. This process takes approximately 4 to 12 minutes (depending on the scenario). Calls coming in during this time receive the default treatment that is configured on the switch. After the standby server become the active server, end users can connect with the CallPilot server without changing any settings.

Automatic failovers

An automatic failover occurs when the AutoStart software determines that something has gone wrong on the active CallPilot server, that is, a critical CallPilot service has failed. The software initiates a failover to the standby CallPilot server without any user interaction. Only a limited number of automatic failover cases are supported in CallPilot 5.0.

The following cases trigger an automatic failover from the active CallPilot server to the standby server:

- A reboot or shut down of the active server.
- Failure of one or more of the critical CallPilot services. The system attempts to restart a failed critical CallPilot service three times before resorting to a failover. These critical services include:

Table 8: Critical CallPilot services

Service name	Description
Adaptive Server Anywhere - DB_SQLANY	Database service
CallPilot AOS Service	Active Operation Server (AOS) Service
CallPilot HAL Monitor	Monitors the Hardware Abstraction Layer (HAL)
CallPilot LDAP Service	Directory server used to set and retrieve the most persistent data except for messages and prompts
CallPilot Multimedia Volume 1	Data management for users, messages, and so on, stored in volume VS1 (VS1T, VS1V, and VS1B)
CallPilot Multimedia Volume 102	Data management for users, messages, and so on, stored in volume VS102 (VS102T, VS102V, and VS102B)
CallPilot Multimedia Volume 103	Data management for users, messages, and so on, stored in volume VS103 (VS103T, VS103V, and VS103B)
CallPilot Multimedia Cache	Cache for multimedia volumes 1, 102, and 103.

Service name	Description
CallPilot Resource Package 1	Middleware resources for MPB board 1
CallPilot Resource Package 2	Middleware resources for MPB board 2
CallPilot Resource Package 3	Middleware resources for MPB board 3
CallPilot Blue Call Router	Routes calls to the CallPilot Blue application
CallPilot Call Channel Router	Telephony channel delivers the voice path of the call
CallPilot SLEE Service	Service Logic Execution Environment (SLEE)
CallPilot Notification Service	Event notification service
CallPilot MTA Service	Message Transfer Agent (MTA)
CallPilot MWI Service	Message Waiting Indication (MWI)

- Optional automatic failover on the loss of connection of the ELAN at the TCP/IP level (that is, failure of the switch to respond to the ping command of the Managed ELAN IP address for a specified period of time). By default, there is no failover on the Path Test failure of the Managed ELAN IP address, which CallPilot 5.0 High Availability servers use to connect to the switch through ELAN. However, the CallPilot 5.0 High Availability system sends a notification e-mail to the administrators when the Path Test failure of the Managed ELAN IP occurs. If necessary, you can also set up the failover on the failure of the Managed ELAN IP address by following the procedure Configuring failovers on the Path Test failures of the Managed ELAN IP address on page 159.

Using the AutoStart console software, you can disable and enable automatic failovers. For more information, see the following procedures:

- Disabling automatic failovers (stop monitoring) on page 180
- Enabling automatic failovers (start monitoring) on page 180

Manual failovers

A manual failover occurs when the server administrator decides to initiate a failure manually using the AutoStart Console. Failovers can also be manually triggered by powering down the active server. The actual failover mechanism is the same as in the automatic case; the only difference is that the failover is manually initiated.

The administrator can choose to perform a manual switchover if there is a problem on the active CallPilot server that is not part of the automatic failover rules. A manual failover can be initiated for the following situations:

- For hardware repairs of failed hardware in the server that requires the server to be powered down (for example, failure of an internal fan)
- For service improvement due to an end-user-reported degradation of service on the server
- For scheduled maintenance

To perform a manual failover, see Initiating a manual failover on page 181.

Chapter 5: Install and configure the High Availability pair

In this chapter

New system installation procedure on page 35

Prepare the switch and install the 1005r or 1006r servers on page 38

Prepare both 1005r or 1006r servers on page 39

Configure CP1 and CP2 using the CallPilot Configuration Wizard on page 42

Connect and verify LAN connections on page 52

Run Stage 1 of the High Availability Configuration Wizard to check CP1 and CP2 configuration on page 58

Install the AutoStart Agent and Console software on page 62

Configure the AutoStart software on page 81

Bring the Resource Groups online on page 92

Test your configuration on page 97

Create the CallPilot Reporter connections on page 98

Add the servers to a Windows domain on page 99

Note:

The screen shots displayed in this chapter are from a 1005r server. The various screens will look slightly different if you are installing and configuring a 1006r server.

New system installation procedure

This chapter describes how to perform a fresh installation of High Availability servers and how to configure the pair of Avaya CallPilot® High Availability servers.

In this NTP, the administrator installs and configures the Avaya CallPilot server.

This installation assumes the following:

- The CallPilot 5.0 image on the 1005r or 1006r server was installed at the factory.
- The additional hardware (two dual-port NIC cards) was installed at the factory.
- The AutoStart software is not installed as part of the CallPilot 5.0 image. The software must be installed by the customer as part of the High Availability installation.

A CallPilot High Availability system consists of two servers that work as peers. At any time, one server is active while the other server is in standby mode. For the purpose of the following procedure, the servers are referred to as CallPilot server 1 (CP1) and CallPilot server 2 (CP2). Initially, CP1 is the active server and CP2 is the standby server.

Important:

The following table outlines the tasks required to install, configure, and test the High Availability feature.

The tasks (and procedures within each task) must be completed in the order presented.

Table 9: High Availability task list

Task	Estimated time	Procedures required to complete the task
Prepare the switch	60 minutes	– Preparing the switch on page 38
Install the two servers	210 minutes per server	– Installing the two 1005r or 1006r servers on page 38
Prepare both servers	120 minutes per server	– Manually changing the server name on page 39 – Manually setting the IP parameters on page 40 (optional) – Installing the antivirus software on page 41 (optional) – Running the CallPilot Setup Wizard on page 41
Configure CP1 and CP2 using the CallPilot Configuration Wizard	40 minutes per server based on two installed languages and three provisioned channels Allow 10 minutes for each additional language	– Configuring the replacement server using the CallPilot Configuration Wizard on page 43 – Configuring CP2 using the CallPilot Configuration Wizard on page 47
Connect and verify the LAN connections	30 minutes	– Connecting and verifying LAN connections on page 52 – Modifying the hosts file on page 55 (optional)

Task	Estimated time	Procedures required to complete the task
		– Testing the host name resolution on page 57
Run Stage 1 of the High Availability Configuration Wizard to check the configuration of CP1 and CP2	5 minutes	– Running Stage 1 of the High Availability Configuration Wizard to check CP1 and CP2 configuration on page 58
Install the AutoStart 5.3 software on CP1	10 minutes	– Installing the AutoStart Agent and Console software on CP1 on page 62
Configure licensing and security on CP1	10 minutes	– Add the node 2 administrator account to the AutoStart Console on node 1 on page 70
Install the AutoStart 5.3 software on CP2	10 minutes	– Installing the AutoStart Agent and Console software on CP2 on page 72
Configure the AutoStart software **Note:** All configuration is completed on CP1.	35 minutes	Configure the AutoStart software on CP1 – Modifying the AutoStart Domain and Verification links on page 81 – Adding the Remote Mirroring Host for CP2 on page 84 – Generating the AutoStart Definition File on page 86
		Import the AutoStart definition file on CP1 – Importing the AutoStart definition file on page 88
		Add the Windows administrator password for the AutoStart utility processes in the AutoStart Console – Adding the Windows administrator account password for the AutoStart Utility Processes on page 89
		Add e-mail addresses to the Managed_ELAN_IP_Failure_Notif rule – Adding e-mail addresses to the Managed_ELAN_IP_Failure_Notif rule on page 91
Bring the Resource Groups online	10 minutes	– Bringing the CallPilot Resource Group online on CP1 on page 93 – Bringing the Resource Groups CallPilot_[CP1] and CallPilot_[CP2] online on page 95
Test your configuration	120 minutes	– Testing the configuration of CP1 and CP2 on page 97
Create the CallPilot Reporter connections	20 minutes	– Creating the CallPilot Reporter connection on page 99

Task	Estimated time	Procedures required to complete the task
Add server to a Windows domain (if required)	30 minutes	– Joining a Windows domain on page 99

Prepare the switch and install the 1005r or 1006r servers

Before you install and configure the High Availability feature you must prepare the switch and servers. Use the following procedures to prepare the switch and install the servers.

Preparing the switch

Configure the Meridian 1 or CS 1000 switch by referring to the following documents:

- *Meridian 1 and CallPilot Server Configuration* (NN44200-302)
- *Communication Server 1000 and CallPilot Server Configuration* (NN44200-312)

Note:

Both High Availability servers must use the same Control Directory Number (CDN). The MGate cards on the switch must provide twice the channel capacity than that of a single High Availability server. However, only half the channels are in use at any one time (the other half of the channels are in standby mode).

Installing the two 1005r or 1006r servers

Refer to *1005r Server Hardware Installation* (NN44200-308) or *1006r Server Hardware Installation* (NN44200-320) and *Installation and Configuration Task List* (NN44200-306) for details about performing the following tasks:

a. Unpack both of the CP1 and CP2 servers.

b. Install the dongle on CP1.

c. Connect the peripheral equipment (monitor, keyboard, and mouse) to both servers.

d. Connect USB modems to each server.

e. Power on both servers.

Result: The servers start and the Windows 2003 Mini-Setup runs. (During the Windows 2003 Mini-Setup, the servers automatically restart twice.)

Prepare both 1005r or 1006r servers

The following procedure is required.

- Manually change the server name. (The CallPilot Configuration Wizard can also be used to change the server name.)

The following procedures can be required depending upon your setup configuration.

- Manually set the IP parameters. (The CallPilot Configuration Wizard can also be used to set the IP parameters.)

  Note:

  The procedure listed in the preceding bullet is performed under the following circumstances:

  a. If you are restoring from a network location. In order to perform a restore the CLAN IP address must first be set.

  b. If you are using a DNS as part of your network solution, then the DNS entries must be manually completed.

- Check the Primary DNS suffix.
- Install antivirus software on both servers. (optional)

  Note:

  For more information about the antivirus software packages that are approved by Avaya for CallPilot, see the P-2007-0101-Global : CallPilot Support for Anti-Virus Applications bulletin.

- Run the CallPilot Setup Wizard

Manually changing the server name

Changing the server name can also be done using the CallPilot Configuration Wizard. This procedure is mandatory.

1. Log on to the server with the default administrator user name and password (administrator / Bvw250).
2. Right-click My Computer and select Properties from the shortcut menu.

   Result: The System Properties window appears.
3. Select the Computer name tab.
4. Click Change.

   Result: The Computer Name Changes window appears.

5. In Computer Name field, enter new computer name.

   Important:
   The computer name must contain only alphanumeric characters. Nonalphanumeric characters (such as a hyphen [-]), are not supported.

6. Click OK.

   Result: A warning message appears prompting you to restart the computer for the changes to take effect.

7. Click OK.

   Result: The System Properties window appears.

8. Click OK.

   Result: A message appears prompting you to restart the computer.

9. Click Yes to restart the computer.

   Result: The system restarts.

Manually setting the IP parameters

Setting the IP parameter can also be done using the CallPilot Configuration Wizard; however, DNS entries and Mirror network interface must be manually configured.

1. Select Start > Settings > Network Connections.

   Result: The Network Connections window appears and displays a list of network connections.

2. Right-click CLAN and select Properties.

   Result: The CLAN Properties window appears.

3. Select Internet Protocol (TCP/IP) and then click Properties.

   Result: The TCP/IP Properties window appears.

4. Enter the following IP information (which is provided by the network administrator):

   - IP address
   - Subnet mask
   - Default gateway
   - Preferred DNS server
   - Alternate DNS server

   Note:
   The DNS entries cannot be configured using the CallPilot Configuration Wizard. The DNS entries must be manually configured.

5. Click OK.

   Result: The CLAN Properties window appears.

6. Click Close.
7. Repeat the preceding steps for the ELAN, HB1, HB2, and Mirror network interfaces.
8. Right-click MIRROR and select Properties. Result: General tab of the MIRROR Properties window opens
9. Only the "Internet Protocol TCP/IP" protocol should be bound to the interface. Uncheck all other items in the list “This connection uses the following items”. Result: “Internet Protocol TCP/IP” item is enabled; "Client for Microsoft Networks", "File and Printer Sharing for Microsoft Networks", “Network Load Balancing” options are disabled
10. Select the "Internet Protocol TCP/IP" item and click Properties. Result: Internet Protocol (TCP/IP) Properties window opens.
11. Click Advanced button at the bottom of the window. Result: Advanced TCP/IP Settings window opens
12. Select WINS tab. Uncheck all options except “Disable NetBIOS over TCP/IP". Result: The item “Disable NetBIOS over TCP/IP" is checked. The option “Enable LMHOSTS lookup” is unchecked.
13. Click OK at the bottom of Advanced TCP/IP Settings window. Result: Advanced TCP/IP Settings window closes.
14. Click OK at the bottom of Internet Protocol (TCP/IP) Properties window. Result: Internet Protocol (TCP/IP) Properties window closes.
15. Click Close at the bottom of MIRROR Properties window. Result: MIRROR Properties window closes.

Installing the antivirus software

This procedure is optional.

1. For information about the antivirus software packages that are approved by Avaya for CallPilot, see the P-2009-0039-Global-Rev3 : CallPilot Support for Anti-Virus Applications bulletin.
2. Install the antivirus software on the CallPilot servers.

   The Antivirus software must be configured to exclude the AutoStart Database directory to ensure uninterrupted processing. The path to the AutoStart Database directory is:

   D:\Program Files\EMC AutoStart<AutoStart-Domain-Name>\<AutoStart-Domain-Name_NodeName>

   See the P-2007-0101-Global : CallPilot Support for Anti-Virus Applications bulletin for detailed instructions on how to exclude the AutoStart Database directory on CallPilot 5.0 High Availability systems.

Running the CallPilot Setup Wizard

The CallPilot Setup Wizard must be run on both CP1 and CP2.

1. Log on to the CallPilot server.

The default password for the administrator account is Bvw250.

Result: When you first log on to the system after powering it up, the Setup Wizard runs automatically. If the Setup Wizard does not open, launch the Setup Wizard by clicking Start > Programs > CallPilot > Setup Wizard.

Result: The Welcome to the CallPilot Setup Wizard window appears.

2. Click Next.

   Result: The Service Update (SU) / PEP Installation window appears.

3. Select one of the following options:

   - If you have SUs or PEPs to install, select the Yes, I have updates that I want to install now option.

     Result: The Installing SU/PEP screen appears. Install the required updates and restart if necessary.

   - If there are no SUs or PEPs to install, select the No, I do not have updates that I want to install now option.

4. Click Next.

   Result: The Performing Platform Validity Check window appears.

5. View the items on the Performing Platform Validity Check screen.

   Note:
   If your server does not meet the minimum hardware and software requirements, contact your support organization.

6. Click Next.

   Result: The Telephony Board Validation window appears.

7. If your board configuration is correct, click Next.

   Result: The Selecting Upgrade of CallPilot window appears.

8. Select the No, I do not have data to restore option.
9. Click Next.

   Result: The Finished window appears.

10. Click Finish to exit the CallPilot Setup Wizard.

Configure CP1 and CP2 using the CallPilot Configuration Wizard

This section provides the procedures to configure CP1 and CP2 using the CallPilot Configuration Wizard within CallPilot Manager.

Important:

If you must go back into the Configuration Wizard at any time to correct any entries, note that the Database, LDAP, and AOS services must be started to gain access to CallPilot Manager.

The D:\Nortel\HA folder contains a file called start_svr.bat that automatically starts any necessary services. This script can be run to start the required services.

Configuring the replacement server using the CallPilot Configuration Wizard

Time required: 20 minutes (assuming one language is installed)

Important:

Ensure that the dongle is installed on the replacement server.

1. Launch the Internet Explorer Web browser.
2. In the address field, enter the following URL to start CallPilot Manager: http://localhost/cpmgr
3. Log on to CallPilot Manager using the administrator mailbox and default password created from the CallPilot Setup Wizard:
   a. Under the User area, enter the following:
      - The administrator mailbox number is 000000.
      - The default password is 124578.
   b. Under the Server area, enter the localhost in the Server field.

   Note:

   All administrative changes must be performed on active server with dongle attached.
4. Click Login.

   Result: The Change User Password window appears.
5. Change the password for the 000000 administrator mailbox by doing the following:
   a. Enter the Current Password.
   b. Enter the New Password.
   c. Reenter the new password in the New Password Re-Entry field.
   d. Click Save.

   Result: The Welcome to CallPilot Manager page appears.
6. Click Configuration Wizard.

   Result: The Configuration Wizard: Welcome page appears.
7. Click Next.

   Result: The Keycode and serial number page appears.
8. Enter the following:

a. In the Serial number field, enter the serial number of the dongle assigned to the CallPilot server. The serial number entered for the replacement server must be the same as the serial number entered for the existing server.

b. In the Keycode field, enter the High Availability-enabled keycode assigned to CallPilot server. The keycode entered for the replacement server must be the same as the keycode entered for the existing server.

9. Click Next.

   Result: The Feature Verification page appears.

10. Ensure that all parameters are correct and that the High Availability feature is set to Mirroring.

11. Click Next.

    Result: The Server Information page appears.

12. On the Server Information page, do the following:

    a. In the Computer Name field, enter the CallPilot server name.

    b. In the Time Zone field, select the correct time zone.

    c. Under Dialing Information, enter the Area Code and Country Code.

    d. Enter the LDAP search base. For example, dc=nortel,dc=ca.

Note:

All values on the Server Information page for the replacement server must be the same as for the existing server. Use Table 4: High Availability system checklist on page 23 that you completed for both nodes.

13. Click Next option.

    Result: The Password Information page appears and the Change the password option is selected.

14. On the Password Information page, do the following:

    a. In the New Password field, enter the new password.

    b. In the Confirm the new password field, reenter the new password.

    c. Click Next.

    Result: A warning message appears.

Figure 3: Change password warning message

15. Click OK to dismiss the warning message.

    Result: The Password Information page reappears.

16. Click Next.

    Result: The Multimedia Allocation page appears.

17. Configure the MPB96 settings.

18. Click Next.

    Result: The M1 Switch Information page appears.

19. Configure the switch information.

    a. Select the Switch Type.

    b. Enter the Switch Customer Number.

    c. Enter the Switch IP Address.

       See the Table 4: High Availability system checklist on page 23 containing the information for both nodes.

    d. Provision the channels, as follows:

       i. Select a channel.

          Result: The Channel Detail window appears.

       ii. Enter the TN, ACD Position ID, and SCN.

       iii. Ensure that Channel Allocation is set to Multimedia.

       iv. Click OK.

          Result: The Meridian 1 Switch Information window appears again.

       v. Continue the provisioning of channels until complete.

       Note:
       To automatically provision a number of channels, you can enter the information for one channel, select the number of channels required, and then click Fill. The Configuration Wizard automatically datafills the channels, and increments the TNs, ACD Position ID, and SCN.

       Note:
       The number of TNs configured on both nodes must be the same.

    Note:
    To obtain switch-provisioning information, see Table 4: High Availability system checklist on page 23.

20. Click Next.

    Result: The Meridian 1 CDN Information page appears.

21. Click New to add a new CDN.

Result: The CDN Details page appears.

Important:
The CDNs must be the same on both nodes.

22. On the CDN Details page, do the following:
    a. In the CDN field, enter the new CDN.
    b. Select the Application Name (Voice Messaging or Multimedia Messaging).
    c. Click OK.

    Result: The new CDN is added and the CDN information page reappears.
23. Click Next.

    Result: The Language Source Directory page appears.
24. Insert the CallPilot 5.0 Language CD into the CD/DVD drive on the replacement server.

    Important:
    You must use a CallPilot 5.0 Language CD.

    Language CDs from previous CallPilot releases are not compatible with CallPilot 5.0. The Configuration Wizard checks the version of the Language CD and blocks the use of the CD if it is not a CallPilot 5.0 CD.
25. On the Language Source Directory Select page, do the following:
    a. Select the Install Language option.
    b. In the Language CD Location field, enter the directory location of the Language disk or file. Typically, CallPilot uses drive Z (therefore, enter Z:).
26. Click Next.

    Result: The Language Installation page appears.
27. On the Language Installation page, do the following:
    a. Select Languages and Automated Speech recognition to be installed.
    b. Select Primary and Secondary Languages.

    Note:
    The Secondary Language is optional.

    Important:
    The same languages must be installed on both nodes.
28. Click Next.

    Result: The CallPilot Local Area Network Interface page appears.

29. On the CallPilot Local Area Network Interface page, do the following:
    a. Select the network interface card from the drop-down list.

       Result: The MAC address, IP address, and Subnet mask values are updated for the network interface card.
    b. Change the ELAN and CLAN IP information (IP address and Subnet Mask).
    c. Select the High Availability mode check box to display the High Availability Network Interfaces.

       Note:

       To enable High Availability, a proper keycode is required and the High Availability Mode check box must be selected. The keycode has the ability to enable High Availability; however, the feature does not have to be enabled and can be done at a later date.
    d. Enter IP information for the HB1, HB2, and MIRROR network interface cards.

       The following table shows the suggested default values for HB1, HB2, and MIRROR on CP1. If you do not use these suggested values, ensure that you use your new values throughout the configuration.

Network Interface Card (NIC)	IP Address	Subnet Mask
Heartbeat 1 (HB1)	192.0.0.10	255.255.255.0
Heartbeat 2 (HB2)	194.0.0.10	255.255.255.0
MIRROR	193.0.0.10	255.255.255.0

30. Click Next.

    Result: The Ready to Configure page appears.
31. Click Finish to start process.

    Result: The system starts the configuration process and the Progress Information screen appears.
32. After the process is complete, restart the CallPilot server.

Configuring CP2 using the CallPilot Configuration Wizard

Time required: 20 minutes (assuming one language is installed)

The dongle does not have to be moved from CP1 to CP2 to run the Configuration wizard on CP2. Using a High Availability-enabled keycode, the Configuration wizard can be run on CP2.

1. Launch a supported Internet Web browser on CP2.
2. In the address field, enter the following URL to start CallPilot Manager: http://localhost/cpmgr

3. Log on to CallPilot Manager using the administrator mailbox and default password created from the CallPilot Setup Wizard:
    a. Under the User area, enter the following:
        - The administrator mailbox number is 000000.
        - The default password is 124578.
    b. Under the Server area, enter the localhost in the Server field.
4. Click Login.

    Result: The Change User Password screen appears.
5. Change the password for the 000000 mailbox by doing the following:
    a. Enter the Current Password.
    b. Enter the New Password.
    c. Reenter the new password in the New Password Re-Entry field.
    d. Click Save.

    Result: The Welcome to CallPilot Manager page appears.
6. Click Configuration Wizard.

    Result: The Configuration Wizard Welcome Back page appears.
7. Click Next.

    Result: The Keycode and serial number page appears.
8. Enter the following:
    a. In the Serial Number field, enter the serial number of the dongle assigned to the CallPilot server. The serial number entered for CP2 must be the same as the serial number entered for CP1.
    b. In the Key Code field, enter the High Availability-enabled keycode assigned to CallPilot server. The keycode entered for CP2 must be the same as the keycode entered for CP1.
9. Click Next.

    Result: The Feature Verification page appears.
10. Ensure that all parameters are correct and that the High Availability feature says Mirroring.
11. Click Next.

    Result: The Server Information page appears.
12. Do the following:
    a. In the Computer Name field, enter the CallPilot server name.
    b. In the Time Zone field, select the correct time zone.
    c. Under Dialing Information, enter the area code and country code.

d. Enter the LDAP Search Base. For example, dc=nortel,dc=ca.

Note:

All values on the Server Information page for CP2 must be the same as CP1. Use Table 4: High Availability system checklist on page 23 that you completed for both CP1 and CP2.

13. Click Next option.

    Result: The Password Information page appears and the Change the password option is selected.

14. On the Password Information page, do the following:

    a. In the New Password field, enter the new password.

    b. In the Confirm the new password field, reenter the new password.

    c. Click Next.

    Result: A warning message appears.

15. Click OK to dismiss the warning message.

    Result: The Password Information page reappears.

16. Click Next.

    Result: The Multimedia Allocation page appears.

17. Configure the MPB96 settings.

18. Click Next.

    Result: The M1 Switch Information page appears.

19. Configure the switch information.

    a. Select the Switch Type. The Switch Type for CP2 must be the same as CP1.

    b. Enter the Switch Customer Number. The Switch Customer Number for CP2 must be the same as CP1.

    c. Enter the Switch IP Address. The Switch IP Address for CP2 must be the same as CP1.

       See Table 4: High Availability system checklist on page 23 containing the information for both the CP1 and CP2 nodes.

    d. Provision the channels, as follows:

       i. Select a channel.

          Result: The Channel Detail window appears.

       ii. Enter the TN, ACD Position ID, and SCN.

       iii. Ensure that Channel Allocation is set to Multimedia.

       iv. Click OK.

Result: The Meridian 1 Switch Information window appears again.

v. Continue the provisioning of channels until complete.

Note:

To automatically provision a number of channels, you can enter the information for one channel, select the number of channels required, and then click Fill. The Configuration Wizard automatically datafills the channels, and increments the TNs, ACD Position ID, and SCN.

The number of TNs configured on CP2 must be the same as the number configured on CP1.

Note:

This is the CP2 switch-provisioning information for the switch. To obtain the CP2 switch-provisioning information, see the completed Table 4: High Availability system checklist on page 23.

20. Click Next.

    Result: The Meridian 1 CDN Information page appears.

21. Click New to add a new CDN.

    Result: The CDN Details page appears.

22. On the CDN Details page, do the following:

    a. In the CDN field, enter the new CDN.

    Note:

    The CDN for CP2 must be the same as the CDN configured on CP1.

    b. Select the Application Name (Voice Messaging or Multimedia Messaging).

    c. Click OK.

    Result: The new CDN is added and the CDN information page reappears.

23. Click Next.

    Result: The Language Source Directory page appears.

24. Insert the CallPilot 5.0 Language CD in to the CD/DVD drive on CP2.

    Important:

    You must use a CallPilot 5.0 Language CD.

    Language CDs from previous CallPilot releases are not compatible with CallPilot 5.0. The Configuration Wizard checks the version of the Language CD and blocks the use of the CD if it is not a CallPilot 5.0 CD.

25. On the Language Source Directory Select page, do the following:

    a. Select Install Language.

b. In the Language CD Location field, enter the directory of the Language disk or file. Typically, CallPilot uses drive Z.

26. Click Next.

    Result: The Language Installation page appears.

27. On the Language Installation page, do the following:

    a. Select Languages and Automated Speech recognition to be installed.

    b. Select Primary and Secondary Languages.

    Note:
    The Secondary Language is optional.

Important:
The same languages must be installed on CP1 and CP2.

28. Click Next.

    Result: The CallPilot Local Area Network Interface page appears.

29. On the CallPilot Local Area Network Interface page, do the following:

    a. Select the network interface card from the drop-down list.

    Result: The MAC address, IP address, and Subnet mask values are updated for the network interface card.

    b. Change the ELAN and CLAN IP information (IP address and Subnet Mask).

    c. Select the High Availability mode check box to display the High Availability Network Interfaces.

    Note:
    To enable High Availability, a proper keycode is required and the High Availability Mode check box must be selected. The keycode has the ability to enable High Availability; however, the feature does not have to be enabled as it can be done at a later date.

    d. Enter IP information for the HB1, HB2, and MIRROR network interfaces cards.

    The following table shows the suggested default values for HB1, HB2, and MIRROR on CP2. If you do not use these suggested values, ensure that you use your new values throughout the configuration.

Network Interface Card (NIC)	IP Address	Subnet Mask
Heartbeat 1 (HB1)	192.0.0.11	255.255.255.0
Heartbeat 2 (HB2)	194.0.0.11	255.255.255.0
MIRROR	193.0.0.11	255.255.255.0

30. Click Next.

Result: The Ready to Configure page appears.

31. Click Finish to start process.

    Result: The system starts the configuration process and displays its progress.

32. After the process is complete, restart the CallPilot server.

Connect and verify LAN connections

Use the following figure and procedure to connect the HB1, HB2, and MIRROR crossover LAN cables, and the ELAN and CLAN cables between the two High Availability servers.

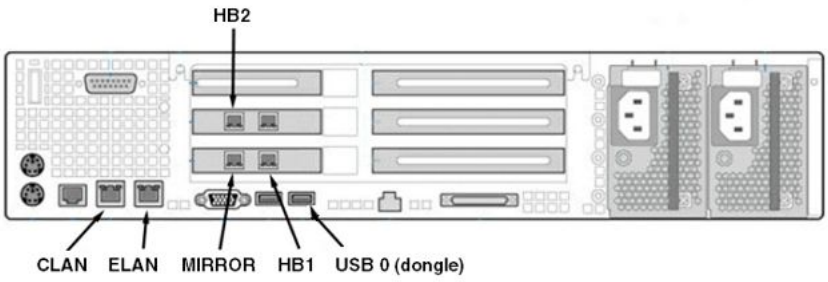


Figure 4: Rear panel of 1005r server showing LAN connections

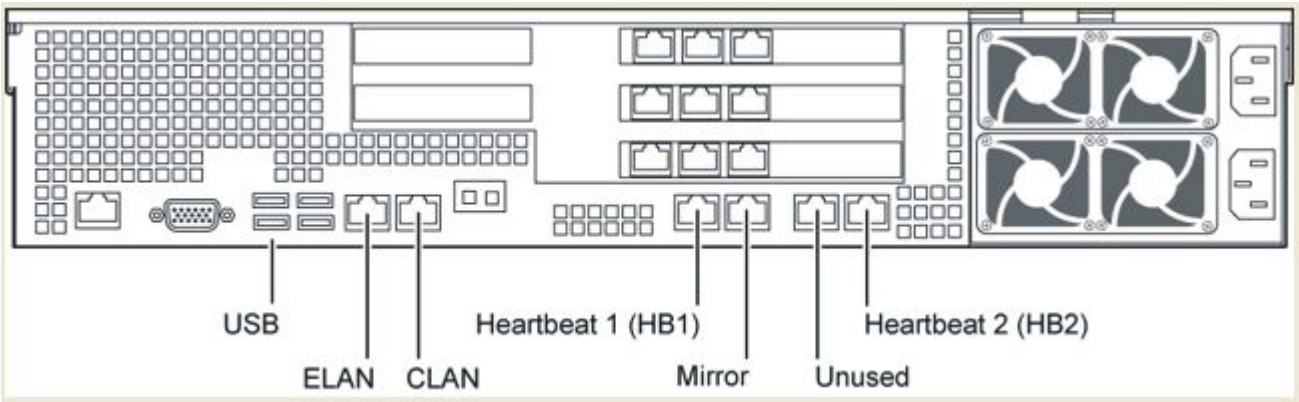


Figure 5: Rear panel of 1006r server showing LAN connections

Connecting and verifying LAN connections

Important:

Do not change the names of default network connections (ELAN, CLAN, MIRROR, HB1, and HB2) created after High Availability servers installation.

1. On CP1 and CP2, select Start > Settings > Network Connections.

   Result: The Network Connection window appears and shows that the HB1, HB2, MIRROR, ELAN, and CLAN connections are not connected.

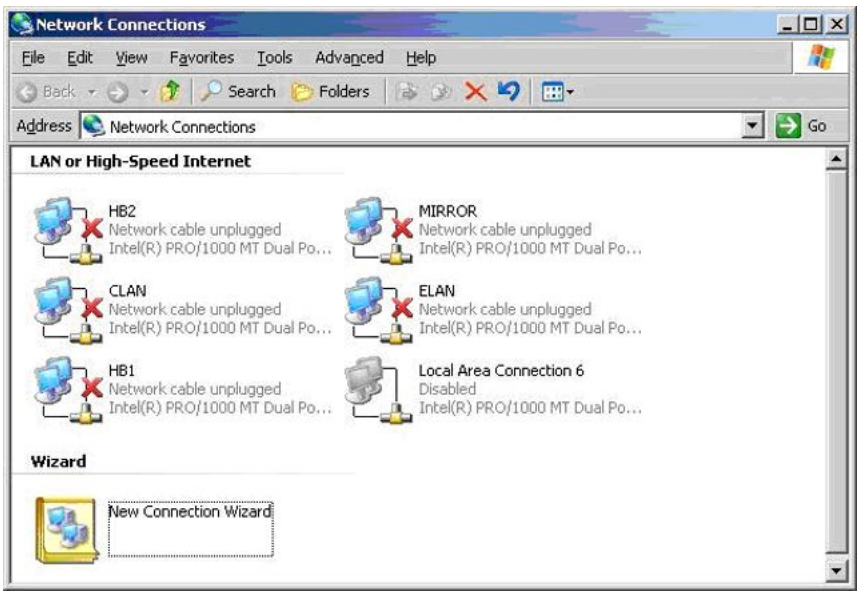


Figure 6: Network Connections - no connections

2. Connect the HB1 crossover LAN cable between both the CP1 and CP2 servers.
3. In the Network Connections window, verify that HB1 shows that it is connected.

   Result: The red X is removed from the HB1 icon, as shown in the following figure.

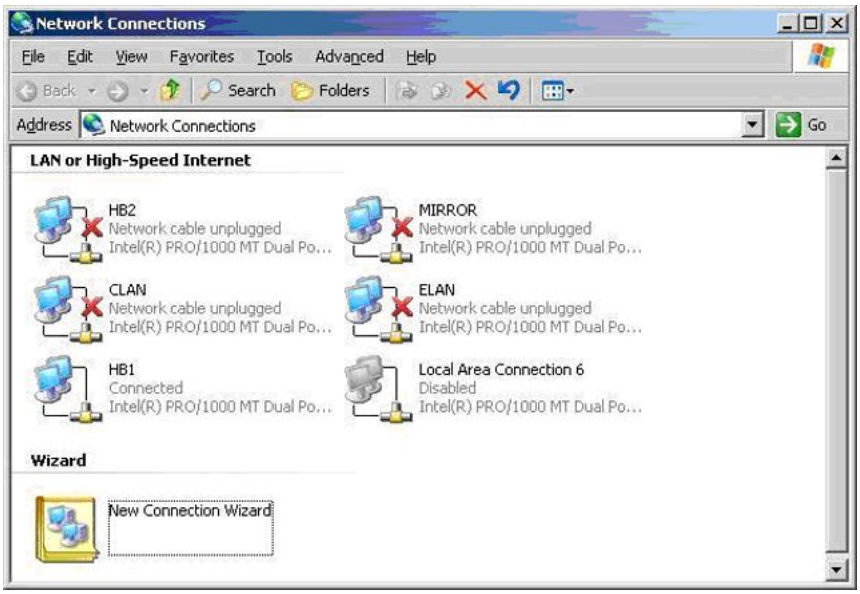


Figure 7: Network Connections - HB1 connected

4. To ensure that the HB1 cable is properly connected, perform the following from CP1:
   a. Open a command prompt.
   b. Enter the command tracert –d 192.0.0.11 to verify the HB1 connection.

Note:

If you are not using the default values for the heartbeat connections, enter tracert -d <IP address of HB1 on CP2>.

c. Confirm that server CP2 can be reached in one hop.

5. Connect the HB2 crossover LAN cable between both the CP1 and CP2 servers.
6. In the Network Connections window, verify that HB2 shows that it is connected.

   Result: The red X is removed from the HB2 icon.
7. To ensure that the HB2 cable is properly connected, perform the following from CP1:

   a. Open a command prompt.

   b. Enter the command tracert –d 194.0.0.11 to verify the HB2 connection.

   Note:

   If you are not using the default values for the heartbeat connections, enter tracert -d <IP address of HB2 on CP2>.

   c. Confirm that server CP2 can be reached in one hop.
8. Connect the MIRROR crossover LAN cable between both the CP1 and CP2 servers.
9. In the Network Connections window, verify that MIRROR shows that it is connected.

   Result: The red X is removed from the MIRROR icon.
10. To ensure that the MIRROR cable is properly connected, perform the following from CP1:

    a. Open a command prompt.

    b. Enter the command tracert –d 193.0.0.11 to verify the MIRROR connection.

    Note:

    If you are not using the default values for the heartbeat connections, enter tracert -d <IP address of Mirror on CP2>.

    c. Confirm that server CP2 can be reached in one hop.
11. Connect the ELAN cable.
12. In the Network Connections window, verify that ELAN shows that it is connected.

    Result: The red X is removed from the ELAN icon.
13. To ensure that the ELAN is properly connected, perform the following from CP1:

    a. Open a command prompt.

    b. Verify that the switch is accessible by running the following command: ping <switch IP address>

c. Verify that CP2 is accessible by running the following command: ping <CP2 ELAN IP address>

14. Connect the CLAN cable.
15. In the Network Connections window, verify that CLAN shows that it is connected.

    Result: The red X is removed from the CLAN icon.
16. To ensure that the CLAN is properly connected, perform the following from CP1:

    a. Open a command prompt.

    b. Verify that the default gateway is accessible by running the following command: ping <CLAN/Avaya server subnet default gateway IP address>

    c. Verify that CP2 is accessible by running the following command: ping <CP2 CLAN IP address>
17. Check the Network Connections window and ensure that all connections are made.

    Result: No red Xs appear on any of the icons (as shown in the following figure).

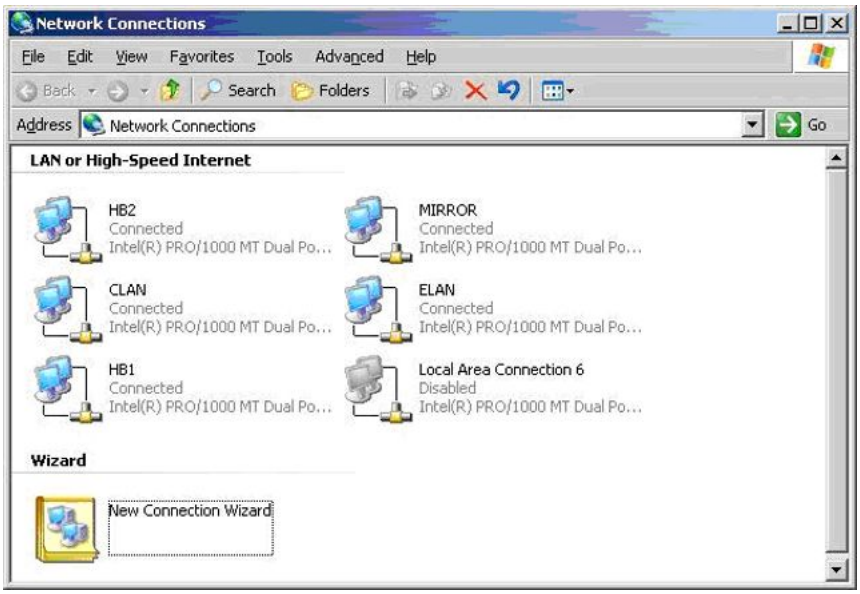


Figure 8: Network Connections - all connections made

Modifying the hosts file

This procedure is required if a DNS server is not used in the network solution or part of the configuration (in particular, where IP address name resolution is preferred). Use the following procedure to resolve the Managed CLAN IP address (virtual CLAN IP address).

On your <server or client PC>, perform the following steps:

a. Open Windows Explorer and navigate to the following folder: C:\WINDOWS \system32\drivers\etc

b. Double-click the hosts file.

Result: The Open with window appears.

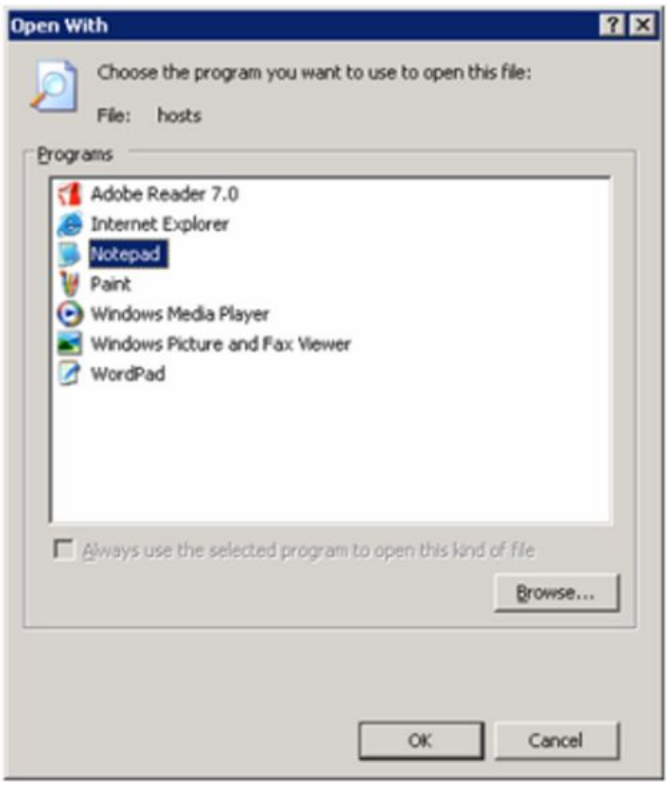


Figure 9: Open With window

c. Select Notepad.

d. Click OK.

   Result: The Notepad application appears and displays the hosts file information.

e. Save a copy of the hosts file (as a backup) before you modify the file.

f. Place the cursor at a new line directly underneath the default entry 127.0.0.1.

g. Enter the Managed CLAN IP address.

   For more information, see Table 4: High Availability system checklist on page 23.

h. Press the Tab key until cursor is underneath the default localhost and enter the Managed CLAN Host Name for the associated Managed CLAN IP address that was just entered.

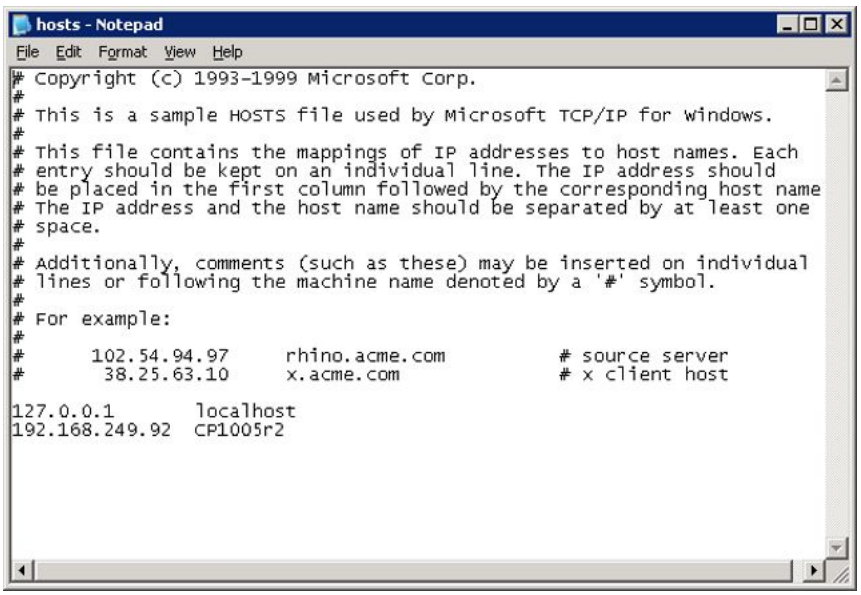


Figure 10: hosts file

i. Press the Enter key to go to next line.

Note:

If a DNS server is used as a solution, ensure Network Administrator has the entries entered into the DNS server configuration.

Use the following procedure to test the host name resolution.

Testing the host name resolution

This procedure is an example of how to test the host name for CP1 and CP2 if the Managed CLAN host name has been added to their respective host files.

1. On CP1, do the following:

   a. Select Start > Run.

      Result: The Run window appears.

   b. In the Open field, type cmd.

      Result: The DOS Command Prompt appears.

   c. Enter the following command: ping <CP2 CLAN Host Name>

      Result: If the CLAN is properly connected and the host file is configured with the IP address and host name information, a reply is displayed showing the Managed CLAN IP address and the time to return.

   d. Repeat (if necessary) with other host names from CP2.

2. On CP2, repeat the preceding steps.

Run Stage 1 of the High Availability Configuration Wizard to check CP1 and CP2 configuration

The High Availability Configuration Wizard is run twice during the configuration of a High Availability server pair:

- Stage 1: The High Availability Configuration Wizard is run for the first time to gather and verify the configuration of the two nodes in the High Availability pair. This is done to ensure that the nodes are correctly configured (for example, to ensure that the networking information is consistent between the two nodes). For more information, see Running Stage 1 of the High Availability Configuration Wizard to check CP1 and CP2 configuration on page 58.
- Stage 2: The High Availability Configuration Wizard is run a second time to verify the AutoStart software installation and to generate the definition file that is imported into the AutoStart Console to provide the initial configuration. For more information, see Generating the AutoStart Definition File on page 86.

Running Stage 1 of the High Availability Configuration Wizard to check CP1 and CP2 configuration

The High Availability Configuration Wizard is only run on CP1.

1. Use Windows Explorer to navigate to the D:\Nortel\HA folder.
2. Double-click the HighAvailabilityConfigurationWizard.exe file.

   Result: The High Availability Configuration Wizard appears.

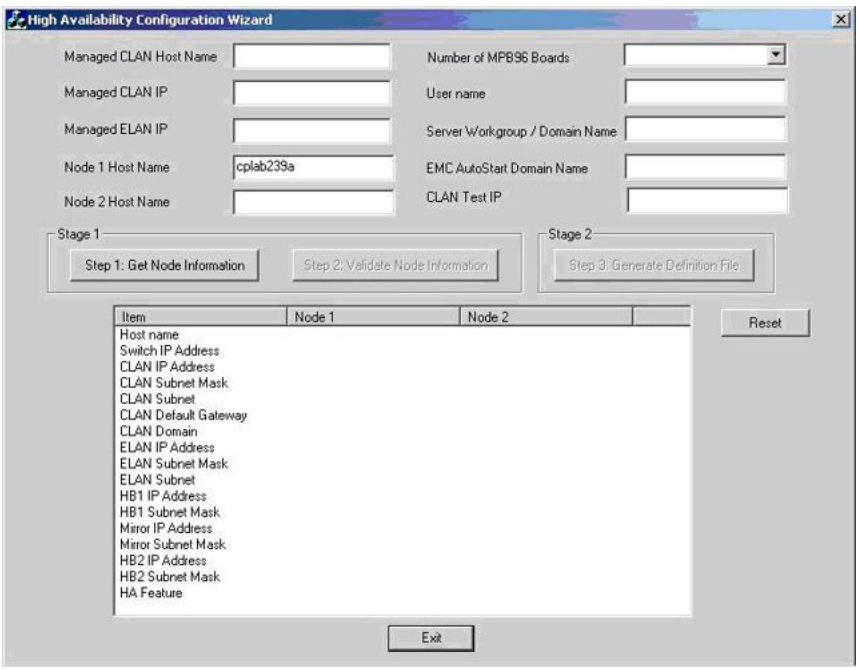


Figure 11: High Availability Configuration Wizard

3. Enter the following information based on the server configuration. This information is completed in Table 4: High Availability system checklist on page 23:

    a. Managed CLAN Host Name: Enter the Host Name of the Managed CLAN.

    b. Managed CLAN IP: Enter the IP address of the Managed CLAN.

    c. Managed ELAN IP: Enter the IP address of the Managed ELAN.

    d. Node 1 Host Name: The Node 1 Host Name is initialized to the name of the server on which the High Availability Configuration Wizard is run. The Host Name is the name of the first CallPilot server (CP1) in the High Availability pair.

    e. Node 2 Host Name: Enter the Host Name of the second CallPilot server (CP2) in the High Availability pair.

    f. Number of MPB96 boards: Enter the number of MPB96 boards installed in the server.

    g. User name: Enter the user name of the administrator account.

    h. Server Workgroup / Domain Name: Enter the name of the Windows workgroup or Windows domain in which the CallPilot servers belong.

    i. EMC AutoStart Domain Name: Enter the domain name of the AutoStart domain.

    The Domain Name must be a unique name and is used as the AutoStart domain for the pair of CallPilot servers. This name must contain only alphanumeric characters and have a maximum length of eight

characters. The domain name must be the same domain name that was used in the High Availability Configuration Wizard.

Note:

This document uses [AutoStart_Domain]. This value must be replaced with your AutoStart domain name.

j. CLAN Test IP: Enter the IP address on the CLAN to be used to verify the CLAN connection. The IP address must be of a device that responds to the ping command. If there is no CLAN connection, enter the loopback IP address (127.0.0.1).

4. Click the Step 1: Get Node Information button to retrieve information from the two servers in the High Availability pair.

   - If there are any errors, a dialog box is displayed with the error details. If the Configuration Wizard is unable to communicate with either of the servers, verify that both servers have all the network cables connected and that the administrator account passwords are the same on both servers.

     Note:

     Under some circumstances, problems with server connections can be resolved with the following workaround:

     a) Open the Services window on the CP1

     b) Open Properties window of the Remote Registry service

     c) Change 'Startup type' of the service from 'Disabled' to 'Manual'

     d) Press Apply button at the bottom of Properties window

     e) Click the Start button

     f) Click OK

     g) Repeat action a) to f) on the CP2

     h) Click the Step 1: Get Node Information button

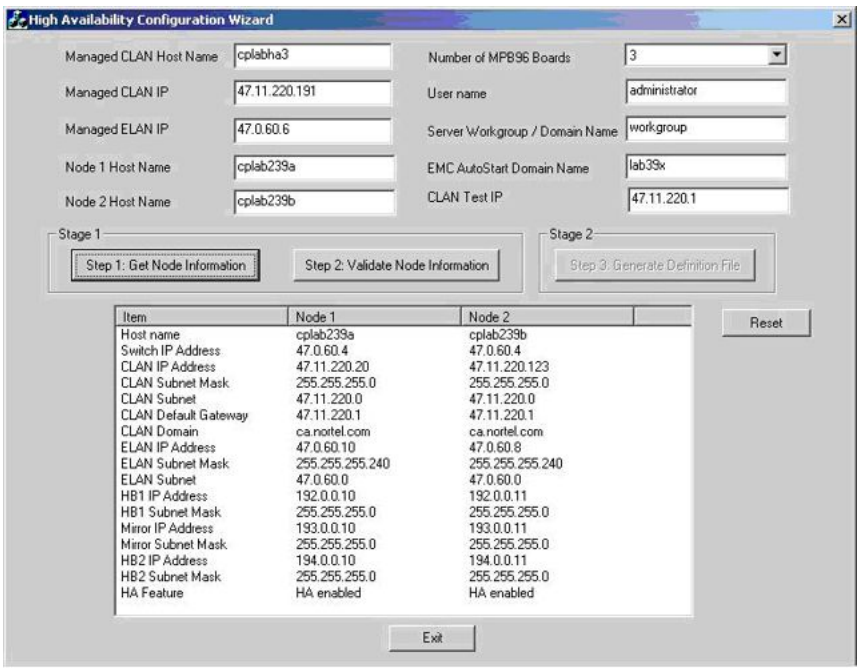
     Warning:

     To prevent possible security attacks, change the Startup type of the Remote Registry service to Disabled after the HA pair configuration is finished.

     Warning:

     Do not change the Startup type of the Remote Registry service back to Disabled until configuration of the HA pair is finished.

   - If there are no errors, the Configuration Wizard is updated with the information from the servers and the Validate Node Information button is enabled.



Item	Node 1	Node 2
Host name	cplab239a	cplab239b
Switch IP Address	47.0.60.4	47.0.60.4
CLAN IP Address	47.11.220.20	47.11.220.123
CLAN Subnet Mask	255.255.255.0	255.255.255.0
CLAN Subnet	47.11.220.0	47.11.220.0
CLAN Default Gateway	47.11.220.1	47.11.220.1
CLAN Domain	ca.nortel.com	ca.nortel.com
ELAN IP Address	47.0.60.10	47.0.60.8
ELAN Subnet Mask	255.255.255.240	255.255.255.240
ELAN Subnet	47.0.60.0	47.0.60.0
HB1 IP Address	192.0.0.10	192.0.0.11
HB1 Subnet Mask	255.255.255.0	255.255.255.0
Mirror IP Address	193.0.0.10	193.0.0.11
Mirror Subnet Mask	255.255.255.0	255.255.255.0
HB2 IP Address	194.0.0.10	194.0.0.11
HB2 Subnet Mask	255.255.255.0	255.255.255.0
HA Feature	HA enabled	HA enabled

Figure 12: Node Information displayed in bottom pane

5. Click the Step 2: Validate Node Information button to check that the configuration of the two servers in the pair match. The Validate Node Information button checks the format of the entered IP addresses, pings the HB1, HB2, and Mirror IP addresses, and compares the workgroup or domain information on both nodes to ensure the information is the same.
   - If there are any errors, a message box is displayed with details of the error. Correct the problem on the server that has the error and then click the Step 2: Validate Node Information button again.
   - If there are no errors, a message displays showing that Stage 1 is complete. You must exit the Configuration Wizard and continue with the installation (or upgrade) process. The information you entered is automatically saved.

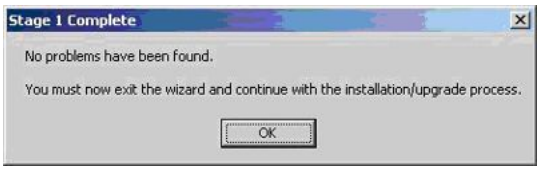


Figure 13: Stage 1 Complete

6. Click the Exit button.
7. Click Yes to confirm the exit from the High Availability Wizard.

Install the AutoStart Agent and Console software

The High Availability feature uses the AutoStart software that must be installed on both servers. The AutoStart software includes both Agent and Console software.

There can also be AutoStart software patches that must be installed.

Note:

Within the AutoStart software, the two CallPilot servers are included in an AutoStart domain. The name of the domain must be unique within the network. For the purposes of this document, the domain name [AutoStart_Domain] is used. This value must be replaced with the AutoStart domain name to be used by the customer. The AutoStart Domain has no association with the customer's network domain and is used only by the AutoStart software.

Install the AutoStart software on CP1

The following procedure installs AutoStart 5.3 SP3 Agent and Console software on the CP1 server. This procedure takes approximately 10 minutes.

Installing the AutoStart Agent and Console software on CP1

Important:

The computer name must be set before you install the AutoStart software. The software requires the computer name. The computer name must contain only alphanumeric characters. Nonalphanumeric characters (such as a hyphen [-]) are not supported.

If you want to change the computer name after installing the server you must uninstall and then reinstall the AutoStart software.

1. Insert the CallPilot Application CD.
2. Navigate to the Z:\EMC folder on the CallPilot Application CD.
3. Double-click EMC_AutoStart_5.3_SP3_Update.exe to unpack the archive to D:\temp folder..

   Result: Three files are unpacked into the D:\temp\EMC_AutoStart_5.3_SP3_Update folder: EAS53_WIN_x86.exe, EAS53SP3_WIN_x86.exe, EMC AutoStart Update Process.pdf
4. Double-click EAS53SP3_WIN_x86.exe file to start the installation.

   Result: The InstallShield Wizard informs you that the AutoStart 5.3 SP3 software is preparing to install (install preparation can take a few minutes). After preparation is complete, Welcome window appears.

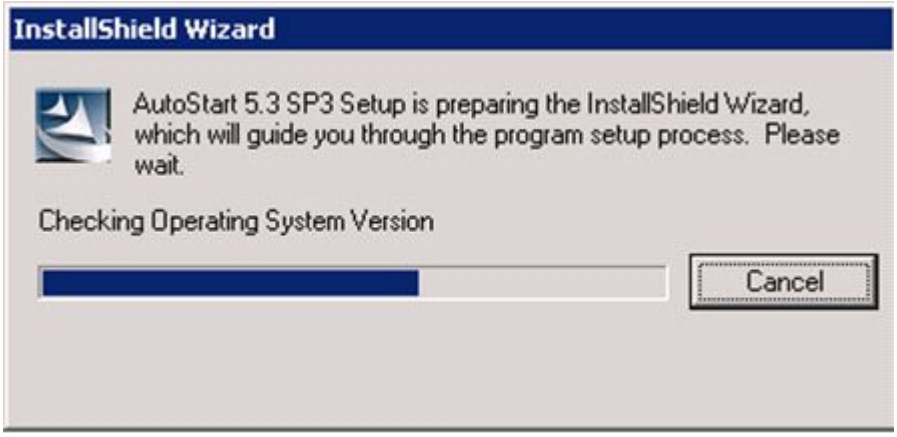


Figure 14: InstallShield Wizard - Preparing to install AutoStart 5.3 SP3 software

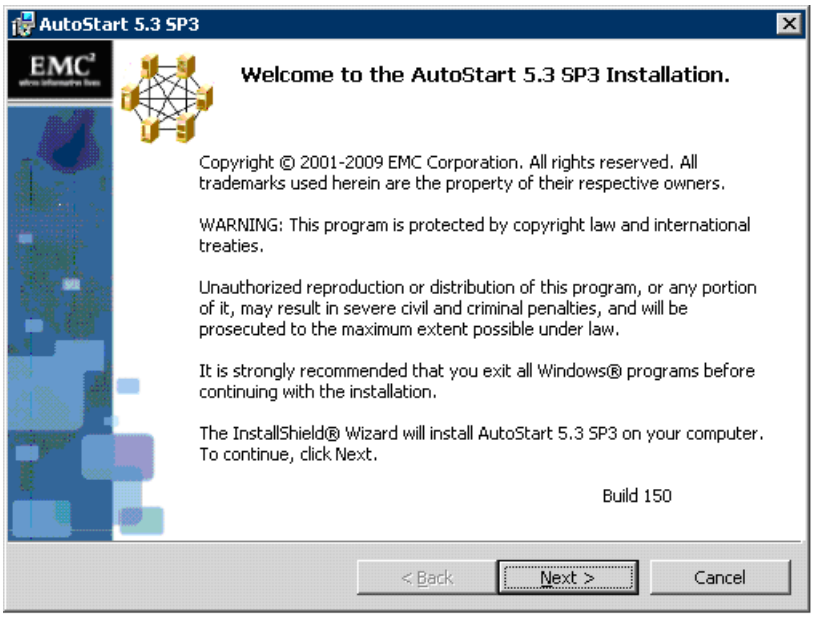


Figure 15: Welcome window

5. Click Next .

   Result: AutoStart 5.3 SP3 reminder to read the documents appears.

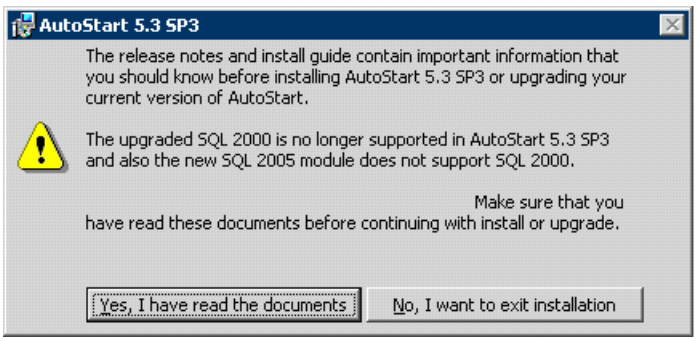


Figure 16: Reminder to read the documents

6. Click Yes, I have read the documents.

   Result: AutoStart 5.3 SP3 reminder is closed.

7. Click Next on Welcome window.

   Result: License Agreement window appears.

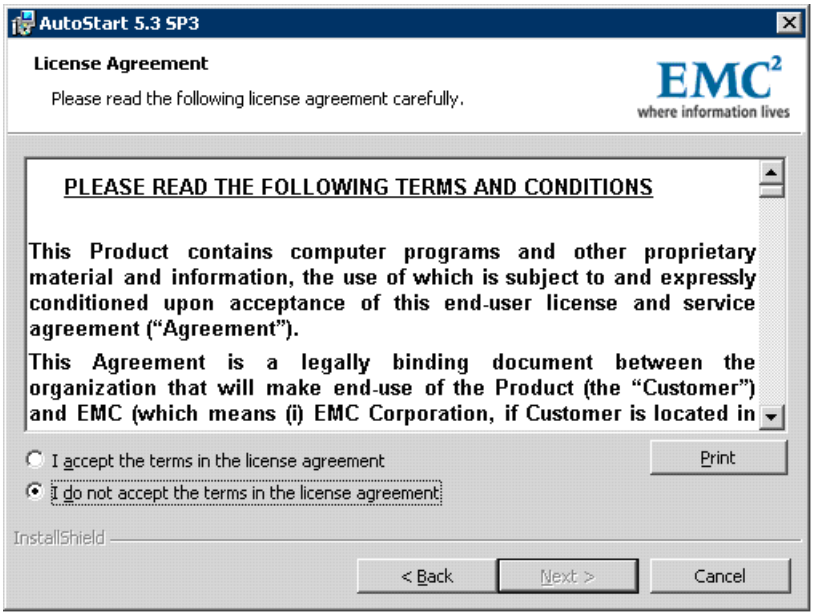


Figure 17: License Agreement window

8. Select the option I accept the terms in the license agreement.
9. Click Next.

   Result:The Custom Setup window appears.

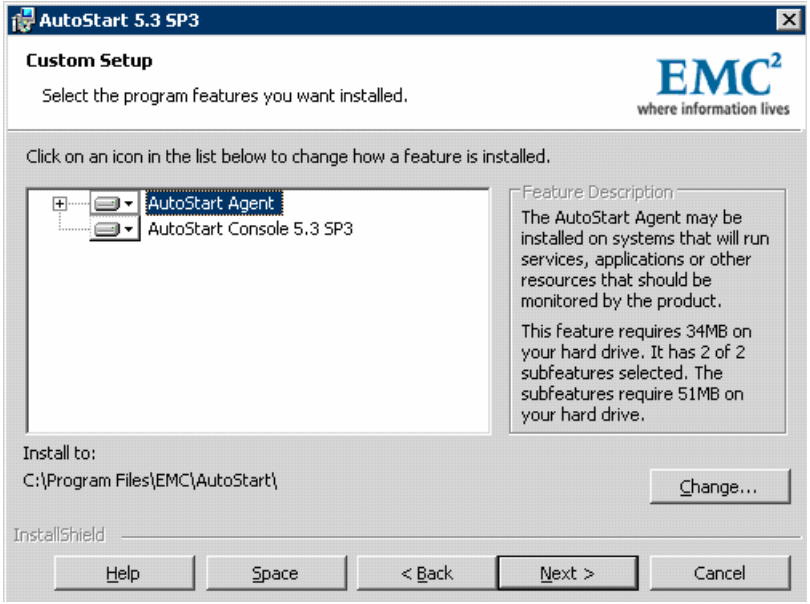


Figure 18: Custom Setup window

10. Click Change to change the installation path.

    Result:The Change Current Destination Folder dialog box appears.

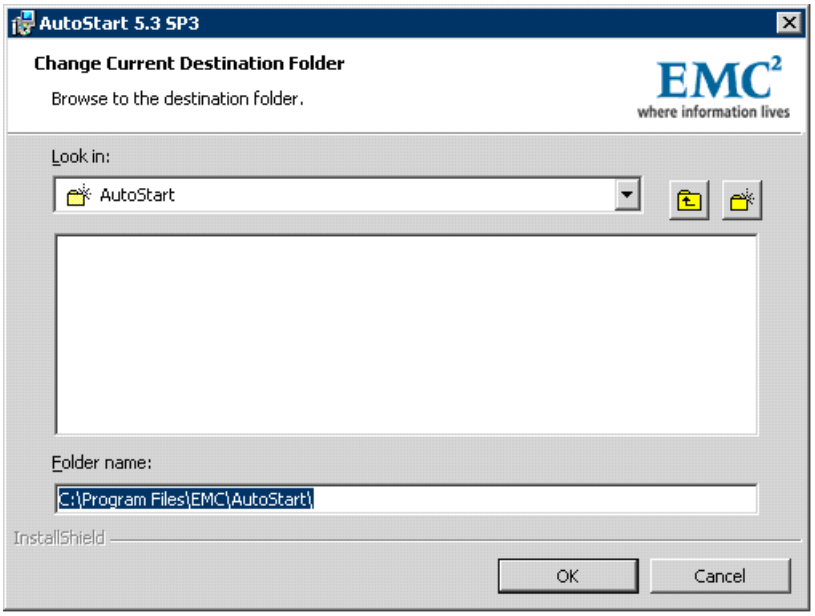


Figure 19: Change Current Destination Folder dialog box

11. In Folder name field, change the drive letter from C to D, change the path to:

    D:\Program Files\EMC AutoStart\

Important:

You must install the software in the D:\Program Files\EMC AutoStart\ directory or the software does not work correctly.

12. Click OK.

    Result:The Change Current Destination Folder dialog box closes and you are returned to the Custom Setup window, which shows the correct installation path.

13. Click Next.

    Result:The Agent Connection Information window appears.

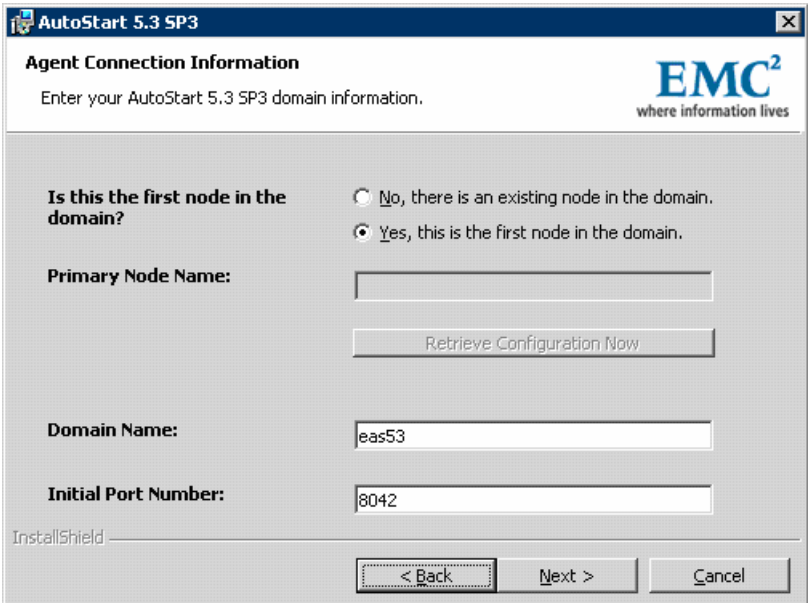


Figure 20: Agent Connection Information window

14. Leave the option Yes, this is the first node in the domain selected.
15. Enter the EMC AutoStartDomain Name. The AutoStart Domain Name must be the same name that you entered in the High Availability Configuration Wizard.

    Note:

    This document uses [AutoStart_Domain]. This value must be replaced with your AutoStart domain name.

16. Leave Initial Port Number unchanged.
17. Click Next

    Result:The Mirroring Network Configuration & Product Licensing window appears.

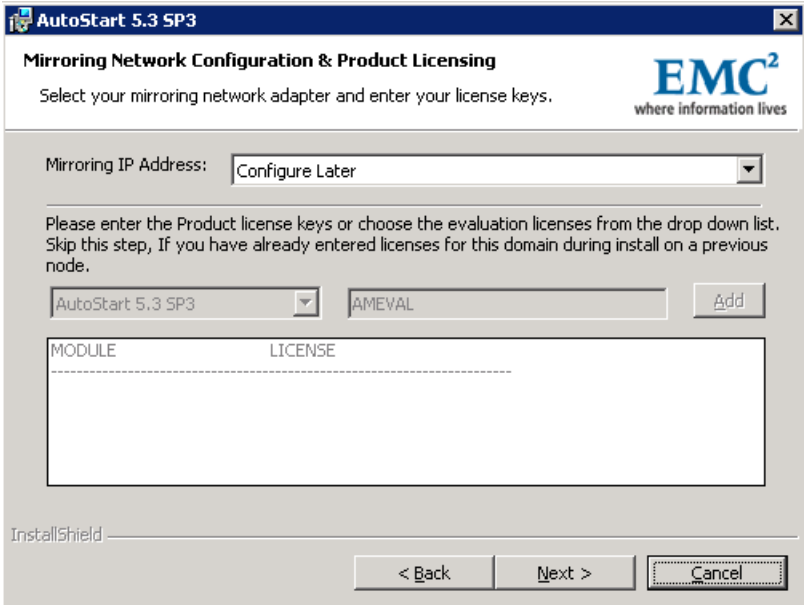


Figure 21: Mirroring Network Configuration and Product Licensing window

18. In the field Mirroring IP Address: select the IP address that was assigned to the Mirror NIC on CP1 server. The default value is Configure Later.
19. By default the AutoStart 5.3 SP3 module is selected from the drop-down list. Enter AutoStart 5.3 SP3 Product license key (provided with your CallPilot server) in the field on the right. Click Add to add the license in the list.

    Result: The AutoStart 5.3 SP3 module is added in the list at the bottom with appropriate license key.

    Note:

    The AutoStart license key is a string of 24 characters plus a dash. There are 8 characters before the dash and 16 characters after the dash (XXXXXXXX-XXXXXXXXXXXXXXXX). When entering the AutoStart license key, you must enter the whole string including the dash.

    Note:

    When you order the High Availability feature, AutoStart 5.3 SP3 license key comes in the form of EMC License Registration Card.

20. For all other five modules in the drop-down list (Exchange 2003, Oracle 3.1, Sql Server, MirrorView, SRDF) do the following:

    a. Select the module from the drop-down list.

       Result: Appropriate evaluation license is displayed in the field on the right.

    b. Click Add

       Result: Evaluation licenses for the five modules are added in the list at the bottom.

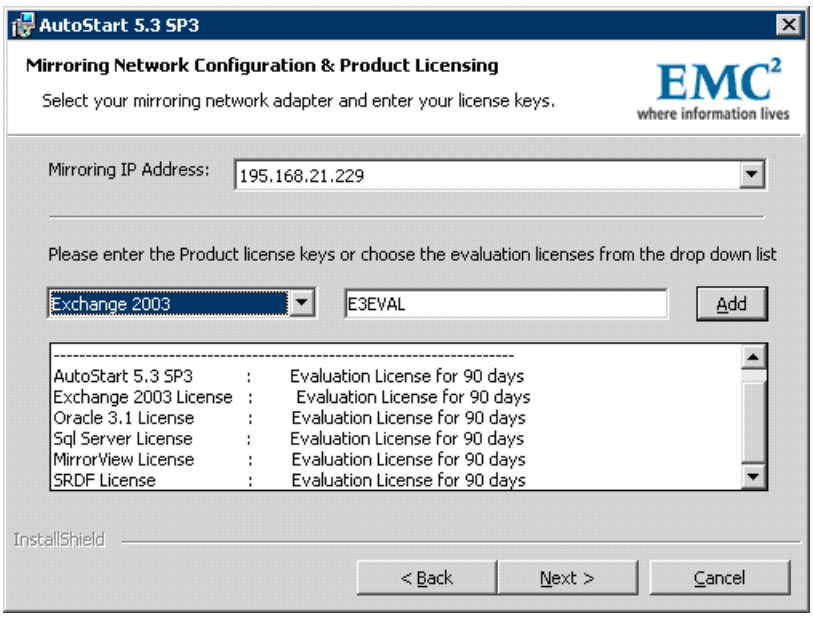


Figure 22: Mirroring Network Configuration and Product Licensing window

21. Click Next to continue.

    Result: The Confirm Settings window appears.

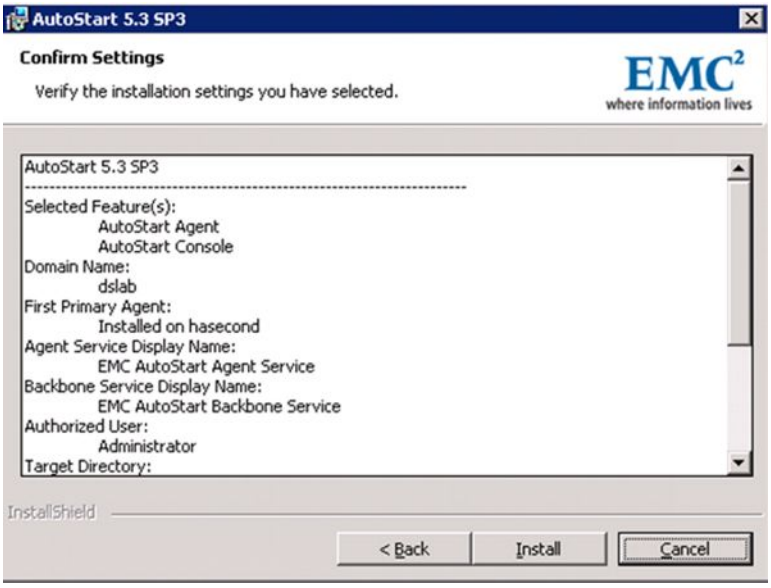


Figure 23: Confirm Settings window

22. Verify that the settings are correct.
23. Click Install to start the installation of the AutoStart Agent and Console software.

    Result:The Installing AutoStart 5.3 SP3 window appears and shows the status of the installation.

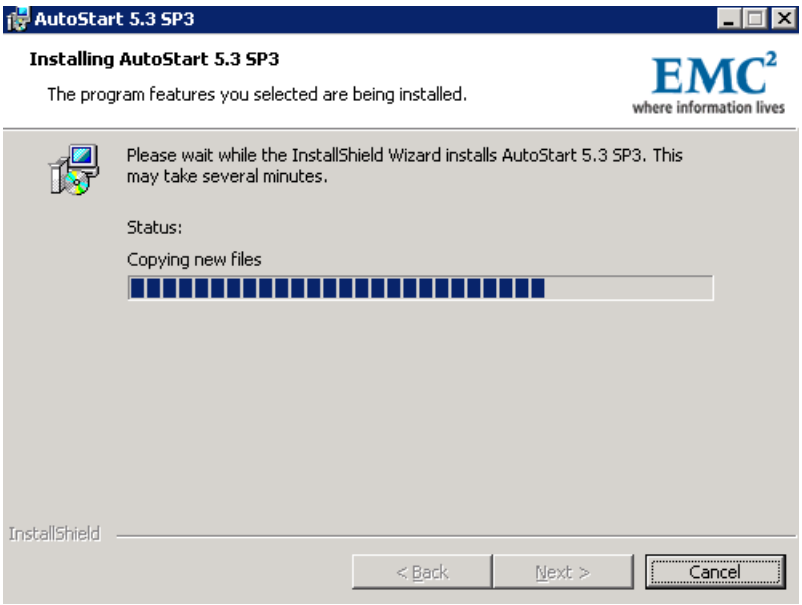


Figure 24: Installing AutoStart 5.3 SP3 window

24. Wait until the installation is complete and the InstallShield Wizard Completed window appears.

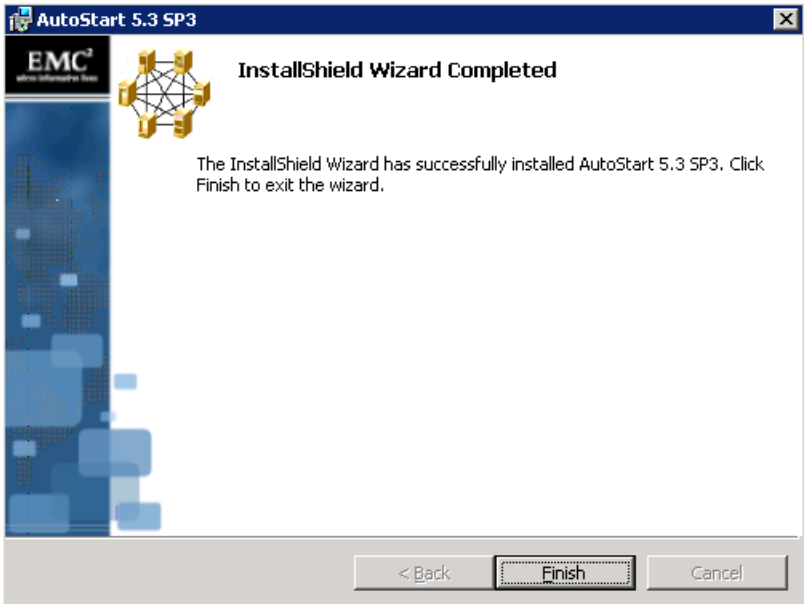


Figure 25: InstallShield Wizard Completed window

25. Click Finish Result: The AutoStart 5.3 SP3 Installer Information dialog box appears.

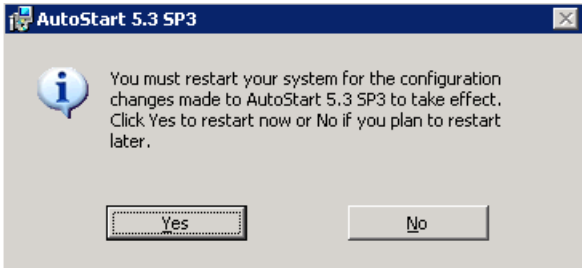


Figure 26: AutoStart 5.3 SP3 dialog box

26. Click No if there are patches to install or click Yes to restart the CP1 server.

    Note:

    If there are patches available for AutoStart 5.3 SP3, install the patches and then restart the CP1 server.

27. Delete the folder D:\temp\EMC_AutoStart_5.3_SP3_Update.

Add the node 2 administrator account to the AutoStart Console on node 1

Add the node 2 administrator account to the AutoStart Console on node 1

This procedure adds the CP2 Administrator Account to the AutoStart Console on CP1.

Important:

The CP2 Administrator Account must be added to the AutoStart Console on CP1 before you install the AutoStart software on CP2. If you try to install the AutoStart software on CP2 before you add the administrator account of CP2 into the AutoStart console on CP1, the AutoStart Agent installed on CP2 cannot communicate with the Agent installed on CP1. You must uninstall the Agent and Console software and then reinstall the software.

1. Log on to CP1.

   Note:

   An error can appear, indicating that “At least one service or driver failed to start.” This is normal, as the AutoStart mirroring service is installed on node 1; however, the service is not yet fully configured so the server cannot start.

2. Launch the AutoStart Console on CP1 by selecting Start > Programs > EMC AutoStart > EMC AutoStart Console 5.3 SP3.

   Result: The AutoStart Console appears.

3. In the Domain pane (left side of the window), click [AutoStart_Domain] where [AutoStart_Domain] is the domain name created when you installed the AutoStart Agent.

Note:

If the domain is not visible and an error is reported, close and reopen the AutoStart Console.

4. Select the Licensing/Security tab.

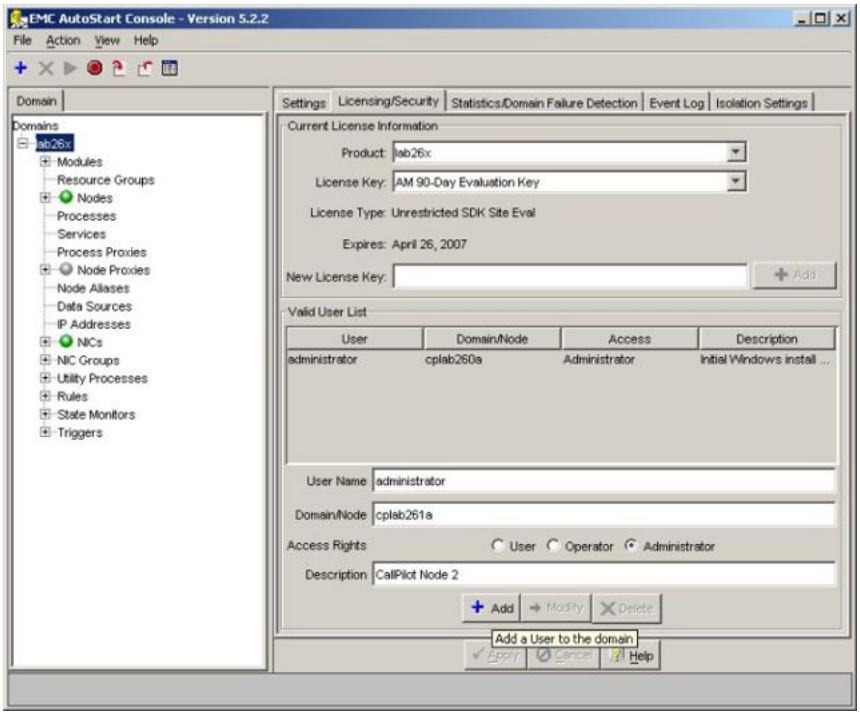


Figure 27: AutoStart Console - Licensing/Security tab - Add Admin User

5. In the Valid User List area, enter the following information:
   a. In the User Name field, enter administrator.
   b. In the Domain/Node field, enter the host name of CP2.
   c. For the Access Rights option, select the Administrator option button.
   d. In the Description field, enter CallPilot Node 2.
6. Click Add.

   Result: A row is added to the Valid User List.

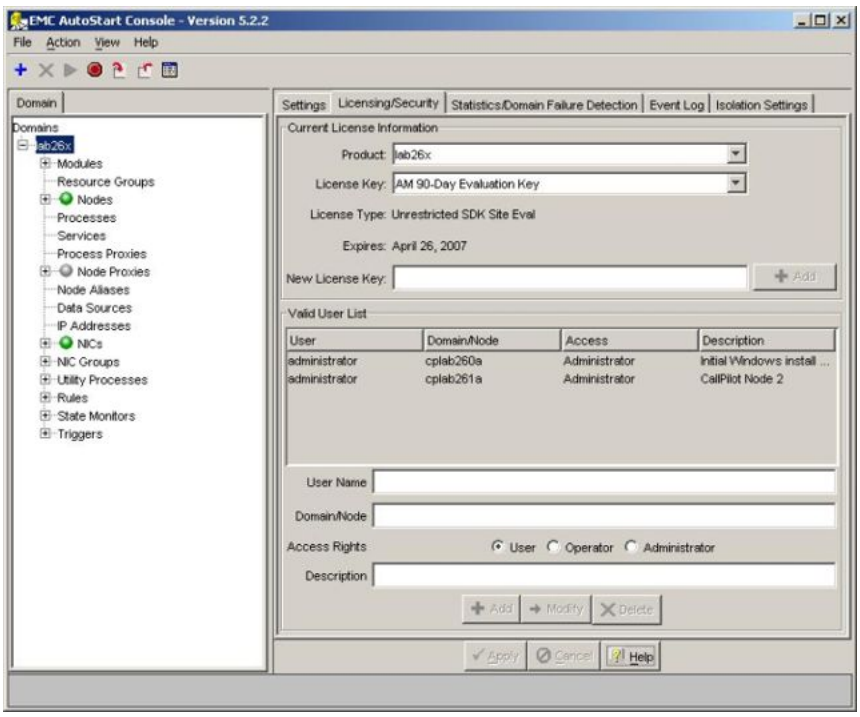


Figure 28: AutoStart Console - Licensing/Security tab - Node 2 Administrator user is added

7. Exit the AutoStart Console on CP1.

Install the AutoStart software on CP2

The following procedure installs AutoStart 5.3 SP3 Agent and Console software on the CP2 server. This procedure takes approximately 10 minutes.

Installing the AutoStart Agent and Console software on CP2

Important:

The computer name must be set before you install the AutoStart software. The software requires the computer name. The computer name must contain only alphanumeric characters. Nonalphanumeric characters (such as a hyphen [-]) are not supported.

If you want to change the computer name after installing the server you must uninstall and then reinstall the AutoStart software.

1. Insert the CallPilot Application CD.
2. Navigate to the Z:\EMC folder on the CallPilot Application CD.
3. Double-click EMC_AutoStart_5.3_SP3_Update.exe to unpack the archive to the D:\temp folder.

Result: Three files are unpacked into the D:\temp \EMC_AutoStart_5.3_SP3_Update folder: EAS53_WIN_x86.exe, EAS53SP3_WIN_x86.exe, EMC AutoStart Update Process.pdf

4. Double-click EAS53SP3_WIN_x86.exe to start the installation.

   Result: The InstallShield Wizard informs you that AutoStart 5.3 SP3 software is preparing to install (this can take a few minutes). After preparation is complete, the Welcome window appears.

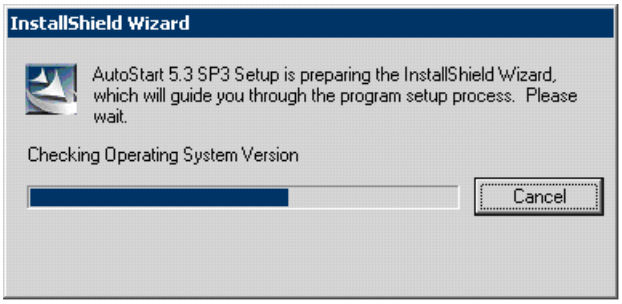


Figure 29: InstallShield Wizard - Preparing to install AutoStart 5.3 SP3 software

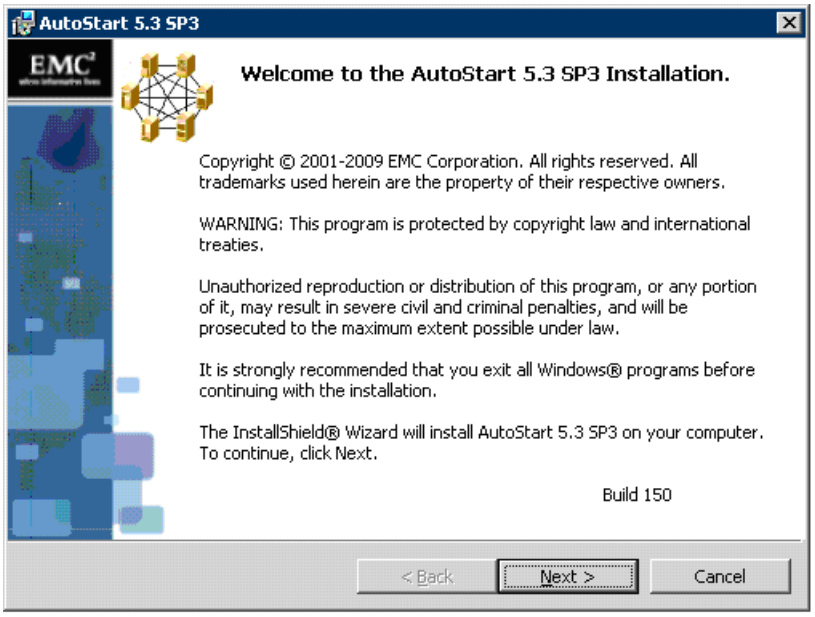


Figure 30: Welcome window

5. Click Next.

   Result: AutoStart 5.3 SP3 reminder to read the documents appears.

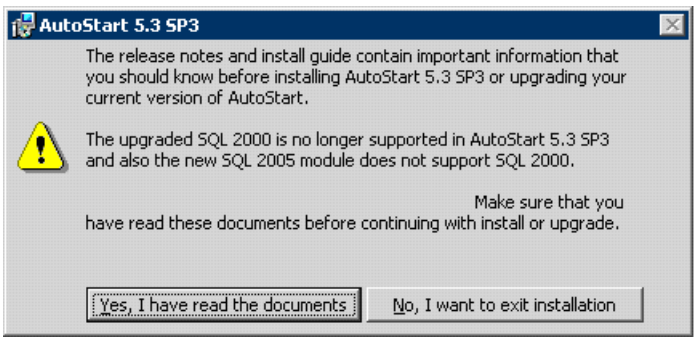


Figure 31: Reminder to read the documents

6. Click Yes, I have read the documents.

   Result: AutoStart 5.3 SP3 reminder is closed.

7. Click Next on the Welcome window.

   Result: The License Agreement window appears.

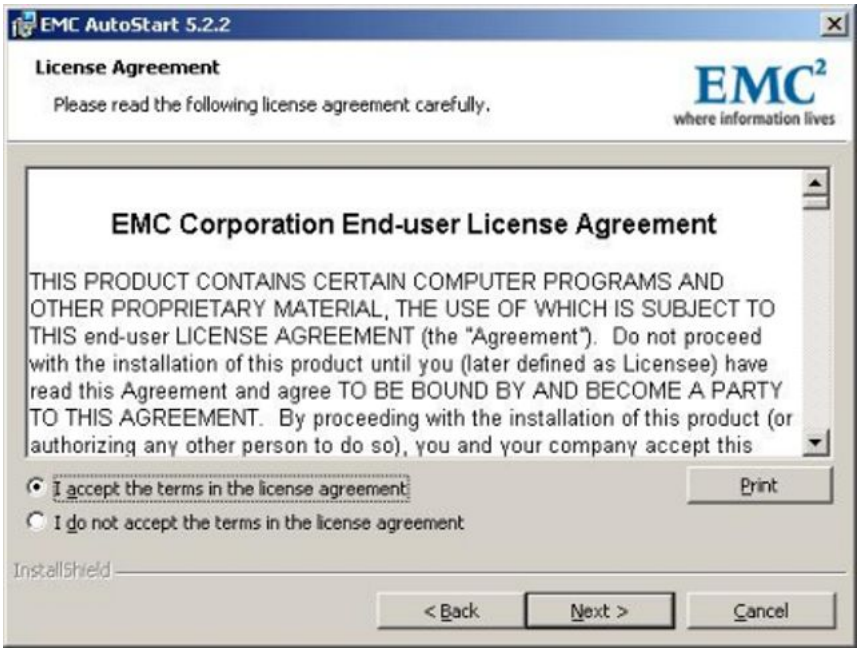


Figure 32: License Agreement window

8. Select the I accept the terms in the license agreement option.
9. Click Next.

   Result: The Custom Setup window appears.

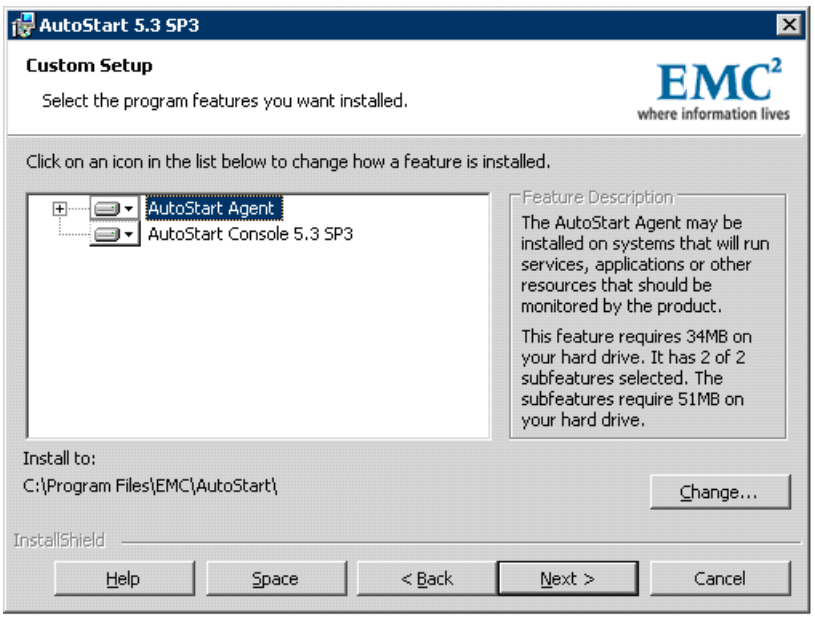


Figure 33: Custom Setup window

10. Click Change to change the installation path.

    Result: The Change Current Destination Folder dialog box appears

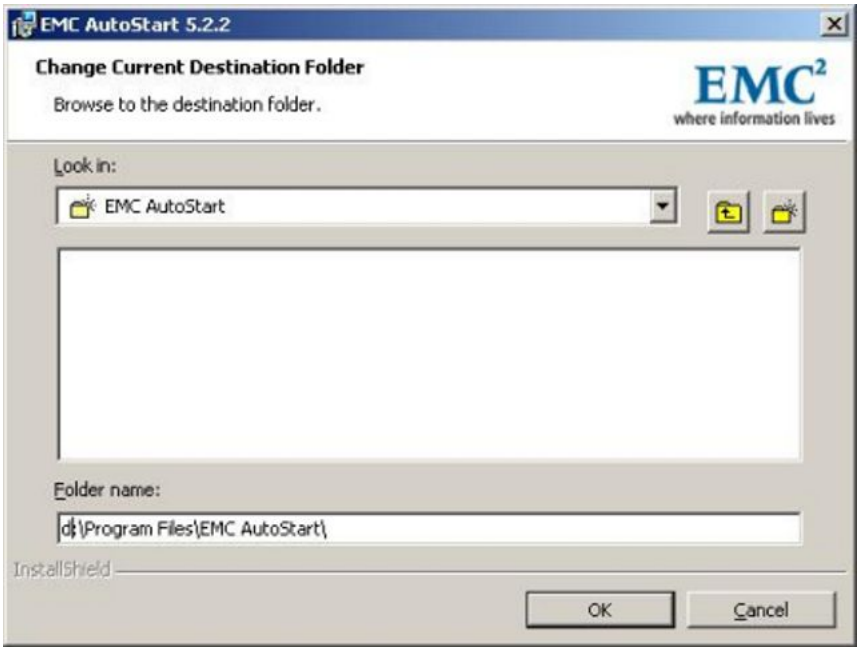


Figure 34: Change Current Destination Folder dialog box

11. In the Folder name field, change the drive letter from C to D, change the path to: D:\Program Files\EMC AutoStart\

Important:

You must install the software in the D:\Program Files\EMC AutoStart\ directory or the software does not work correctly.

12. Click OK.

    Result: The Change Current Destination Folder dialog box closes and you are returned to the Custom Setup window, which shows the correct installation path.

13. Click Next.

    Result: The Agent Connection Information window appears.

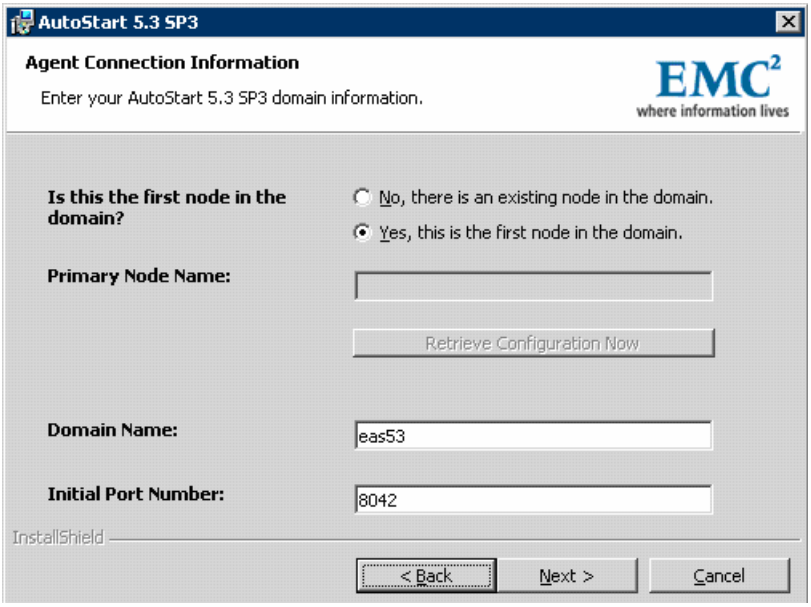


Figure 35: Agent Connection Information window

14. Select the No, there is an existing node in the domain option button.

    Result:The field Primary Node Name is highlighted.

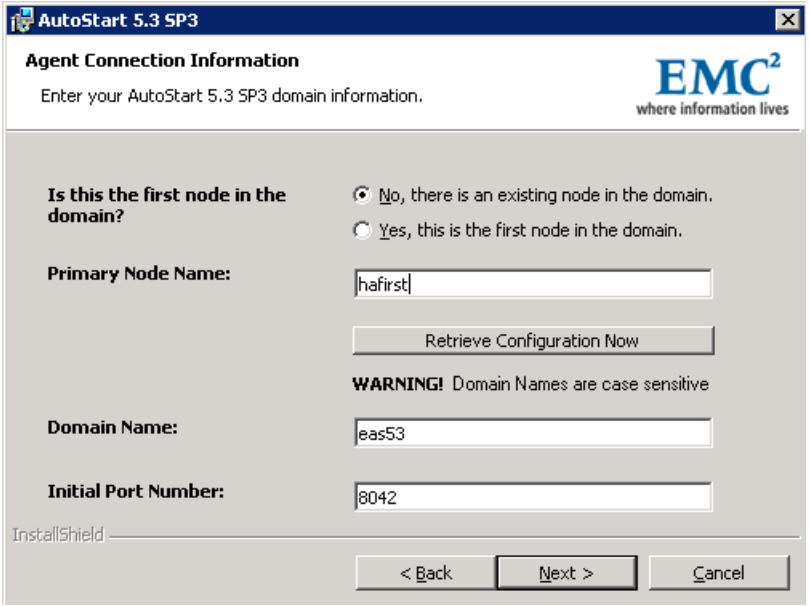


Figure 36: Agent Connection Information window – there is an existing node in the domain

15. Enter the host name of CP1 server in the Primary Node Name field.
16. Enter the EMC AutoStart Domain Name. The AutoStart Domain Name must be the same name that you entered in the High Availability Configuration Wizard.

    Note:

    This document uses [AutoStart_Domain]. This value must be replaced with your AutoStart domain name.

17. Leave the Initial Port Number unchanged.
18. Click Next.

    Result:The Mirroring Network Configuration & Product Licensing window appears. The list of licenses is disabled.

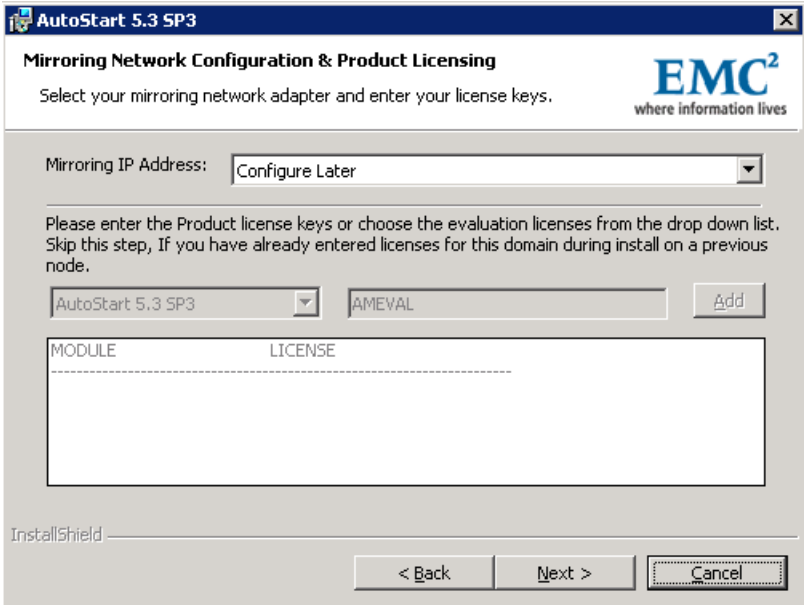


Figure 37: Mirroring Network Configuration and Product Licensing window

Note:

If you enter an invalid Primary Node Name, or the AutoStart Agent is not running on the specified node, an error message is displayed (similar to the following). Check that the Primary Node Name is correct and that the networking is configured so that the name can be resolved on another node. Click OK to return to the Agent Connection Information window.

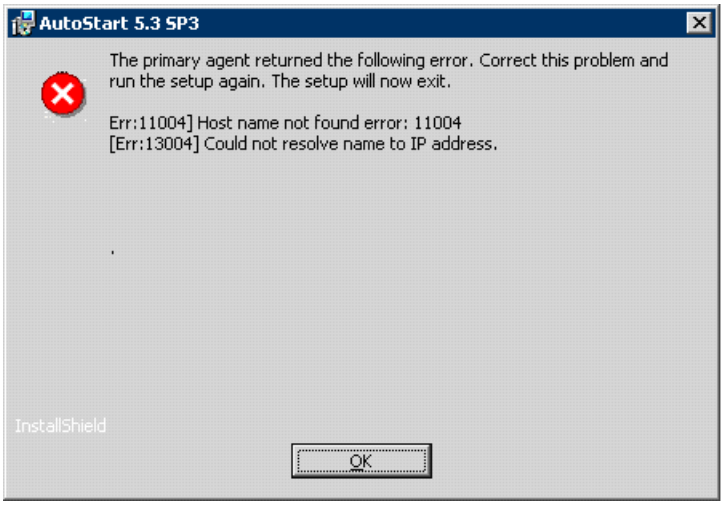


Figure 38: Error: Invalid name or agent not running on Primary node

Note:

: If you forgot to add the administrator account of CP2 server into the AutoStart domain, the following error is displayed. Click OK to return to the Agent Connection Information window. Configure licensing and security on the CP1

server according to the chapter Add the node 2 administrator account to the AutoStart Console on node 1 on page 70.

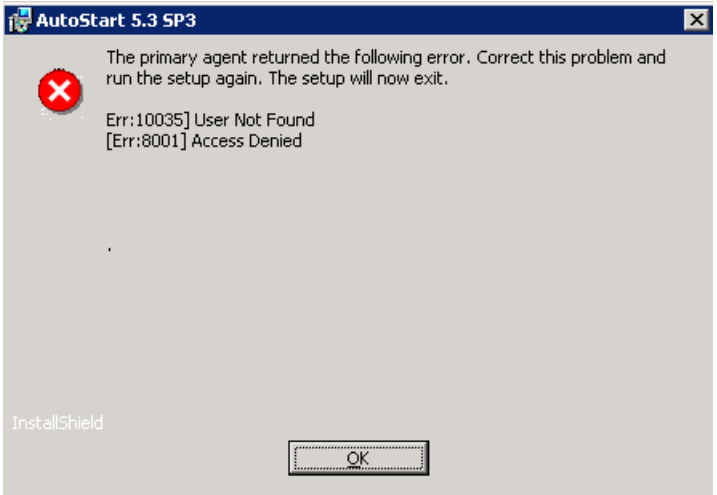


Figure 39: Primary Agent error

19. In the field Mirroring IP Address: select the IP address that was assigned to the Mirror NIC on CP2 server. The default value is Configure Later.
20. Click Next.

    Result: The Confirm Settings window appears.

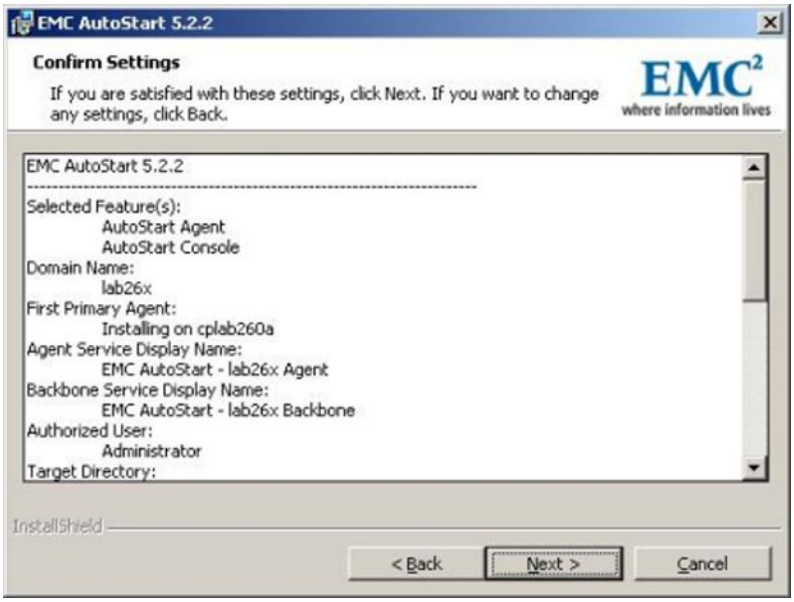


Figure 40: Confirm Settings window

21. Verify that the settings are correct.
22. Click Install to start the installation of the AutoStart Agent and Console software.

Result:The Installing AutoStart 5.3 SP3 window appears and shows the status of the installation.

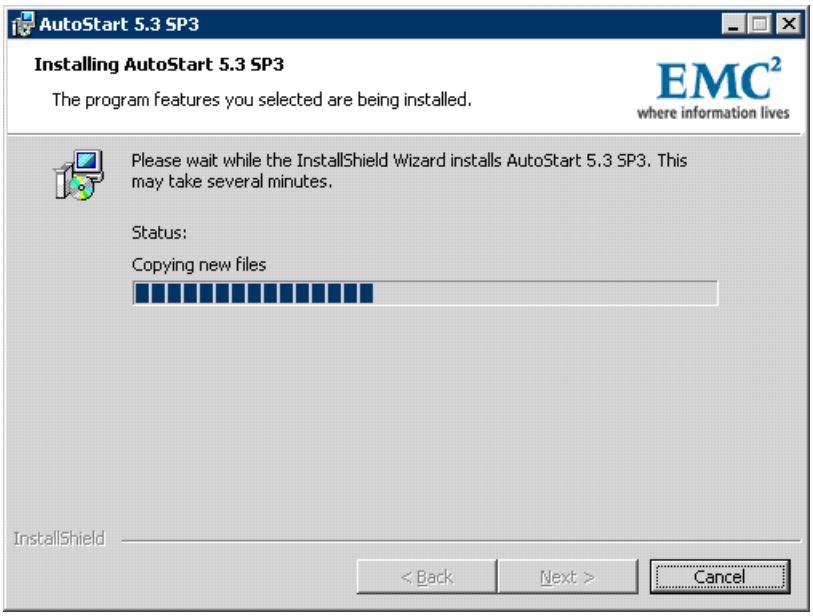


Figure 41: Installing AutoStart 5.3 SP3 window

23. Wait until the installation is complete and the InstallShield Wizard Completed window appears.

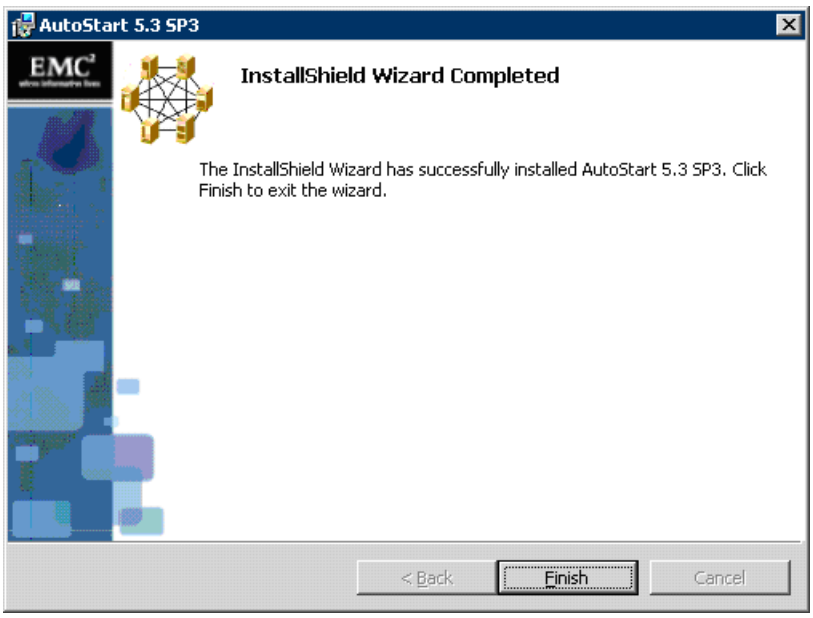


Figure 42: InstallShield Wizard Completed window

24. Click Finish.

    Result: AutoStart 5.3 SP3 Installer Information dialog box appears.

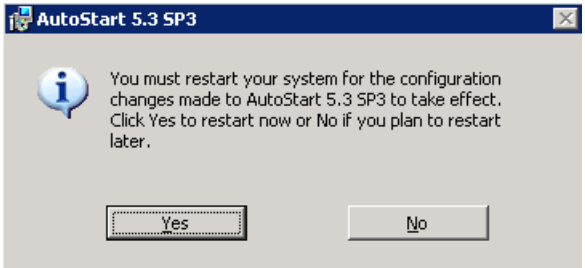


Figure 43: AutoStart 5.3 SP3 dialog box

25. Click No if there are patches to install or click Yes to restart the CP2 server.

    Note:
    If there are patches available for AutoStart 5.3 SP3 software, install the patches and then restart the CP2 server.

26. Delete the folder D:\temp\EMC_AutoStart_5.3_SP3_Update.

Configure the AutoStart software

To configure the AutoStart software, both servers (CP1 and CP2) must be running and have the HB1, HB2, and MIRROR LANs connected so that the two servers can communicate using the LAN connections.

Configure the AutoStart software on CP1

Use the procedures in the following section to configure the AutoStart software on CP1.

Modifying the AutoStart Domain and Verification links

1. Launch the AutoStart Console by selecting Start > Programs > EMC AutoStart > EMC AutoStart Console 5.3 SP3.

   Warning:
   Do not continue the configuration process until CP2 is finished rebooting.

   Warning:
   Wait for both servers under Domains > [AutoStart_Domain] > Nodes to appear green before making any changes in the AutoStart Console. Failure to do so can

result in losing configured information for verification links upon the next reboot.

2. In the Domains pane, select the CP1 node (Domains > [AutoStart_Domain] > Nodes > <CP1 Node Name>).

   a. Select the Failure Detection and Mirroring tab.

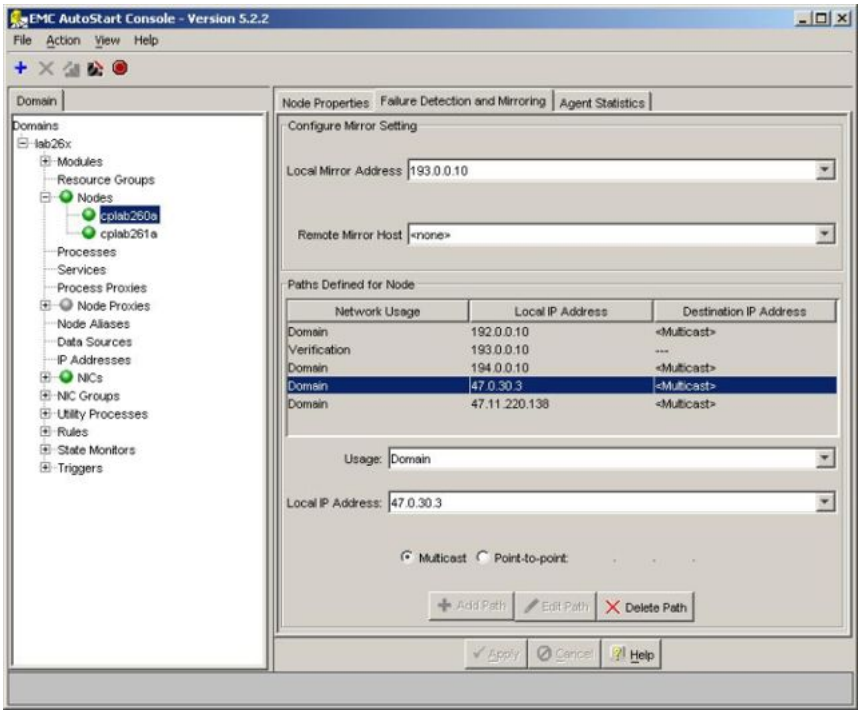


Figure 44: AutoStart Console - Failure Detection and Mirroring tab

   b. In the Paths Defined for Node list, select the entry that has the ELAN IP address for CP1.

   c. Click Delete Path.

   d. In the Usage drop-down list, select Verification.

   e. In the Local IP Address drop-down list, select the ELAN IP address for CP1.

   f. Click Add Path.

   g. In the Paths Defined for Node list, select the entry that has the CLAN IP address for CP1.

   h. Click Delete Path.

   i. In the Usage drop-down list, select Verification.

   j. In the Local IP Address drop-down list, select the CLAN IP address for CP1.

   k. Click Add Path.

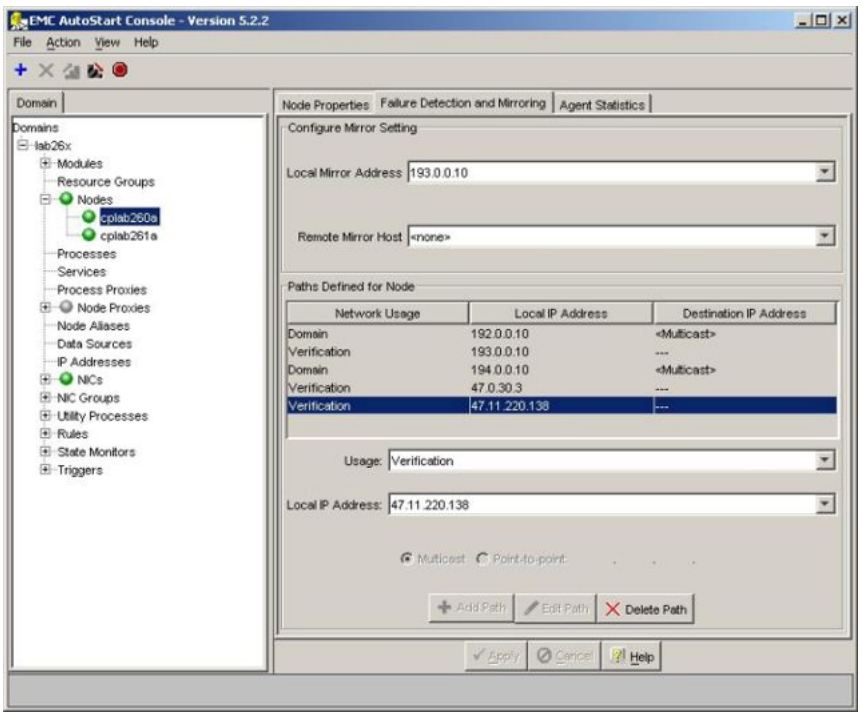


Figure 45: AutoStart Console - Failure Detection and Mirroring tab - Adding path

l. Click Apply.

m. Click Yes, if you are prompted to restart the agent to apply the changes.

Note:

It takes a few minutes for the agent to restart.

3. In the Domains pane, select the CP2 node (Domains > [AutoStart_Domain] > Nodes > <CP2 Node Name>).

   a. Select the Failure Detection and Mirroring tab.

   b. In the Paths Defined for Node list, select the entry that has the ELAN IP address for CP2.

   c. Click Delete Path.

   d. In the Usage drop-down list, select Verification.

   e. In the Local IP Address drop-down list, select the ELAN IP address for CP2.

   f. Click Add Path.

   g. In the Paths Defined for Node list, select the entry that has the CLAN IP address for CP2.

   h. Click Delete Path.

   i. In the Usage drop-down list, select Verification.

j. In the Local IP Address drop-down list, select the CLAN IP address for CP2.

k. Click Add Path.

l. Click Apply.

m. Click Yes, if you are prompted to restart the agent to apply the changes.

Note:

It takes a few minutes for the agent to restart.

4. Wait for the CP1 node and the CP2 node to start.

   The icon for the nodes (in the left-hand pane of the AutoStart console) turn green after the AutoStart Agent starts.

Adding the Remote Mirroring Host for CP2

1. On CP1, and in the Domains pane, select the CP2 node (Domains > [AutoStart_Domain] > Nodes > <CP2 Node Name>).
2. Select the Failure Detection and Mirroring tab.
3. Ensure that the value in the Local Mirror Address field is set to the IP address assigned to the MIRROR NIC on CP2. (The default value is 193.0.0.11.)

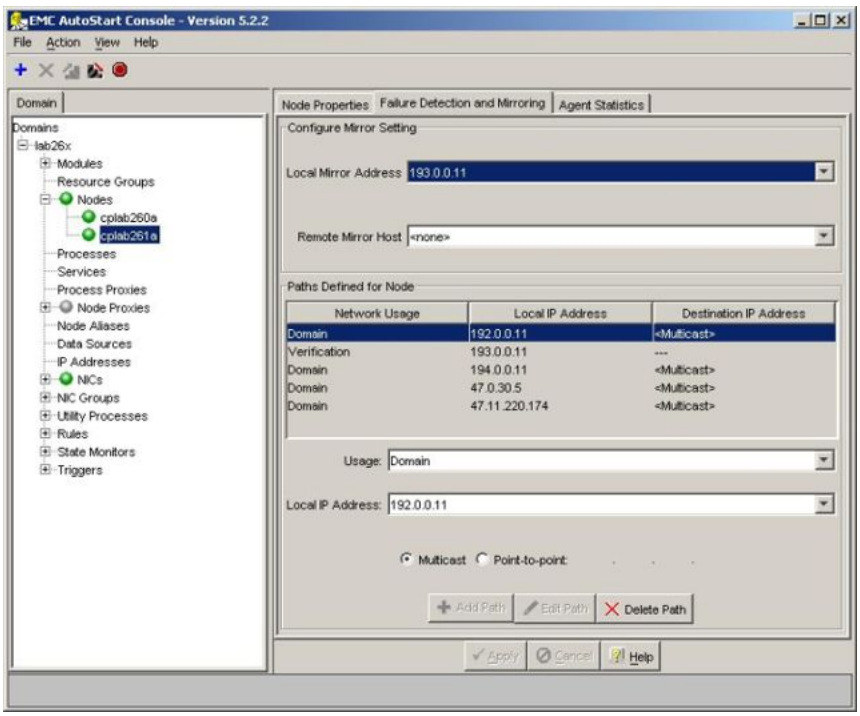


Figure 46: AutoStart Console - Failure Detection and Mirroring tab - Local Mirror Address

4. Change the value in the Remote Mirror Host field to the host name of node CP1.

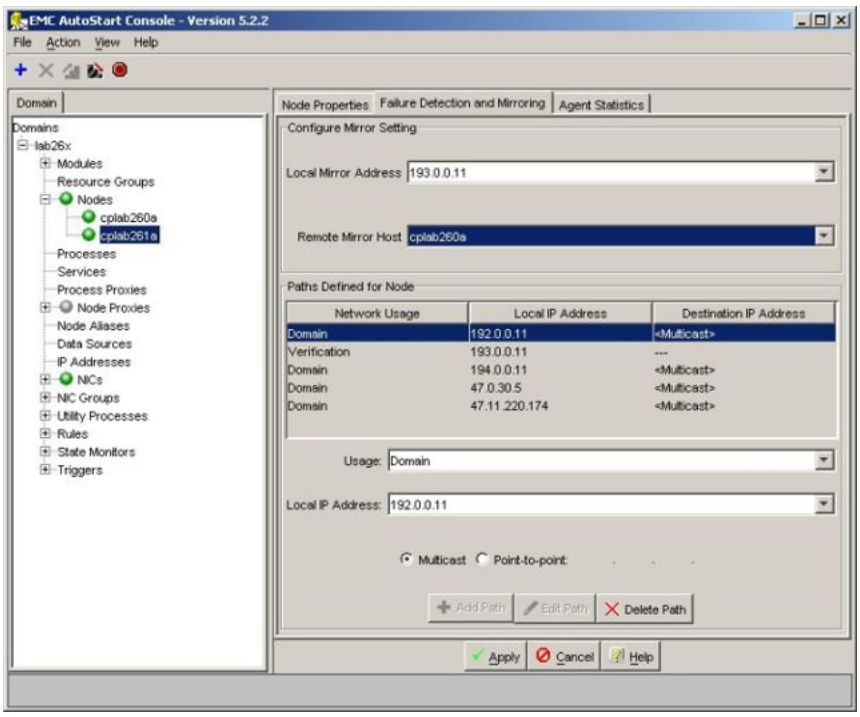


Figure 47: AutoStart Console - Failure Detection and Mirroring tab - Remote Mirror Host

5. Click Apply.
6. Click Yes, if you are prompted to restart the agent to apply the changes.
7. In the Domains pane, select the CP1 node (Domains > [AutoStart_Domain] > Nodes > <CP1 Node Name>).
8. Select the Failure Detection and Mirroring tab.

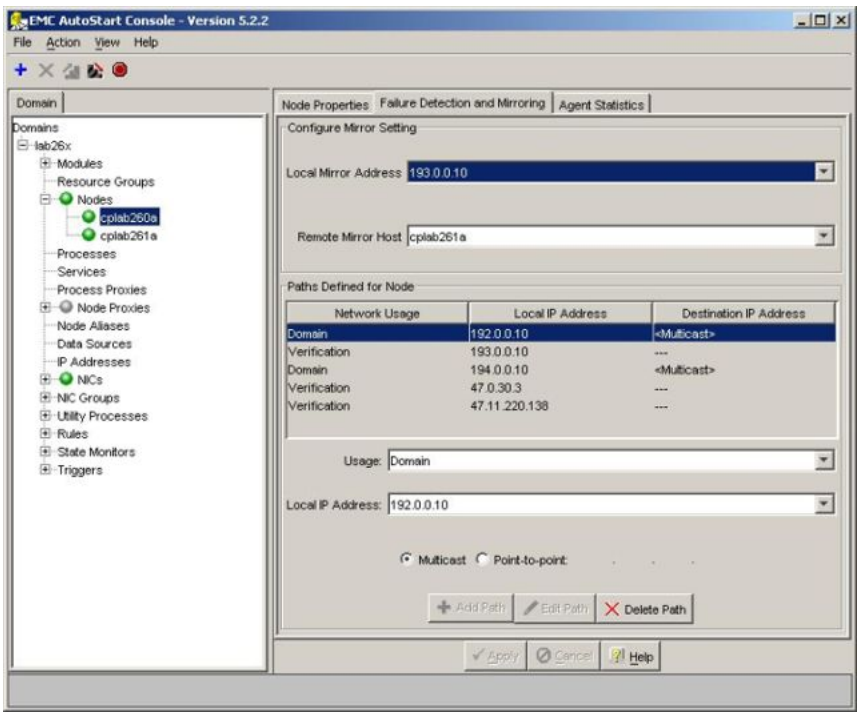


Figure 48: AutoStart Console - Failure Detection and Mirroring tab - Verify Local and Remote Mirrors

9. Verify that the value in the Local Mirror Address field is set to the IP address assigned to the MIRROR NIC on CP1. (The default value is 193.0.0.10.)
10. Verify that the value in the Remote Mirror Host field is set to the host name of node CP2.

Generating the AutoStart Definition File

Generating the AutoStart Definition File is required to set the node-specific settings in the AutoStart Definition Template file.

1. In Windows Explorer, navigate to the D:\Nortel\HA folder.
2. Double-click the HighAvailabilityConfigurationWizard.exe file.

   Result: The High Availability Configuration Wizard appears.

   The information that was previously entered is automatically loaded and the node information validation is automatically rerun.

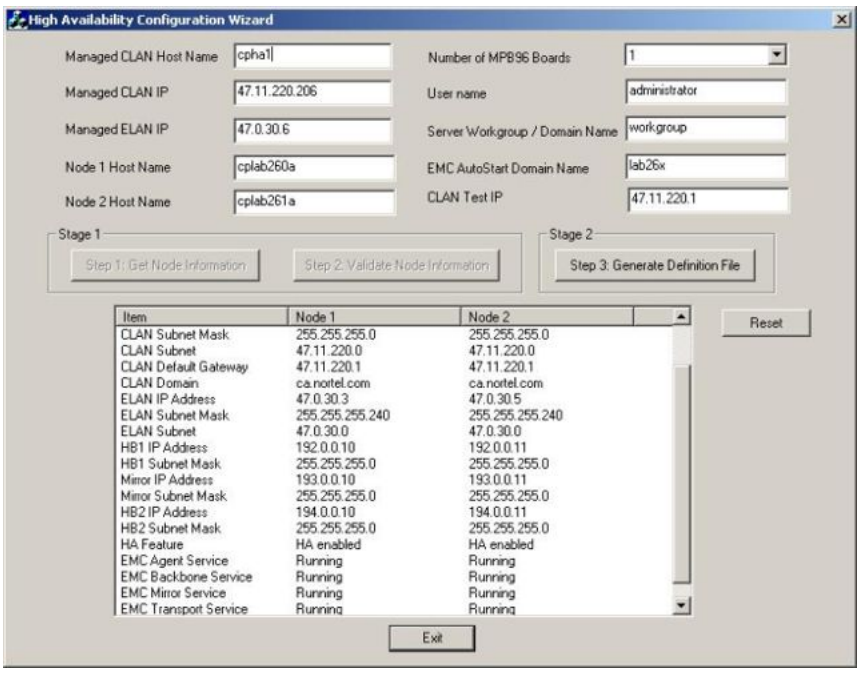


Figure 49: High Availability Configuration Wizard

3. Click the Step 3: Generate Definition File button to validate the AutoStart software configuration and generate the Definition File.

   - If there are any errors, a message box is displayed with the error. Correct the problem and then click the Step 3: Generate Definition File button again.
   - If there are no errors, a message is displayed that the Definition File is successfully generated and that you can exit the High Availability Configuration Wizard.

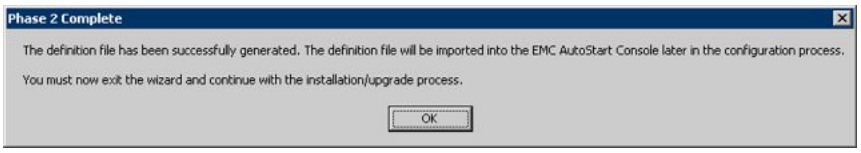


Figure 50: Phase 2 Complete

4. Click OK to return to the High Availability Configuration Wizard.
5. Click Exit and then confirm that you want to exit from the High Availability Configuration Wizard.

Import the AutoStart definition file on CP1

Import the AutoStart definition file (CallPilot-Mirroring.def or CallPilot-Mirroring-Single.def) in the AutoStart Console on CP1 by using the following the procedure. Two AutoStart definition files are available, as follows:

- CallPilot-Mirroring-Single.def (For systems with one MPB96 board.)
- CallPilot-Mirroring.def (For systems with three MPB96 boards.)

Importing the AutoStart definition file

1. Open the AutoStart Console window.
2. Expand Domains.
3. Right-click [AutoStart_Domain]. (This is the domain name created when the AutoStart agent is installed.)
4. Select the Import Domain Information option.

   Result: The Import dialog box appears.
5. In the Import window, select CallPilot-Mirroring.def or CallPilot-Mirroring-Single.def from the D:\Nortel\HA\ToolkitInstaller2.0 folder.

   The AutoStart definition file is named either CallPilot-Mirroring-Single.def (for systems with one MPB96 board) or CallPilot-Mirroring.def (for systems with three MPB96 boards).
6. Click Import.

   The import process takes approximately one minute to complete.

   Warning:
   During the Import process the AutoStart Console does not respond.
7. Verify that the AutoStart definition file was successfully imported by doing the following:

   a. Check the information bar at the bottom of the AutoStart Console window for any error or warning messages.

   b. In the AutoStart Console, expand Data Sources and check that the drvE and drvF data sources were created.

   c. In the AutoStart Console, expand Resource Groups and check that the CallPilot resource group was created.

Add the Windows administrator password for the AutoStart Utility Processes

Important:

If the Windows administrator account names or passwords are different on servers CP1 and CP2, the AutoStart software does not work correctly after it is installed and configured.

You must ensure that the Windows administrator account is the same on both High Availability servers for the AutoStart software to work properly.

The AutoStart software requires that the Windows administrator account be updated for each Utility Process in the AutoStart software.

Use the following procedure to enter the Windows administrator account information for each AutoStart Utility Process on CP1.

Adding the Windows administrator account password for the AutoStart Utility Processes

1. Open the AutoStart Console window.
2. Expand Domains.
3. Expand [AutoStart_Domain]. (This is the domain name created when the AutoStart agent is installed.)
4. Expand Utility Processes.

   Result: The Utility Processes are displayed:

   - DisableAOS
   - KillServices
   - LoadDN
   - LoadTSP
   - UnloadTSP
   - UnloadTSPOnStandbyServer
5. Select the DisableAOS Utility Process.
6. Select the Settings tab and do the following:

   a. In the Login Info section, enter the password for the Windows administrator account in the Password and Confirm fields.

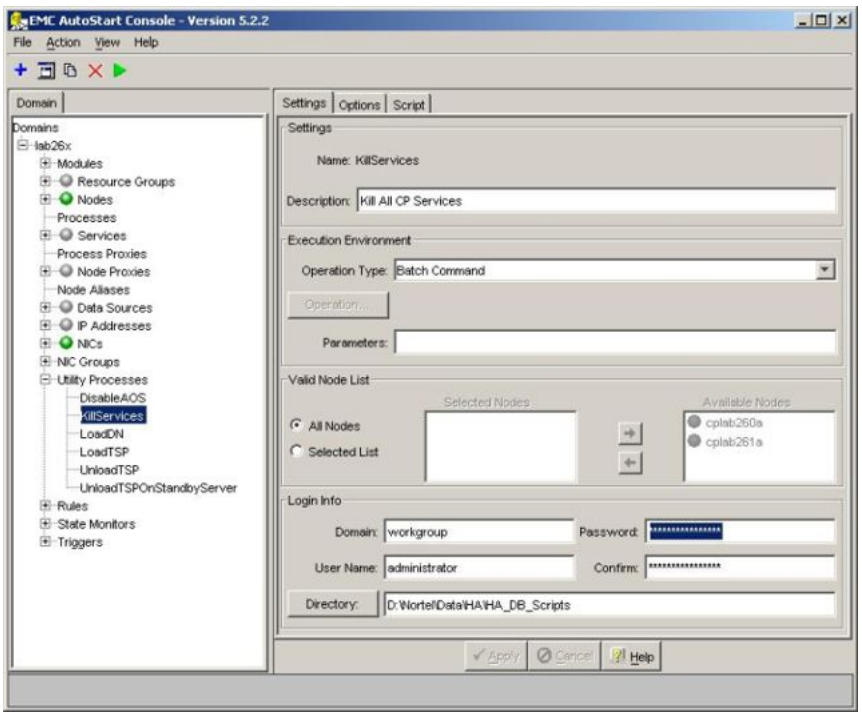


Figure 51: AutoStart Console - Utility Processes

b. Check the Domain, User Name, and Directory fields to ensure they are right.

- Domain must be the Windows domain that the CallPilot servers are on (if applicable) or the Windows workgroup in which the servers are located.
- User name must be the administrator account for selected domain.
- The default directory is D:\Nortel\Data\HA\HA_DB_Scripts.

c. Click Apply.

7. Repeat Step 6 for each of the remaining Utility Processes.

Add e-mail addresses to the Managed_ELAN_IP_Failure_Notif rule

Use the following procedure to add e-mail addresses into the script of the Managed_ELAN_IP_Failure_Notif rule so that the AutoStart software can send out notification e-mail to the administrators when the Path Test failure of the Managed ELAN IP occurs.

Adding e-mail addresses to the Managed_ELAN_IP_Failure_Notif rule

1. Open the AutoStart Console.
2. On the left pane of the AutoStart Console, expand Rules.
3. Select Managed_ELAN_IP_Failure_Notif.

   Result: The Settings tab for the Managed_ELAN_IP_Failure_Notif rule appears.

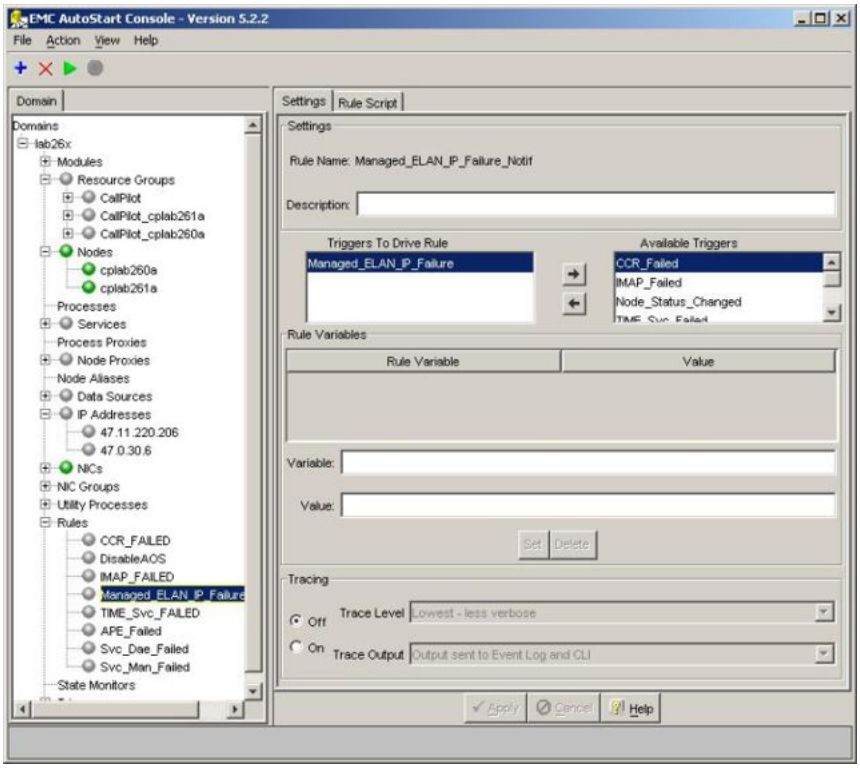


Figure 52: Rules - Managed_ELAN_IP_Failure_Notif

4. Select the Rule Script tab.

   Result: The rule script appears in the right pane of the AutoStart Console.

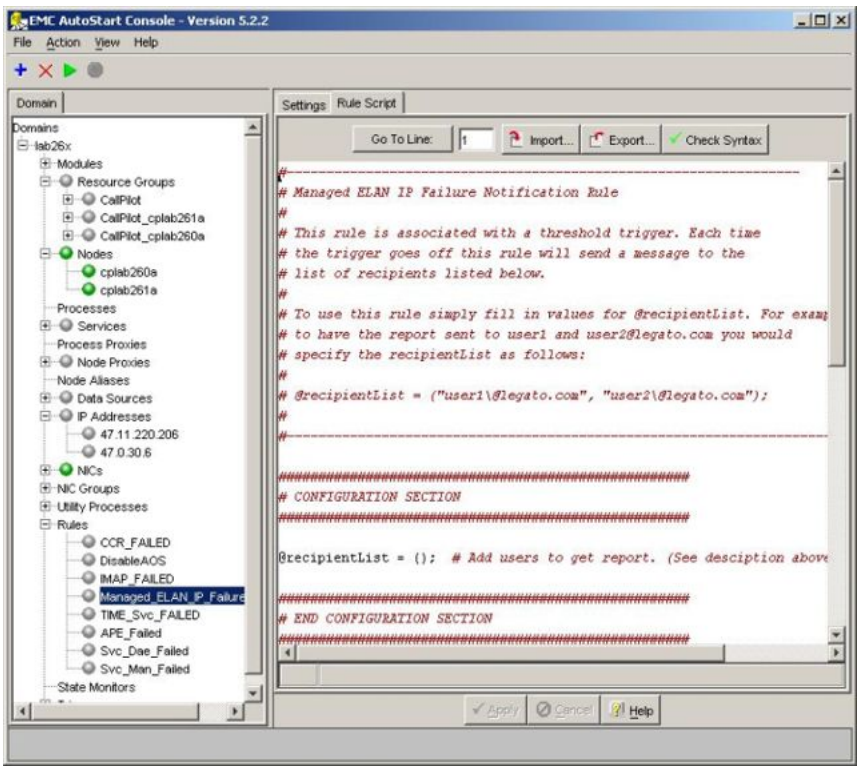


Figure 53: Rule Script tab for Managed_ELAN_IP_Failure_Notif rule

5. Look for the @recipientList = () line in the rule script.
6. Add the recipient's e-mail address in the parenthesis () of the @recipientList line. You must add the backslash symbol (\) before the at symbol (@) in the e-mail address.

   If multiple e-mail addresses are added, separate each e-mail address by a comma (,).
7. Click Apply.
8. Configure the Simple Mail Transfer Protocol (SMTP) server so that the AutoStart software can provide e-mail notification for failovers and resource group state changes. The SMTP server domain must first be configured for recipients to receive notification that a failover or state change has occurred. See Configuring the SMTP Server for a domain on page 154.

Bring the Resource Groups online

This section provides the procedures for bringing the following resource groups online:

- CallPilot Resource Group
- CallPilot_[CP1] and CallPilot_[CP2] Resource Groups

Bring the CallPilot Resource Group online on CP1

Using the AutoStart Console, bring the CallPilot Resource Group online on CP1 to activate the High Availability feature. Bringing the CallPilot Resource Group online does the following:

- Assigns the shared drives to server CP1.
- Assigns the Managed ELAN/CLAN (virtual) IP addresses so that they point to CP1.
- Loads the CallPilot database tables back to the CallPilot database.
- Starts all CallPilot services.

Bringing the CallPilot Resource Group online on CP1

1. In the AutoStart Console window, expand Resource Groups (Domains > [AutoStart_Domain] > Resource Groups).
2. Right-click CallPilot.
3. Select the Bring Online option, and then select <CP1 node name>.

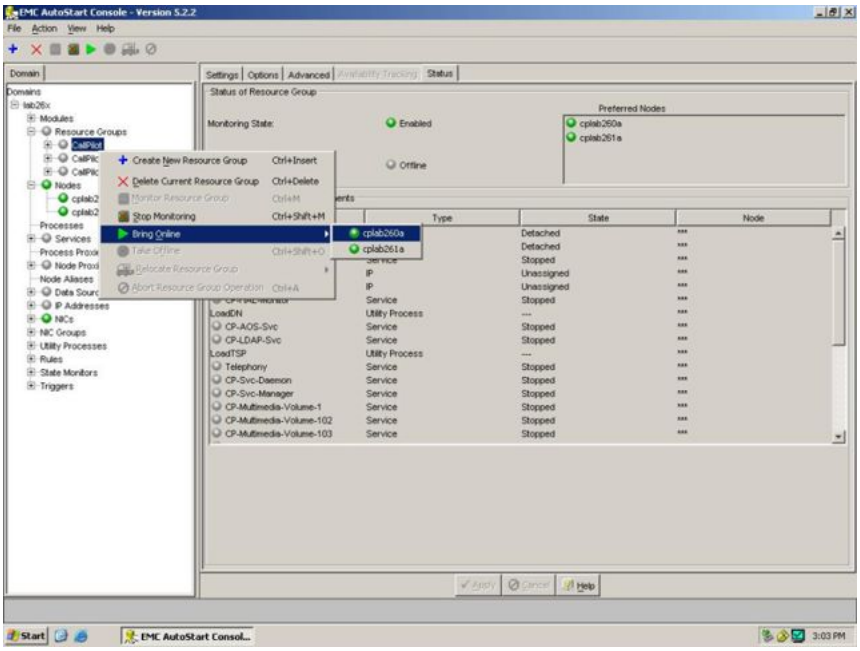


Figure 54: AutoStart Console - Bring Online - CallPilot Resource Group

Result: The following occurs:

- The Group State changes to Online Pending.
- The data sources (drive E and drive F) are automatically attached and initialized. While the data sources are initialized, they are in the warning state and their icons are yellow.

- The CallPilot services start on CP1.

Note:

A message is displayed informing you that a data source is being mirrored and the status of the data source is updated to show the progress of the synchronization. It can take between 30 minutes to 2 hours for the data sources to be mirrored between the two servers.

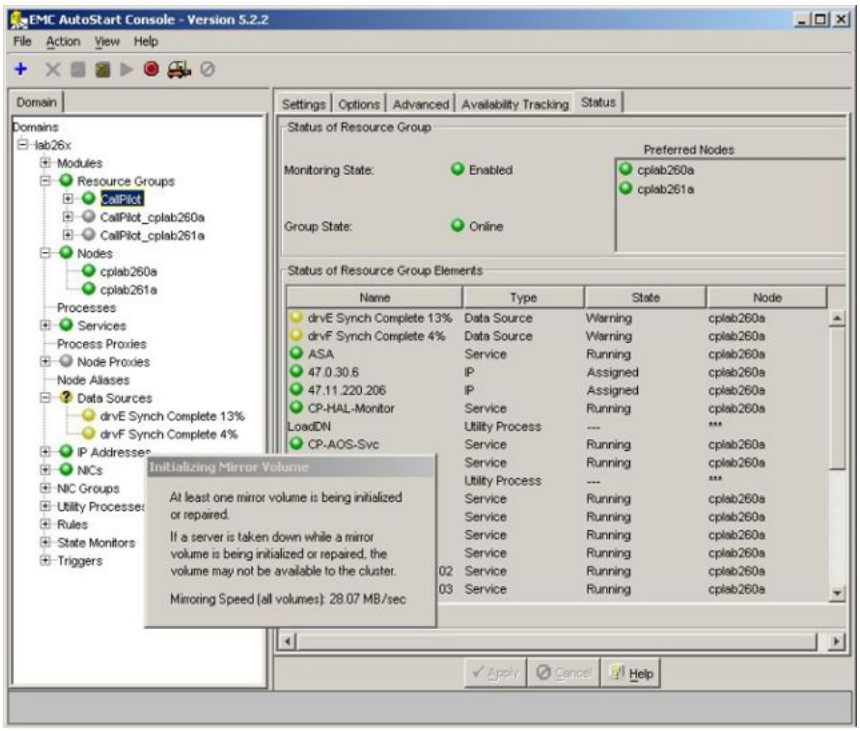


Figure 55: AutoStart Console - Initializing Volume Mirror message

4. Wait while the data sources are mirrored.
5. Verify that the Group State field turns green and shows as Online.

   Result: When the Group State appears green and online, CallPilot is started.

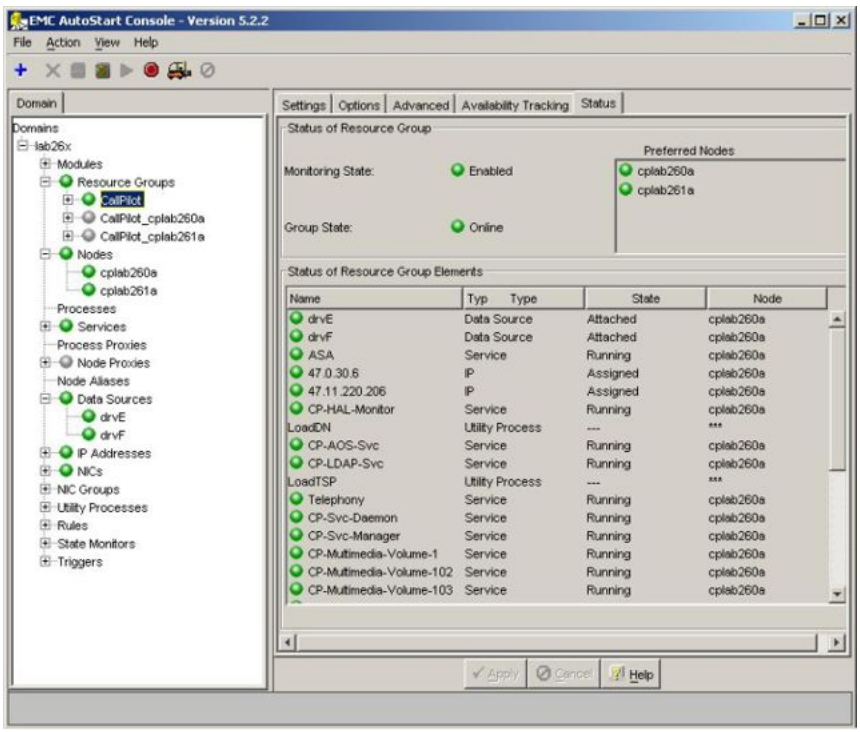


Figure 56: AutoStart Console - Monitoring and Group States

Bring the Resource Groups CallPilot_[CP1] and CallPilot_[CP2] online

Use the following procedure to bring the CallPilot_[CP1] and CallPilot_[CP2] resource groups online.

Bringing the Resource Groups CallPilot_[CP1] and CallPilot_[CP2] online

1. In the AutoStart Console window, expand Resource Groups (Domains > [AutoStart_Domain] > Modules > Resource Groups).
2. Bring CallPilot_[CP1] online (where [CP1] is the name of the CP1 server).
    a. Right-click CallPilot_[CP1].
    b. Select the Bring Online option, and then select <CP1 node name>.

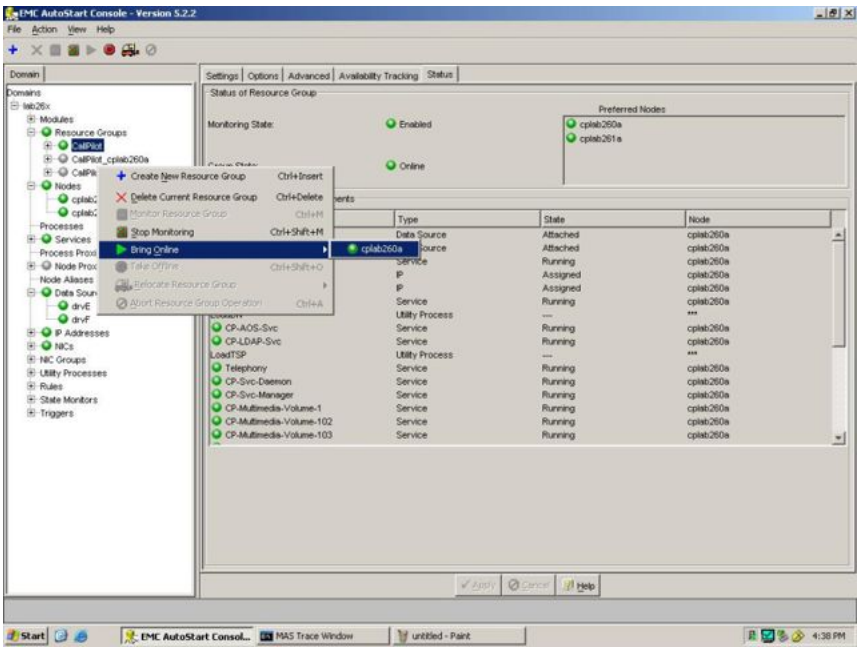


Figure 57: AutoStart Console - Bring Online - CallPilot_[CP1] Resource Group

3. Bring CallPilot_[CP2] online (where [CP2] is the name of the CP2 server).
    a. Right-click CallPilot_[CP2].
    b. Select the Bring Online option, and then select <CP2 node name>.
4. Verify that both Resource Groups are green and show a Group State of Online.

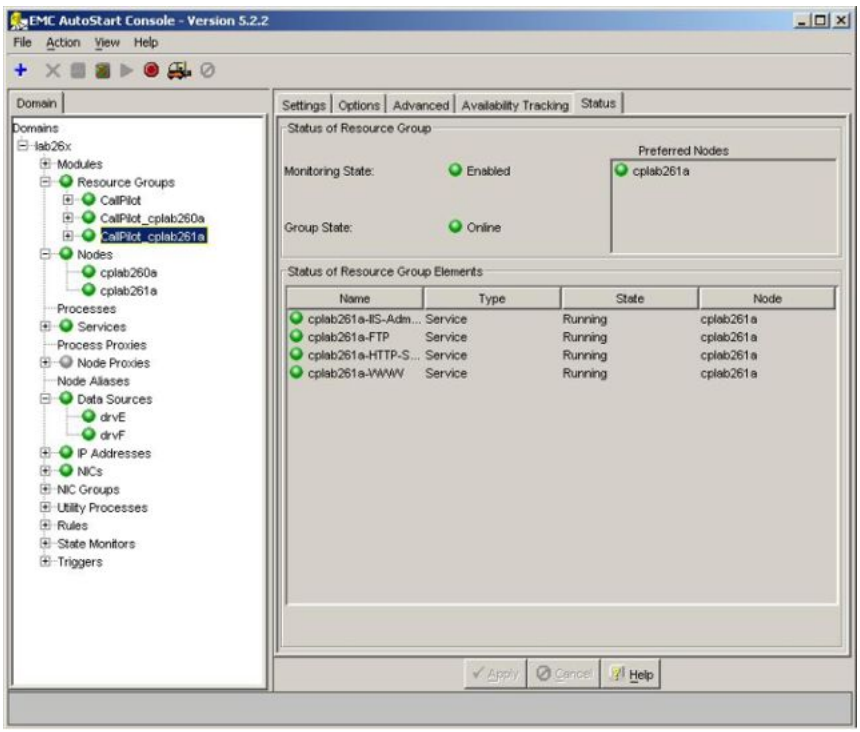


Figure 58: AutoStart Console - Verify status of both CallPilot_[CP1] and CallPilot_[CP2] Resource Groups

Test your configuration

Use the following procedure to test the configuration of CP1 and CP2.

Testing the configuration of CP1 and CP2

1. Verify that server CP1 is running and accepting calls. Test the server CP1 to make sure that all channels and DSP resources are working correctly.
2. Using the AutoStart console, manually cause a failover by relocating the Resource Group CallPilot to server CP2.

   ⚠ Warning:

   Do not attempt to failover from CP1 to CP2 until the mirroring started in Bringing the CallPilot Resource Group online on CP1 on page 93 is complete.

   For more information, see Initiating a manual failover on page 181.
3. Ensure that server CP2 takes over and can accept calls.

4. Move the dongle from server CP1 to server CP2.
5. Test the server CP2 to make sure that all channels and DSP resources are working correctly.

Note:
At this point server CP2 is running as the active server and CP1 is the standby server.

Create the CallPilot Reporter connections

CallPilot Reporter connects to the pair of High Availability servers using the Managed (virtual) host name. After CallPilot Reporter first connects to the pair of servers, the active server returns the Managed host name, rather than the actual host name of the active server. Because the Managed host name is returned (and not the actual host name of the active server), CallPilot Reporter is unaware that it is connected to a pair of High Availability servers.

Any reports generated are based on the Managed host name, independent of which server is currently the active server. Both High Availability servers must first register with the CallPilot Reporter to make the CallPilot Reporter work with the High Availability system.

Note:
If you are not performing a new installation of CallPilot 5.0 High Availability system, a backup of CallPilot Reporter must be performed prior this procedure and the backup must be restored on the Reporter stand-alone PC right after this registration. This note applies only to the following:

- upgrading to CallPilot 5.0 High Availability system
- changing the computer name of the Reporter stand-alone PC
- using a new Reporter stand-alone PC

Important:
To make both High Availability servers register with CallPilot Reporter, perform the following manual procedure the very first time you connect the CallPilot Reporter to a CallPilot 5.0 High Availability system.

For CallPilot Reporter, the failover process is the same as if a server goes down and then comes back into service (even though the active server goes down and the standby server comes into service as the new active server). The CallPilot Reporter recovery mechanism pings the Managed host name and automatically reconnects when the server comes back into service. Because the database is mirrored from the active High Availability to the standby High Availability server, CallPilot Reporter can download any additional Operational Measurements (OM) that are buffered during the failover process.

Use the following the following procedure the first time you bring up the High Availability system and register it to the CallPilot Reporter Server.

Creating the CallPilot Reporter connection

1. Ensure that CallPilot Reporter is online.
2. Connect CallPilot Reporter to the High Availability system using the Managed host name (where CP1 is the active server and CP2 is the standby server).
3. Perform a manual failover. See Initiating a manual failover on page 181.

   Result: The active server (CP1) goes down and the standby server (CP2) comes into service as the new active server.
4. Wait for CP2 to become the active server and ensure that the server is ready to accept calls.
5. In CallPilot Reporter, click Log out and Erase.
6. Log back on to CallPilot Reporter.
7. Ensure that CallPilot Reporter is online.

   Result: CallPilot Reporter creates a record using the Managed host name and places all incoming data from the active High Availability server (it does not matter which High Availability server in the pair) under that record.

Add the servers to a Windows domain

This following procedure is optional. It is only required if the CallPilot servers will be members of a Windows domain. Avaya recommends using the Windows default workgroup to first configure the High Availability system, and then join the customer domain after the High Availability system is working (if the system has to join the domain). If the CallPilot 5.0 High Availability system is installed and configured under a workgroup, use the following procedure to join a domain.

Note:

Adding the CallPilot 5.0 High Availability system into a domain makes the system dependent on the domain controller, the DNS server, and the CLAN connection. If the system lost the connection to the domain controller after joining a domain (which can be caused by losing the CLAN connection), then the CallPilot 5.0 High Availability system cannot properly perform failovers because of domain user validation failure. (The domain user information is needed for the AutoStart Utilities to run after joining a domain.) However, for a CallPilot 5.0 High Availability system in a workgroup, the loss of the CLAN connection has no impact to the failover performance. Avaya does not recommend that you add your CallPilot 5.0 High Availability system into a domain unless it must be part of the domain.

Joining a Windows domain

This procedure assumes that CP1 is the active server and CP2 is the standby server.

1. Log on to CP1.
2. Launch the AutoStart Console on CP1 by selecting Start > Programs > EMC AutoStart > EMC AutoStart Console 5.3 SP3.

   Result: The AutoStart Console appears.
3. Select the [AutoStart_Domain].
4. Select the Licensing/Security tab.
5. In the Valid User List area, enter the following information:
   a. In the User Name field, enter administrator.
   b. In the Domain/Node field, enter the Windows domain name that the CallPilot system will be joining.
   c. For the Access Rights option, select the Administrator option button.
   d. In the Description field, enter Windows domain.
6. Click Add.

   Result: A row is added to the Valid User List.
7. On CP1, stop monitoring. See Disabling automatic failovers (stop monitoring) on page 180.
8. Take the CallPilot resource group offline on CP1. See Taking the CallPilot resource group offline on page 177.
9. On CP1, do the following:
   a. Right-click My Computer.

      Result: The System Properties window appears.
   b. Select the Computer Name tab and click Change.

      Result: The Computer Name Changes window appears.

Figure 59: Computer Name Changes

c. In the Member of section, select the Domain option.

d. Enter the name of the domain and click OK.

   Result: The Domain Administrator Privileges window appears.

e. Enter the domain administrator and password.

   Contact your network administrator for this information.

   Result: The Welcome to Domain window appears.

f. Click OK.

   Result: A warning window appears prompting you to restart the computer in order for changes to take effect.

g. Click OK.

   Result: The System Properties window appears.

h. Click OK.

   Result: The System Settings Changes window appears prompting you to restart the computer.

i. Click Yes to restart CP1.

j. Log on to CP1 using the domain user account which is a member of the Domain Administrators group.

10. On CP2, do the following:
    a. Right-click My Computer.

       Result: The System Properties window appears.
    b. Select the Computer Name tab and click Change.

       Result: The Computer Name Changes window appears.
    c. In the Member of section, select the Domain option.
    d. Enter the name of the domain and click OK.

       Result: The Domain Administrator Privileges window appears.
    e. Enter the domain administrator and password.

       Contact your network administrator for this information.

       Result: The Welcome to Domain window appears.
    f. Click OK.

       Result: A warning window appears prompting you to restart the computer in order for changes to take effect.
    g. Click OK.

       Result: The System Properties window appears.
    h. Click OK.

       Result: The System Settings Changes window appears prompting you to restart the computer.
    i. Click Yes to restart CP2.
    j. Log on to CP2 using the domain user account which is a member of the Domain Administrators group.
11. On CP1, launch the AutoStart Console window.
12. Expand Domains.
13. Expand [AutoStart_Domain]. (This is the domain name created when the AutoStart agent was installed.)
14. Expand Utility Processes.

    Result: The Utility Processes are displayed:

    - DisableAOS
    - KillServices
    - LoadDN
    - LoadTSP
    - UnloadTSP
    - UnloadTSPOnStandbyServer

15. Select the DisableAOS Utility Process.
16. Select the Settings tab and to the following:
    a. Update the Domain, User Name, and Directory fields.
        - Domain must be the Windows domain that the CallPilot servers are on (if applicable) or the Windows workgroup in which the servers are located.
        - User name must be the domain administrator account for selected domain.
        - The default directory is D:\Nortel\Data\HA\HA_DB_Scripts.
    b. In the Login Info section, enter the password for the Windows administrator account in the Password and Confirm fields.

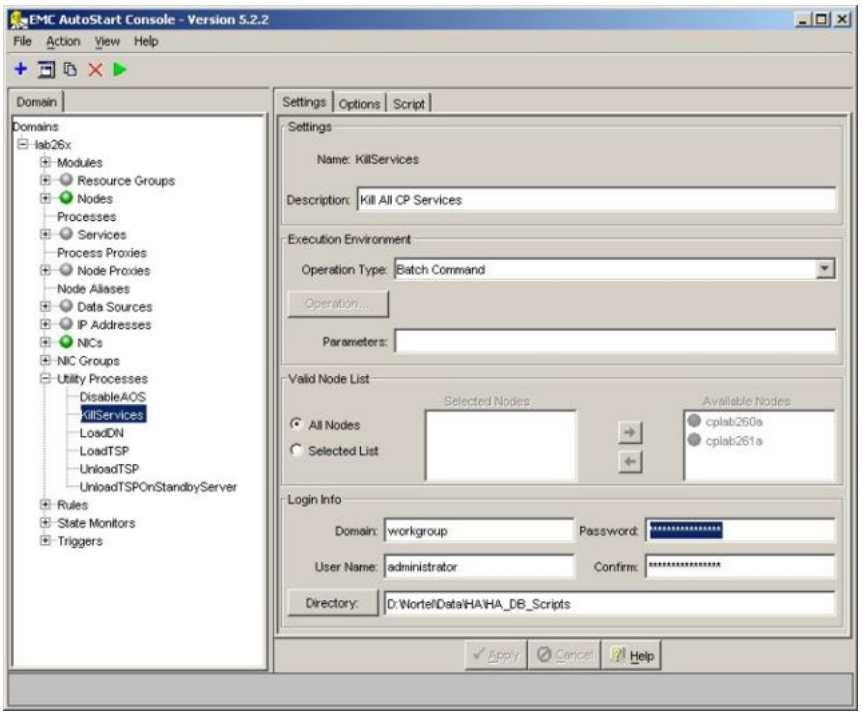


Figure 60: AutoStart Console - Utility Processes

    c. Click Apply.
17. Repeat Step 16 for each of the remaining Utility Processes.
18. On CP1, enable monitoring. See Enabling automatic failovers (start monitoring) on page 180.
19. Bring the CallPilot resource group online on CP1. See Bringing the CallPilot resource group online on page 176.

Chapter 6: Maintaining a High Availability system

In this chapter

Avaya CallPilot® Configuration Wizard on page 106

Working with domains and workgroups on page 147

EMC AutoStart Agent and Console on page 153

Support on page 195

RAID splitting for HA systems on page 226

CallPilot Manager, Channel Monitor on page 231

This chapter outlines the procedures used to maintain a High Availability system.

Note:

It is good practice and highly recommended to split RAID on both nodes prior to performing any maintenance activities on a High Availability system.

Note:

The screen shots displayed in this chapter are from a 1005r server. The various screens will look slightly different if you are maintaining a High Availability system on a pair of 1006r servers.

Note:

If drives E and drive F are both in a warning state, and a message appears in the application log indicating that the local drive is `DEGRADED`, perform the following actions for each drive:

1. In the AutoStart Console, select **Domains** > **[AutoStart_Domain]** > **Data Sources**.
2. Right-click the drive.
3. Select **Restart Mirror** and click **Yes** to continue.
4. Wait until mirroring is completed for the drive.

Avaya CallPilot® Configuration Wizard

The EMC AutoStart software stores some information (including host names and IP addresses) from both servers in a High Availability pair to provide the data mirroring and failover mechanisms. As a result, when changing the configuration of a server using the Configuration Wizard, additional steps are required to ensure that the pair of servers continues to function correctly. Use the following procedure for rerunning the Configuration Wizard after the system is configured.

Change the Server Information

The Server Information page of the Configuration Wizard can be used to change the computer name, time zone, dialing information, LDAP search base and the administrator account password

- To change the time zone, dialing information, or LDAP search base, see Changing the Server Information on page 106.
- To change a computer name, see Figure 59: Computer Name Changes on page 101.
- To change the administrator account password, see Administrator account changes on page 111.

Changing the Server Information

Use this procedure to change the time zone, dialing information, and LDAP search base.

1. On CP1 (the active High Availability server) do the following:
   a. Ensure the dongle is plugged into CP1. If the dongle is not on CP1, move it to CP1 and wait for three minutes.

      For more information about the dongle, see 1005r Server Hardware Installation (NN44200-308) or 1006r Server Hardware Installation (NN44200-320).
   b. Launch the AutoStart Console.
   c. Stop monitoring on the Avaya CallPilot resource group. For more information, see Disabling automatic failovers (stop monitoring) on page 180.
   d. Stop Rules on the CallPilot resource group. In the left pane of the AutoStart Console, expand **Rules**, right click **APE_Failed**, and click **Disable Rule** if the rule is enabled (in green). The Confirm Disable of Rule window appears.

e. Click **Yes** to confirm disabling of the rule. Right-click the **CCR_FAILED** rule and then click **Disable Rule** if the rule is enabled (in green). The **APE_Failed** and **CCR_FAILED** rules are disabled.

f. Log on to CallPilot Manager on CP1 and start the Configuration Wizard.

g. Select the CallPilot Individual Feature Configuration (Express Mode) option and then click Next.

   Result: The Configuration Wizard: Express Configuration List screen appears.

h. Select the Server Information check box.

   Result: The Server Information window appears.

i. If necessary, change the Time Zone, Dialing Information, or LDAP Search Base.

   Note:
   Do not change the computer name using this procedure, see Computer name changes on page 109.

j. Click Next.

   Result: The Password Information window appears.

k. Select the Leave password unchanged option.

   Note:
   Do not the change the password using this procedure, see Administrator account changes on page 111.

l. Click Next.

m. Click Finish to complete the Configuration Wizard.

n. Perform a manual failover. For more information, see Initiating a manual failover on page 181.

   Result: The CallPilot resource group is automatically brought online on the standby High Availability server (CP2).

o. After the CallPilot resource group is online on CP2, restart CP1.

2. Move the dongle to CP2.

   For more information about the dongle, see 1005r Server Hardware Installation (NN44200-308) or 1006r Server Hardware Installation (NN44200-320).

3. On CP2, do the following:

   a. Launch the AutoStart Console.

   b. Wait until node CP1 and both drive E and drive F are online and show green in the AutoStart Console.

c. If required, disable monitoring for the CallPilot resource group. For more information, see Disabling automatic failovers (stop monitoring) on page 180.

d. Stop Rules on the CallPilot resource group. In the left pane of the AutoStart Console, expand **Rules**, right click **APE_Failed**, and then click **Disable Rule** if the rule is enabled (in green). The **Confirm Disable of Rule** window displays.

e. Click **Yes** to confirm the disabling of the rule.

f. Right-click the **CCR_FAILED** rule and then click **Disable Rule** if the rule is enabled (in green). The **APE_Failed** and **CCR_FAILED** rules are disabled.

g. Log on to CallPilot Manager on CP2 and start the Configuration Wizard.

h. Select the CallPilot Individual Feature Configuration (Express Mode) option and then click Next.

   Result: The Configuration Wizard: Express Configuration List screen appears.

i. Select the Server Information check box.

   Result: The Server Information window appears.

j. If necessary, change the Time Zone, Dialing Information, or LDAP Search Base.

   Note:
   Do not change the computer name using this procedure, see Computer name changes on page 109.

k. Click Next.

   Result: The Password Information window appears.

l. Select the Leave password unchanged option.

   Note:
   Do not change the password using this procedure, see Administrator account changes on page 111.

m. Click Next.

n. Click Finish to complete the Configuration Wizard.

o. Perform a manual failover. For more information, see Initiating a manual failover on page 181.

   Result: The CallPilot resource group is automatically brought online on the standby High Availability server (CP1).

p. After the CallPilot resource group is online on CP1, restart CP2.

4. On CP1, do the following:

a. Launch the AutoStart Console.

b. Wait until node CP2 and both drvE and drvF are online/green in the AutoStart Console.

c. Enable monitoring for the CallPilot resource group. For more information, see Enabling automatic failovers (start monitoring) on page 180.

Computer name changes

After the AutoStart software is installed, it is possible to change the name of either of the servers in a High Availability pair. However, to do so you must uninstall and reinstall the AutoStart software after making the change. Use the procedures in this section to change the computer name of the following types of servers:

- Servers in a workgroup (For more information, see Changing the name of a server in a workgroup on page 109.)
- Servers in a Windows domain (For more information, see Changing the name of a server in a Windows domain on page 110.)

Changing the name of a server in a workgroup

Use the following procedure to change the computer name of a High Availability server that is in a workgroup.

1. Disable the AutoStart Monitoring. For more information, see Disabling automatic failovers (stop monitoring) on page 180.
2. Take the CallPilot resource group offline. For more information, see Taking the CallPilot resource group offline on page 177.
3. Uninstall the AutoStart Agent and AutoStart Console, including their patches on both nodes. For more information, see Uninstall the AutoStart software on page 192.
4. Change the computer name. For more information, see Manually changing the server name on page 39.

   Important:

   The computer name must contain only alphanumeric characters. Nonalphanumeric characters (such as a hyphen [-]) are not supported.

5. Restart both nodes.
6. Reinstall AutoStart Agent and Console and configure the High Availability system by performing all the tasks and procedures:
   - from Running Stage 1 of the High Availability Configuration Wizard to check CP1 and CP2 configuration on page 58
   - to Test your configuration on page 97

Note:

You do not have to perform all the steps in the testing procedure. Stop after you have performed the manual failover.

Changing the name of a server in a Windows domain

Use the following procedure to change the computer name of a High Availability server that is in a Windows domain.

1. From the AutoStart Console, stop monitoring. For more information, see Disabling automatic failovers (stop monitoring) on page 180.
2. Take the AutoStart resource group offline. For more information, see Taking the CallPilot resource group offline on page 177.

   Note:

   This takes the CallPilot Server out of service.
3. Remove the server from the Windows domain.
4. Set the server back to WORKGROUP using a domain account that has permissions to do so.
5. Restart the server.
6. After the server restarts, log on as an administrator.
7. Change the server name. For more information, see Manually changing the server name on page 39.
8. Restart the server.
9. After the server restarts, log on as an administrator.
10. Rejoin the domain.
11. Restart the server.
12. After the server restarts, log on using the CallPilot High Availability server domain account.
13. Uninstall, reinstall, and reconfigure the AutoStart software. For more information, see the following:
    - Uninstall the AutoStart software on page 192
    - Reinstall the AutoStart software on page 195
    - Configure the AutoStart software on page 81
14. Bring the Resource group online. For more information, see Bringing the CallPilot resource group online on page 176.
15. Reenable the AutoStart monitoring after all CallPilot services are up. For more information, see Enabling automatic failovers (start monitoring) on page 180.

Administrator account changes

Use the following procedure to change the administrator password of a High Availability system using the Configuration Wizard.

Changing the administrator password of High Availability system using the Configuration Wizard

1. If the High Availability system is currently on a workgroup, proceed to the next step. Otherwise, move the CallPilot 5.0 High Availability pair from the domain to a workgroup. For more information, see Joining a workgroup on page 147.
2. On CP1 (the active High Availability server) do the following:
   a. Ensure the dongle is plugged into CP1. If the dongle is not on CP1, move it to CP1 and wait for 3 minutes.

      For more information about the dongle, see 1005r Server Hardware Installation (NN44200-308) or 1006r Server Hardware Installation (NN44200-320).
   b. Launch the AutoStart Console.
   c. Stop monitoring on the CallPilot resource group. For more information, see Disabling automatic failovers (stop monitoring) on page 180.
   d. Log on to CallPilot Manager on CP1 and start the Configuration Wizard.
   e. Select the CallPilot Individual Feature Configuration (Express Mode) option and then click Next.

      Result: The Configuration Wizard: Express Configuration List screen appears.
   f. Select the Server Information check box.

      Result: The Server Information window appears.
   g. Click Next.

      Result: The Password Information window appears.
   h. Select the Change the password option.

      Result: When this option is selected, three additional password options appear.
   i. Enter the Current password.
   j. Enter the New password.
   k. Reenter the new password in the Confirm the password field.
   l. Click Next.

Result: A warning message appears informing you to change the password on the other High Availability server (CP2) and to also change the administrator password for the AutoStart Utility Processes.

m. Click OK to dismiss the warning message.

n. Click Finish to complete the Configuration Wizard.

o. Perform a manual failover. For more information, see Initiating a manual failover on page 181.

Result: The CallPilot resource group is automatically brought online on the standby High Availability server (CP2).

p. After the CallPilot resource group is online on CP2, restart CP1.

3. Move the dongle to CP2.

For more information about the dongle, see 1005r Server Hardware Installation (NN44200-308) or 1006r Server Hardware Installation (NN44200-320).

4. On CP2, do the following:

a. Launch the AutoStart Console.

b. Wait until node CP1 and both drvE and drvF are green/online in the AutoStart Console.

c. If required, disable monitoring for the CallPilot resource group. For more information, see Disabling automatic failovers (stop monitoring) on page 180.

d. Log on to CallPilot Manager on CP2 and start the Configuration Wizard.

e. Select the CallPilot Individual Feature Configuration (Express Mode) option and then click Next.

Result: The Configuration Wizard: Express Configuration List screen appears.

f. Select the Server Information check box.

Result: The Server Information window appears.

g. Click Next.

Result: The Password Information window appears.

h. Select the Change the password option.

Result: When this option is selected, three additional password options appear.

i. Enter the Current password.

j. Enter the New password.

k. Reenter the new password in the Confirm the password field.

l. Click Next.

Result: A warning message appears informing you to change the password on the other High Availability server (CP1 - which you have

already completed) and to also change the administrator password for the AutoStart Utility Processes.

m. Click OK to dismiss the warning message.

n. Click Finish to complete the Configuration Wizard.

o. Change the administrator password for each of the Utility Processes. For more information, see Changing the Utility Processes administrator password on page 132.

p. Perform a manual failover. For more information, see Initiating a manual failover on page 181.

Result: The CallPilot resource group is automatically brought online on the standby High Availability server (CP1).

q. After the CallPilot resource group is online on CP1, restart CP2.

5. On CP1, do the following:

a. Launch the AutoStart Console.

b. Wait until node CP2 and both drvE and drvF are online/green in the AutoStart Console.

c. Enable monitoring for the CallPilot resource group. For more information, see Enabling automatic failovers (start monitoring) on page 180.

Change the Media Allocation

Use the following procedure to modify the MPB96 board or DSP resource settings.

Changing the Media Allocation

1. On CP1 (the active High Availability server) do the following:

a. Ensure the dongle is plugged into CP1. If the dongle is not on CP1, move it to CP1 and wait for 3 minutes.

For more information about the dongle, see 1005r Server Hardware Installation (NN44200-308) or 1006r Server Hardware Installation (NN44200-320).

b. Launch the AutoStart Console.

c. Stop monitoring on the CallPilot resource group. For more information, see Disabling automatic failovers (stop monitoring) on page 180.

d. Log on to CallPilot Manager on CP1 and start the Configuration Wizard.

e. Select the CallPilot Individual Feature Configuration (Express Mode) option and then click Next.

Result: The Configuration Wizard: Express Configuration List screen appears.

f. Select the Media Allocation check box.

   Result: The Media Allocation window appears.

g. Select the MPB96 board to be modified.

h. Change the DSP resources as required.

i. Click Next.

j. Click Finish to complete the Configuration Wizard.

k. Perform a manual failover. For more information, see Initiating a manual failover on page 181.

   Result: The CallPilot resource group is automatically brought online on the standby High Availability server (CP2).

l. After the CallPilot resource group is online on CP2, restart CP1.

2. Move the dongle to CP2.

   For more information about the dongle, see 1005r Server Hardware Installation (NN44200-308) or 1006r Server Hardware Installation (NN44200-320).

3. On CP2, do the following:

   a. Launch the AutoStart Console.

   b. Wait until node CP1 and both drvE and drvF are green/online in the AutoStart Console.

   c. If required, disable monitoring for the CallPilot resource group. For more information, see Disabling automatic failovers (stop monitoring) on page 180.

   d. Log on to CallPilot Manager on CP2 and start the Configuration Wizard.

   e. Select the CallPilot Individual Feature Configuration (Express Mode) option and then click Next.

      Result: The Configuration Wizard: Express Configuration List screen appears.

   f. Select the Media Allocation check box.

      Result: The Media Allocation window appears.

   g. Select the MPB96 board to be modified.

   h. Change the DSP resources as required.

   i. Click Next.

   j. Click Finish to complete the Configuration Wizard.

   k. Perform a manual failover. For more information, see Initiating a manual failover on page 181.

Result: The CallPilot resource group is automatically brought online on the standby High Availability server (CP1).

l. After the CallPilot resource group is online on CP1, restart CP2.

4. On CP1, do the following:

   a. Launch the AutoStart Console.

   b. Wait until node CP2 and both drvE and drvF are online/green in the AutoStart Console.

   c. Enable monitoring for the CallPilot resource group. For more information, see Enabling automatic failovers (start monitoring) on page 180.

Change the Switch Configuration

Use the following procedure to change the switch configuration on a working CallPilot 5.0 High Availability system. This procedure can be used to change the following in the Switch Configuration:

- Changing the Switch Information (switch type, customer number, and switch IP address)

  Important:

  If you are changing the switch IP Address, you must first change the switch IP address in the AutoStart Console. For more information, see Change the Switch IP address in AutoStart Console on page 172. Then use the following procedure to complete the change of the switch IP Address.

- Changing the TNs
- Changing the CDNs

Changing the Switch Configuration

CP1 is the active High Availability server and CP2 is the standby High Availability server.

1. On CP1 (the active High Availability server) do the following:

   a. Ensure the dongle is plugged into CP1. If the dongle is not on CP1, move it to CP1 and wait for 3 minutes.

      For more information about the dongle, see 1005r Server Hardware Installation (NN44200-308) or 1006r Server Hardware Installation (NN44200-320).

   b. Launch the AutoStart Console.

   c. Stop monitoring on the CallPilot resource group. For more information, see Disabling automatic failovers (stop monitoring) on page 180.

   d. Log on to CallPilot Manager on CP1 and start the Configuration Wizard.

e. Select the CallPilot Individual Feature Configuration (Express Mode) option and then click Next.

   Result: The Configuration Wizard: Express Configuration List screen appears.

f. Select the Switch Configuration check box.

   Result: The Meridian 1 Switch Information window appears.

g. If required, change the Switch Type, Switch Customer Number, or Switch IP Address.

   Important:
   Before changing the Switch IP Address in the Configuration Wizard, you must have changed the IP address in the AutoStart Console.

h. If required, change or add the TNs on CP1 and click Next.

i. If required, change or add the CDNs on CP1 and click Next.

j. Click Finish to complete the Configuration Wizard.

k. Perform a manual failover. For more information, see Initiating a manual failover on page 181.

   Result: The CallPilot resource group is automatically brought online on the standby High Availability server (CP2).

l. After the CallPilot resource group is online on CP2, restart CP1.

2. Move the dongle to CP2.

   For more information about the dongle, see 1005r Server Hardware Installation (NN44200-308) or 1006r Server Hardware Installation (NN44200-320).

3. On CP2, do the following:

   a. Launch the AutoStart Console.

   b. Wait until node CP1 and both drvE and drvF are green and show as online in the AutoStart Console.

   c. If required, disable monitoring for the CallPilot resource group. For more information, see Disabling automatic failovers (stop monitoring) on page 180.

   d. Log on to CallPilot Manager on CP2 and start the Configuration Wizard.

   e. Select the CallPilot Individual Feature Configuration (Express Mode) option and then click Next.

      Result: The Configuration Wizard: Express Configuration List screen appears.

   f. Select the Switch Configuration check box.

      Result: The Meridian 1 Switch Information window appears.

g. If required, change the Switch Type, Switch Customer Number, or Switch IP Address.

Important:
Before changing the Switch IP Address in the Configuration Wizard, you must have changed the IP address in the AutoStart Console.

h. If required, change or add the TNs on CP2 and click Next.

i. If required, change or add the CDNs on CP2 and click Next.

j. Click Finish to complete the Configuration Wizard.

k. Perform a manual failover. For more information, see Initiating a manual failover on page 181.

Result: The CallPilot resource group is automatically brought online on the standby High Availability server (CP1).

l. After the CallPilot resource group is online on CP1, restart CP2.

4. On CP1, do the following:

a. Launch the AutoStart Console.

b. Wait until node CP2 and both drvE and drvF are online/green in the AutoStart Console.

c. Enable monitoring for the CallPilot resource group. For more information, see Enabling automatic failovers (start monitoring) on page 180.

5. Test new or changed TNs or CDNs to ensure system functionality.

Install a new language

Use the following procedure to install additional languages or speech recognition on the High Availability system.

Installing a new language

1. On CP1 (the active High Availability server) do the following:

a. Ensure the dongle is plugged into CP1. If the dongle is not on CP1, move it to CP1 and wait for 3 minutes.

For more information about the dongle, see 1005r Server Hardware Installation (NN44200-308) or 1006r Server Hardware Installation (NN44200-320).

b. Launch the AutoStart Console.

c. Stop monitoring on the CallPilot resource group. For more information, see Disabling automatic failovers (stop monitoring) on page 180.

d. Log on to CallPilot Manager on CP1 and start the Configuration Wizard.

e. Select the CallPilot Individual Feature Configuration (Express Mode) option and then click Next.

   Result: The Configuration Wizard: Express Configuration List screen appears.

f. Select the Language Installation check box.

   Result: The Language Source Directory window appears.

g. Insert the Language Source CD into the DVD drive.

h. Ensure the Install Language option is selected.

i. Ensure that the Language CD Location is set to z:.

j. Click Next.

   Result: The Language Installation window appears.

k. On the Language Installation page, do the following:

   i. Select Languages and Automated Speech recognition to be installed.

   ii. If required, change the Primary Language or select Secondary Languages.

   Note:
   The Secondary Language is optional.

   Important:
   The same languages must be installed on CP1 and CP2.

l. Click Next.

m. Click Finish to complete the Configuration Wizard.

n. Perform a manual failover. For more information, see Initiating a manual failover on page 181.

   Result: The CallPilot resource group is automatically brought online on the standby High Availability server (CP2).

o. After the CallPilot resource group is online on CP2, restart CP1.

2. Move the dongle to CP2.

   For more information about the dongle, see 1005r Server Hardware Installation (NN44200-308) or 1006r Server Hardware Installation (NN44200-320).

3. On CP2, do the following:

   a. Launch the AutoStart Console.

   b. Wait until node CP1 and both drvE and drvF are online/green in the AutoStart Console.

c. If required, disable monitoring for the CallPilot resource group. For more information, see Disabling automatic failovers (stop monitoring) on page 180.

d. Log on to CallPilot Manager on CP2 and start the Configuration Wizard.

e. Select the CallPilot Individual Feature Configuration (Express Mode) option and then click Next.

   Result: The Configuration Wizard: Express Configuration List screen appears.

f. Select the Language Installation check box.

   Result: The Language Source Directory window appears.

g. Insert the Language Source CD into the DVD drive.

h. Ensure the Install Language option is selected.

i. Ensure that the Language CD Location is set to z:.

j. Click Next.

   Result: The Language Installation window appears.

k. On the Language Installation page, do the following:

   i. Select Languages and Automated Speech recognition to be installed.

   ii. If required, change the Primary Language or select Secondary Languages.

   Note:
   The Secondary Language is optional.

   Important:
   The same languages must be installed on CP1 and CP2.

l. Click Next.

m. Click Finish to complete the Configuration Wizard.

n. Perform a manual failover. For more information, see Initiating a manual failover on page 181.

   Result: The CallPilot resource group is automatically brought online on the standby High Availability server (CP1).

o. After the CallPilot resource group is online on CP1, restart CP2.

4. On CP1, do the following:

   a. Launch the AutoStart Console.

   b. Wait until node CP2 and both drvE and drvF are online/green in the AutoStart Console.

c. Enable monitoring for the CallPilot resource group. For more information, see Enabling automatic failovers (start monitoring) on page 180.

Change the Network Interface Card configuration and network settings

To provide the Managed IP service that is used to make the pair of High Availability servers appear as one server to the external network, the AutoStart software must know the local IP addresses of the ELAN Subnet and Avaya Server Subnet (CLAN) of the pair of servers. If changes are made to the ELAN Subnet IP address and Avaya Server Subnet IP address on either server after the AutoStart software is installed, the AutoStart software no longer works correctly. Depending on the state of the server when the change is made, this can cause a failover to the standby server or it can break the failover process.

Important:

Before changing any IP address or host name, Avaya recommends that you take note of the IP addresses and host name. It is good practice to save them to a safe location just in case you need them again (for example, if you need to recover the server).

The IP addresses and host names are in the following locations:

- ELAN or CLAN IP addresses—Run the command ipconfig /all command to check the current IP addresses.
- Managed host name—Navigate to the E:\Nortel\HA folder and open the AutoStart_Configuration.ini file to find the Managed host name. The Managed host name is mapped to the Managed CLAN IP address.
- Managed ELAN IP address (Virtual ELAN IP address)—This IP address is also saved in the E:\Nortel\HA\AutoStart_Configuration.ini file.

All of the configuration data (including Managed ELAN/CLAN IP addresses) required by the AutoStart software is also saved in a customized AutoStart definition file. This definition file is in the following folder: D:\Program Files\ [AutoStart_Domain]\Module\Tool Kit 2.0.

Depending on your system, the AutoStart definition file has a different name, as follows:

- For systems with one MPB96 board, the definition file is called CallPilot-Mirroring-Single.def.
- For systems with three MPB96 boards, the definition file is called CallPilot-Mirroring.def.

Local networking settings

The following procedures are used to change the local IP settings on either of the two servers that make up a CallPilot High Availability pair.

Note:

These procedures do not apply to the Managed ELAN and CLAN IP settings. For more information, see Managed networking settings on page 126.

Use the procedures in this section to change the following:

- ELAN or CLAN IP address changes on page 121
- HB1, HB2, and Mirroring IP address changes on page 123

ELAN or CLAN IP address changes

You can use this procedure to change the local ELAN or CLAN IP address on either one of the servers in a High Availability configuration after the AutoStart software is installed.

Changing the ELAN or CLAN IP address

1. Disable the AutoStart Monitoring.

   For more information, see Disabling automatic failovers (stop monitoring) on page 180.

2. Take the resource group CallPilot offline.

   For more information, see Taking the CallPilot resource group offline on page 177.

3. Attach drive E and drive F to the node whose ELAN IP address or CLAN IP address has to be changed. Perform the following for drive E and drive F:

   a. In the AutoStart Console, select the [AutoStart_Domain] > Data Sources.

   b. Right-click the drive you want to connect.

   c. Select Attach Data Source.

4. Use the Windows Services utility to manually start the following CallPilot services individually and in the following order:

   - Adaptive Server Anywhere - DB_SQLANY
   - CallPilot HAL Monitor
   - CallPilot LDAP
   - CallPilot AOS
   - CallPilot Multimedia Volume 1

- CallPilot Multimedia Volume 102
- CallPilot Multimedia Volume 103
- CallPilot Multimedia Cache

5. Log on to CallPilot Manager and run the Configuration Wizard as follows:

   a. On the main CallPilot Manager screen, click the Configuration Wizard icon.

      Tip: You can also start the Configuration Wizard by clicking Tools > Configuration Wizard.

      Result: A dialog box appears, prompting you to choose either an Express or Standard setup.

   b. Select OK to dismiss the dialog box.

      Result: The Configuration Wizard: Configuration Mode screen appears.

   c. Select the CallPilot Individual Feature Configuration (Express Mode) option and then click Next.

      Result: The Configuration Wizard: Express Configuration List screen appears.

   d. Select the Network Interface Card Configuration (ELAN and CLAN) check box.

   e. Change the ELAN or CLAN network setting as required.

   f. Click Next.

      Result: The Ready to Configure screen appears.

   g. Click Finish.

      Result: A dialog box prompts you to confirm the configuration.

   h. Click OK to configure CallPilot.

      Result: The configuration is applied to the server. This task can take from 5 to 10 minutes to complete. The Configuration Wizard displays progress information.

      After the configuration is applied to the server, a dialog box reminds you to restart the server for the configuration to take effect.

   i. Click OK to dismiss the dialog box.

      Result: The system returns you to the main CallPilot Manager screen.

   j. Log off CallPilot Manager and close the Web browser.

6. If prompted, restart the server after the Configuration Wizard is complete.

7. Update the name resolution mechanism. (Update the DNS/WINS/hosts file information on both nodes if they are used, especially for the CLAN IP address, which normally is mapped to the node name on the DNS server.)

8. Launch the AutoStart Console and do the following:
    a. Expand the node list in the AutoStart Console.
    b. From the Paths Defined for Node list, delete the Verification links that use the previous ELAN or CLAN IP addresses.
    c. Create new Verification links that will use the new ELAN or CLAN IP addresses.
9. If the ELAN IP or CLAN IP addresses on another node also have to be changed, repeat step 3 to step 8 on that node as well.
10. Bring the CallPilot resource group online (see Bringing the CallPilot resource group online on page 176) and then enable AutoStart Monitoring (see Enabling automatic failovers (start monitoring) on page 180.

HB1, HB2, and Mirroring IP address changes

Warning:

Avaya recommends that you do not change the IP address used for the Heartbeat (HB1), Heartbeat backup (HB2), or Mirroring links after the AutoStart software is installed.

If the Heartbeat (HB1), Heartbeat backup (HB2), or Mirroring link IP addresses are changed, you must uninstall and reinstall the AutoStart software on both servers as part of changing the IP addresses. For more information, see the following:

- Uninstall the AutoStart software on page 192
- Reinstall the AutoStart software on page 195.

Changing the HB1, HB2, and Mirroring IP addresses

1. Uninstall the AutoStart on both High Availability servers. For more information, see Uninstall the AutoStart software on page 192.
2. Move the dongle to the server where you will run Configuration Wizard to perform the IP address change and wait 3 minutes.
3. Use the Windows Services utility to manually start the following CallPilot services individually and in the following order:
    - Adaptive Server Anywhere - DB_SQLANY
    - CallPilot HAL Monitor
    - CallPilot LDAP
    - CallPilot AOS
    - CallPilot Multimedia Volume 1
    - CallPilot Multimedia Volume 102
    - CallPilot Multimedia Volume 103
    - CallPilot Multimedia Cache
4. Log on to CallPilot Manager and run the Configuration Wizard as follows:

a. On the main CallPilot Manager screen, click the Configuration Wizard icon.

   Tip: You can also start the Configuration Wizard by clicking Tools > Configuration Wizard.

   Result: A dialog box appears prompting you to choose either an Express or Standard setup.

b. Select OK to dismiss the dialog box.

   Result: The Configuration Wizard: Configuration Mode screen appears.

c. Select the CallPilot Individual Feature Configuration (Express Mode) option and then click Next.

   Result: The Configuration Wizard: Express Configuration List screen appears.

d. Select the Network Interface Card Configuration (ELAN and CLAN) check box.

e. Change the IP addresses as required.

f. Click Next.

   Result: The Ready to Configure screen appears.

g. Click Finish.

   Result: A dialog box prompts you to confirm the configuration.

h. Click OK to configure CallPilot.

   Result: The configuration is applied to the server. This task can take from 5 to 10 minutes to complete. The Configuration Wizard displays progress information.

   After the configuration is applied to the server, a dialog box reminds you to restart the server for the configuration to take effect.

i. Click OK to dismiss the dialog box.

   Result: The system returns you to the main CallPilot Manager screen.

j. Log off CallPilot Manager and close the Web browser.

5. Restart the server.
6. Repeat the previous steps if the same IP change is required on the other High Availability server.
7. Connect the LAN.

   For more information, see Connect and verify LAN connections on page 52 and complete the following procedures:

   - Connecting and verifying LAN connections on page 52
   - Modifying the hosts file on page 55 (optional)

- Testing the host name resolution on page 57

8. Check the configuration of CP1 and CP2.

   For more information, see Running Stage 1 of the High Availability Configuration Wizard to check CP1 and CP2 configuration on page 58.

9. Install the AutoStart Software on CP1.

   For more information, see Installing the AutoStart Agent and Console software on CP1 on page 62.

10. Add the CP2 Administrator account to the AutoStart Console.

    For more information, see Add the node 2 administrator account to the AutoStart Console on node 1 on page 70.

11. Install the AutoStart software on CP2.

    For more information, see Installing the AutoStart Agent and Console software on CP2 on page 72.

12. To configure the AutoStart software, do the following:

    a. Configure the AutoStart software.

       For more information, see Configure the AutoStart software on page 81.

       Warning:
       You must wait for both servers under Domains > [AutoStart_Domain] > Nodes to appear green before making any changes in the AutoStart Console. Failure to do so can result in the loss configured information for verification links upon the next restart.

       i. Modify the AutoStart Domain and Verification links.

          For more information, see Modifying the AutoStart Domain and Verification links on page 81.

       ii. Add the Remote Mirroring Host for the new 1005r or 1006r server (CP2).

          For more information, see Adding the Remote Mirroring Host for CP2 on page 84.

    b. Generate the AutoStart Definition File.

       For more information, see Generating the AutoStart Definition File on page 86.

    c. Import the AutoStart Definition File.

       For more information, see Importing the AutoStart definition file on page 88.

    d. Add the Windows administrator account password for the AutoStart Utility Processes.

For more information, see Adding the Windows administrator account password for the AutoStart Utility Processes on page 89.

13. Bring the Resource Groups online.

    For more information, see Bring the Resource Groups online on page 92.

    a. Bring the CallPilot Resource Group online on CP1.

       For more information, see Bringing the CallPilot Resource Group online on CP1 on page 93.

    b. Bring the CallPilot_[CP1] and CallPilot_[CP2] Resources Groups online.

       For more information, see Bringing the Resource Groups CallPilot_[CP1] and CallPilot_[CP2] online on page 95.

14. Create the CallPilot Reporter connections. For more information, see Creating the CallPilot Reporter connection on page 99.

Managed networking settings

After the AutoStart software is installed, it is possible to change the Managed networking settings, which include the following settings:

- Managed CLAN host name (See Changing the Managed CLAN host name on page 126.)
- Managed CLAN IP address (See Changing the Managed CLAN IP address on page 127.)
- Managed ELAN IP address (See Changing the Managed ELAN IP address on page 129.)

Caution:

An incorrect or unreachable test IP address may result in the status of the CLAN IP address changing to “Path Failed” (indicator shows red with “?”). To change the status back to “Assigned” (green), perform the following steps:

- Correct or remove test IP address(es) and then click apply.
- Unassign CLAN IP address.
- Assign CLAN IP address.

Changing the Managed CLAN host name

1. Ensure DNS or host files are updated with new Managed CLAN host name.
2. Replace the old Managed host name with the new Managed host name in the AutoStart_Configuration.ini file by doing the following:

   a. Navigate to the E:\Nortel\HA folder.

b. Double-click the AutoStart_Configuration.ini file to open the file.

c. Edit the VirtualHostname with the new Managed CLAN host name.

d. Save the file.

Changing the Managed CLAN IP address

This procedure changes only the Managed CLAN IP address. (It does not change the physical CLAN IP settings.)

1. Change the Managed host name mapping to the new Managed CLAN IP address on your DNS server or in the appropriate hosts file.
2. Disable the AutoStart Monitoring. For more information, see Disabling automatic failovers (stop monitoring) on page 180.
3. Take the CallPilot resource group offline. For more information, see Taking the CallPilot resource group offline on page 177.
4. Open the AutoStart Console and delete the Managed CLAN IP resources in the Startup and Shutdown sequences by doing the following:

   a. Expand [AutoStart_Domain] > Resource Groups.

   b. Select the CallPilot resource group.

   c. Select the Settings tab.

   d. Under Startup Sequence, select the Managed CLAN IP address and click Delete. Verify the adapter from the shutdown sequence is also deleted.
5. On the AutoStart Console, delete the Managed CLAN IP resource in the IP resource list by doing the following:

   a. Expand [AutoStart_Domain] > IP Addresses.

   b. Select the Managed CLAN IP address.

   c. Click Delete the current IP address .
6. Create the new Managed CLAN IP resource by doing the following:

   a. Expand [AutoStart_Domain] > IP Addresses.

   b. Right-click IP Addresses and select Create New IP Address.

   Result: The New Manage IP Address window appears.

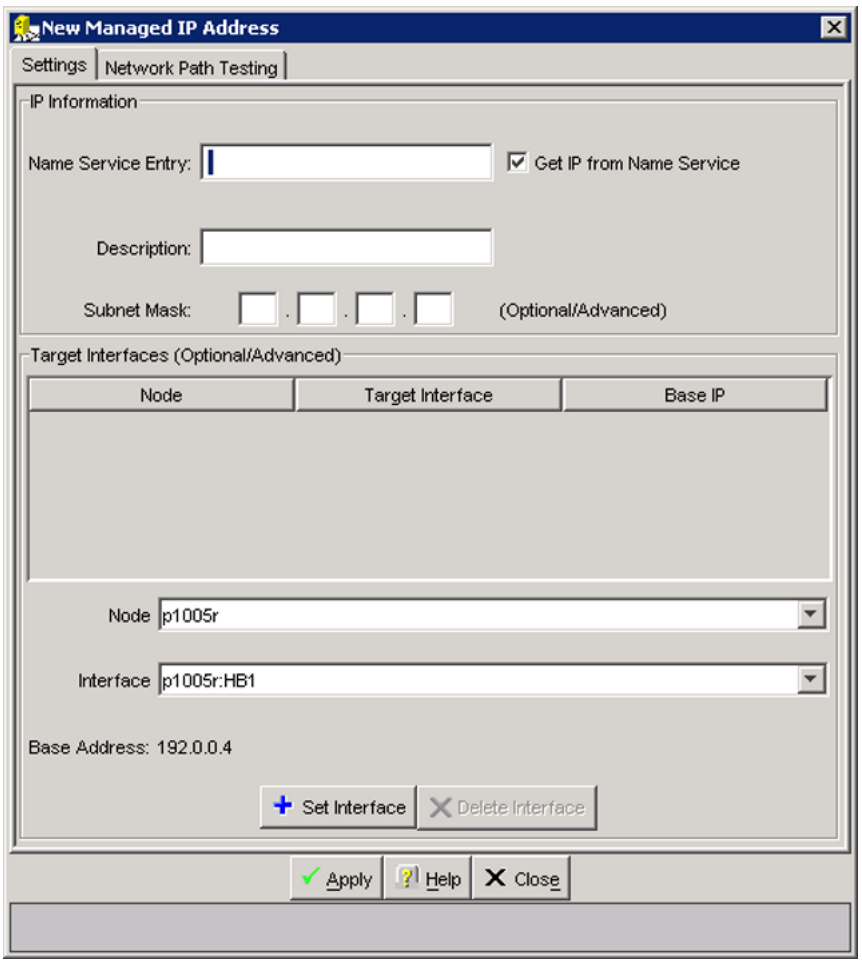


Figure 61: New Managed IP Address

c. Under IP Information, clear the Get IP from Name Service check box.

   Result: The IP address field appears.

d. Enter the new Managed CLAN IP address and subnet mask.

e. Select the Network Path Testing tab.

f. Enter the test IP address of the new Managed CLAN IP address.

g. Click Add IP Address.

h. Click Apply.

7. On the AutoStart Console, add the new Managed CLAN IP resource into the Startup and Shutdown sequences of the CallPilot resource group. Using the arrows, move the Managed CLAN IP back to its original location, which is:

   - directly after the Managed ELAN IP in the Startup Sequence list
   - directly before the Managed ELAN IP in the Shutdown Sequence list

   a. Expand [AutoStart_Domain] > Resource Groups > CallPilot.

b. Select the Settings tab.

c. Under Startup Sequence select new CLAN address, selectIP from the drop down list and click Add.

d. Clear the Failure Response Settings check boxes.

e. Click Apply.

f. Under the Startup Sequence, select the new Managed CLAN IP address and move it directly below the Managed ELAN IP address.

g. Under the Shutdown Sequence, select the new Managed CLAN IP address and move it directly above the Managed ELAN IP address.

h. Click Apply.

8. Bring the CallPilot resource group online. For more information, see Bringing the CallPilot resource group online on page 176.

9. Enable the AutoStart Monitoring. For more information, see Enabling automatic failovers (start monitoring) on page 180.

Changing the Managed ELAN IP address

This procedure changes only the Managed ELAN IP address. (It does not change the physical ELAN IP settings.)

1. Disable the AutoStart Monitoring. For more information, see Disabling automatic failovers (stop monitoring) on page 180.

2. Take the CallPilot resource group offline. For more information, see Taking the CallPilot resource group offline on page 177.

3. Open the Managed_ELAN_IP_Failure trigger and remove Managed ELAN IP from the Selected Items.

4. Click Apply.

5. Open the AutoStart Console and delete the Managed ELAN IP resources in the Startup and Shutdown sequences by doing the following:

   a. Expand [AutoStart_Domain] > Resource Groups.

   b. Select the CallPilot resource group.

   c. Select the Settings tab.

   d. Under Startup Sequence, select the Managed ELAN IP address and click Delete. Verify the adapter from the shutdown sequence is also deleted.

6. On the AutoStart Console, delete the Managed ELAN IP resource in the IP resource list by doing the following:

   a. Expand [AutoStart_Domain] > IP Addresses.

   b. Select the Managed ELAN IP address.

   c. Click Delete the current IP address.

7. Create the new Managed ELAN IP resource by doing the following:

   a. Expand [AutoStart_Domain] > IP Addresses.

b. Right-click IP Addresses and select Create New IP Address.

Result: The New Manage IP Address window appears.

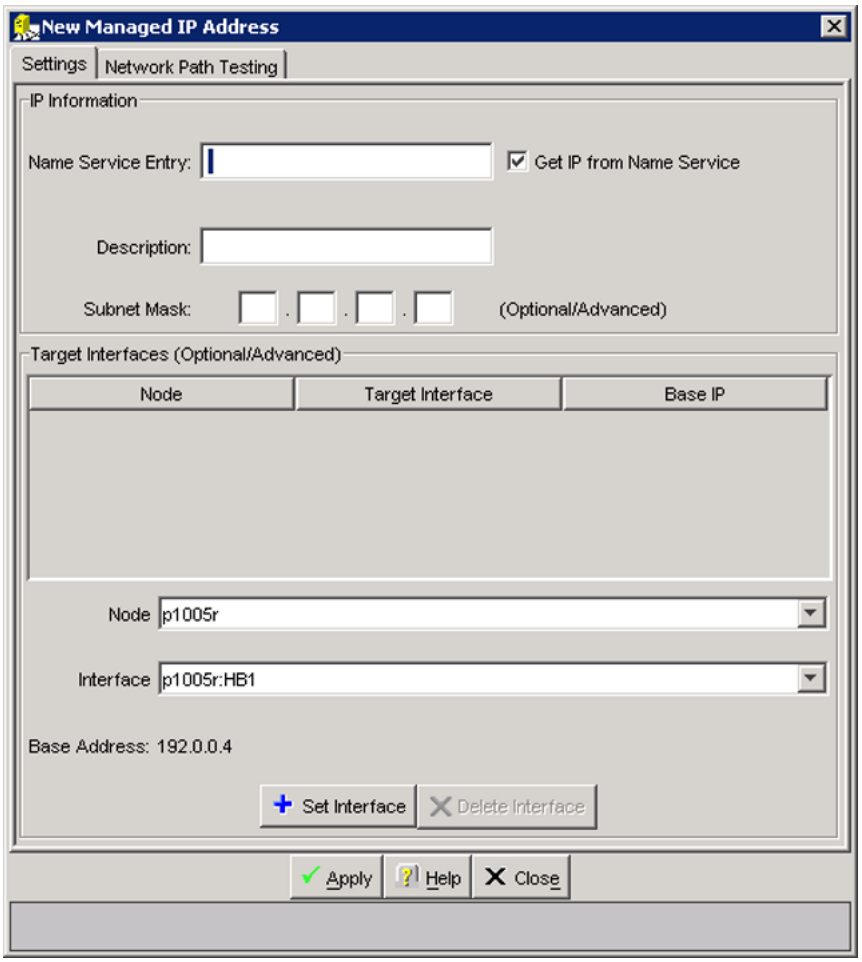


Figure 62: New Managed IP Address

c. Under IP Information, clear the Get IP from Name Service check box.

d. Enter the new Managed ELAN IP address and subnet mask.

e. Enter the switch IP address as the Test Path of the new Managed ELAN IP address.

f. Click Apply.

8. On the AutoStart Console, add the new Managed ELAN IP resource into the Startup and Shutdown sequences of the CallPilot resource group. Ensure that the Managed ELAN IP address resource is in its original location, which is:

   - directly before the Managed CLAN IP address on the Startup sequence
   - directly after the Managed CLAN IP address on the Shutdown sequence

   a. Expand [AutoStart_Domain] > Resource Groups > CallPilot.

   b. Select the Settings tab.

c. Under Startup Sequence select new ELAN address, select IP from the drop down list and click Add.

d. Clear the Failure Response Settings check boxes.

e. Click Apply.

f. Under the Startup Sequence, select the Managed ELAN IP address and move it directly above the Managed CLAN IP address.

g. Under the Shutdown Sequence, select the Managed ELAN IP address and move it directly below the Managed CLAN IP address.

h. Click Apply.

9. Attach drive E to one of the High Availability servers.

   a. In the AutoStart Console, select the [AutoStart_Domain] > Data Sources.

   b. Right-click drive E.

   c. Select Attach Data Source.

10. Replace the old Managed ELAN IP address with the new Managed ELAN IP address in the AutoStart_Configuration.ini file that is in the E:\Nortel\HA folder.

11. Detach drive E.

    a. In the AutoStart Console, select the [AutoStart_Domain] > Data Sources.

    b. Right-click drive E.

    c. Select Detach Data Source.

12. Open the Managed_ELAN_IP_Failure trigger and move Managed ELAN IP to the Selected Items.

13. Click Apply.

14. Bring the resource group online. For more information, see Bringing the CallPilot resource group online on page 176.

15. Enable the AutoStart Monitoring. For more information, see Enabling automatic failovers (start monitoring) on page 180.

Change the administrator account password for the Utility Processes

The administrator passwords must be the same on both High Availability servers.

On the active server, you can use either the Windows utility or the Configuration Wizard to change the administrator password after the AutoStart Monitoring is disabled. However, on the standby server, you must use the Windows utility to change the administrator passwords.

When the administrator password is changed on both servers, you must also update the administrator password used by the AutoStart utilities in the AutoStart Console as described in the following procedure.

Changing the Utility Processes administrator password

1. On the AutoStart Console, expand [AutoStart_Domain] > Utility Processes.

   Result: The Utility Processes are displayed:

   - DisableAOS
   - KillServices
   - LoadDN
   - LoadTSP
   - UnloadTSP
   - UnloadTSPOnStandbyServer

2. Click one of the utilities to open the utility.

   Result: The Settings tab for that utility appears.

3. In the Login Info area, enter the new administrator password in the Password and Confirm fields.

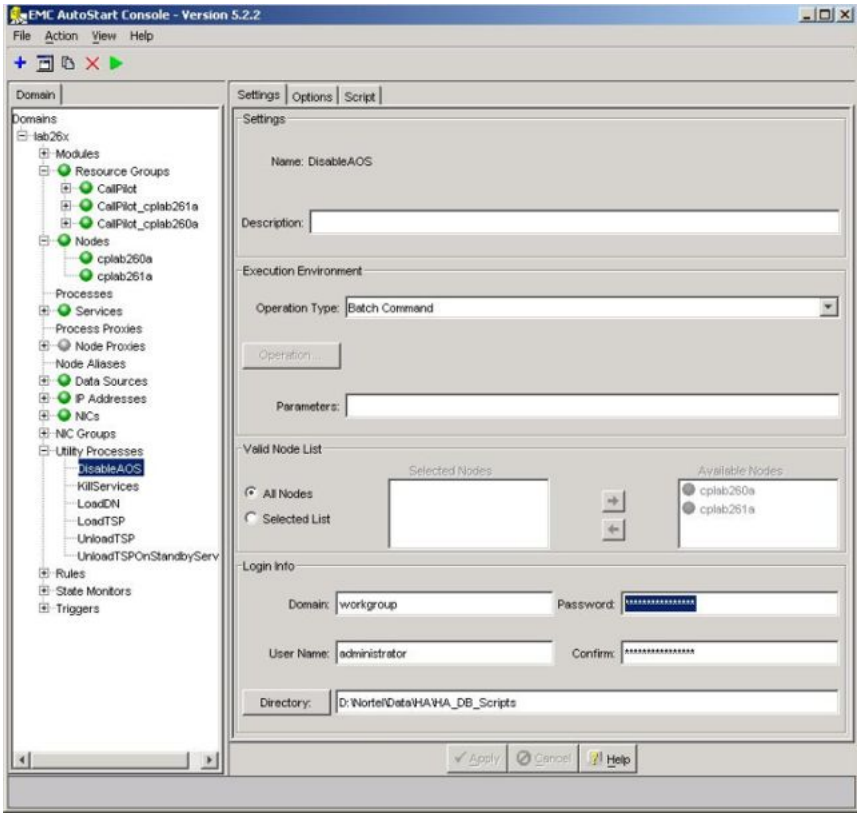


Figure 63: Change the administrator password

4. Click Apply.
5. Repeat the preceding steps for each of the remaining utilities in the Utility Processes list.

Increase software licenses

The following procedure provides the steps for adding additional seats (using a new keycode) to a pair of High Availability servers.

Only one server in the pair is in service at a time, and therefore, both servers share one dongle. As a result, they both have the same serial number and share the same keycode. The information in the keycode is stored in the CallPilot database so it is automatically mirrored to the standby server.

Increasing software licenses on a pair of CallPilot 5.0 1005r or 1006r High Availability servers

1. Use the AutoStart Console to stop monitoring (to disable automatic failovers).

   For more information, see Disabling automatic failovers (stop monitoring) on page 180.
2. On the active CallPilot server (CP1), log on to CallPilot Manager.
   a. Launch Internet Explorer.
   b. Enter http://<Active Server Name (CP1) or IP address>/cpmgr in the URL address box.

      Result: The CallPilot Manager Logon Web page appears.
   c. Log on using your existing CallPilot logon information. Enter information into the following:
      - Mailbox Number—Enter your existing mailbox number.
      - Password—Enter your password.
      - Server—Specify the name or the IP address of the CallPilot server that you want to configure. (The server name may have changed during the upgrade or platform migration.)

      Note:

      When you launch Internet Explorer, you may see a dialog box that says "M/S IE Enhanced Security config is currently enabled on your server. This advanced level of security reduces risk." Avaya recommends that you do not lower the security level. Avaya also recommends that you do not select the check box to not show the message again. If you do lower the security level and you try to access a Web site off the server, it may be blocked by the security setting. You do not receive a warning, but a blank screen appears.

d. Click Login.

3. Run the Configuration Wizard and enter the new keycode.

   a. On the main CallPilot Manager screen, click the Configuration Wizard icon.

      Tip: You can also start the Configuration Wizard by clicking Tools > Configuration Wizard.

      Result: A dialog box appears, prompting you to choose either an Express or Standard setup.

   b. Select OK to dismiss the dialog box.

      Result: The Configuration Wizard: Configuration Mode screen appears.

   c. Select the CallPilot System Configuration (Standard Mode) option and then click Next.

      Result: The Configuration Wizard: Welcome screen appears.

   d. On the Welcome screen, click Next.

      Result: The Keycode and serial number screen appears.

   e. Enter your Serial number and the new Keycode. This new keycode includes the increased licenses.

   f. Ensure that the Serial number and Keycode are correct, and then click Next.

      Result: The Feature Verification screen appears.

   g. Ensure that the details on the Feature Verification screen match your expectations and click Next.

      Note:
      If a feature is missing or is not what you expected, acquire a new keycode from your Avaya distributor.

      Result: The Server Information screen appears.

   h. Verify the information on the Server Information screen, modify it if necessary, and then click Next.

      Result: The Password Information screen appears.

   i. Select the Leave the password unchanged option. (If prompted, change the default password. Store the password in a safe location.)

   j. Click Next.

      Result: The Multimedia Allocation screen appears.

   k. Verify the number of MPB boards and, if applicable, DSP cards, and ensure that they match the hardware installed in the CallPilot server. Verify the Port Allocations.

l. Click Next.

   Result: The Switch Information screen appears.

m. Ensure that the following settings are correct on the Switch Information screen and click Next.

   Result: The CDN Information screen appears.

n. Verify the CDN configuration and click Next.

   Result: The Language Source Directory screen appears.

o. Select the Skip Language Installation option.

p. Click Next.

   Result: The CallPilot Local Area Network Interface screen appears.

q. Verify the settings on the CallPilot Local Area Network Interface page. Do not change any settings. Ensure that the High Availability mode check box is selected and the HB1, HB2, and MIRROR information is correct.

r. Click Next.

   Result: The Ready to Configure screen appears.

s. Click Finish.

   Result: A dialog box prompts you to confirm the configuration.

t. Click OK to configure CallPilot.

   Result: The configuration is applied to the server. This task can take from 5 to 10 minutes to complete. The Configuration Wizard displays progress information.

   After the configuration is applied to the server, a dialog box reminds you to restart the server for the configuration to take effect.

u. Click OK to dismiss the dialog box.

   Result: The system returns you to the main CallPilot Manager screen.

v. Log off CallPilot Manager and close the Web browser.

4. If prompted, restart the server after the Configuration Wizard is complete.
5. Use the AutoStart Console to start monitoring (to enable automatic failovers). For more information, see Enabling automatic failovers (start monitoring) on page 180.
6. Ensure that the CallPilot resource group is online. If it is not online, bring the resource group online (which starts up CallPilot). For more information, see Bring a resource group online on page 176.

Increasing software licenses and CallPilot channel capacity on a pair of CallPilot 5.0 1005r or 1006r High Availability servers.

1. Use the AutoStart Console to stop monitoring (to disable automatic failovers). For more information, see Disabling automatic failovers (stop monitoring) on page 180
2. On the active CallPilot server (CP1), log on to CallPilot Manager.
   a. Launch Internet Explorer.
   b. Enter http://<Active Server Name (CP1) or IP address>/cpgmr in the URL address box.

      Result: The CallPilot Manager Logon Web page appears.
   c. Log on using your existing CallPilot logon information. Enter information into the following:
      - Mailbox Number—Enter your existing mailbox number.
      - Password—Enter your password.
      - Server—Specify the name or the IP address of the CallPilot server that you want to configure. (The server name may have changed during the upgrade or platform migration.)

      Important:
      When you launch Internet Explorer, you may see a dialog box that says "M/S IE Enhanced Security config is currently enabled on your server. This advanced level of security reduces risk." Avaya recommends that you do not lower the security level. Avaya also recommends that you do not select the check box to not show the message again. If you do lower the security level and you try to access a Web site off the server, it may be blocked by the security setting. You do not receive a warning, but a blank screen appears.
   d. Click Login.
3. Run the Configuration Wizard and enter the new keycode.
   a. On the main CallPilot Manager screen, click the Configuration Wizard icon.

      Tip: You can also start the Configuration Wizard by clicking Tools > Configuration Wizard.

      Result: A dialog box appears, prompting you to choose either an Express or Standard setup.
   b. Select OK to dismiss the dialog box.

   Result: The Configuration Wizard: Configuration Mode screen appears.
   a. Select the CallPilot System Configuration (Standard Mode) option and then click Next.

      Result: The Configuration Wizard: Welcome screen appears.

b. On the Welcome screen, click Next.

   Result: The Keycode and serial number screen appears.

c. Enter your Serial number and the new Keycode. This new keycode includes the increased licenses and channels.

d. Ensure that the Serial number and Keycode are correct, and then click Next.

Result: The Feature Verification screen appears.

Ensure that the details on the Feature Verification screen match your expectations and click Next.

Important:

If a feature is missing or is not what you expected, acquire a new keycode from your Avaya distributor.

Result: The Server Information screen appears.

a. Verify the information on the Server Information screen, modify it if necessary, and then click Next. Result:The Password Information screen appears.

b. Select the Leave the password unchanged option. (If prompted, change the default password. Store the password in a safe location.)

c. Click Next.

   Result: The Multimedia Allocation screen appears.

d. Verify the number of MPB boards and, if applicable, DSP cards, and ensure that they match the hardware installed in the CallPilot server. Verify the Port Allocations.

e. Click Next. Result: The Switch Information screen appears.

f. Add additional switch TNs and ensure that the settings are correct on the Switch Information screen and click Next. Result:The CDN Information screen appears.

g. Verify the CDN configuration and click Next.

   Result:The Language Source Directory screen appears.

h. Select the Skip Language Installation option.

i. Click Next.

   Result: The CallPilot Local Area Network Interface screen appears.

j. Verify the settings on the CallPilot Local Area Network Interface page. Do not change any settings. Ensure that the High Availability mode check box is selected and the HB1, HB2, and MIRROR information is correct.

k. Click Next.

   Result:The Ready to Configure screen appears.

l. Click Finish.

Result: A dialog box prompts you to confirm the configuration.

m. Click OK to configure CallPilot.

Result: The configuration is applied to the server. This task can take from 5 to 10 minutes to complete. The Configuration Wizard displays progress information. After the configuration is applied to the server, a dialog box reminds you to restart the server for the configuration to take effect.

n. Click OK to dismiss the dialog box.

Result:The system returns you to the main CallPilot Manager screen.

o. Log off CallPilot Manager and close the Web browser.

p. Perform a manual failover. For more information, see Initiating a manual failover on page 181.

Result: The CallPilot resource group is automatically brought online on the standby High Availability server (CP2).

q. After the CallPilot resource group is online on CP2, restart CP1.

4. Move the dongle to CP2. For more information about the dongle, see 1005r Server Hardware Installation (NN44200-308) or 1006r Server Hardware Installation (NN44200-320).

5. On CP2, do the following:

   a. Launch the AutoStart Console.

   b. Wait until node CP1 and both drvE and drvF are green and show as online in the AutoStart Console.

   c. If required, disable monitoring for the CallPilot resource group.

   For more information, see Disabling automatic failovers (stop monitoring) on page 180.

6. On the active CallPilot server (CP2), log on to CallPilot Manager.

   a. Launch Internet Explorer.

   b. Enter http://<Active Server Name (CP2) or IP address>/cpmgr in the URL address box.

   Result: The CallPilot Manager Logon Web page appears.

   c. Log on using your existing CallPilot logon information. Enter information into the following:

      - Mailbox Number— Enter your existing mailbox number.
      - Password— Enter your password.
      - Server— Specify the name or the IP address of the CallPilot server that you want to configure. (The server name may have changed during the upgrade or platform migration.)

Important:

When you launch Internet Explorer, you may see a dialog box that says "M/S IE Enhanced Security config is currently enabled on your

server. This advanced level of security reduces risk." Avaya recommends that you do not lower the security level. Avaya also recommends that you do not select the check box to not show the message again. If you do lower the security level and you try to access a Web site off the server, it may be blocked by the security setting. You do not receive a warning, but a blank screen appears.

d. Click Login.

7. Run the Configuration Wizard and enter the new keycode.

   a. On the main CallPilot Manager screen, click the Configuration Wizard icon.

      Tip: You can also start the Configuration Wizard by clicking Tools > Configuration Wizard.

      Result: A dialog box appears, prompting you to choose either an Express or Standard setup.

   b. Select OK to dismiss the dialog box.

      Result: The Configuration Wizard: Configuration Mode screen appears.

   c. Select the CallPilot System Configuration (Standard Mode) option and then click Next.

      Result: The Configuration Wizard: Welcome screen appears.

   d. On the Welcome screen, click Next.

      Result: The Keycode and serial number screen appears.

   e. Enter your Serial number and the new Keycode (if required). This new keycode includes the increased licenses and channels.

   f. Ensure that the Serial number and Keycode are correct, and then click Next.

      Result:The Feature Verification screen appears.

   g. Ensure that the details on the Feature Verification screen match your expectations and click Next.

      Important:
      If a feature is missing or is not what you expected, acquire a new keycode from your Avaya distributor.

      Result: The Server Information screen appears.

   h. Verify the information on the Server Information screen, modify it if necessary, and then click Next. Result: The Password Information screen appears.

   i. Select the Leave the password unchanged option. (If prompted, change the default password. Store the password in a safe location.)

   j. Click Next.

Result: The Multimedia Allocation screen appears.

k. Verify the number of MPB boards and, if applicable, DSP cards, and ensure that they match the hardware installed in the CallPilot server. Verify the Port Allocations.

l. Click Next.

Result: The Switch Information screen appears.

m. Add additional switch TNs and ensure that the settings are correct on the Switch Information screen and click Next.

Result: The CDN Information screen appears.

n. Verify the CDN configuration and click Next.

Result: The Language Source Directory screen appears.

o. Select the Skip Language Installation option

p. Click Next.

Result: The CallPilot Local Area Network Interface screen appears.

q. Verify the settings on the CallPilot Local Area Network Interface page. Do not change any settings. Ensure that the High Availability mode check box is selected and the HB1, HB2, and MIRROR information is correct.

r. Click Next.

Result: Result: The Ready to Configure screen appears.

s. Click Finish.

Result: A dialog box prompts you to confirm the configuration.

t. Click OK to configure CallPilot.

Result: The configuration is applied to the server. This task can take from 5 to 10 minutes to complete. The Configuration Wizard displays progress information.

After the configuration is applied to the server, a dialog box reminds you to restart the server for the configuration to take effect.

a. Click OK to dismiss the dialog box.

Result: The system returns you to the main CallPilot Manager screen.

b. Log off CallPilot Manager and close the Web browser.

c. Perform a manual failover. For more information, see Initiating a manual failover on page 181.

Result: The CallPilot resource group is automatically brought online on the standby High Availability server (CP1).

d. After the CallPilot resource group is online on CP1, restart CP2.

8. Use the AutoStart Console to start monitoring (to enable automatic failovers). For more information, see Enabling automatic failovers (start monitoring) on page 180.

Increase CallPilot channel capacity by adding MPB96 boards

If the pair of 1005r or 1006r servers each have one MPB96 board installed, the servers can be upgraded to have three MPB96 boards. This hardware expansion is required if the servers each have one MPB96 board installed and you want to increase capacity to a value greater than 96 MPUs or 96 channels. Three MPB96 boards have 192 channels and 288 MPUs.

Increasing channel capacity by adding MPB96 boards in a pair of CallPilot 5.0 1005r or 1006r High Availability servers

1. Disable AutoStart Monitoring. For more information, see Disabling automatic failovers (stop monitoring) on page 180.
2. Take the CallPilot resource group offline. For more information, see Take a resource group offline on page 177.
3. Disable the DisableAOS rule on the AutoStart Console.
4. Power down both servers.
5. Install the two additional MPB96 boards in each server. Refer to either 1005r Server Maintenance and Diagnostics (NN44200-704) or 1006r Server Maintenance and Diagnostics (NN44200-709) for details.
6. Connect all the required cables.
7. Power on both servers.
8. On CP1, open Windows Explorer.
9. Navigate to the D:\Nortel\HA\Toolkit Installer 2.0 folder.
10. Run the command HighAvailabilityConfigurationWizard.exe.

    Result: The High Availability Configuration Wizard appears.
11. In the Number of MPB96 boards field, select 3.
12. Fill the remaining fields on the High Availability Configuration Wizard using Step 3 in Running Stage 1 of the High Availability Configuration Wizard to check CP1 and CP2 configuration on page 58.
13. On CP1, attach drive E and drive F to the High Availability server. Perform the following steps for both drive E and drive F.
    a. In the AutoStart Console, select the [AutoStart_Domain] > Data Sources.
    b. Right-click the drive you want to connect.
    c. Select Attach Data Source.

14. Perform step 4 of the High Availability Configuration Wizard. For more information, see Running Stage 1 of the High Availability Configuration Wizard to check CP1 and CP2 configuration on page 58.
15. Import the new definition file on the AutoStart Console.

    For more information, see Importing the AutoStart Definition file on page 164.
16. Update the AutoStart Utilities logon information (that is, update the passwords for each utility as a result of reimporting the new definition file).
17. On CP1, use the Windows Service utility to manually start the following CallPilot services individually and in the following order:
    - Adaptive Server Anywhere - DB_SQLANY
    - CallPilot HAL Monitor
    - CallPilot LDAP
    - CallPilot AOS (Enable the CallPilot AOS service first)
    - CallPilot Multimedia Volume 1
    - CallPilot Multimedia Volume 102
    - CallPilot Multimedia Volume 103
    - CallPilot Multimedia Cache
18. Move the dongle to the CP1 server (if the dongle is not already on the server).
19. Run the CallPilot Configuration Wizard to change the switch configuration to match the switch settings.

    Result: The Configuration Wizard unloads the CallPilot Database tables again (which were previously unloaded).

    a. On the main CallPilot Manager screen, click the Configuration Wizard icon.

       Tip: You can also start the Configuration Wizard by clicking Tools > Configuration Wizard.

       Result: A dialog box appears, prompting you to choose either an Express or Standard setup.

    b. Select OK to dismiss the dialog box.

       Result: The Configuration Wizard: Configuration Mode screen appears.

    c. Select the CallPilot System Configuration (Standard Mode) option and then click Next.

       Result: The Configuration Wizard: Welcome screen appears.

    d. On the Welcome screen, click Next.

       Result: The Keycode and serial number screen appears.

    e. Verify your Serial number and Keycode and then click Next.

Result: The Feature Verification screen appears.

f. Ensure that the details on the Feature Verification screen match your expectations and click Next.

Note:

If a feature is missing or is not what you expected, acquire a new keycode from your Avaya distributor.

Result: The Server Information screen appears.

g. Verify the information on the Server Information screen, modify it if necessary, and then click Next.

Result: The Password Information screen appears.

h. Select the Leave the password unchanged option. (If prompted, change the default passwords. Store passwords in a safe location.)

i. Click Next.

Result: The Multimedia Allocation screen appears.

j. Verify the number of MPB boards and, if applicable, DSP cards, and ensure that they match the hardware installed in the CallPilot server.

k. Change the Port Allocations as required.

l. Click Next.

Result: The Switch Information screen appears.

m. Ensure that the following settings are correct:

- Ensure the switch type and the switch IP addresses are correct.
- If you are expanding the number of channels, configure the new channels from this screen.
- After you configure the channels, click Next.

Result: The CDN Information screen appears.

n. Verify the CDN configuration.

If you need to make changes, do the following:

i. Click New to add a new CDN.

Result: The system prompts you for the CDN and the name of the application to dedicate to the CDN.

ii. Specify the CDN, choose the application, and then click OK.

Result: The system returns you to the CDN Information page.

o. Click Next.

Result: The Language Source Directory screen appears.

p. Select the Skip Language Installation option.

q. Click Next.

   Result: The CallPilot Local Area Network Interface screen appears.

r. Verify the information on the CallPilot Local Area Network Interface page. Do not change any settings. Ensure that the High Availability mode check box is selected and that the HB1, HB2, and MIRROR information is correct.

s. Click Next.

   Result: The Ready to Configure screen appears.

t. Click Finish.

   Result: A dialog box prompts you to confirm the configuration.

u. Click OK to configure CallPilot.

   Result: The configuration is applied to the server. This task can take from 5 to 10 minutes to complete. The Configuration Wizard displays progress information.

   After the configuration is applied to the server, a dialog box reminds you to restart the server for the configuration to take effect.

v. Click OK to dismiss the dialog box.

   Result: The system returns you to the main CallPilot Manager screen.

w. Log off CallPilot Manager and close the Web browser.

20. Restart the CP1 server.

21. On CP2, attach drive E and drive F to CP2 from the AutoStart Console. Perform the following for both drive E and drive F:

    a. In the AutoStart Console, select the [AutoStart_Domain] > Data Sources.

    b. Right-click the drive you want to connect.

    c. Select Attach Data Source.

22. On CP2, use the Windows Service utility to manually start the following CallPilot services individually and in the following order:

    - Adaptive Server Anywhere - DB_SQLANY
    - CallPilot HAL Monitor
    - CallPilot LDAP
    - CallPilot AOS (Enable the CallPilot AOS service first)
    - CallPilot Multimedia Volume 1
    - CallPilot Multimedia Volume 102
    - CallPilot Multimedia Volume 103
    - CallPilot Multimedia Cache

23. Move the dongle to CP2.
24. Run the CallPilot Configuration Wizard to change the switch configuration to match the switch settings.

    Result: The Configuration Wizard unloads the CallPilot Database tables again (which were previously unloaded).

    a. On the main CallPilot Manager screen, click the Configuration Wizard icon.

       Tip: You can also start the Configuration Wizard by clicking Tools > Configuration Wizard.

       Result: A dialog box appears, prompting you to choose either an Express or Standard setup.

    b. Select OK to dismiss the dialog box.

       Result: The Configuration Wizard: Configuration Mode screen appears.

    c. Select the CallPilot System Configuration (Standard Mode) option and then click Next.

       Result: The Configuration Wizard: Welcome screen appears.

    d. On the Welcome screen, click Next.

       Result: The Keycode and serial number screen appears.

    e. Verify your Serial number and Keycode.

       Result: The Feature Verification screen appears.

    f. Ensure that the details on the Feature Verification screen match your expectations and click Next.

       Note:
       If a feature is missing or is not what you expected, acquire a new keycode from your Avaya distributor.

       Result: The Server Information screen appears.

    g. Verify the information on the Server Information screen, modify it if necessary, and then click Next.

       Result: The Password Information screen appears.

    h. Select the Leave the password unchanged option. (If prompted, change the default passwords. Save the password in a safe location.)

    i. Click Next.

       Result: The Multimedia Allocation screen appears.

    j. Verify the number of MPB boards and, if applicable, DSP cards, and ensure that they match the hardware installed in the CallPilot server.

    k. Change the Port Allocations as required.

l. Click Next.

   Result: The Switch Information screen appears.

m. Ensure that the following settings are correct:

   - Ensure the switch type and the switch IP addresses are correct.
   - If you are expanding the number of channels, configure the new channels from this screen.
   - After you configure the channels, click Next.

   Result: The CDN Information screen appears.

n. Verify the CDN configuration.

   If you need to make changes, do the following:

   i. Click New to add a new CDN.

      Result: The system prompts you for the CDN and the name of the application to dedicate to the CDN.

   ii. Specify the CDN, choose the application, and then click OK.

      Result: The system returns you to the CDN Information page.

o. Click Next.

   Result: The Language Source Directory screen appears.

p. Select the Skip Language Installation option.

   Result: The CallPilot Local Area Network Interface screen appears.

q. Verify the information on the CallPilot Local Area Network Interface page. Do not change any settings. Ensure that the High Availability mode check box is selected and that the HB1, HB2, and MIRROR information is correct.

r. Click Next.

   Result: The Ready to Configure screen appears.

s. Click Finish.

   Result: A dialog box prompts you to confirm the configuration.

t. Click OK to configure CallPilot.

   Result: The configuration is applied to the server. This task can take from 5 to 10 minutes to complete. The Configuration Wizard displays progress information.

   After the configuration is applied to the server, a dialog box reminds you to restart the server for the configuration to take effect.

u. Click OK to dismiss the dialog box.

   Result: The system returns you to the main CallPilot Manager screen.

v. Log off CallPilot Manager and close the Web browser.

25. Restart the CP2 server.
26. Ensure that both servers are completely started.
27. Bring the CallPilot resource group online on either of the two High Availability servers. For more information, see Bringing the CallPilot resource group online on page 176.

Working with domains and workgroups

Use the procedures in this section to work with domains and workgroups.

Moving from a domain to a workgroup

If the CallPilot 5.0 High Availability system must be moved to a workgroup (from a domain), use the following procedure to join a workgroup.

Joining a workgroup

This procedure assumes that CP1 is the active server and CP2 is the standby server.

1. On CP1, launch the AutoStart Console and stop monitoring. For more information, see Disabling automatic failovers (stop monitoring) on page 180.
2. Take the CallPilot resource group offline on CP1. For more information, see Taking the CallPilot resource group offline on page 177.
3. On CP1, do the following:

   a. Right-click My Computer.

      Result: The System Properties window appears.

   b. Select the Computer Name tab and click Change.

      Result: The Computer Name Changes window appears.

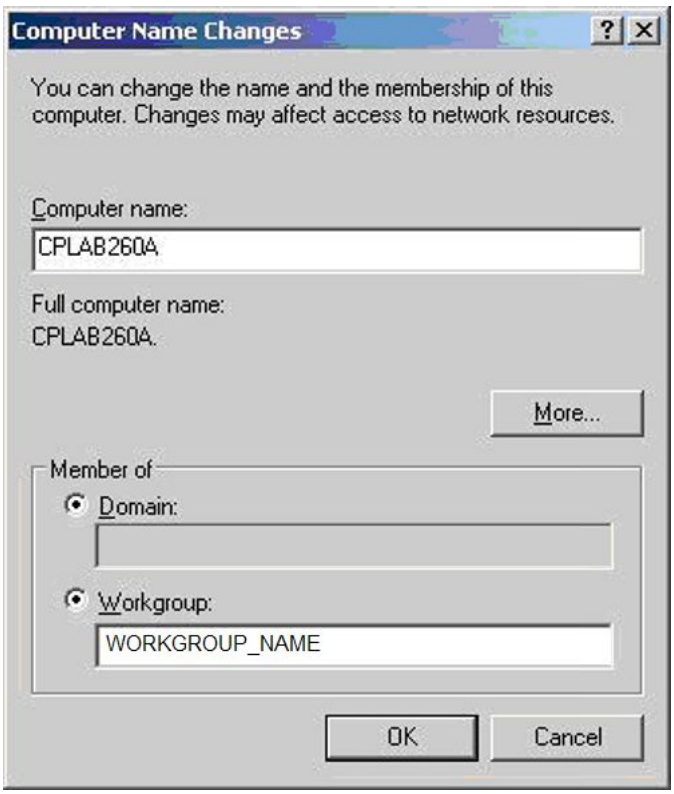


Figure 64: Computer Name Changes

c. In the Member of section, select the Workgroup option.

d. Enter the name of the workgroup and click OK.

   Result: The Domain Administrator Privileges window appears.

e. Enter the domain administrator and password.

   Contact your network administrator for this information.

   Result: The Welcome to Workgroup window appears.

f. Click OK.

   Result: A warning window appears prompting you to restart the computer in order for changes to take effect.

g. Click OK.

   Result: The System Properties window appears.

h. Click OK.

   Result: The System Settings Changes window appears prompting you to restart the computer.

i. Click Yes to restart CP1.

j. Log on to CP1 using the domain user account which is a member of the Workgroup Administrators group.

4. On CP2, do the following:
    a. Right-click My Computer.

       Result: The System Properties window appears.
    b. Select the Computer Name tab and click Change.

       Result: The Computer Name Changes window appears.
    c. In the Member of section, select the Workgroup option.
    d. Enter the name of the workgroup and click OK.

       Result: The Workgroup Administrator Privileges window appears.
    e. Enter the workgroup administrator and password.

       Contact your network administrator for this information.

       Result: The Welcome to Workgroup window appears.
    f. Click OK.

       Result: A warning window appears prompting you to restart the computer in order for changes to take effect.
    g. Click OK.

       Result: The System Properties window appears.
    h. Click OK.

       Result: The System Settings Changes window appears prompting you to restart the computer.
    i. Click Yes to restart CP2.
    j. Log on to CP2 using the domain user account which is a member of the Domain Administrators group.
5. On CP1, launch the AutoStart Console window.
6. Expand Domains.
7. Expand [AutoStart_Domain]. (This is the domain name created when the AutoStart agent was installed.)
8. Expand Utility Processes.

   Result: The Utility Processes are displayed:

   - DisableAOS
   - KillServices
   - LoadDN
   - LoadTSP
   - UnloadTSP
   - UnloadTSPOnStandbyServer

9. Select the DisableAOS Utility Process.
10. Select the Settings tab and to the following:
    a. Update the Domain, User Name, and Directory fields.
        - Domain must be the Windows domain that the CallPilot servers are on (if applicable) or the Windows workgroup in which the servers are located.
        - User name must be the domain administrator account for selected domain.
        - The default directory is D:\Nortel\Data\HA\HA_DB_Scripts.
    b. In the Login Info section, enter the password for the Windows administrator account in the Password and Confirm fields.

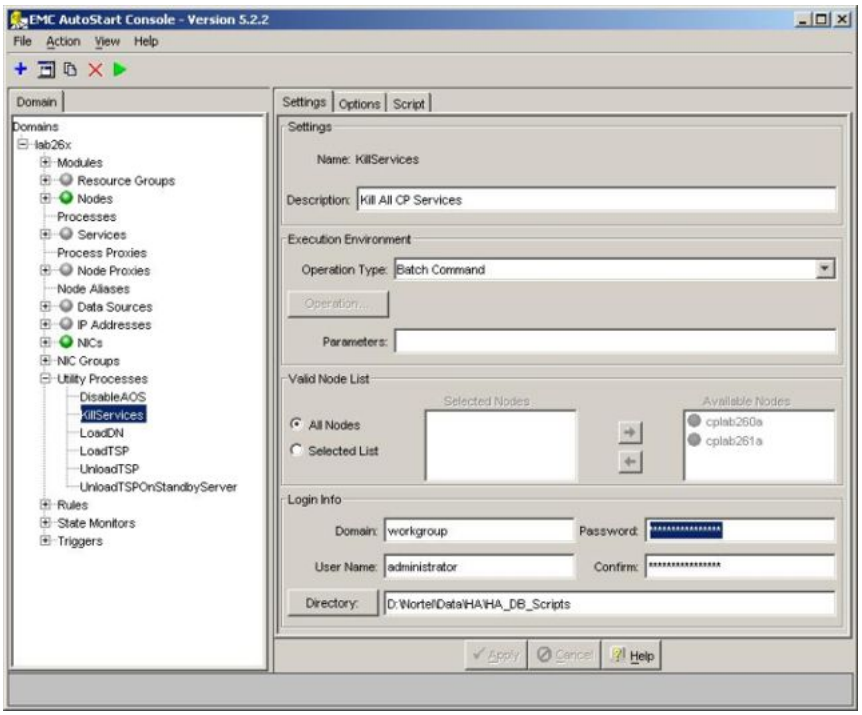


Figure 65: AutoStart Console - Utility Processes

    c. Click Apply.
11. Repeat Step 10 for each of the remaining Utility Processes.
12. On CP1, enable monitoring. For more information, see Enabling automatic failovers (start monitoring) on page 180.
13. Bring the CallPilot resource group online on CP1. For more information, see Bringing the CallPilot resource group online on page 176.

Manually change the administrator password

If you must change the password of the local administrator account or the password of the domain administrator account, the password must be changed on both High Availability servers.

Use the following procedure if you must change the password of the local administrator account or the password of the domain administrator account. The administrator password must be the same on both servers in the High Availability pair.

Manually changing the password of the local administrator account or the domain administrator account

1. On CP1 (the active High Availability server) do the following:
   a. Ensure the dongle is plugged into CP1. If the dongle is not on CP1, move it to CP1 and wait for 3 minutes.

      For more information about the dongle, see *1005r Server Hardware Installation* (NN44200-308) or *1006r Server Hardware Installation* (NN44200-320).
   b. Launch the AutoStart Console.
   c. Stop monitoring on the CallPilot resource group. For more information, see Disabling automatic failovers (stop monitoring) on page 180.
2. On CP1, press Ctrl+Alt+Del to display the Windows Security window.
3. Click Change Password.

   Result: The Change Password window appears.
4. Enter the User Name of the administrator account.
5. From the Log on to field, select one of the following:
   - If on a workgroup, select the local host name of the computer. For example, P1005r (this computer).
   - If on a domain, select the domain name associated with the computer. For example, avaya.innlab.com

     Note:

     If you are on a domain, both the local host name and the domain name are available in the Log on to drop-down list. Select the name you want to change.
6. Enter the Old Password.
7. Enter the New Password.
8. Reenter the new password in the Confirm New Password field.

9. Click OK.
10. Perform a manual failover on CP1. For more information, see Initiating a manual failover on page 181.

    Result: The CallPilot resource group is automatically brought online on the standby High Availability server (CP2).
11. Restart CP1.
12. Move the dongle to CP2.

    For more information about the dongle, see *1005r Server Hardware Installation* (NN44200-308) or *1006r Server Hardware Installation* (NN44200-320).
13. On CP2, do the following:

    a. Launch the AutoStart Console.

    b. Wait until node CP1 and both drvE and drvF are green/online in the AutoStart Console.

    c. If required, disable monitoring for the CallPilot resource group. For more information, see Disabling automatic failovers (stop monitoring) on page 180.
14. On CP2, press Ctrl+Alt+Del to display the Windows Security window.
15. Click Change Password.

    Result: The Change Password window appears.
16. Enter the User Name of the administrator account.
17. From the Log on to field, select one of the following:

    - If on a workgroup, select the local host name of the computer. For example, P1005r (this computer).
    - If on a domain, select the domain name associated with the computer. For example, avaya.innlab.com

    Note:

    If you are on a domain, both the local host name and the domain name are available in the Log on to drop-down list. Select the name you want to change.
18. Enter the Old Password.
19. Enter the New Password.
20. Reenter the new password in the Confirm New Password field.
21. Click OK.
22. Change the administrator password for each of the Utility Processes. For more information, see Changing the Utility Processes administrator password on page 132.
23. Perform a manual failover on CP2. For more information, see Initiating a manual failover on page 181.

Result: The CallPilot resource group is automatically brought online on the standby High Availability server (CP1).

24. After the CallPilot resource group is online on CP1, restart CP2.
25. On CP1, do the following:
    a. Launch the AutoStart Console.
    b. Wait until node CP2 and both drvE and drvF are online/green in the AutoStart Console.
    c. Enable monitoring for the CallPilot resource group. For more information, see Enabling automatic failovers (start monitoring) on page 180.

EMC AutoStart Agent and Console

The EMC AutoStart software is used to maintain a High Availability system. This section includes the following:

- AutoStart maintenance on page 153
- Work with resource groups on page 175
- Software operations on page 183

AutoStart maintenance

Use the procedures in this section to perform maintenance tasks within the EMC AutoStart software.

- Configure the AutoStart notification settings on page 154
- Add e-mail addresses to the Managed_ELAN_IP_Failure_Notif rule on page 156
- Configure failover on the Path Test failures of the Managed ELAN IP address on page 158
- License administration on page 160
- Check the status of the servers and failovers using AutoStart on page 161
- Import and export of the AutoStart Definition file on page 164
- Recreate the AutoStart definition file on page 167
- Change the Switch IP address in AutoStart Console on page 172

Configure the AutoStart notification settings

The AutoStart software can provide e-mail notification for failovers and resource group state changes. The Simple Mail Transfer Protocol (SMTP) server domain must first be configured for recipients to receive notification that a failover or state change has occurred.

Configuring the SMTP Server for a domain

1. From the AutoStart Console, select Domains > [AutoStart_Domain] for the domain that you want to monitor.
2. Select the Settings tab.

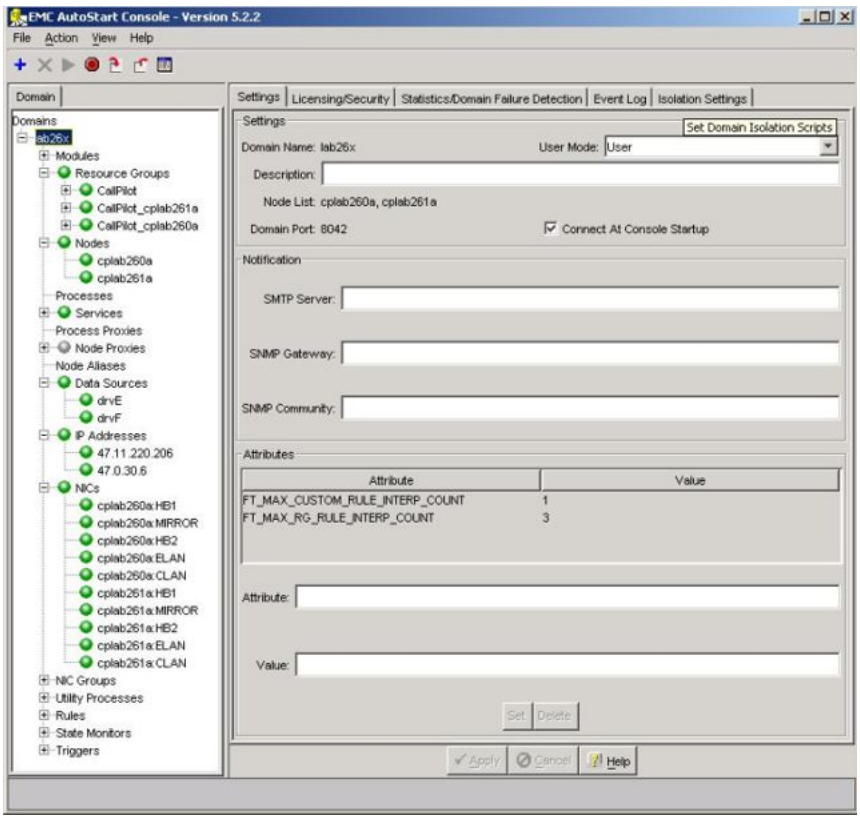


Figure 66: Setting the SMTP server attribute value

3. Under the Notification area, enter the SMTP Server, SMTP Gateway, and SMTP Community.
4. Under the Attributes area, click the attribute to edit.
5. In the Value field, enter the name of the SMTP server.

   For example, mail.servername.com.

6. Repeat for each attribute.
7. Click Apply.

   Result: When the SMTP server is in the domain attributes, the Send Email To text box (on the Options tab) becomes active. However, this value does not become active until the agents are restarted.

Configuring the User Notification Settings

1. Expand Domains > [AutoStart_Domain] > Resource Groups > CallPilot.
2. Select the Options tab.

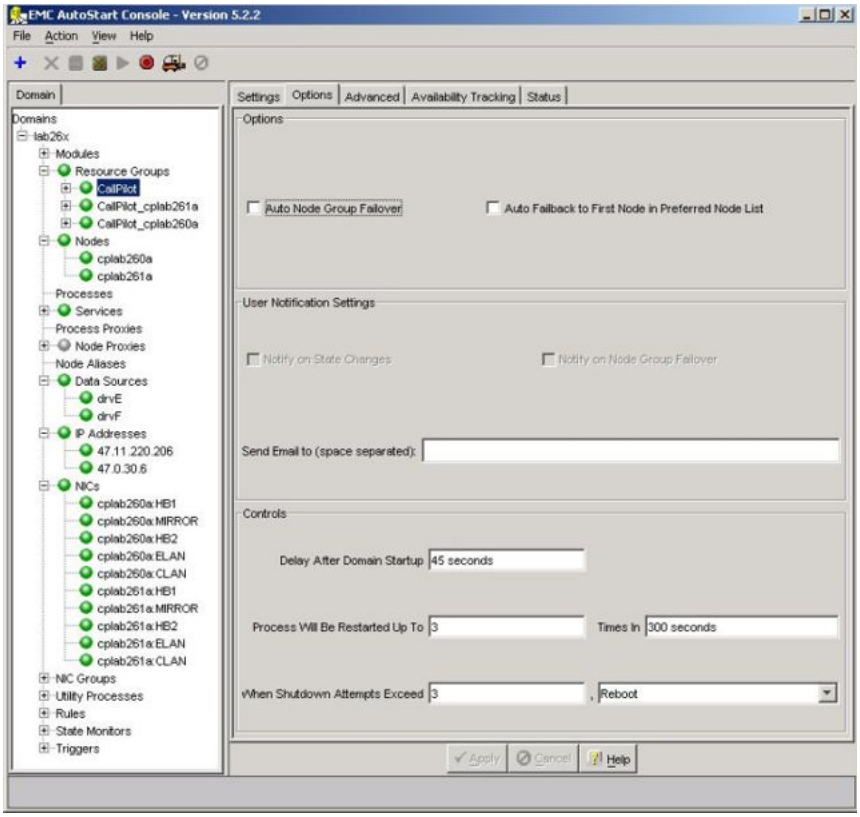


Figure 67: Options tab - User Notification Settings

3. To receive a notification e-mail that the state of a resource group has changed, do the following:

   a. In the Send Email to field, enter the e-mail addresses of those who must receive notification that a failover has occurred.

   b. Under the User Notification Settings, select the Notify on State Change check box.

4. To receive a notification e-mail when a node group failover occurs, do the following:

   a. In the Send Email to field, enter the e-mail addresses of those who must receive notification that a failover has occurred.

b. Under the User Notification Settings, select the Notify on Node Group Failover check box.

5. Click Apply.
6. Perform a manual failover to test if notification is received.

   See Initiating a manual failover on page 181.

Add e-mail addresses to the Managed_ELAN_IP_Failure_Notif rule

Use the following procedure to add e-mail addresses into the script of the Managed_ELAN_IP_Failure_Notif rule so that the AutoStart software can send out notification e-mail to the administrators when the Path Test failure of the Managed ELAN IP occurs.

Adding e-mail addresses to the Managed_ELAN_IP_Failure_Notif rule after the system is configured

1. Open the AutoStart Console.
2. Take the CallPilot resource group offline (if it is online). See Taking the CallPilot resource group offline on page 177.
3. On the left pane of the AutoStart Console, expand Rules.
4. Select Managed_ELAN_IP_Failure_Notif.

   Result: The Settings tab for the Managed_ELAN_IP_Failure_Notif rule appears.

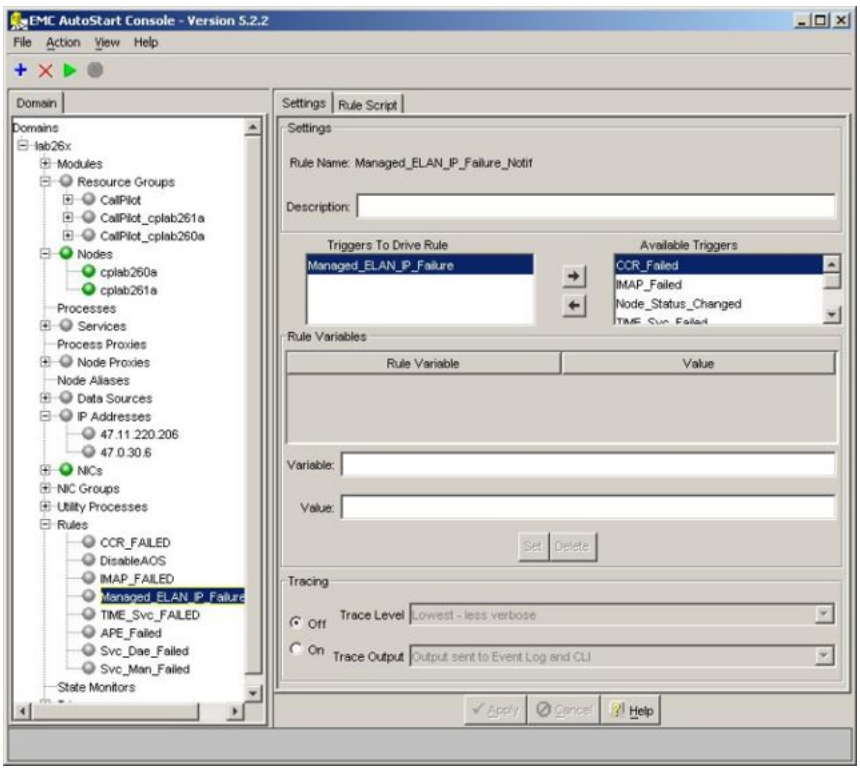


Figure 68: Rules - Managed_ELAN_IP_Failure_Notif

5. Select the Rule Script tab.

   Result: The rule script appears in the right pane of the AutoStart Console.

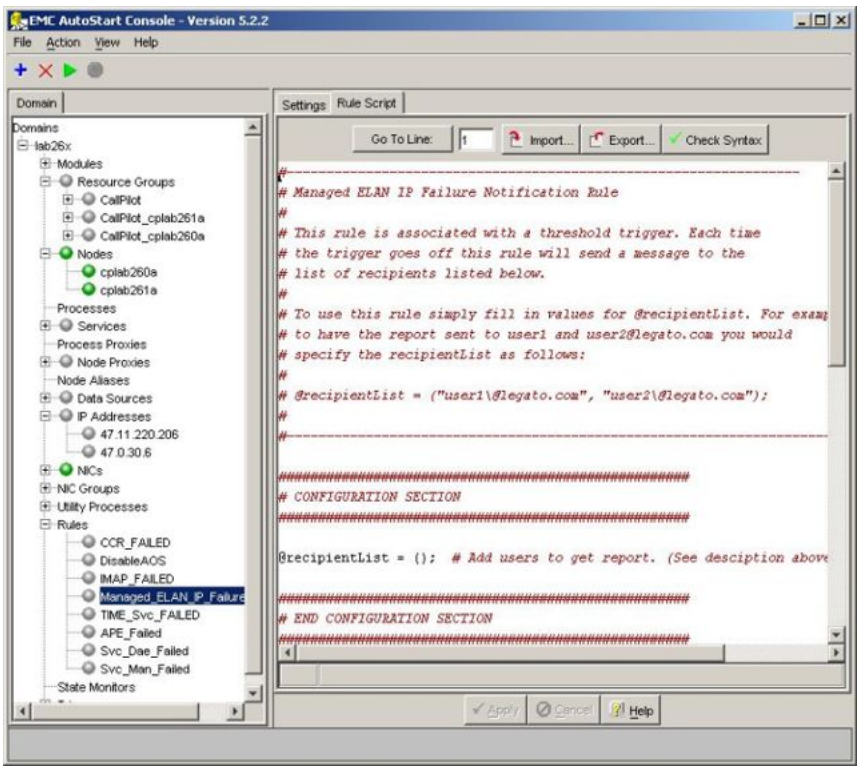


Figure 69: Rule Script tab for Managed_ELAN_IP_Failure_Notif rule

6. Look for the @recipientList = () line in the rule script.
7. Add the recipient's e-mail address in the parenthesis () of the @recipientList line. You must add the backslash symbol (\) before the at symbol (@) in the e-mail address.

   If multiple e-mail addresses are added, separate each e-mail address by a comma (,).
8. Click Apply.
9. Bring the CallPilot resource group online (if it was taken offline at the beginning of this procedure). See Bringing the CallPilot resource group online on page 176.
10. Configure the Simple Mail Transfer Protocol (SMTP) server so that the AutoStart software can provide e-mail notification for failovers and resource group state changes. The SMTP server domain must first be configured for recipients to receive notification that a failover or state change has occurred. See Configuring the SMTP Server for a domain on page 154.

Configure failover on the Path Test failures of the Managed ELAN IP address

There is a small chance (less than 1%) that the Midnight Audit will trigger a failover because of the very short switch ELAN down time if the High Availability system connects to a Meridian

1 51/61/81 switch instead of Meridian 1 Option 11C. Use the following procedure to configure failovers on the Path Test failures of the Managed ELAN IP address.

Configuring failovers on the Path Test failures of the Managed ELAN IP address

1. Open the AutoStart Console.
2. Expand Resource Groups.
3. Take the CallPilot resource group offline. See Taking the CallPilot resource group offline on page 177.
4. For the CallPilot resource group, select the Settings tab.
5. Select the Managed ELAN IP address. For example, 47.0.30.6 (as shown in the following figure).

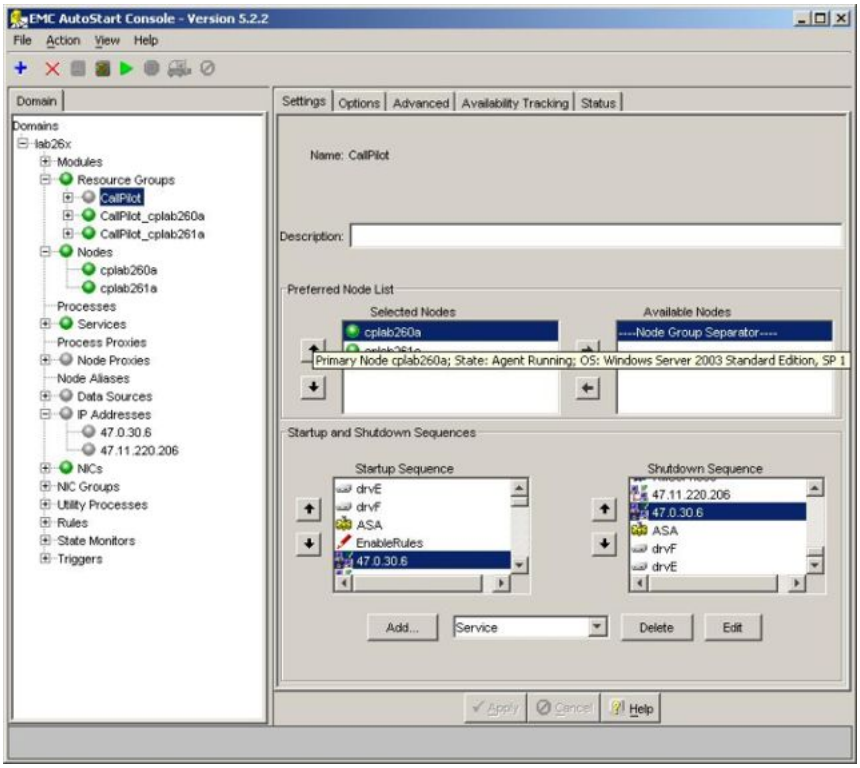


Figure 70: Settings tab - Managed ELAN IP address

6. Click Edit.

   Result: The IP Address Properties window appears.

Figure 71: IP Address Properties

7. Select the check boxes for both of the following options:
   - Relocate Resource Group on Path Failed State
   - Relocate Resource Group on Unassigned State
8. Click Apply.
9. Click Apply again on the Settings tab.
10. Bring the CallPilot resource group back online. See Bringing the CallPilot resource group online on page 176.

License administration

During the installation process, the AutoStart software is configured to use an AutoStart license key that is provided by Avaya with the CallPilot software. Use the following procedure to update the license key.

Updating the license key

1. On the CallPilot server, click Start > Programs > EMC AutoStart > EMC AutoStart Console 5.3 SP3 to start the AutoStart Console.

   Result: The AutoStart Console appears.
2. On the AutoStart Console window, click Domains > [AutoStart_Domain].
3. Select the Licensing/Security tab.
4. In the New License Key field, enter the new license key.

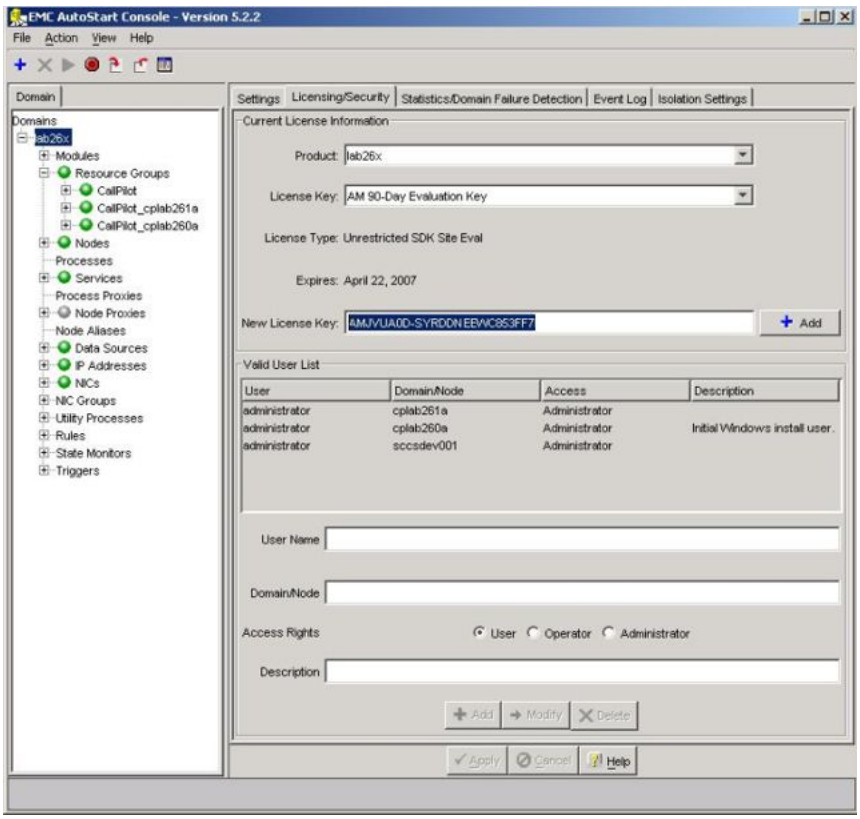


Figure 72: Licensing/Security tab - New License Key

5. Click Add.

   Result: The new license key is added to the list in the License Key field.
6. From the License Key list, select the newly entered license key.
7. Click Apply.

Check the status of the servers and failovers using AutoStart

Use the following procedures to check the status of the following:

- Server and failover status
- HB1, HB2, and Mirroring link status

Checking the status of the servers and failovers

1. On the Console window, expand Domains > [AutoStart_Domain] > Resource Groups > CallPilot.
2. Select the Status tab.

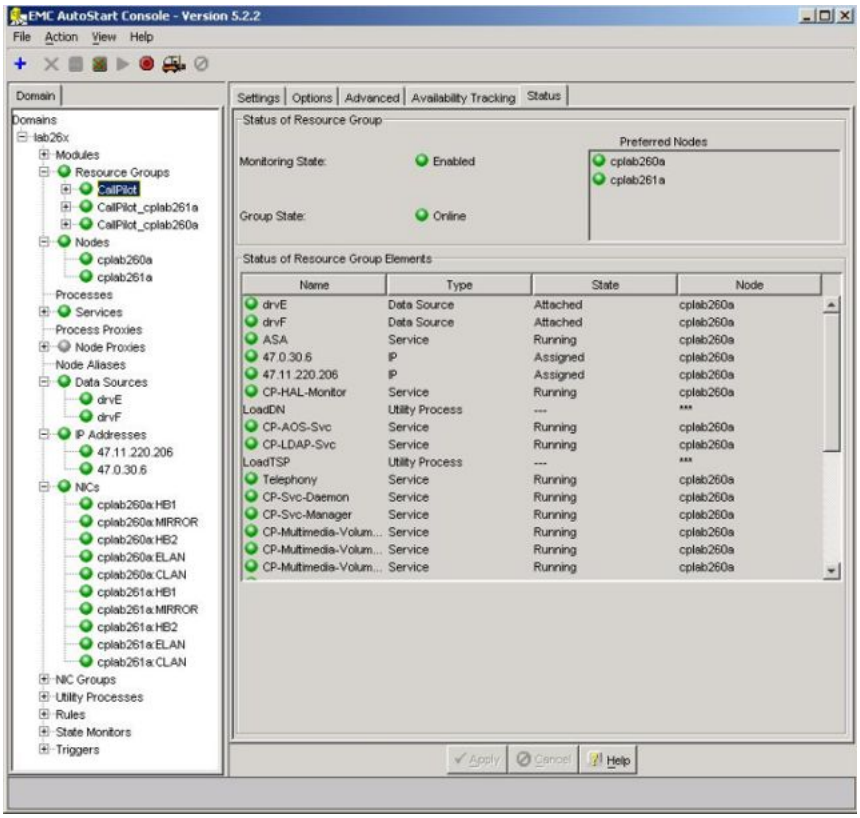


Figure 73: Status tab

Result: The fields in the Status of Resource Group area show the status of the system. The AutoStart Console users both icons and text to show system status (as described in the following two tables).

Table 10: Status of Resource Group fields

Field name	Status	Description
Monitoring State	Enabled	Automatic failover is enabled.
	Disabled	Automatic failover is disabled.
	Unknown	AutoStart is unable to determine the failover status.
Group State	Online	All resources under the current group on the current active server are up and working.

Field name	Status	Description
	Offline	All resources under the current group on the current active server are down.
	Online pending	Some resources under the current group on the current active server are up; however, some services are in either starting or stopping status.
Preferred Nodes		This area shows all the CallPilot servers and their overall status.

Status icons are displayed for each object to indicate the status of the object. The color of the icon describes the state of the object.

Table 11: Light status

Light	Status
Green	The object is online and in a working state.
Blue	The object is in a starting state.
Yellow	The object is in a warning state.
Yellow with a question mark	The object is entering warning state.
Red	The object has failed.
Red with a question mark	The object is failing.
Gray	The object is offline.

In the Status of Resource Group Elements area, the Node column shows on which server the CallPilot services are up and working. Usually this column shows one CallPilot server node name (active CallPilot server name) for all the resource group elements (although the node names do not have to be the same).

Checking the status of the HB1, HB2, and Mirroring links

1. On the AutoStart Console, expand Domain > [AutoStart_Domain] > NICs.

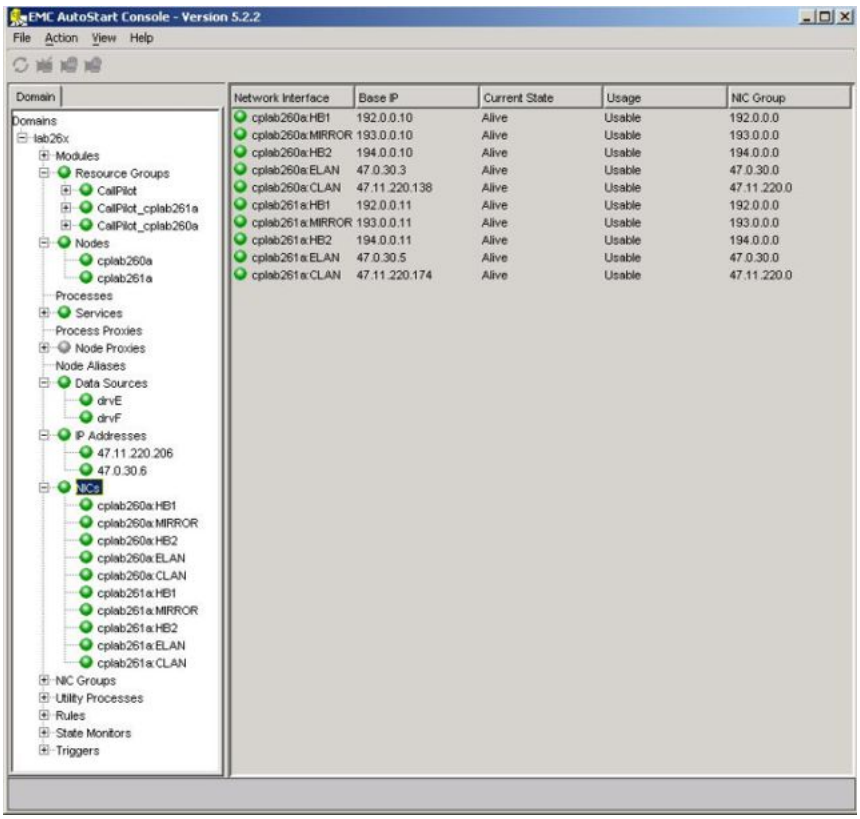


Figure 74: NICs

2. View the information in the right pane to check the status of the HB1, HB2, and Mirroring links. The status of the CLAN and ELAN is also displayed.

Import and export of the AutoStart Definition file

As part of the AutoStart configuration, the administrator imports the customized AutoStart Definition file on the AutoStart Console. It is also possible to export the AutoStart configuration data into a definition file as a backup after the AutoStart configuration. This section describes the procedures for importing and exporting the AutoStart Definition file.

Importing the AutoStart Definition file

1. On the AutoStart Console window, expand Domains.
2. Right-click the [AutoStart_Domain] and select Import Domain Information from the shortcut menu.

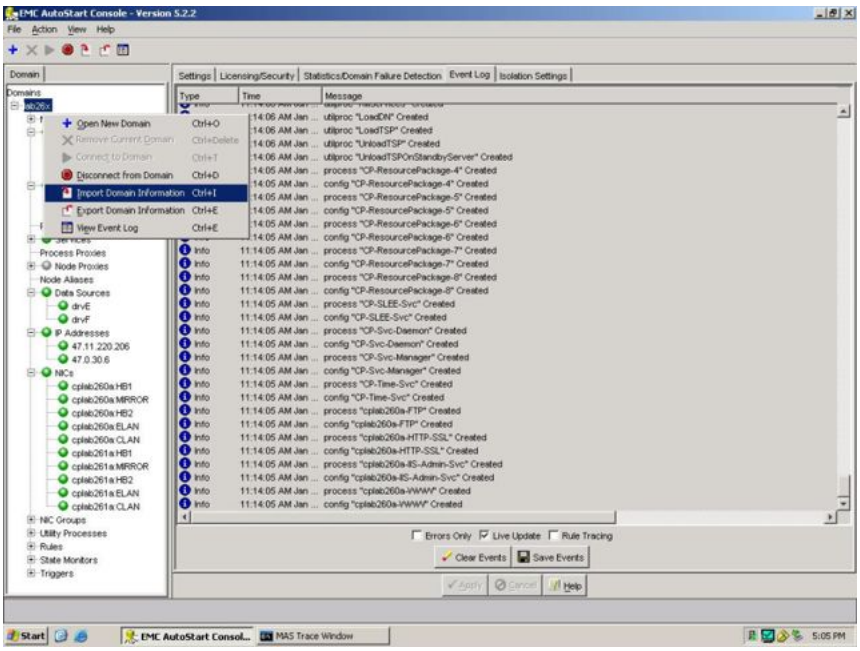


Figure 75: Import Domain Information

Result: The Import dialog box appears.

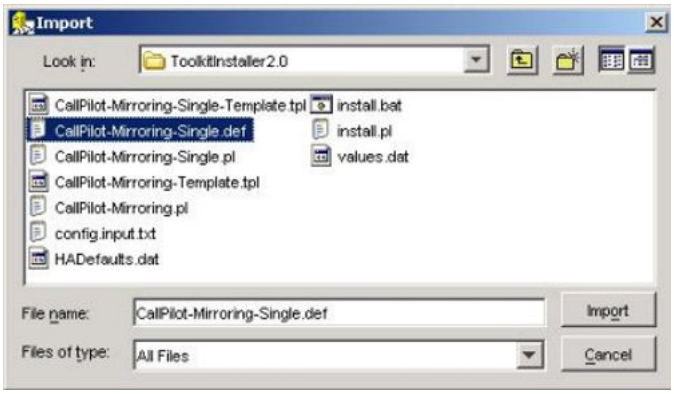


Figure 76: Import dialog box

3. Navigate to the D:\Nortel\HA\ToolkitInstaller2.0 folder (if that folder is not already open by default).
4. Select one of the following AutoStart definition files:
   - CallPilot-Mirroring-Single.def (for systems with one MPB96 board)
   - CallPilot-Mirroring.def (for systems with three MPB96 boards)
5. Click Import.

   Result: The import process takes up to one minute to complete.

Exporting the AutoStart Definition file

1. On the AutoStart Console window, expand Domains.
2. Right-click your [AutoStart_Domain] and select Export Domain Information from the shortcut menu.

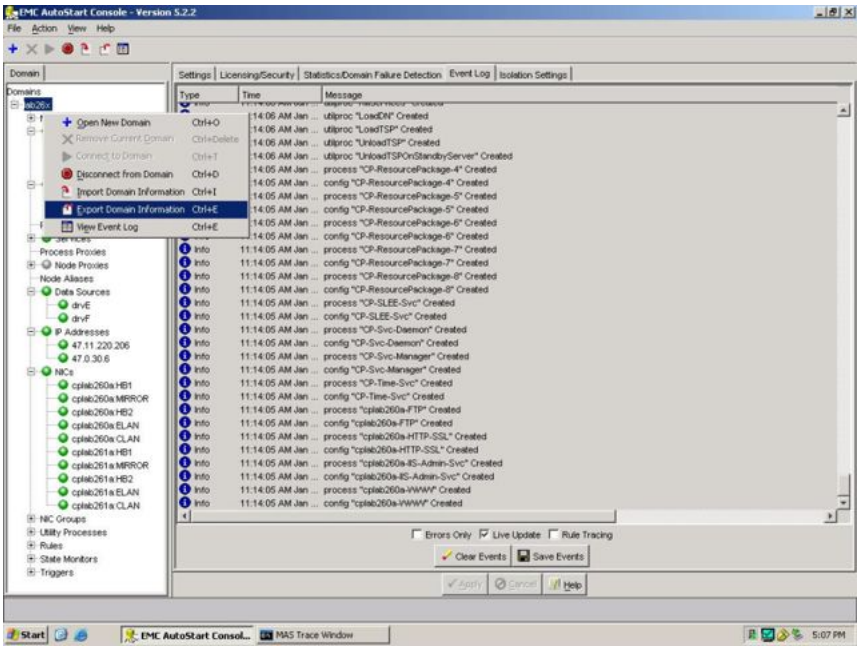


Figure 77: Export Domain Information

Result: The Export dialog box appears.

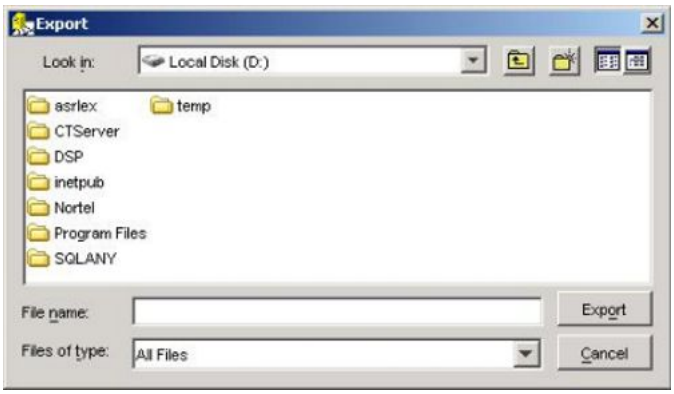


Figure 78: Export dialog box

3. Select the location and file name for the new definition file to be created.
4. Click Export to export the AutoStart configuration data into the new definition file.

Recreate the AutoStart definition file

Use the following procedure to recreate the AutoStart Definition file. To do this, you must do the following on the fully configured and running CallPilot 5.0 High Availability system:

- run the High Availability Wizard (HighAvailabilityConfigurationWizard.exe under D:\Nortel\HA)
- reimport the new definition file into AutoStart Console (*.def under D:\Nortel\HA\ToolkitInstaller2.0)

For example, you must use this procedure after installing the CallPilot 5.0 PEP, which replaces the AutoStart definition template files used to generate the definition file on the working CallPilot 5.0 High Availability systems.

Recreating the AutoStart definition file

1. Open the AutoStart Console on the High Availability server which had the original definition file previously imported into AutoStart.
2. Take the CallPilot resource group offline (if it is online). See Taking the CallPilot resource group offline on page 177.
3. In the left pane of the AutoStart Console, expand Resource Groups, right click the CallPilot resource group, and then click Delete Current Resource Group.

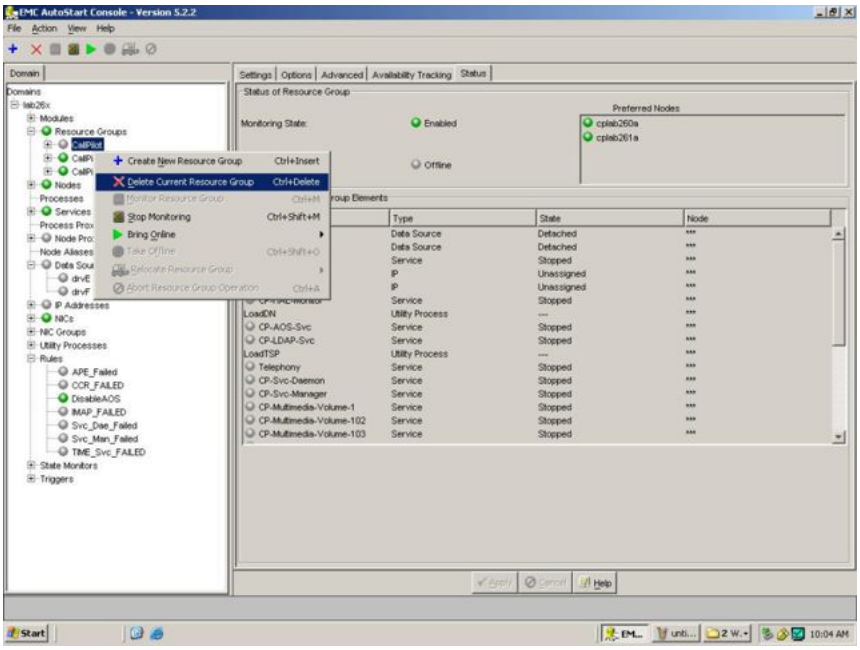


Figure 79: Delete CallPilot resource group

Result: The Confirm Delete of Resource Group window appears.

4. Click Yes to confirm the deletion of the CallPilot resource group.
5. In the left pane of the AutoStart Console, expand Data Sources, right click drvE, and then click Delete Current Data Source.

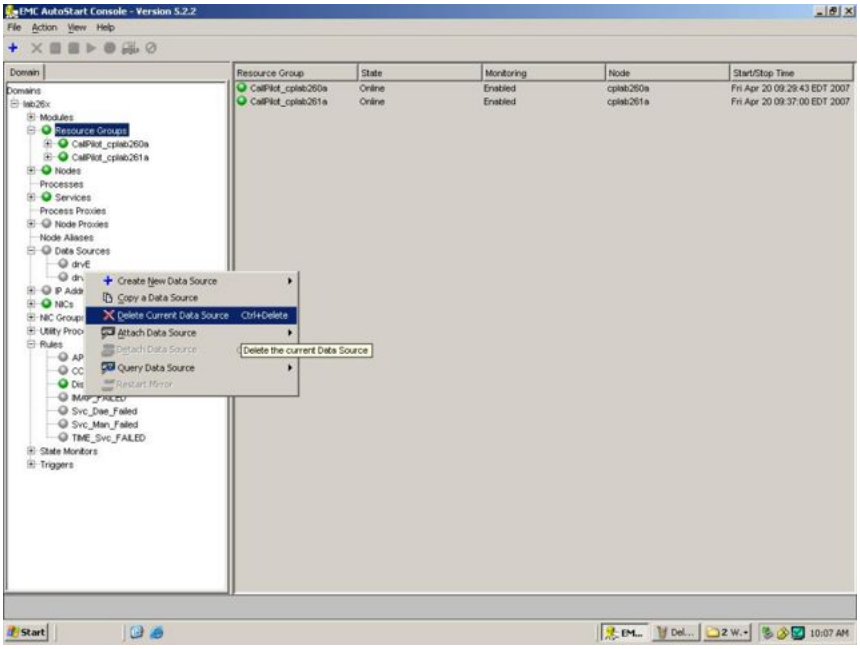


Figure 80: Delete drvE

Result: The Confirm Delete of Datasource window appears.

6. Click Yes to confirm the deletion of drvE.
7. In the left pane of the AutoStart Console, expand Data Sources, right click drvF, and then click Delete Current Data Source.

   Result: The Confirm Delete of Datasource window appears.

8. Click Yes to confirm the deletion of drvF.
9. In the left pane of the AutoStart Console, expand Rules, right click DisableAOS, and then click Disable Rule if the rule Disable Rule is enabled (in green).

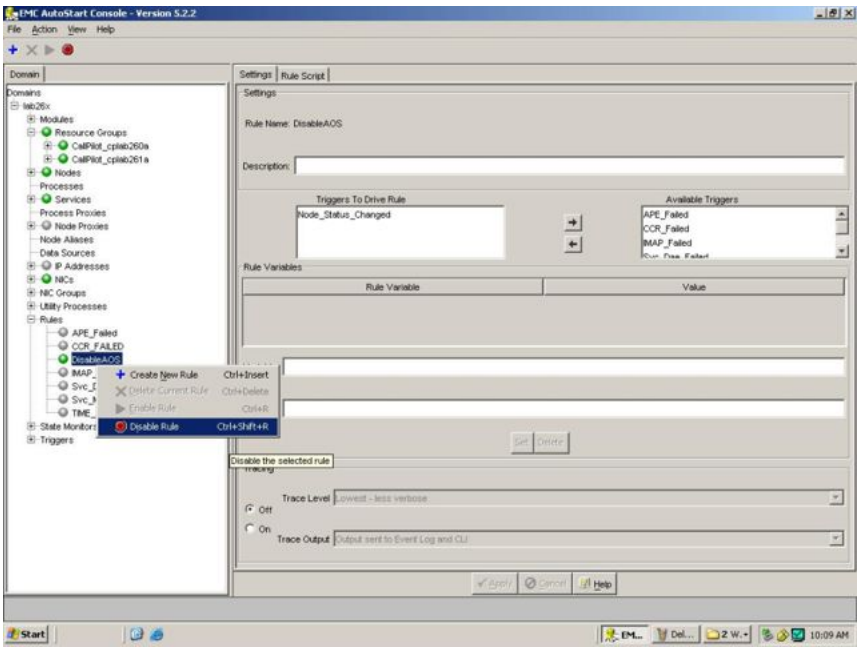


Figure 81: Disable Rule

Result: The Confirm Disable of Rule window appears.

10. Click Yes to confirm the disabling of the rule.
11. Navigate to D:\Nortel\HA folder.
12. Launch HighavailabilityConfigurationWizard.exe.

    Result: The High Availability Configuration Wizard appears.

13. Click the Reset button in the High Availability Configuration Wizard.

Note:

Do not close High Availability Configuration Wizard at this time. If you close High Availability Configuration Wizard, you must reenter the data requested by the High Availability Configuration Wizard.

14. Click Step 1: Get Node Information.
15. Click Step 2: Validate Node Information.

    Result: The Stage 1 Complete window appears if there are errors.

16. On the Stage 1 Complete window, click OK.
17. Close the High Availability Configuration Wizard.

    Result: The Confirm Exit Request window appears.

18. Click Yes.
19. Navigate to D:\Nortel\HA folder.
20. Launch HighavailabilityConfigurationWizard.exe.

Result: The High Availability Configuration Wizard appears.

21. Click Step 3: Generate Definition File.

    Result: The Phase 2 Complete window appears when the definition file has been successfully generated.

22. Click OK.
23. Close the High Availability Configuration Wizard.

    Result: The Confirm Exit Request window appears.

24. Click Yes.
25. In the AutoStart Console, right click the [AutoStart_Domain] name and then click Import Domain Information.

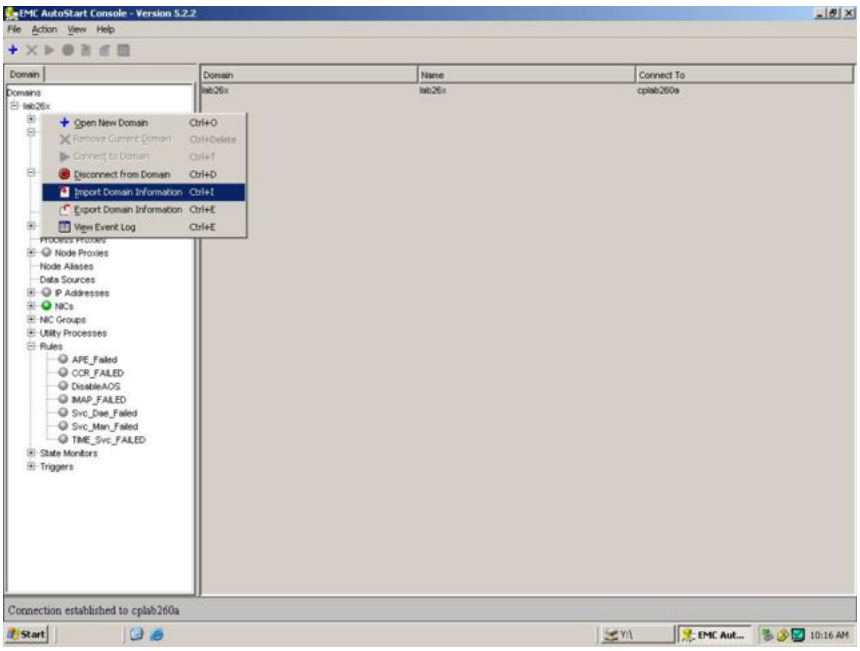


Figure 82: Import Domain Information

Result: The Import dialog box appears.

26. Under the D:\Nortel\HA\ToolkitInstaller2.0 folder, select the new definition file, and then click Import.

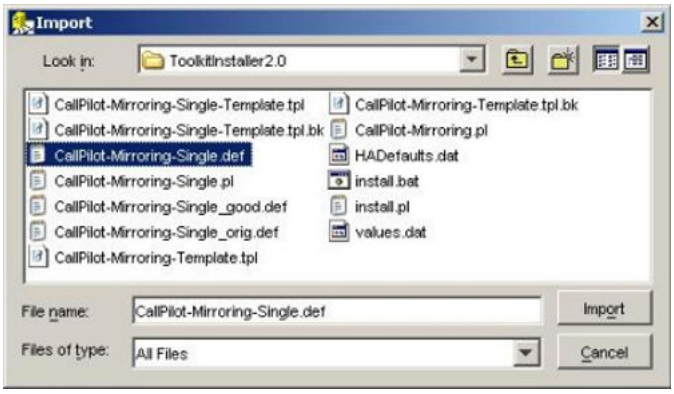


Figure 83: Import dialog box

27. Wait for approximately one minute.
28. Verify that the import was successful:
    - the drvE and drvF data sources are created.
    - the CallPilot resource group is created
    - no error message or warning message appears in the information bar at the bottom of the AutoStart Console

    Also check that any new items or new settings introduced by the new definition file are created. For example, the new trigger Managed_ELAN_IP_Failure and the new rule Managed_ELAN_IP_Failure_Notif.

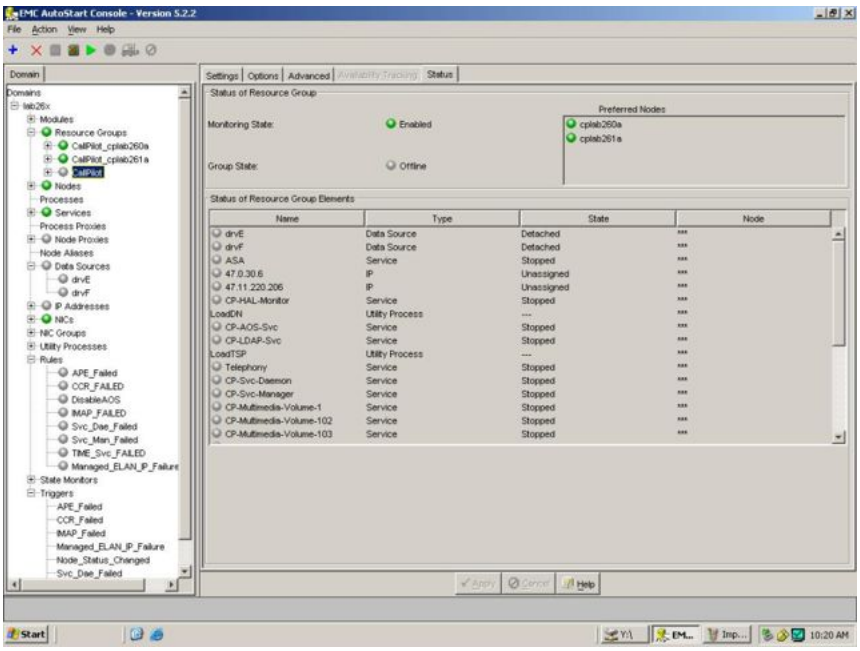


Figure 84: Successful import

29. In the left pane of the AutoStart Console, expand Utility Processes, and update the Login Information (Password, Domain name, and User name) on the Settings tab of each utility process under Utility Processes (DisableAOS, KillServices, LoadDN, LoadTSP, UnloadTSP, and UnloadTSPOnSandbyServer). See Adding the

Windows administrator account password for the AutoStart Utility Processes on page 89.

30. Bring the CallPilot resource group online. See Bringing the CallPilot resource group online on page 176.

Change the Switch IP address in AutoStart Console

If the switch IP address is changed, you must update the switch IP address in multiple locations:

- The switch IP address used in NIC Group Test IP on the Testing Options page of the ELAN NIC group.
- The switch IP address used on the Network Isolation Addresses list on the Isolation Settings page of the AutoStart domain.
- The switch IP address used in the list IP Addresses to Test on the Network Path Testing page of the Virtual ELAN IP Address (Managed ELAN IP Address) on AutoStart Console.

If the switch IP has to be changed, you must use the following procedure to update the switch IP on a CallPilot 5.0 High Availability system.

Changing the switch IP address

1. Disable the monitoring on the AutoStart Console.

   For more information, see Disabling automatic failovers (stop monitoring) on page 180.
2. Change the ELAN IP address on the switch.
3. Expand NIC Groups on the left pane of the AutoStart Console.
4. Select the NIC group with the ELAN subnet IP address.
5. Click the Testing Options tab.

   Result: The Testing Options page appears.
6. In the NIC Group Test IPs area, select the NIC Group Test IP address that has the old switch IP address.

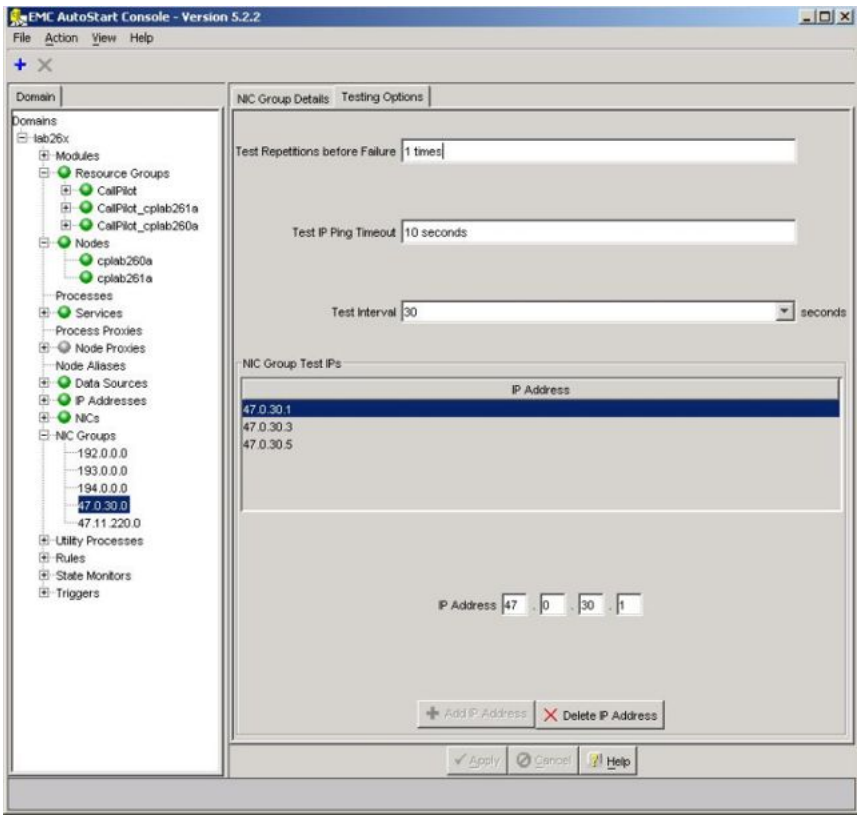


Figure 85: Testing Option tab

7. Click Delete IP Address to delete the old IP address.
8. Enter the new switch IP Address.
9. Click Add IP Address.
10. Click Apply.
11. In the AutoStart Console, select the [AutoStart_Domain].
12. Click the Isolation Settings tab.

    Result: The Isolation Settings page appears.
13. In the Network Isolation Addresses area, select the old switch IP address from the IP Address list.

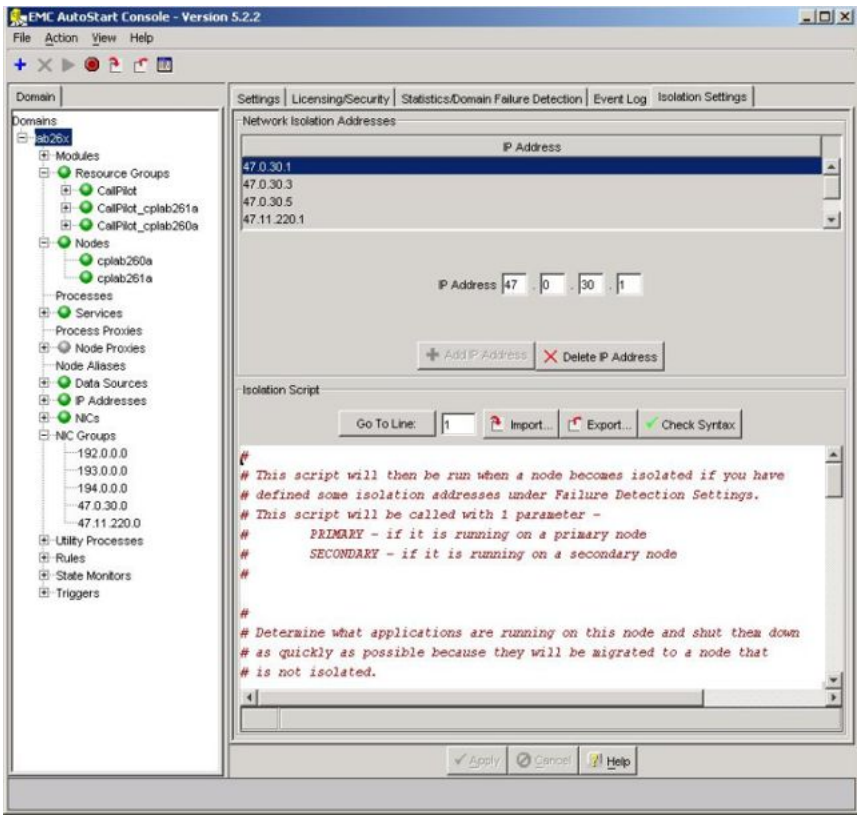


Figure 86: Isolation Settings tab

14. Click Delete IP Address.
15. Enter the new switch IP Address.
16. Click Add IP Address.
17. Click Apply.
18. In the AutoStart Console, expand IP Addresses.
19. Click the IP Address that is the Managed ELAN IP address.
20. Click the Network Path Testing tab.

    Result: The Network Path Testing page appears.
21. In the IP Address to Test area, select the old switch IP address from the IP Address list.

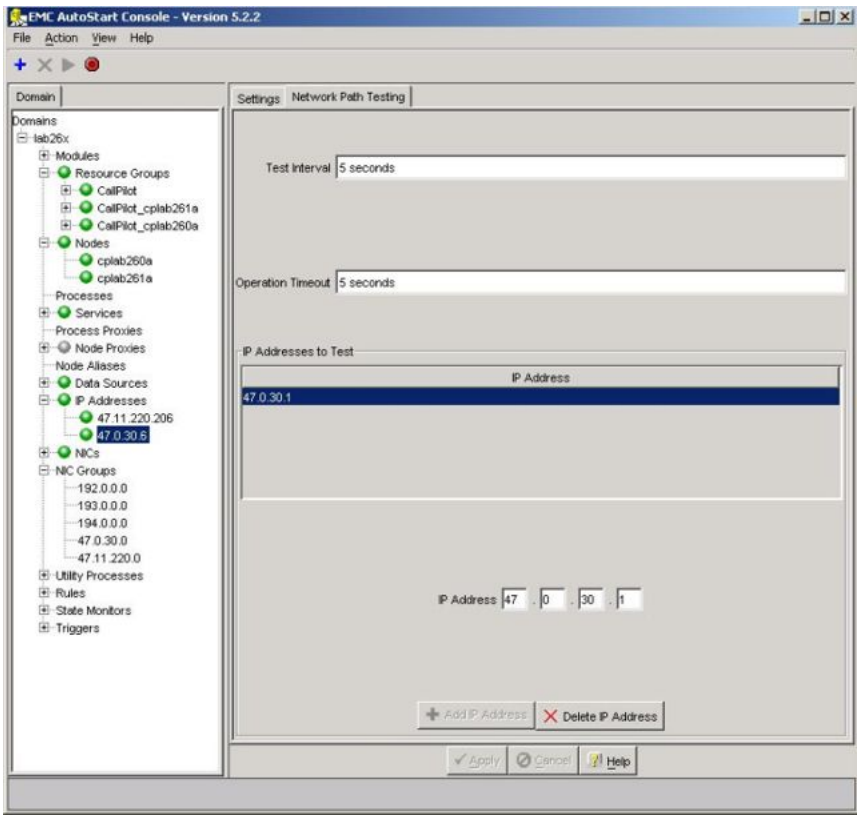


Figure 87: Network Path Testing tab

22. Click Delete IP Address to delete the old IP address.
23. Enter the new switch IP Address.
24. Click Add IP Address.
25. Click Apply.

Work with resource groups

A resource group is a collection of resources (such as CallPilot services, disks, scripts) that must be managed as a group.

This section includes the following procedures:

- Bring a resource group online on page 176
- Take a resource group offline on page 177
- Perform failovers and monitoring on page 179

Bring a resource group online

You must bring all the AutoStart resource groups online to make the CallPilot 5.0 High Availability system work after importing the AutoStart definition file (which is imported to configure AutoStart environment).

Use the following procedure to bring a resource group online by bringing the CallPilot resource group online.

Bringing the CallPilot resource group online

1. On the AutoStart Console window, select Domains > Resource Groups.
2. Right-click the CallPilot resource group.
3. From the shortcut menu, select the Bring Online option, and then select the node name on which the CallPilot resource group will be brought up.

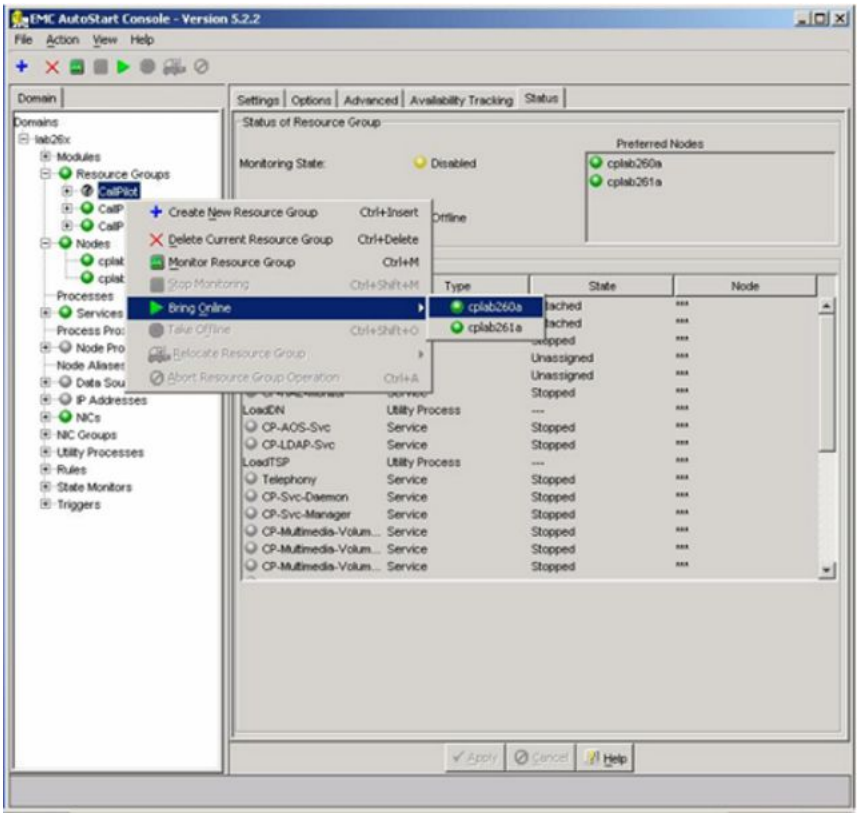


Figure 88: CallPilot resource group - Bring Online

4. Wait until the Group State turns green and shows Online. This can take a few minutes.

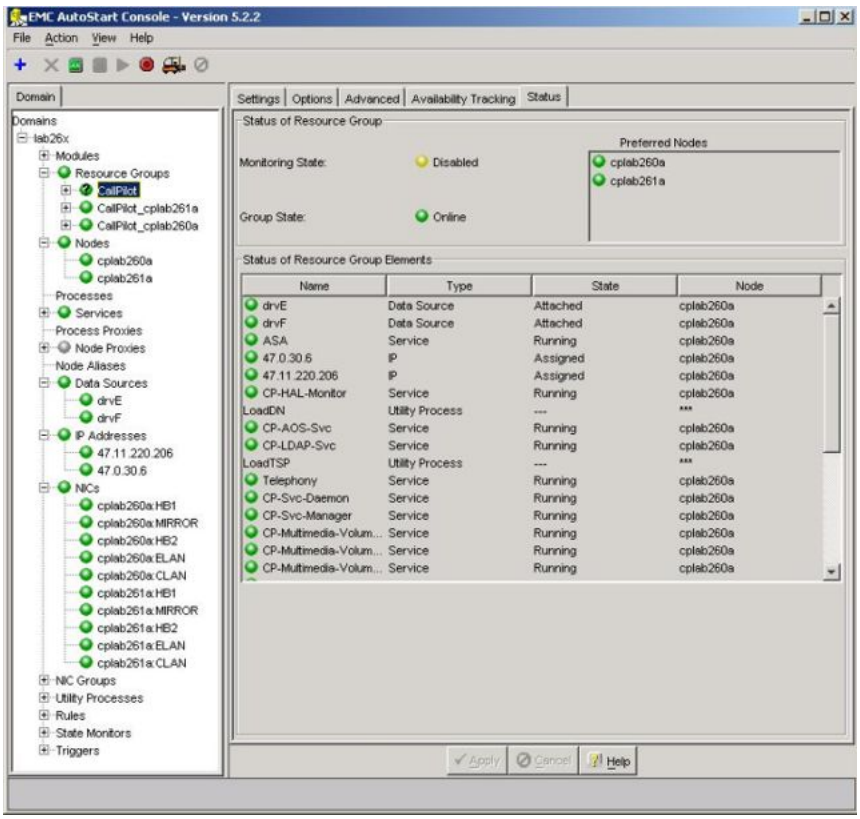


Figure 89: CallPilot resource group is online

Take a resource group offline

The failover CallPilot resource group CallPilot is occasionally taken offline for maintenance. After the CallPilot resource group is taken offline, the following occurs:

- There is no access to the mirrored drives (that is, no access to the CallPilot database and MMFS volumes).
- All services are stopped.
- The Windows operating system continues to function (along with IIS and WWW).

Use the following procedure to take a resource group offline by taking the CallPilot resource group offline.

Taking the CallPilot resource group offline

1. On the AutoStart Console window, select Domains > Resource Groups.
2. Right-click the CallPilot resource group.
3. From the shortcut menu, select the Take Offline option.

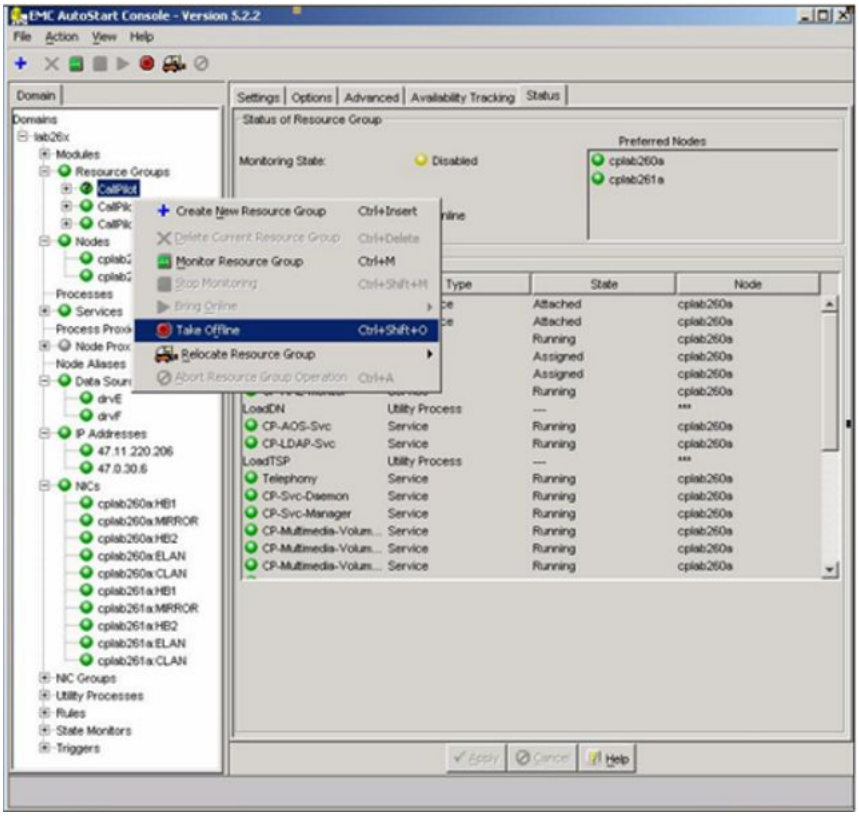


Figure 90: CallPilot resource group - Take Offline

4. Wait until the Group State turns gray and shows Offline. This can take a few minutes.

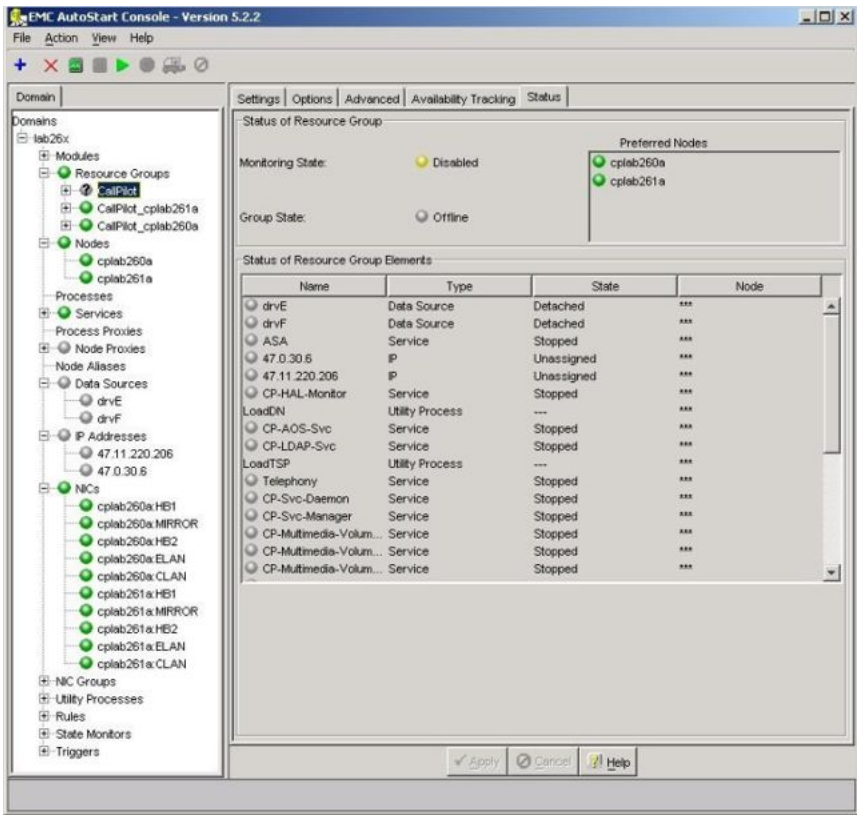


Figure 91: CallPilot resource group is offline

Perform failovers and monitoring

Use the procedures in this section to enable and disable automatic failovers, and to initiate a manual failover.

Automatic failovers

When performing maintenance on the active or standby server, it can be necessary to temporarily disable automatic failovers from the active to the standby CallPilot server. You can later enable the automatic failover.

Using the AutoStart console software, you can disable and enable automatic failovers by performing the following procedures.

Disabling an automatic failover is the same as stopping monitoring, and enabling an automatic failover is the same as starting monitoring.

Disabling automatic failovers (stop monitoring)

Assumption: This procedures assumes that automatic failovers are currently enabled.

1. On AutoStart Console window, expand Domains > [AutoStart_Domain] > Resource Groups and then select CallPilot.
2. Click the Status tab.
3. Right-click Resource Groups > CallPilot.
4. From the shortcut menu, select Stop Monitoring.

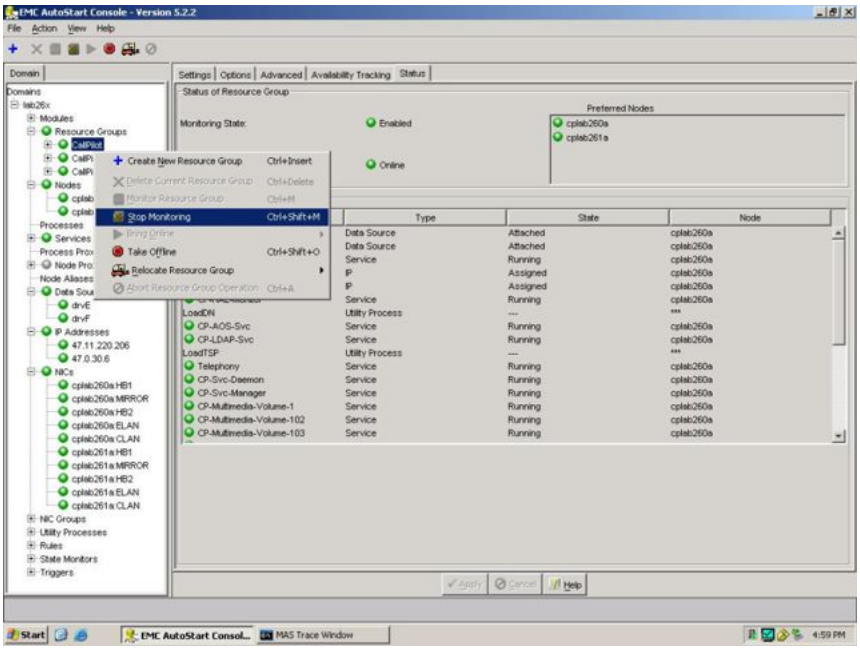


Figure 92: Stop Monitoring

Result: On the Status tab, the Monitoring State turns to yellow and shows a status of Disabled. On the Domains pane, the Resource Groups > CallPilot changes to a green light with a black question mark. The automatic failover is disabled.

Enabling automatic failovers (start monitoring)

Assumption: This procedure assumes that automatic failovers are currently disabled.

1. On the AutoStart Console window, expand Domains > [AutoStart_Domain] > Resource Groups and then select CallPilot.
2. Click the Status tab.
3. Right-click Resource Groups > CallPilot.
4. From the shortcut menu, select Monitor Resource Group.

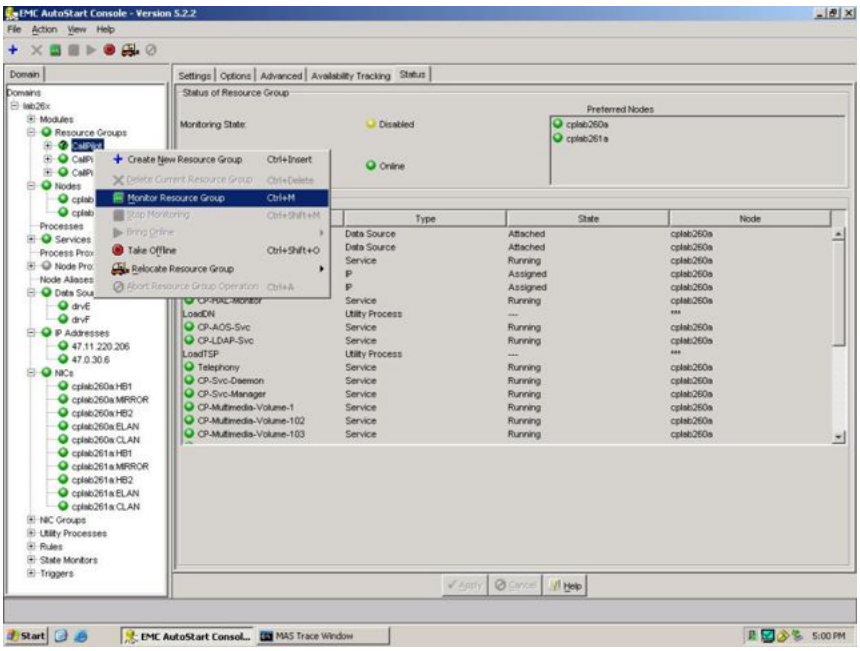


Figure 93: Monitor Resource Group

Result: On Status tab, the Monitoring State turns to green and shows a status of Enabled. On the Domains pane, the Resource Groups > CallPilot changes to green. The automatic failover is enabled.

Manual failovers

If you are the administrator, you can perform a manual failover if there is a problem on the active CallPilot server that is not detected by the automatic failover rules.

Initiating a manual failover

1. On the AutoStart Console window, expand Domains > [AutoStart_Domain] > Resource Groups and then select CallPilot.
2. Click the Status tab.

   Result: The Status tab shows the status of the Resource Groups. For this procedure, the CallPilot server cplab261a is used as an example. Notice that this server is active (green and shows Online).
3. Right-click Resource Groups > CallPilot.
4. On the shortcut menu, select Relocate Resource Group, and then select the <standby CallPilot server>. (This server is the standby CallPilot server.)

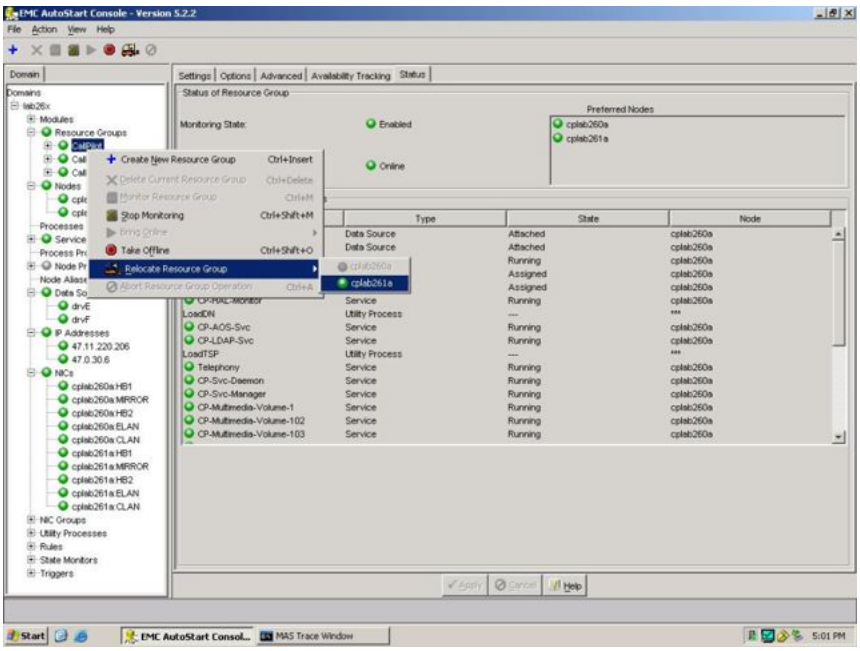


Figure 94: Status tab

Note:

This action stops the CallPilot services on the active server. This action also puts the standby server in service (that is, makes it the active server).

Result: The Confirm Relocated of Resource Group dialog box appears.

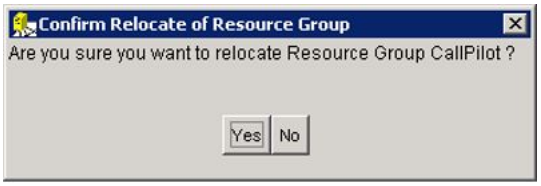


Figure 95: Confirm Relocate of Resource Group

5. Click Yes.

   Result: The failover starts in seconds. It takes more than 10 minutes to finish the failover to the standby server if the CallPilot Diagnostic Tools are enabled, or less than 5 minutes if the CallPilot Diagnostic Tools are disabled. (Start > Programs > CallPilot > System Utilities > Diagnostic Tools)

Software operations

Use the following procedures to install, uninstall, and reinstall the EMC AutoStart software.

- Install the AutoStart Console on a stand-alone PC on page 183
- Uninstall the AutoStart software on page 192
- Reinstall the AutoStart software on page 195
- EMC software updates (AutoStart Agent/Console) on page 195

Install the AutoStart Console on a stand-alone PC

The AutoStart Console is used to administer the AutoStart Agent that provides the mirroring and heartbeat signals between the active and standby CallPilot servers. The AutoStart Console also provides the managed (virtual) IP service that is used on the CLAN and ELAN to mask the fact that there are two different servers.

By default, the AutoStart Console software is installed on both CallPilot servers. However, it is possible to install the AutoStart Console software on a stand-alone PC.

After the AutoStart Console is installed on a stand-alone PC, it can be used to manage multiple pairs of CallPilot High Availability servers (that is, multiple AutoStart domains). Use the following procedure to install the AutoStart Console software on a stand-alone PC for administration of the Avaya server subnet (CLAN).

Installing the AutoStart Console on a stand-alone PC

1. Insert the CallPilot Application CD.
2. Navigate to the Z:\EMC folder on the CallPilot Application CD.
3. Double-click EMC_AutoStart_5.3_SP3_Update.exe to unpack the archive in theD:\temp folder.

   Result: Three files are unpacked into the D:\temp \EMC_AutoStart_5.3_SP3_Update folder: EAS53_WIN_x86.exe, EAS53SP3_WIN_x86.exe, EMC AutoStart Update Process.pdf
4. Double-click EAS53SP3_WIN_x86.exe to start the installation.

   Result: The installShield Wizard informs you that AutoStart 5.3 SP3 software is preparing to install (install preparation can take a few minutes). After preparation is complete, the Welcome window appears.

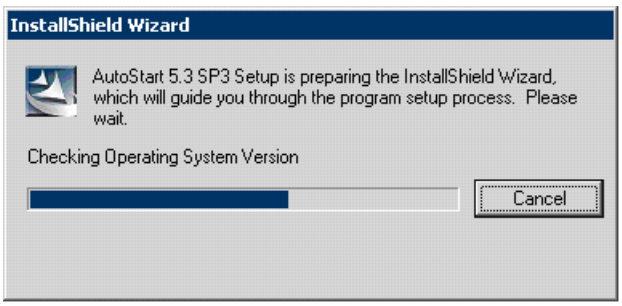


Figure 96: InstallShield Wizard - Preparing to install AutoStart 5.3 SP3 software

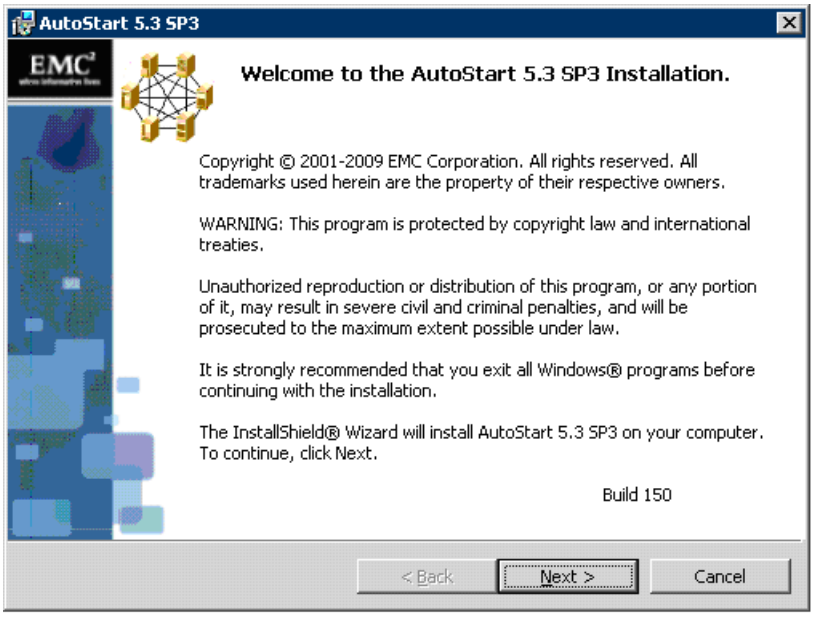


Figure 97: Welcome window

5. Click Next.

   Result:AutoStart 5.3 SP3 reminder to read the documents appears.

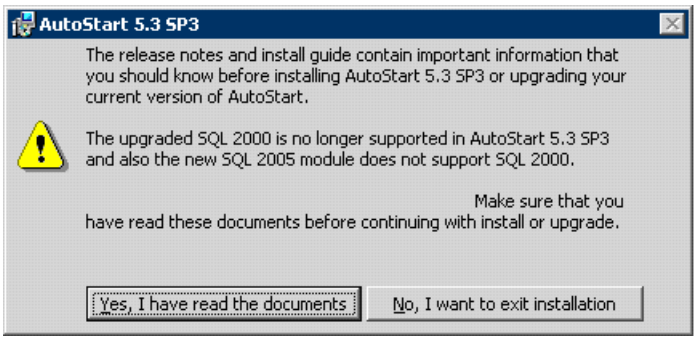


Figure 98: Reminder to read the documents

6. Click Yes, I have read the documents.

   Result: AutoStart 5.3 SP3 reminder is closed.

7. Click Next on the Welcome window.

   Result: The License Agreement window appears.

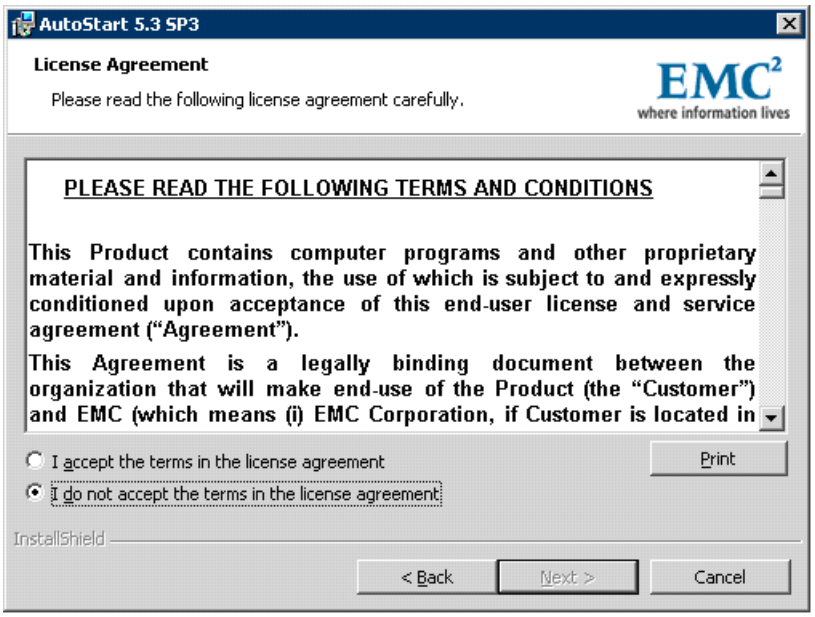


Figure 99: License Agreement window

8. Select the I accept the terms in the license agreement option.
9. Click Next.

   Result: The Custom Setup window appears.

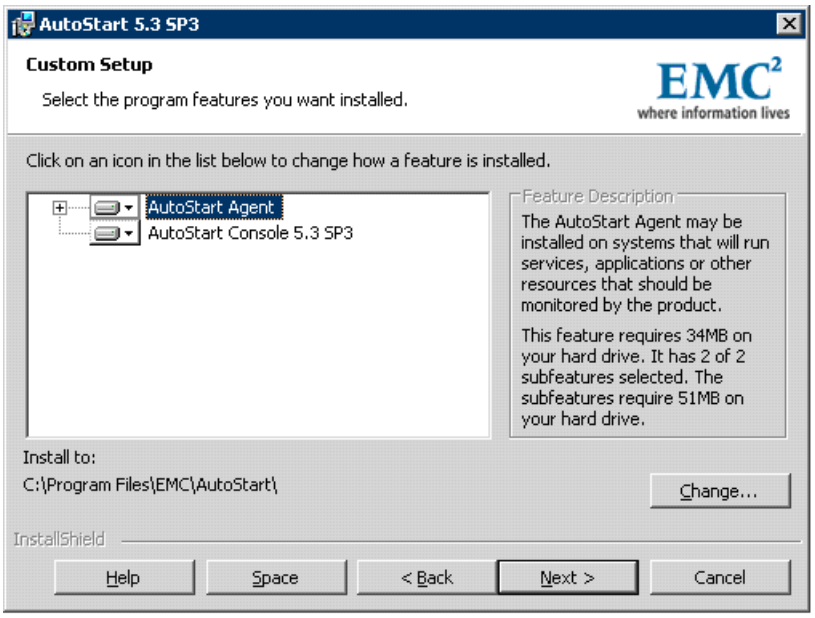


Figure 100: Custom Setup window

10. Click the AutoStart Agent drop-down list and then select This feature will not be available.

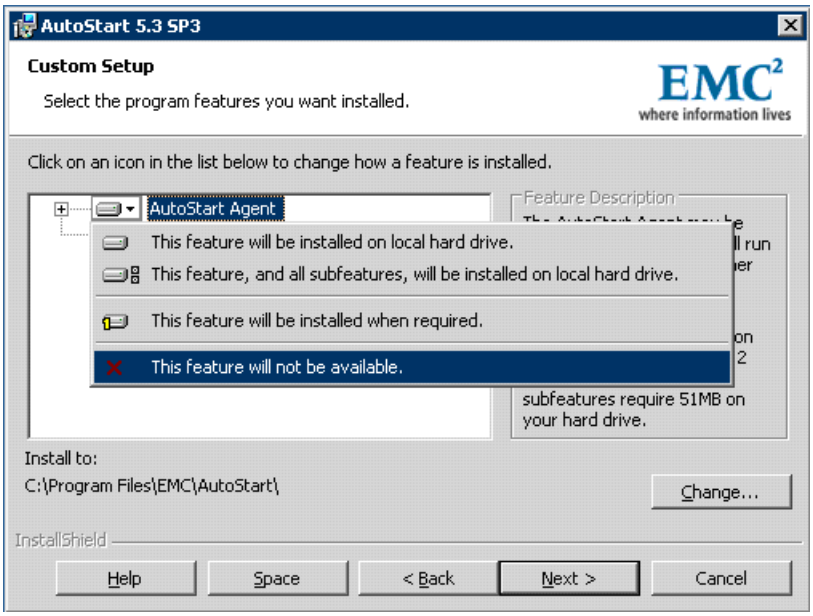


Figure 101: Custom Setup - AutoStart Agent configuration

Result: The Custom Setup window shows a red X next to AutoStart Agent option.

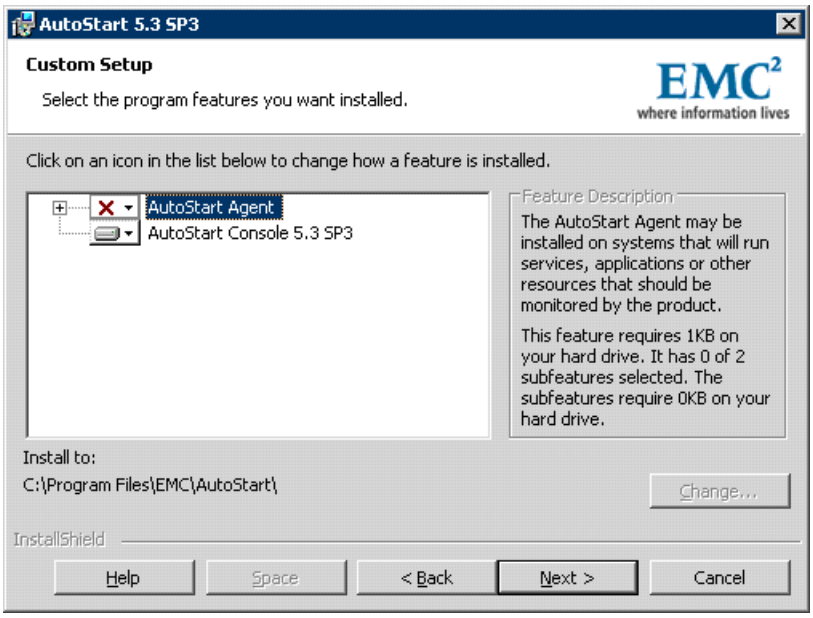


Figure 102: Custom Setup - AutoStart Agent will not be installed

11. Select the AutoStart Console 5.3 SP3 from the list.

    Result: The Change button is highlighted.

12. Click the Change button to change the installation path.

Result: The Change Current Destination Folder dialog box appears.

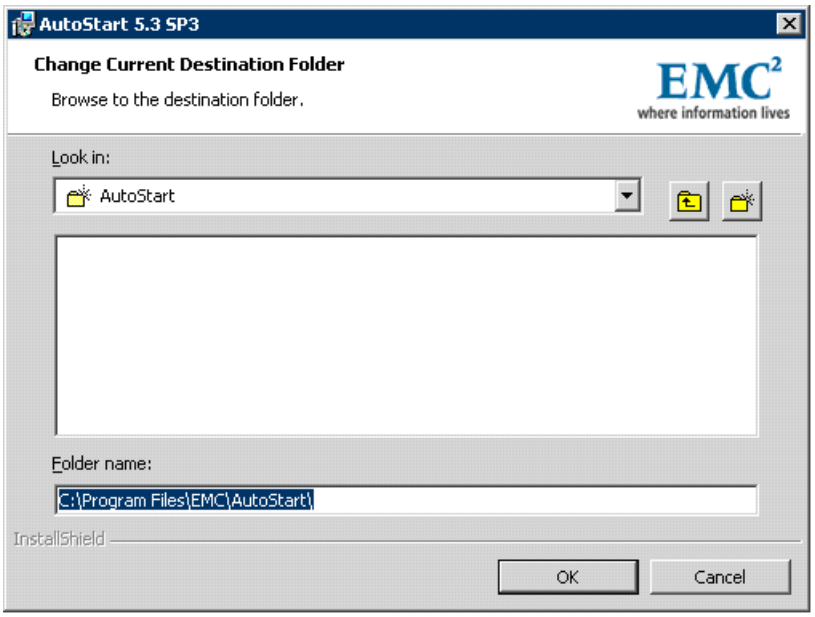


Figure 103: Change Current Destination Folder dialog box

13. In the Folder name field, change the drive letter from C to D, change the path to: D:\Program Files\EMC AutoStart\

    Important:

    You must install the software in the D:\Program Files\EMC AutoStart\ directory or the software does not work correctly.

14. Click OK

    Result: The Change Current Destination Folder dialog box closes and you are returned to the Custom Setup window, which shows the correct installation path.

15. Click Next

    Result: The Confirm Settings window appears.

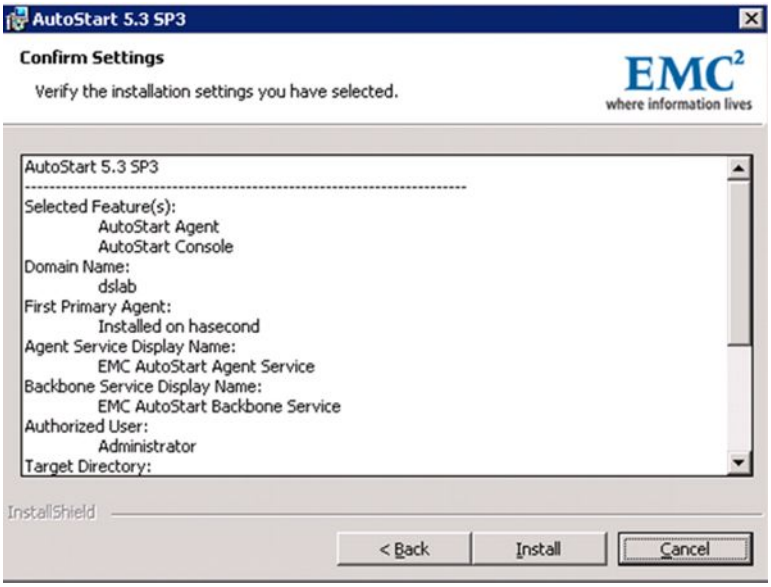


Figure 104: Confirm Settings window

16. Click Install.

    Result: The Installing AutoStart 5.3 SP3 window appears.

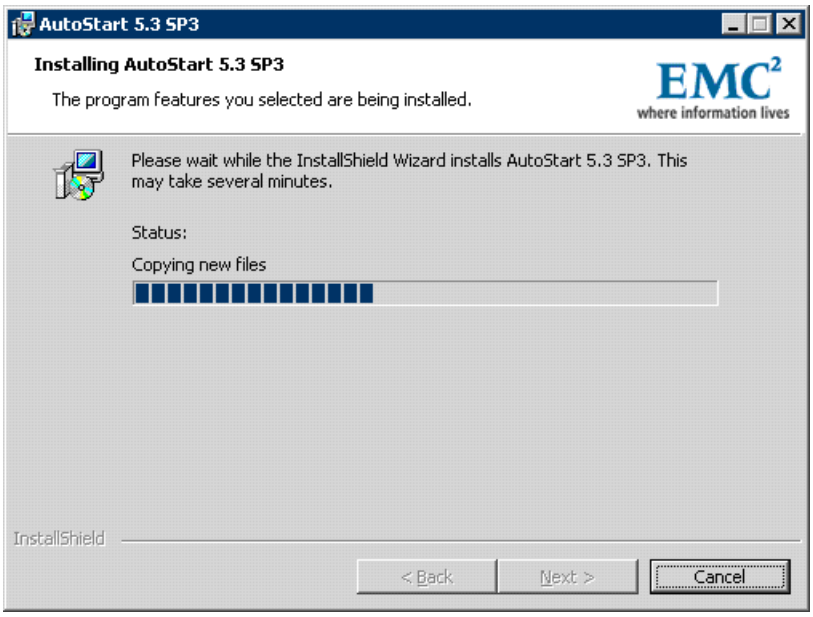


Figure 105: Installing AutoStart 5.3 SP3

17. Wait for the installation to complete.

    Result: The InstallShield Wizard Completed window appears.

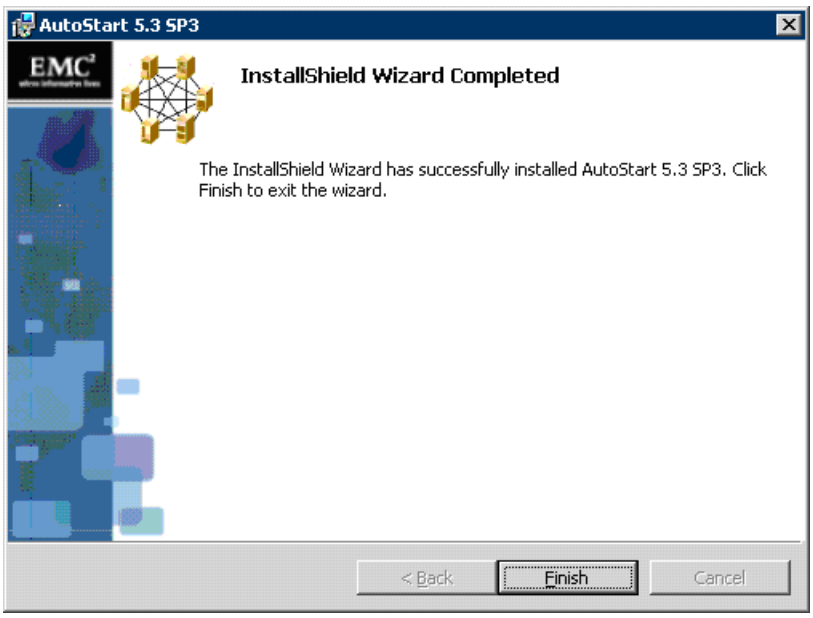


Figure 106: InstallShield Wizard Completed window

18. Click Finish
19. Delete the folder D:\temp\EMC_AutoStart_5.3_SP3_Update.

In order for the AutoStart Console (on the stand-alone PC) to manage an AutoStart domain (that is, a pair of CallPilot High Availability servers), the user ID used to log on to the stand-alone PC must be registered in the AutoStart domain that is to be managed. To do this, you must do the following:

1. Add the user ID into the Valid User List of the AutoStart domain on the AutoStart Console installed on one of the High Availability servers. For more information, see Adding a user ID to the AutoStart domain on page 189.
2. After the user ID is registered, create a connection to the pair of High Availability servers by launching the AutoStart Console on the stand-alone PC and enter the AutoStart domain name and node names. For more information, see Adding a remote AutoStart domain to the AutoStart Console on page 191.

Adding a user ID to the AutoStart domain

1. Launch the AutoStart Console on either of the two servers that are members of the AutoStart domain.
2. Expand Domains.
3. Select the Licensing/Security tab.

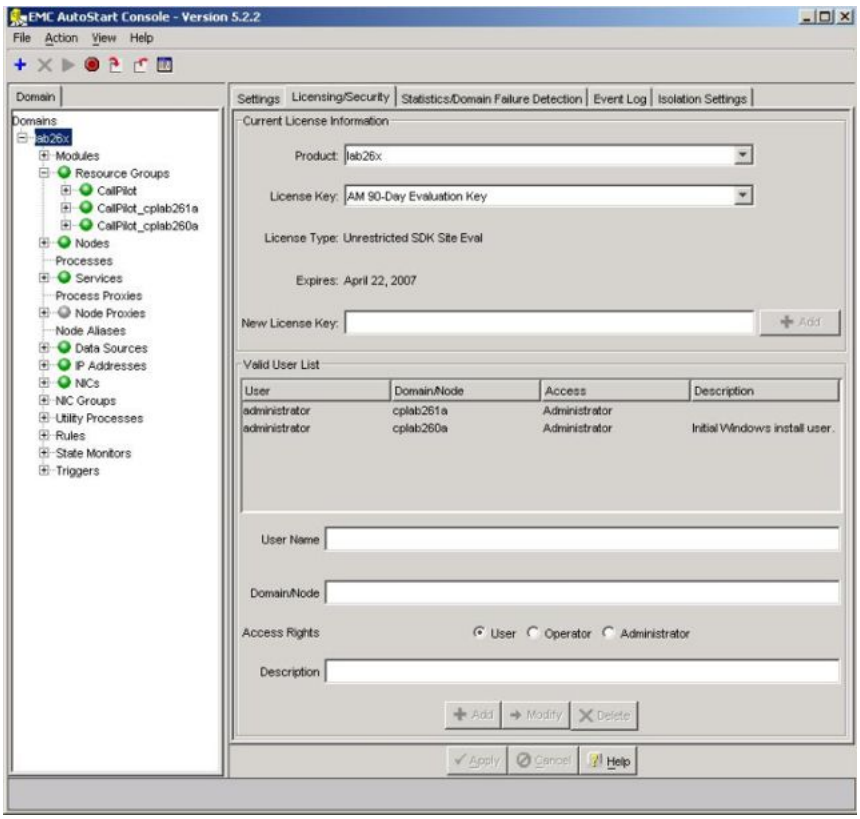


Figure 107: Licensing/Security tab

4. In the User Name field, enter the user ID of the user who must be given access to the AutoStart domain.
5. In the Domain/Node field, enter one of the following:
   - The Windows domain name, if the user has a Windows domain user ID.
   - The server name that the user ID is defined on, if the user is not a member of a Windows domain.
6. For the Access Rights field, select either the User, Operator, or Administrator option.
7. Click Add.

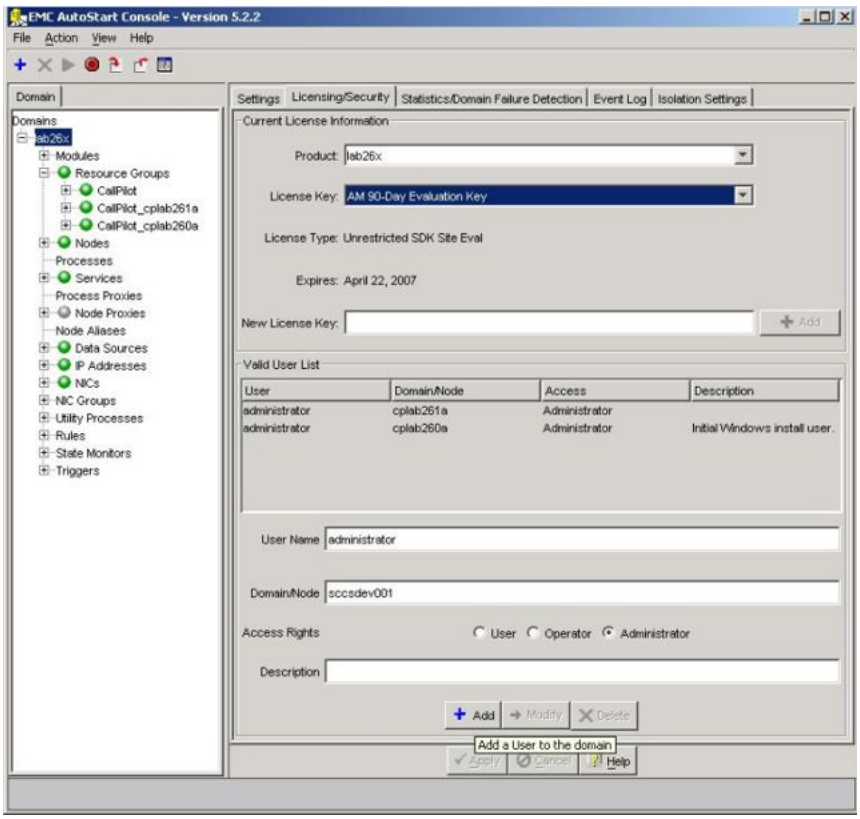


Figure 108: Add user

Result: The user is added to the Valid User List.

Adding a remote AutoStart domain to the AutoStart Console

1. Launch the AutoStart Console that is installed on the stand-alone PC.

   Result: The New Domain dialog box appears.

   Note:

   If the AutoStart Console does not launch automatically, select Action > Open New Domain to display the New Domain dialog.

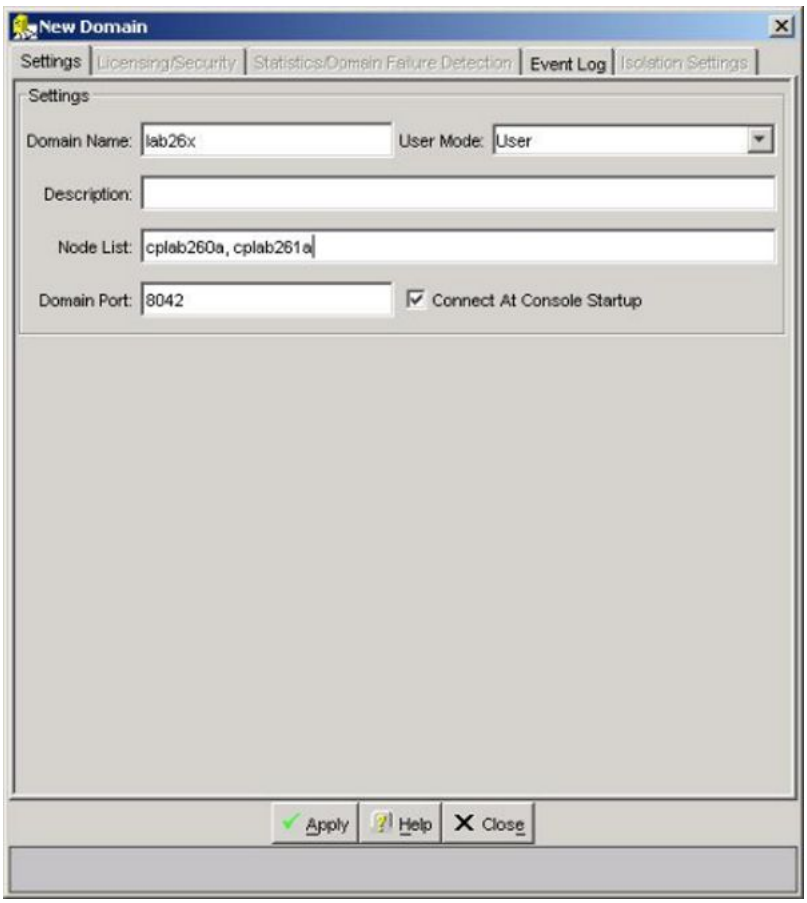


Figure 109: New Domain

2. In the Domain Name field, enter the name of the AutoStart domain to which you want to connect.
3. In the Node List field, enter a comma-separated list of the two node names that are members of the AutoStart domain to which you want to connect.
4. Click Apply.

   Result: The AutoStart Console window updates and the newly added AutoStart domain is connected using the user ID that is currently logged on to the stand-alone PC.

Uninstall the AutoStart software

Use the following procedure if you must uninstall the AutoStart software.

Uninstalling the AutoStart software

1. Launch the AutoStart Console.
2. In the AutoStart Console, take the CallPilot resource group offline.

   For more information, see Take a resource group offline on page 177.
3. Remove the CallPilot resource group by doing the following:
   a. Right-click the CallPilot Resource group.
   b. Select Remove Current Resource Group.
4. Delete the data sources (drive E and drive F).
5. Close the AutoStart Console.
6. Click Start > Settings > Control Panel.
7. Double-click the Add/Remove Programs icon in the Control Panel.

   Result: The Add or Remove Programs window appears.
8. Select AutoStart 5.3 SP3 from the list.

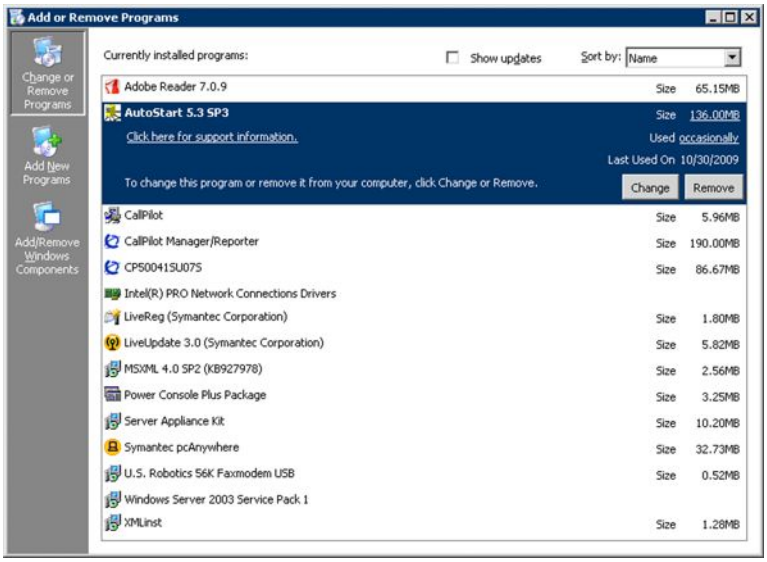


Figure 110: Add or Remove Programs - AutoStart 5.3 SP3

9. Click Remove.

   Result:The Add or Remove Programs conformation window appears.

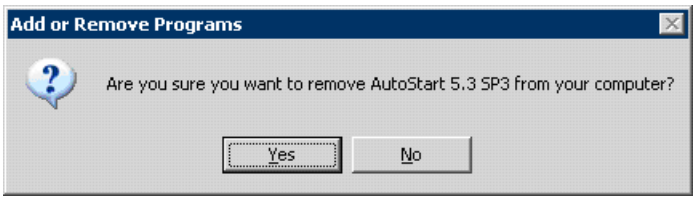


Figure 111: Add or Remove Programs – confirmation window

10. Click Yes

    Result: Uninstalling EMC AutoStart window appears and displays the progress of uninstallation.

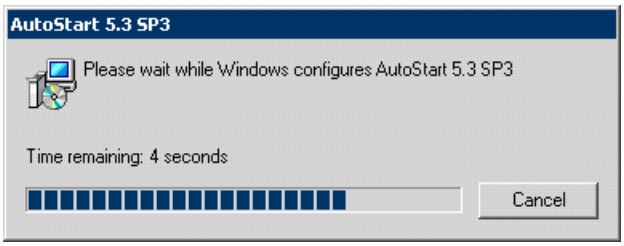


Figure 112: AutoStart 5.3 SP3 Installer - Status of uninstallation

If the AutoStart Console is in use, the following message appears. Close the AutoStart Console and click Retry to continue.

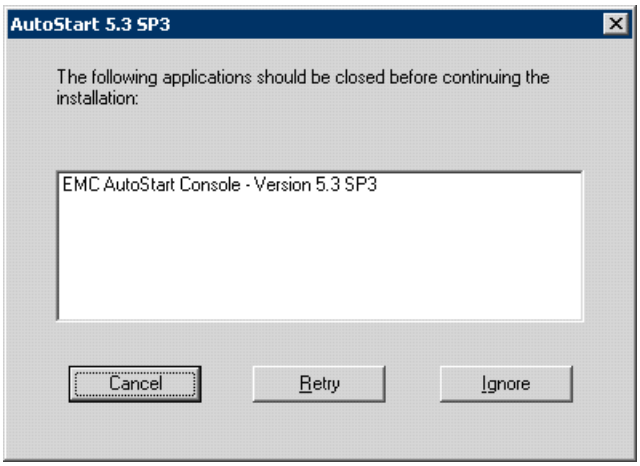


Figure 113: AutoStart 5.3 SP3 Installer - AutoStart Console is in use

11. The AutoStart 5.3 SP3 Installer Information dialog box appears.
12. Click Yes to restart the node.

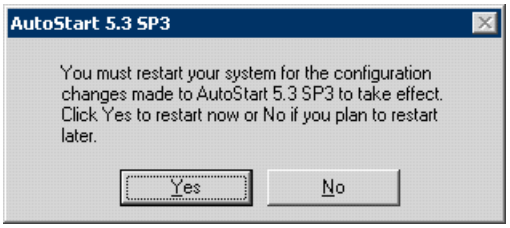


Figure 114: AutoStart 5.3 SP3 Installer Information

Reinstall the AutoStart software

Use the following procedure if you must uninstall and then reinstall the AutoStart software. This procedure must be completed on both servers in the High Availability pair.

Reinstalling the AutoStart software

This procedure must be used on each node of a CallPilot High Availability pair.

1. Uninstall the AutoStart patches by doing the following:
   a. Rerun each patch.
   b. Select the Remove option.
2. Uninstall the AutoStart Console by following the procedure Uninstalling the AutoStart software on page 193, which first deletes the AutoStart Data Sources.
3. Reinstall the AutoStart Agent and Console, including their patches. For more information, see Install the AutoStart Agent and Console software on page 62.
4. Restart the server.

EMC software updates (AutoStart Agent/Console)

Avaya must approve all EMC AutoStart updates. Do not apply any software updates unless the update is provided by Avaya. Contact your support organization for more information.

All of the required EMC software is included on the CallPilot 5.0 Applications CD. This version of the EMC software is tested and verified to work correctly with the CallPilot 5.0 High Availability feature. The EMC software on the CallPilot server must not be updated or patched unless the new software or patch is tested and validated by Avaya.

Support

Install PEPs

To ensure that the pair of CallPilot servers functions correctly, both CallPilot servers must be running the same PEPs and Service Updates (SUs). Due to the mirroring software, the mirrored

drives cannot be accessed on the standby server. As a result, PEPs that impact the database or MMFS must be installed on the active CallPilot server.

This section includes the procedure for installing PEPs.

ws

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

Important:

Please make sure that both nodes are in the green status on the Nodes list of the AutoStart Console.

1. On CP1, do the following:

   a. Launch the AutoStart Console.

   b. Stop monitoring for CallPilot, CallPilot_[CP1] and CallPilot_[CP2] resource groups.

      For more information, see Disabling automatic failovers (stop monitoring) on page 180.

   c. Take CallPilot, CallPilot_[CP1] and CallPilot_[CP2] resource groups offline (shut down CallPilot).

      For more information, see Taking the CallPilot resource group offline on page 177.

   d. Wait for all resource groups to go offline.

   e. Attach the mirror drives, drive E and drive F (Note: Repeat the steps i, ii, iii on drive E and drive F) to CP1 so that the disks can be accessed from CP1.

      Important:

      Attaching and detaching drives can take a few minutes.

      i. In the AutoStart Console, select the [AutoStart_Domain] > Data Sources.

      ii. Right-click the drive you want to connect.

      iii. Select Attach Data Source.

   f. Install the PEPs.

      Note:

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

   g. Detach the data source.

      i. In the AutoStart Console, select the [AutoStart_Domain] > Data Sources.

ii. Right-click the drive/data source.

iii. Select Detach Data Source.

h. Restart the server (if required).

Result: CP1 now has the new software, registry settings, and database updates. Because the resource group is offline and monitoring is disabled, CallPilot does not automatically restart after the restart.

Important:

Wait till the CP1 is turned to green on the Nodes list of the AutoStart Console.

2. On CP2, do the following:

   a. Launch the AutoStart Console.

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

   Important:

   Attaching and detaching drives can take a few minutes.

   i. In the AutoStart Console, select the [AutoStart_Domain] > Data Sources.

   ii. Right-click the drive you want to connect.

   iii. Select Attach Data Source.

   c. Install the PEPs.

   Important:

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

   d. Restart the server (if required).

Result: CP2 now has the new software, registry settings, and database updates. Because the resource group is offline and monitoring is disabled, CallPilot does not automatically restart after the restart.

Important:

Please refer to the CP5.0 DTR or the PEP README files to see whether or not there is any additional procedure which has to be done before the next step or bringing the resource group CallPilot online.

3. On CP1, do the following:

   a. Launch the AutoStart Console.

   b. Start monitoring for CallPilot, CallPilot_[CP1] and CallPilot_[CP2] resource groups (to enable automatic failovers).

   For more information, see Enabling automatic failovers (start monitoring) on page 180.

c. Bring CallPilot, CallPilot_[CP1] and CallPilot_[CP2] resource groups online (start up CallPilot).

For more information, see Bringing the CallPilot resource group online on page 176.

Result: Both servers are updated with the PEPs.

Uninstall PEPs

To ensure that the pair of CallPilot servers functions correctly, both CallPilot servers must be running the same PEPs and Service Updates (SUs). Due to the mirroring software, the mirrored drives cannot be accessed on the standby server. As a result, PEPs that impact the database or MMFS must be uninstalled from the active CallPilot server.

This section includes the procedure for uninstalling PEPs.

Uninstalling PEPs

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

1. On CP1, do the following:

   a. Launch the AutoStart Console.

   b. Stop monitoring for CallPilot, CallPilot_[CP1] and CallPilot_[CP2] resource groups.

   For more information, see Disabling automatic failovers (stop monitoring) on page 180.

   a. Take CallPilot, CallPilot_[CP1] and CallPilot_[CP2] resource groups offline (shut down CallPilot). For more information, see Taking the CallPilot resource group offline on page 177.

   b. Wait for all resource groups to go offline.

   c. Attach the mirror drives (drive E and drive F) to CP1 so that the disks can be accessed from CP1.

   Note:

   Attaching and detaching drives can take a few minutes.

   - In the AutoStart Console, select the [AutoStart_Domain] > Data Sources.
   - Right-click the drive you want to connect.
   - Select Attach Data Source.

Uninstall the PEPs.

Note:

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

a. Detach the data source.

- In the AutoStart Console, select the [AutoStart_Domain] > Data Sources.
- Right-click the drive/data source.
- Select Detach Data Source.

b. Restart the server (if required).

Result: CP1 now does not have the software, registry settings, and database updates. Because the resource group is offline and monitoring is disabled, CallPilot does not automatically restart after the restart.

2. On CP2, do the following:

a. Launch the AutoStart Console.

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

Note:

Attaching and detaching drives can take a few minutes.

- In the AutoStart Console, select the [AutoStart_Domain] > Data Sources.
- Right-click the drive you want to connect.
- Select Attach Data Source.

c. Uninstall the PEPs.

Note:

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

Restart the server (if required).

Result:CP2 now does not have the software, registry settings, and database updates. Because the resource group is offline and monitoring is disabled, CallPilot does not automatically restart after the restart.

3. On CP1, do the following:

a. Launch the AutoStart Console.

b. Start monitoring for CallPilot, CallPilot_[CP1] and CallPilot_[CP2] resource groups to enable automatic failovers. For more information, see Enabling automatic failovers (start monitoring) on page 180.

c. Bring CallPilot, CallPilot_[CP1] and CallPilot_[CP2] resource groups online (start up CallPilot). For more information, see Bringing the CallPilot resource group online on page 176.

   Result:PEPs are uninstalled from both the servers.

Microsoft Hotfixes

Microsoft Hotfixes generally affect only the base operating system. Hotfixes may or may not require a restart.

- If the hotfix does not require a restart, the hotfix can be installed in parallel on the active and the standby CallPilot servers.
- If the hotfix does require a restart, the installation process requires a failover, which temporarily takes the CallPilot server out of service.

Remote support

USB modem dial-in

CallPilot 5.0 High Availability systems support the PCAnywhere Remote Modem-to-Modem dial-in connection without field assistance. CallPilot 5.0 High Availability systems do not support PCAnywhere Remote TCP/IP because the Routing and Remote Access Services (RRAS) are stopped and their Startup Type is set to Disabled and Manual.

The following diagram shows the remote support setup for High Availability systems.

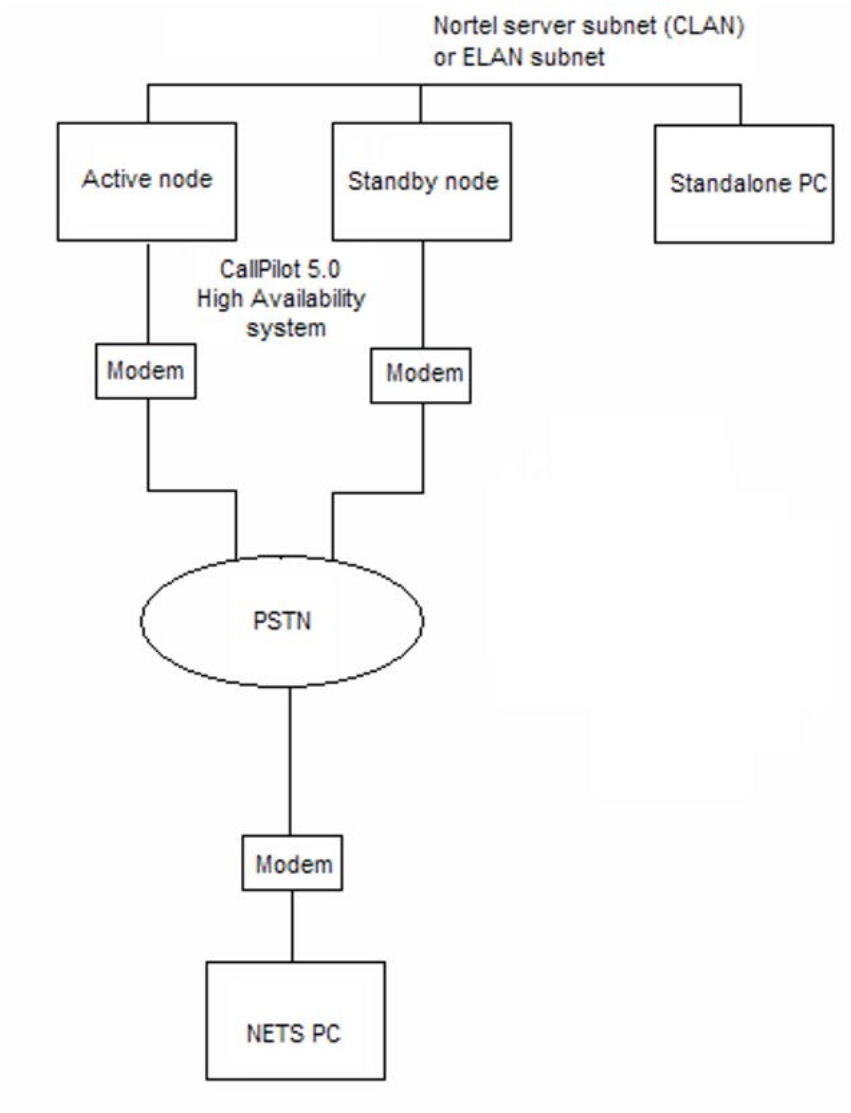


Figure 115: Remote support setup for High Availability

You can dial directly into the active High Availability server (through the USB modem) using PCAnywhere Remote Modem on the remote PC. The PCAnywhere Host on the active High Availability server is launched and is waiting for the incoming modem calls.

However, to dial into the standby High Availability server, you must use the following procedure.

Dialing into the standby High Availability server

1. Dial into the active High Availability server using PCAnywhere Remote Modem.
2. Launch the AutoStart Console.

3. Select Domains > [AutoStart_Domain] > Utility Processes > UnloadTSPOnStandbyServer.
4. Right-click UnloadTSPOnStandbyServer and then select Start Utility Process from the shortcut menu.
5. Select the host name of the standby High Availability server.

   This utility does the following on the standby High Availability server:

   - unloads the TSP
   - stops the PCAnywhere Host
   - starts the telephony server (TAPI)
   - restarts the PCAnywhere Host
6. Wait approximately 5 minutes for the script to complete running on the standby High Availability server.
7. Dial into the standby High Availability server using the PCAnywhere Remote Modem.
8. After the dial-in session finishes, the server must be restarted so that the Standby HA server is clean and ready to accept the coming failover.

If you have to connect or reconnect the USB modem to the active High Availability server after the High Availability system is running (that is, CallPilot is in service [the CallPilot resource group is online]), you must follow one of the following methods to make the PCAnywhere Host launch properly:

Method 1:

1. Take the CallPilot resource group offline. For more information, see Taking the CallPilot resource group offline on page 177.
2. Connect the USB modem.
3. Bring the CallPilot resource group online. For more information, see Bringing the CallPilot resource group online on page 176.
4. Using Windows Device Manger, right click Modems and then select Scan for hardware changes.

Method 2:

1. Manually trigger a failover by shutting down the server. For more information, see Initiating a manual failover on page 181.
2. Using Windows Device Manger, right click Modems and then select Scan for hardware changes.

Remote Access tools

The following tools can be used to access the servers in the CallPilot 5.0 High Availability system:

- LogMeIn Rescue (Customer assistance is required.)
- VPN (Access permission is required.)
- Remote Desktop (Normally blocked by enterprise gateways. Avaya does not recommend this tool to access the active High Availability server.)
- PCAnywhere (Normally blocked by enterprise gateways.)

Backup and restore

For the High Availability system, the backup device must be defined on both the active and the standby servers. If the backup device is not defined and a failover occurs, scheduled backups do not run on the standby server.

If you must remotely connect to CallPilot Manager to perform a backup, Avaya recommends that you use the Managed CLAN host name or the Managed CLAN IP address to connect to a server in the High Availability pair.

On a CallPilot 5.0 High Availability system, use the following procedures to:

- create a backup device
- schedule an archive backup
- perform a full system backup

Note:

The following procedure is not required if you must create a full-system backup to a tape on a CallPilot 5.0 High Availability system. Backing up to tape requires that a tape drive must be physically attached to each High Availability server to ensure that scheduled backups can run after a failover. The 1006r server requires a USB to SCSI adapter in addition to the tape drive.

Creating a backup device (network disk)

For this procedure, CP1 is the active server and CP2 is the standby server.

1. Ensure that the dongle is on CP1 (which is the active server of the High Availability pair).
2. On CP1, log on to CallPilot Manager.
3. Select System > Backup/Restore.

   Result: The Backup/Restore window appears.

4. From the Select a task drop-down list, select Maintain and configure backup devices.
5. Under Backup Devices, click Add Device.

   Result: The Backup Device window appears.
6. On the Backup Device window, do the following:

   a. Enter a unique Device Name.
   b. Enter the Path to the backup device.
   c. Verify that the Type field is set to Disk.
   d. Under the Connect to network folder as area, enter the User name and User Password. Then reenter the password in the Confirm Password field.

      This is user name and password to access the path/folder where the backup is located.
   e. Click Save.

      Result:The <Device Name>.dev file is created in the D:\Nortel\Data \backup\Devices folder.
7. On CP1 (the active server), navigate to folder D:\Nortel\Data\backup.
8. Right-click the Devices folder and select Sharing and Security.

   Result: The Devices Properties window opens.
9. Select the Sharing tab.
10. Select the Share this folder option.
11. Click Permissions.

    Result: The Permission for Devices window opens.
12. Enter a Share name for the shared folder.

    Write down the name of this shared folder as it is used in a later step.
13. Under Groups or User Names, select Everyone.
14. Under Permissions for Everyone, select the Allow check box for the Read row.
15. Click OK.

    Result: The Permission for Devices window closes and the Properties window for the Devices folder appears.
16. Click OK.

    Result: The Devices Properties window closes.
17. On CP2 (the standby server), right-click My Computer and select Map Network Drive.

    Result: The Map Network Drive window opens.

18. Select an available Drive letter.
19. In the Folder field, map the shared folder (D:\Nortel\Data\backup\Devices) on CP1 by entering the following:

    \\<Computer name of CP1>\<Share name of D:\Nortel\Data\backup\Devices on CP1>
20. Click OK.
21. On CP2, from the mapped drive that was just created, copy the new <Device Name>.dev file you just created on CP1 to D:\Nortel\Data\backup\Devices folder on CP2 (the standby server).
22. On CP2 (the standby server), right-click My Computer and select Disconnect Network Drive.

    Result: The Disconnect Network Drives window opens.
23. Select mapped network drive and click OK.

Use the following procedure to create a scheduled archive backup.

Scheduling an archive backup

1. Ensure that a backup device exists. For more information, see Creating a backup device (network disk) on page 203.
2. On CP1, log on to CallPilot Manager.
3. Select System > Backup/Restore.

   Result: The Backup/Restore window appears.
4. From the Select a task drop-down list, select Review and schedule backup.
5. Under Scheduled Backups, click Add Backup.

   Result: The Add New Backup Schedule window appears.
6. From the Backup Type drop-down list, select the type of archive backup.
7. Under Device Name, select the backup device.
8. If applicable, select the Additional Options.
9. Click Next.
10. Select the backup frequency.
11. Select the Month, Date and Time for the scheduled backup.
12. Enter a Description for the backup.
13. Click Next.

    Result: The Confirm Backup Schedule window appears.
14. Click Finish.

    Result: The Backup/Restore window appears and shows the newly scheduled backup under Scheduled Backups.

15. On CP1 (the active server), navigate to folder D:\Nortel\Data\backup.
16. Right-click the Definitions folder and select Sharing and Security.

    Result: The Definitions Properties window opens.
17. Select the Sharing tab.
18. Select the Share this folder option.
19. Click Permissions.

    Result: The Permission for Definitions window opens.
20. Enter a Share name for the shared folder.

    Write down the name of this shared folder as it is used in a later step.
21. Under Groups or User Names, select Everyone.
22. Under Permissions for Everyone, select the Allow check box for the Read row.
23. Click OK.

    Result: The Permission for Definitions window closes and the Properties window for the Definitions folder appears.
24. Click OK.

    Result: The Definitions Properties window closes.
25. On CP2 (the standby server), right-click My Computer and select Map Network Drive.

    Result: The Map Network Drive window opens.
26. Select an available Drive letter.
27. In the Folder field, map the shared folder (D:\Nortel\Data\backup\Definitions) on CP1 by entering the following:

    \\<Computer name of CP1>\<Share name of D:\Nortel\Data\backup\Definitions on CP1>
28. Click OK.
29. On CP2, from the mapped drive that was just created, copy the new <backup_options>.bsp files you just created on CP1 to D:\Nortel\Data\backup \Definitions folder on CP2 (the standby server).

    The .bsp files created depend on the type of backup that you selected.
30. On CP2 (the standby server), right-click My Computer and select Disconnect Network Drive.

    Result: The Disconnect Network Drives window opens.
31. Select mapped network drive and click OK.

Use the following procedure to perform a full system backup on the active High Availability server. This single backup is used to restore both High Availability servers. For more information on restoring, see Restoring the High Availability system on page 208.

Important:

If your system is backed up to tape, the backup is saved only on the tape drive for the active High Availability server. Since both High Availability servers have physical tape drives attached, you must track which server was active when the backup occurred. When you perform the restore from tape, this ensures that you are using the most current backup.

Performing a full system backup of the High Availability system

CP1 is the active is the active server and CP2 is the standby server.

1. Ensure that a backup device exists for CP1 and CP2. For more information, see Creating a backup device (network disk) on page 203.
2. On CP1, log on to CallPilot Manager.
3. Select System > Backup/Restore.

   Result: The Backup/Restore window appears.
4. From the Select a task drop-down list, select Review and schedule backup.
5. Under Scheduled Backups, click Add Backup.

   Result: The Add New Backup Schedule window appears.
6. From the Backup Type drop-down list, select Full System Backup.
7. Under Device Name, select the backup device for CP1.
8. If applicable, select the Additional Options.
9. Click Next.
10. Under Select the backup frequency, select how often you want the backup to occur.
11. Select the current Month, Date and Time for the full system backup.
12. Enter a Description for the backup.
13. Click Next.

    Result: The Confirm Backup Schedule window appears.
14. Click Finish.

    Result: The Backup/Restore window appears and shows the newly scheduled backup for CP1 under Scheduled Backups.
15. If you want to perform the backup immediately, complete the following steps. Otherwise, the backup occurs at the scheduled date and time.

    a. Select the check box adjacent to the name of the backup.

    b. Click Backup Now.

       Result: A message appears asking you to start the backup.

    c. Click OK to start the full system backup.

Restoring the High Availability system

If your High Availability system fails due to database corruption or an unforeseen disaster (causing both CP1 and CP2 to be unavailable), you must use the following guidelines to restore your system:

- If the existing CP1 and CP2 servers are being reused, then load the CallPilot 1005r or 1006r image onto each server. For more information, see the Software Administration and Maintenance Guide (NN44200-600) for information on recovering system software.
- If you are replacing the CP1 and CP2 servers with new servers, see the 1005r Server Hardware Installation (NN44200-308) or 1006r Server Hardware Installation (NN44200-320). The new server comes with the appropriate CallPilot image preinstalled from the factory.
- If database corruption occurs, you must reimage both High Availability servers and then restore the two servers from a full system backup.

The following task list provides a high-level overview of restoring the High Availability system:

1. Run the Setup Wizard on CP1 and CP2.
   - On CP1, when prompted to perform a restore, select the full system backup.
   - On CP2, when prompted to perform a restore, select the full system backup.
2. Run the Configuration Wizard on CP1 and CP2. If required, update the switch information (such as TNs and CDNs).
3. Connect and verify the LAN connections.
4. Run Stage 1 of the High Availability Configuration Wizard to check the configuration of CP1 and CP2.
5. Install the AutoStart software on CP1.
6. Install the AutoStart 5.3 software on CP1.
7. Install the AutoStart software on CP2.
8. Configure licensing and security on CP1.
9. Install the AutoStart 5.3 software on CP2.
10. Configure the AutoStart software.
11. Bring the Resource Groups online.
12. Test your configuration.
13. Create the CallPilot Reporter connections.
14. Add server to a Windows domain (if required).

Reimage or replace a server in the High Availability pair

Use the following procedure to reimage a server or to replace a server in the High Availability pair.

Important:

For the purpose of the following procedure, the servers from High Availability pair are referred to as existing server and replacement server. Where existing server is used, it refers to the server in the HA pair which is in service and is not being replaced. Where replacement server is used, it refers to the new server which is replacing a failed server in the pair.

Warning:

The server that is reimaged or replaced must maintain the same TCP/IP networking information (such as IP addresses and local host name) in order for the High Availability pair to operate correctly.

When the reimaged or replaced server is running, you can change the local host name, local ELAN/CLAN parameters (such as IP address and host name), or HB1/HB2/Mirror parameters (such as IP addresses).

Reimaging or replacing one of the High Availability servers

1. Use the AutoStart Console on the existing server to disable monitoring. For more information, see Disabling automatic failovers (stop monitoring) on page 180.
2. Disconnect the network cables from the failed server (the server to be reimaged or replaced).
3. If the failed server is being reused, load the appropriate CallPilot image onto the server. For more information, see the *Software Administration and Maintenance Guide* (NN44200-600) for information on recovering system software.

   If you are replacing the failed server with a new server, see either the *1005r Server Hardware Installation* (NN44200-308) or the *1006r Server Hardware Installation* (NN44200-320). new server comes with the matching CallPilot image preinstalled from the factory.
4. Install the antivirus software on the replacement server if necessary.

   Note:

   For more information about the antivirus software packages that have been approved by Avaya for CallPilot, see the *P-2007-0101-Global : CallPilot Support for Anti-Virus Applications* bulletin.
5. On the replacement server, run the Setup Wizard and apply any CallPilot PEPs and SUs.
6. Log on to CallPilot Manager on the replacement server.

7. On the replacement server, run the Configuration Wizard to configure the server. For more information, see Configuring the replacement server using the Configuration Wizard on page 252.
8. Restart the replacement server.
9. Connect all the network cables to the replacement server. For more information, see Connecting and verifying LAN connections on page 52.
10. On the replacement server, install the AutoStart Agent and Console software (including any required patches) by entering the node name of the existing server. Follow the steps in Install the AutoStart software on CP1 on page 62 .

Note:

You must enter the local host name of the existing CallPilot server when installing the AutoStart software.

Important:

The following step takes your CallPilot High Availability system offline. Your CallPilot system will not process calls.

11. Take the CallPilot resource group offline on the existing server. For more information, see Taking the CallPilot resource group offline on page 177.
12. On the existing server, use the AutoStart Console to select Resource Groups > CallPilot and then expand the CallPilot resource group.

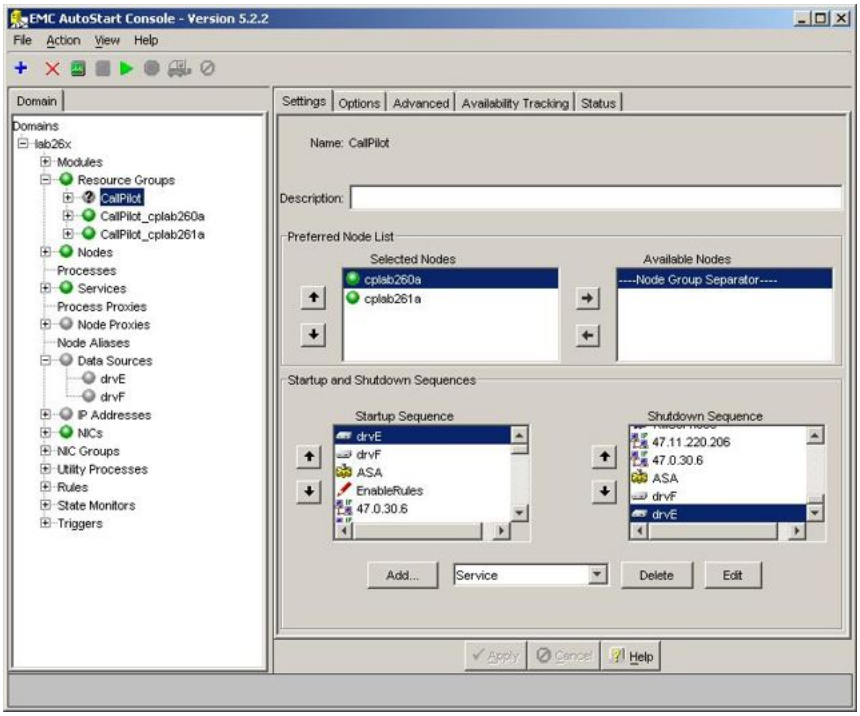


Figure 116: Resource group: Settings tab

a. Click the Settings tab.

b. Under theStartup Sequence, do the following:

i. Select drive E (drvE) and then click Delete.

ii. Select drive F (drvF) and then click Delete.

c. Click Apply.

13. On the existing server, use the AutoStart Console to expand Data Sources.

a. Right-click the drvE Data Resource and then click the Delete Current Data Source option to delete drive E.

b. Right-click the drvF Data Resource and then click the Delete Current Data Source option to delete drive F.

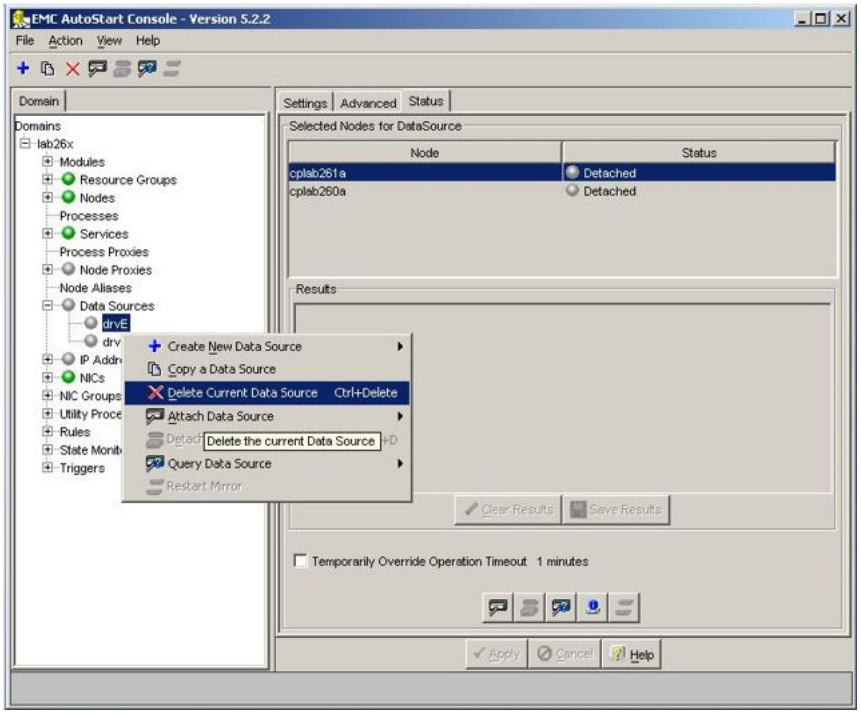


Figure 117: Delete Current Data Source

14. On the existing server, use the AutoStart Console to select the first node (expand [AutoStart_Domain] > Nodes > existing server) and do the following:

a. Select the Failure Detection and Mirroring tab.

b. Under Configure Mirror Settings, change the Remote Mirror Host value to None.

c. Click Apply.

15. On the existing server, use the AutoStart Console to select the second node (expand [AutoStart_Domain] > Nodes > replacement server) and do the following:

a. Select the Failure Detection and Mirroring tab.

b. Under Configure Mirror Settings, change the Remote Mirror Host value to None.

c. Click Apply.

16. Restart both servers.
17. On the existing server, use the AutoStart Console to select the first node (expand [AutoStart_Domain] > Nodes > existing server) and do the following:

    a. Select the Failure Detection and Mirroring tab.

    b. Under Configure Mirror Settings, change the Remote Mirror Host value to the hostname of replacement server.

    c. Click Apply.

18. On the existing server, use the AutoStart Console to select the second node (expand [AutoStart_Domain] > Nodes > CP2) and do the following:

    a. Select the Failure Detection and Mirroring tab.

    b. Under Configure Mirror Settings, change the Remote Mirror Host value to the hostname of existing server.

    c. Click Apply.

19. On the existing server, recreate drive E (drvE) and drive F (drvF) and select the existing server as the source node:

    a. Right-click Data Sources on AutoStart Console.

    b. Select Create New Data Source > EMC Mirroring for Windows.

    Result: The New EMC Mirroring for Windows Data Source appears.

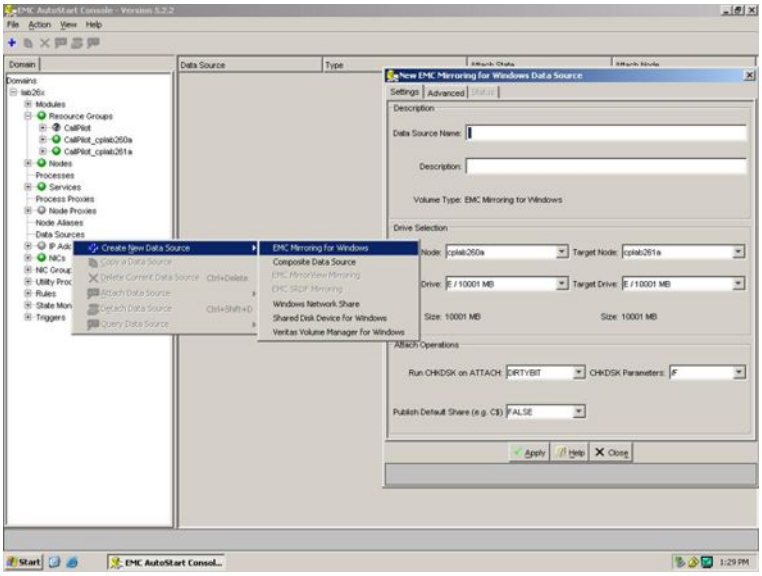


Figure 118: Create New Data Source - EMC Mirroring for Windows

    c. In the New EMC Mirroring for Windows Data Source window, do the following:

        i. Under the Description area, enter the Data Source Name - drvE and Description - drive E.

ii. Under the Drive Selection area, select hostname of existing server from the Source Node drop-down list and drive E from the Source Drive drop-down list.

iii. Under the Drive Selection area, also select the hostname of replacement server from the Target Node drop-down list and drive E from the Target Drive drop-down list.

iv. Click Apply.

v. Click Yes to dismiss the warning message.

d. Right-click Data Sources on AutoStart Console.

e. Select Create New Data Source > EMC Mirroring for Windows. Result: The New EMC Mirroring for Windows Data Source appears.

f. In the New EMC Mirroring for Windows Data Source window, do the following:

i. Under the Description area, enter theData Source Name - drvF and Description - drive F.

ii. Under the Drive Selection area, select the hostname of existing server from the Source Node drop-down list and drive F from the Source Drive drop-down list.

iii. Under the Drive Selection area, also select the hostname of replacement server from the Target Node drop-down list and drive F from the Target Drive drop-down list.

iv. Click Apply.

v. Click Yes to dismiss the warning message.

20. Select Resource Groups > CallPilot.
21. Select the Settings tab.
22. Under the Startup and Shutdown Sequences area, select Data Source from the drop-down list which adjacent to the Add button.
23. Click Add.

    Result: The Data Source Properties window appears.

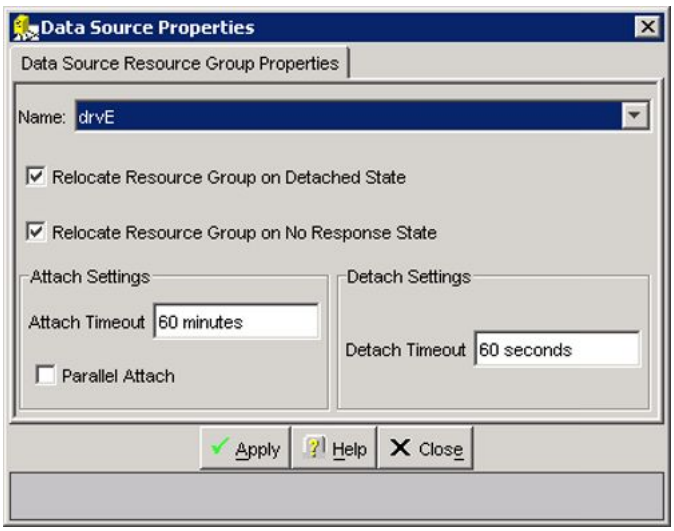


Figure 119: Data Source Properties

24. From the Name drop-down list, select drvE and leave all other fields with the default selections.
25. Click Apply.
26. Under the Startup and Shutdown Sequences area, select Data Source from the drop-down list which adjacent to the Add button.
27. Click Add.

    Result: The Data Source Properties window appears.
28. From the Name drop-down list, select drvF and leave all other fields with the default selections.
29. Click Apply.
30. Click Apply (on the Settings tab).
31. Under the Startup and Shutdown Sequences area, do the following:
    a. Under Startup Sequence, use the Up arrow to move drvE and drvF to the top of the Startup Sequence list.
    b. Under Shutdown Sequence, use the Down arrow to move drvE and drvF to the bottom of the Shutdown Sequence list.
32. Click Apply.
33. Attach drive E and drive F to the existing server. Perform the following for both drives:
    a. In the AutoStart Console, select the [AutoStart_Domain] > Data Sources.
    b. Right-click the drive you want to connect.
    c. Select Attach Data Source.

Result: The data sources (drive E and drive F) are in the warning state and their icons are yellow.

Note:

A message is displayed informing you that the data source is being mirrored and the status of data source is updated to show the progress of synchronization. It can take between 30 minutes to 2 hours for the data sources to be mirrored between the two servers.

34. Wait while the data sources are mirrored and have Attached status.
35. Detach drive E and drive F. Perform the following for both drives:
    a. In the AutoStart Console, select [AutoStart_Domain] > Data Sources.
    b. Right-click the drive you want to detach.
    c. Select Detach Data Source.

    Result: Data Sources are detached.
36. On the existing server, use the AutoStart Console to bring the CallPilot resource group online (if they are not already online). For more information, see Bringing the CallPilot Resource Group online on CP1 on page 93.
37. On the existing server, use the AutoStart Console to bring the remaining resource groups online (if they are not already online). For more information, see Bringing the Resource Groups CallPilot_[CP1] and CallPilot_[CP2] online on page 95.
38. On the existing server, use the AutoStart Console to enable AutoStart monitoring. For more information, see Enabling automatic failovers (start monitoring) on page 180.
39. If you have scheduled backups configured, do the following:
    a. On the replacement server, browse to the shared D:\Nortel\Data\backup\Devices folder of the existing server and copy the contents of the Devices folder.
    b. On the replacement server, paste the contents in to the Devices folder on the replacement server.
    c. On the replacement server, browse to the shared D:\Nortel\Data\backup\Definitions folder of the existing server and copy the contents of the Definitions folder.
    d. On the replacement server, paste the contents in to the Definitions folder on the replacement server.

Installing the AutoStart software on the replacement server

The following procedure installs AutoStart 5.3 SP3 Agent and Console software on the replacement server. This procedure takes approximately 10 minutes.

Important:

The computer name must be set before you Install the AutoStart software. The software requires the computer name. The computer name must contain only alphanumeric characters. Non-alphanumeric characters (such as a hyphen [-]) are not supported. If you want to change the computer name after installing the server you must uninstall and then reinstall the AutoStart software.

Installing the AutoStart software on the replacement server

1. Insert the CallPilot Application CD.
2. Navigate to the Z:\EMC folder on the CallPilot Application CD.
3. Double-click the EMC_AutoStart_5.3_SP3_Update.exe to unpack the archive to the D:\temp folder.

   Result: These files are unpacked into the D:\temp \EMC_AutoStart_5.3_SP3_Update folder: EAS53_WIN_x86.exe EAS53SP3_WIN_x86.exe EMC AutoStart Update Process.pdf.
4. Double-click the EAS53SP3_WIN_x86.exe file to start the installation.

   Result: InstallShield Wizard informs you that AutoStart 5.3 SP3 software is preparing to install (install preparation can take a few minutes). After preparation is complete, Welcome window Appears.

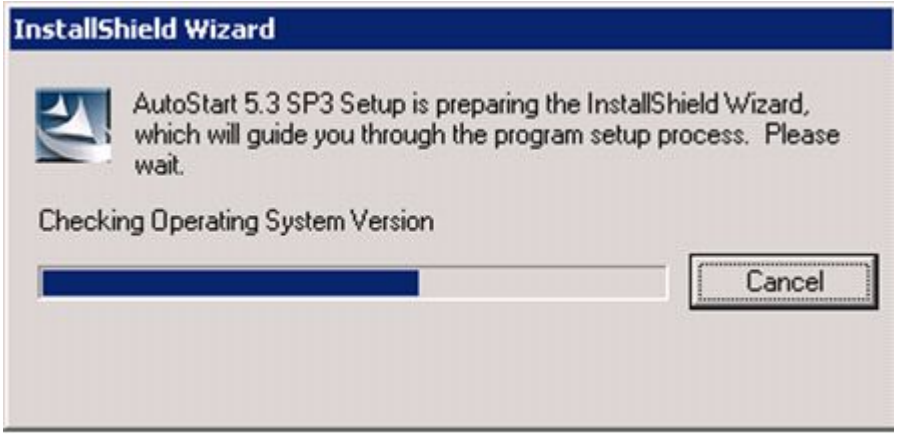


Figure 120: InstallShield Wizard - Preparing to install AutoStart 5.3 SP3 software

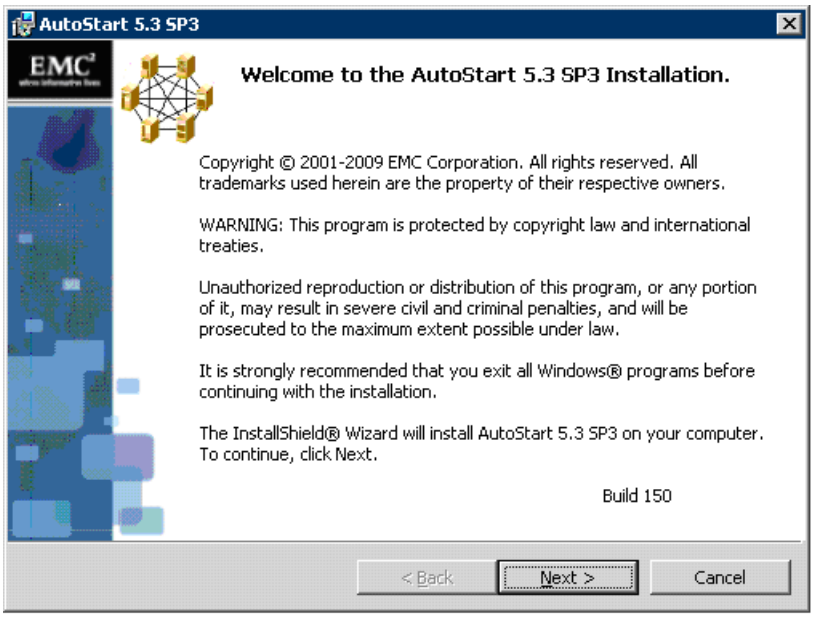


Figure 121: Welcome window

5. Click Next.

   Result: AutoStart 5.3 SP3 reminder to read the documents appears.

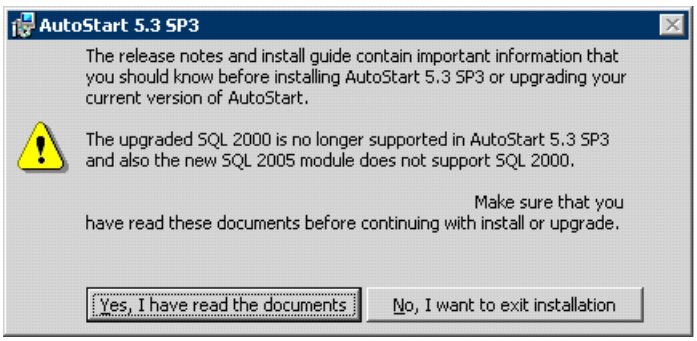


Figure 122: Reminder to read the documents

6. Click Yes, I have read the documents.

   Result: AutoStart 5.3 SP3 reminder is closed.

7. Click Next on the Welcome window.

   Result: The License Agreement window appears.

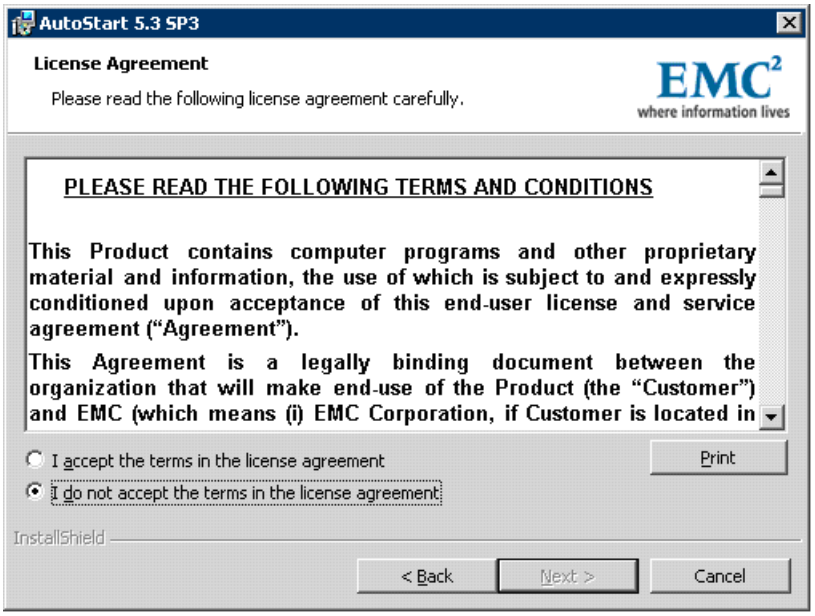


Figure 123: License Agreement window

8. Select the I accept the terms in the license agreement option.
9. Click Next.

   Result: The Custom Setup window appears.

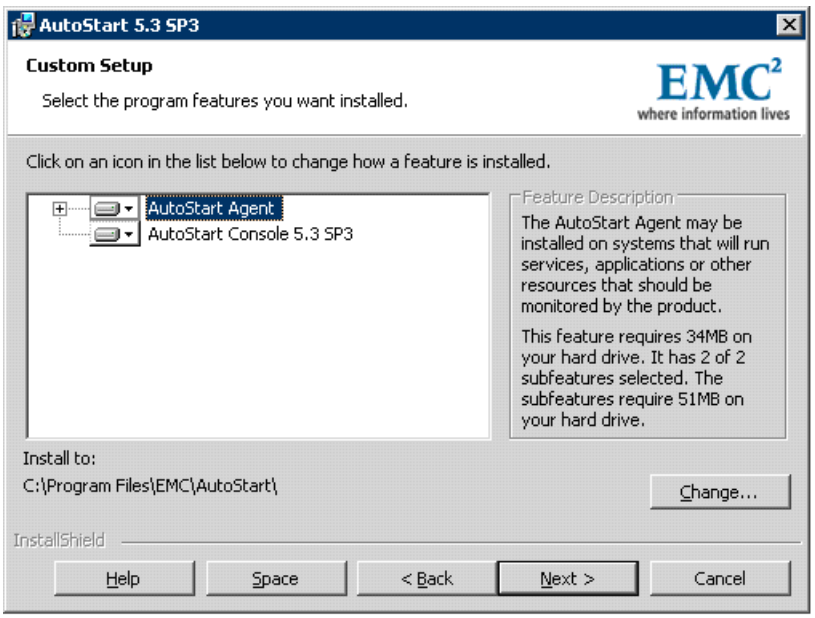


Figure 124: Custom Setup window

10. Click Change to change the installation path.

    Result: The Change Current Destination Folder dialog box appears.

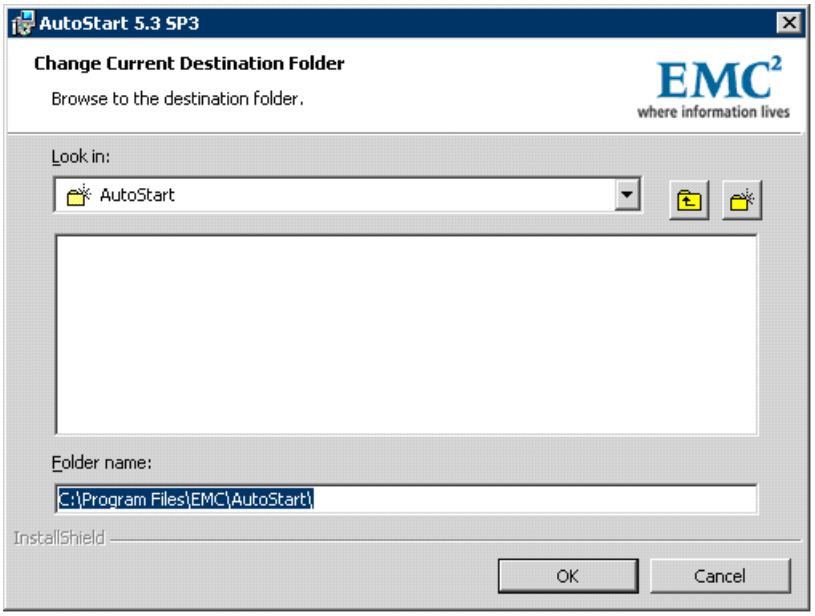


Figure 125: Change Current Destination Folder dialog box

11. In the Folder name field, change the drive letter from C to D, change the path to D:\Programs Files\EMC AutoStart.

Important:

You must install the software in the D:\Program Files\EMC AutoStart directory or the software does not work correctly.

12. Click OK.

    Result: Change Current Destination Folder dialog box closes and you are returned to Custom Setup window, which shows the correct installation path.

13. Click Next.

    Result: The Agent Connection Information window appears.

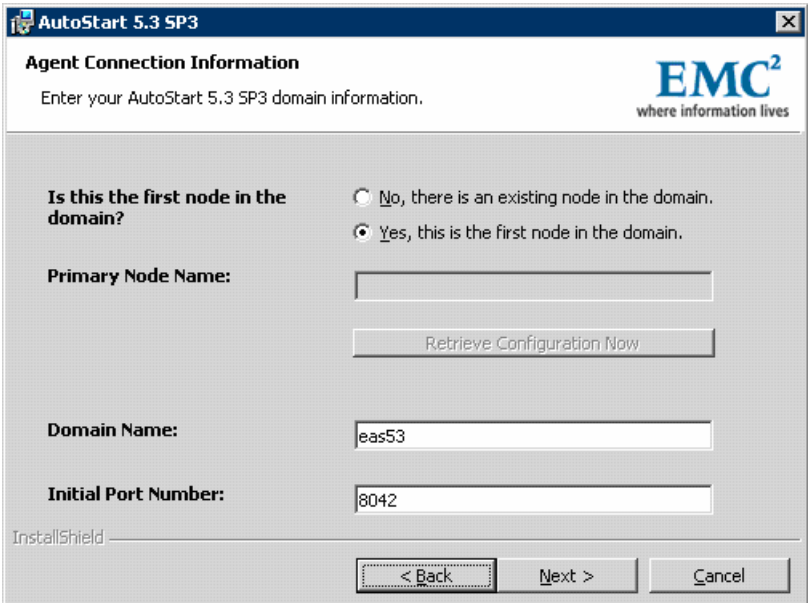


Figure 126: Agent Connection Information window

14. Select No, there is an existing node in the domain option button.

    Result: The field Primary Node Name is highlighted.

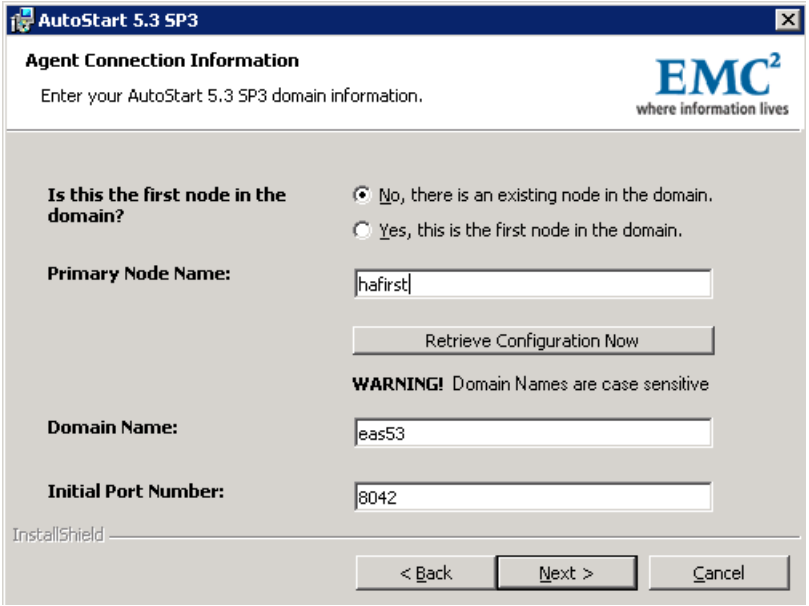


Figure 127: Agent Connection Information window - There is an existing node in the domain

15. Enter the host name of the existing server in Primary Node Name field.

Note:

"Retrieve Configuration Now" button can be pressed to see if Primary Node is accessible. If a primary node is accessible, Domain Name field will be filled automatically. Two next steps (16, 17) can be skipped. If a primary node is not accessible for some reason, the following error message appears:

Figure 128: AutoStart 5.3 SP3 warning message

Press OK to close the warning message; resolve the issue and proceed with the AutoStart 5.3 SP3 installation.

16. Enter the EMC AutoStart Domain Name. The AutoStart Domain Name must be the same name that you entered in the High Availability Configuration Wizard.

Note:

This document uses [AutoStart_Domain]. This value must be replaced with your AutoStart domain name.

17. Leave the Initial Port Number unchanged.
18. Click Next.

Result: The Mirroring Network Configuring and Product Licensing window appears. The list of licenses is disabled.

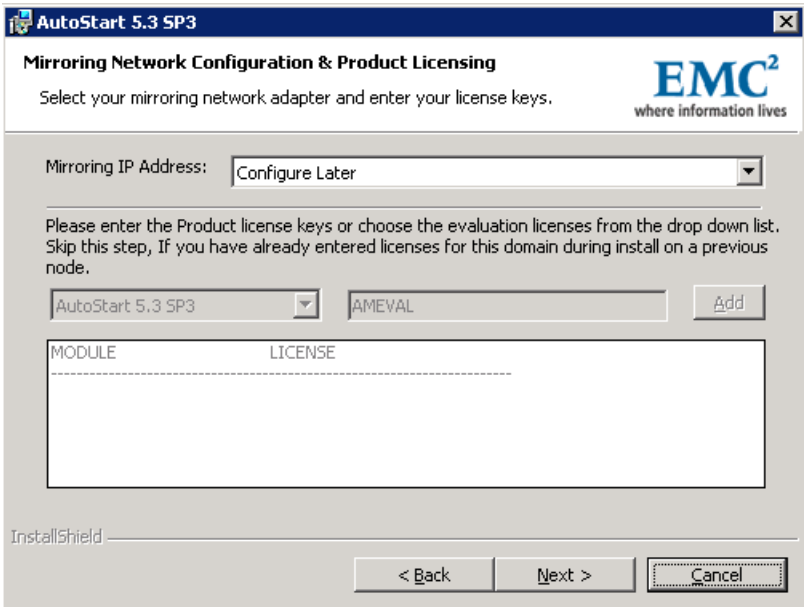


Figure 129: Mirroring Network Configuration and Product Licensing window

Note:

If you enter an invalid Primary Node Name, or the AutoStart Agent is not running on the specified node, an error message is displayed (similar to the following). Confirm that the Primary Node Name is correct and that the network is configured so that the name can be resolved on another node. Click OK to return to the Agent Connection Information window.

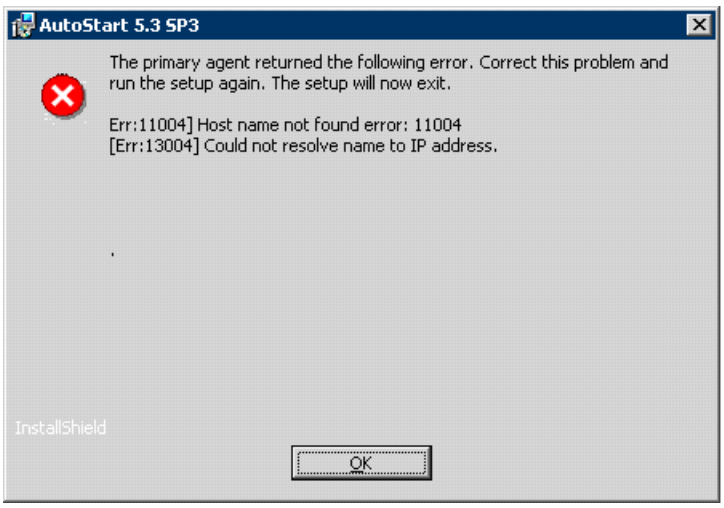


Figure 130: Error: Invalid name or agent not running on Primary node

Note:

If the administrator account of the replacement server does not exist in the AutoStart domain, the following error is displayed. Click OK to return to the Agent Connection Information window. Configure licensing and security on the existing server according to the chapter Add the node 2 administrator account to the AutoStart Console on node 1 on page 70.

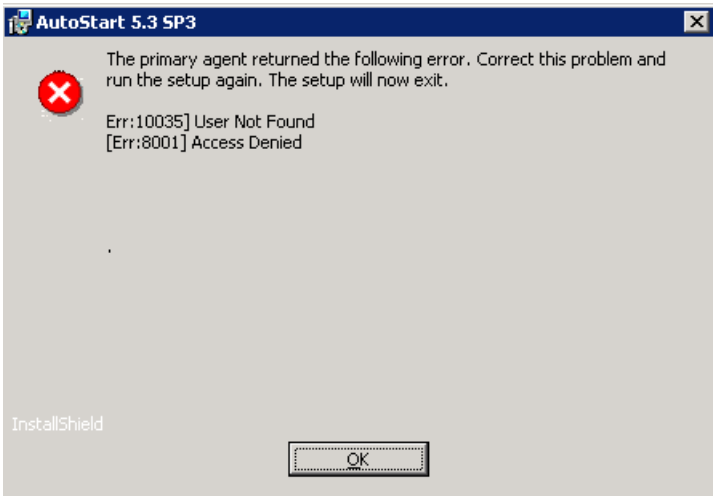
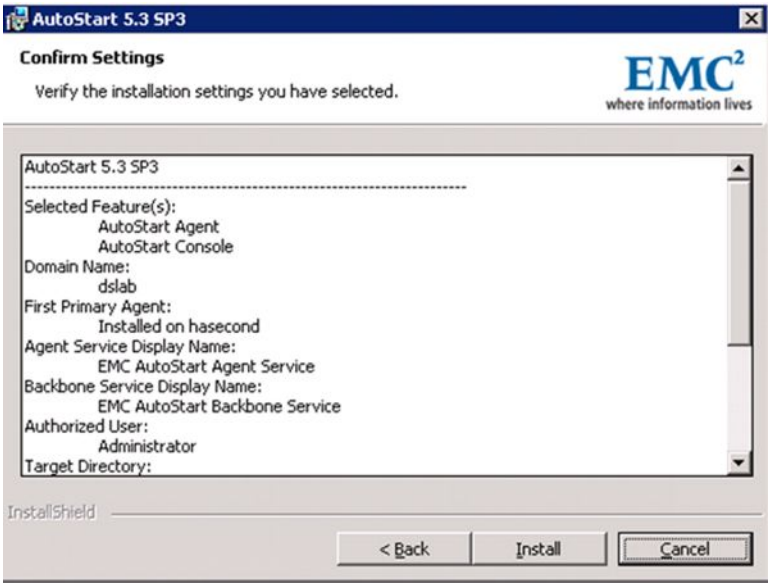


Figure 131: Primary Agent error

19. In the field Mirroring IP Address, select the IP address that was assigned to the Mirror NIC on the replacement server. The default value is Configure Later.
20. Click Next to continue.

    Result: Confirm Settings window appears.



21. Verify that the settings are correct.
22. Click Install to start the installation of the AutoStart Agent and Console software.

    Result: the Installing AutoStart 5.3 SP3 window appears and shows the status of installation.

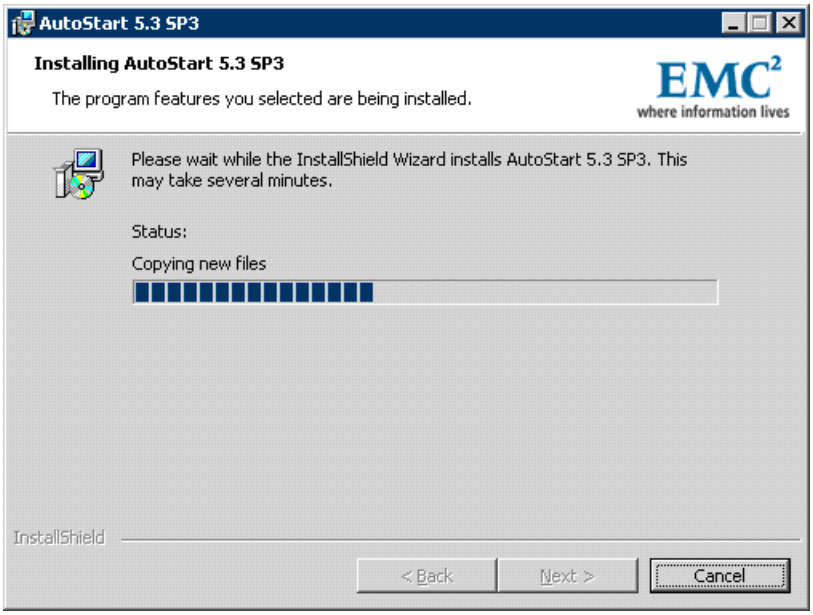


Figure 132: Installing AutoStart 5.3 SP3 window

23. Wait until the installation is complete and InstallShield Wizard Completed window appears.

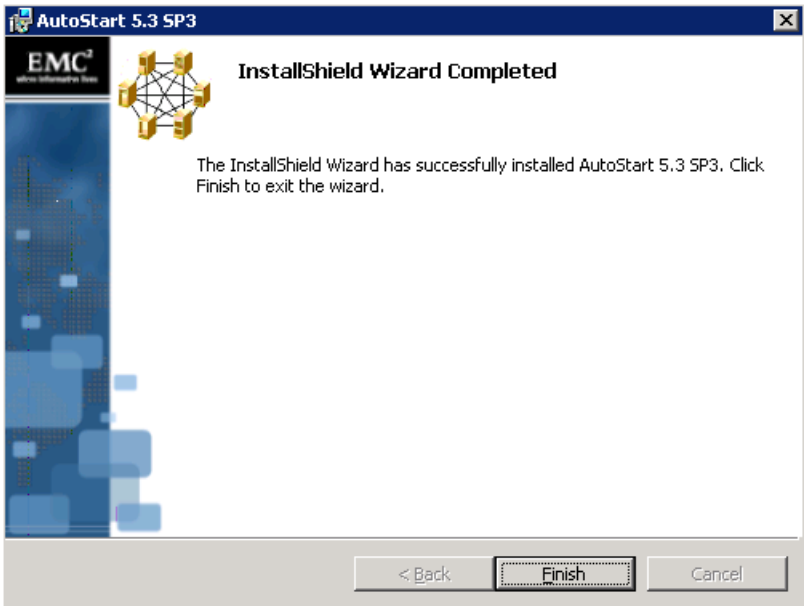


Figure 133: InstallShield Wizard Completed window

24. Click Finish.

    Result: The AutoStart 5.3 SP3 Installer Information dialog box appears.

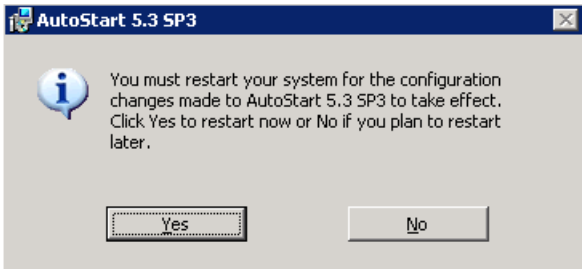


Figure 134: AutoStart 5.3 SP3 dialog box

25. Click No if there are patches to install or click Yes to restart the replacement server.

    Note:

    If there are any patches available for AutoStart 5.3 SP3 software, install the patches and then restart the replacement server.

26. Delete the directory EMC_AutoStart_5.3_SP3_Update from D:\temp.

RAID splitting for HA systems

Important:

Verifying consistency on the drives step must be performed on both nodes before any operations with RAID. See either *1005r Server Maintenance and Diagnostics* (NN44200-704) or *1006r Server Maintenance and Diagnostics* (NN44200-709) for details.

To perform any maintenance procedure

1. Split the RAID as described in Splitting the RAID on a 1005r server on page 226 or Splitting the RAID on a 1006r server on page 229.
2. Perform intended maintenance actions.
3. Perform synchronization of the RAID if no error or abnormal issues were encountered as described in Synchronize the RAID on a 1005r server after a successful maintenance procedure on page 227 or Synchronize the RAID on a 1006r server after a successful maintenance procedure on page 230. To return the system back to its original configuration if something has gone wrong, perform the following procedure: Synchronize the RAID on a 1005r server after an unsuccessful maintenance procedure on page 228 or Synchronize the RAID on a 1005r server after an unsuccessful maintenance procedure on page 228.

Splitting the RAID on a 1005r server

Ensure that your system is in full working order and the RAID hardware configuration is set up properly. See *1005r Server Maintenance and Diagnostics* (NN44200-704) for details.

Important:

As an added precaution, Avaya recommends that you perform a full system backup prior to performing a RAID-split. For more information about system backups, see the CallPilot Manager online Help.

Split the RAID on a 1005r server

1. On the active CP server, do the following:
   a. Launch the AutoStart Console
   b. Stop monitoring. For more information, see Disabling automatic failovers (stop monitoring) on page 180
   c. Take the resource group CallPilot offline (shutting down CallPilot). For more information, see Taking the CallPilot resource group offline on page 177

d. Wait for the resource group CallPilot to go offline

2. On the active CP server, load the MegaRAID console. Select Start > Programs > PowerConsole Plus > MegaRAID client
3. Ensure that Access Mode > Full Access is selected.
4. Click OK. The MegaRAID Power Console Plus window appears.
5. Ensure all drives are in ONLINE state (marked green).
6. In the Physical Devices section, right-click the second drive. The drives are displayed as follows: (0)A1-1-Onln (1)A1-2-Onln
7. Select Tools>Fail Drive from the shortcut menu. A message appears advising that marking the online drive Failed results in changes.
8. Ignore the warning and click OK. The drive status changes to FAILED and the color of the icon changes to red (for example, A01-2-Failed).

   At this point, the RAID is split, and the backup drive marked as FAILED is no longer written to. See Figure 135: RAID split on page 227.

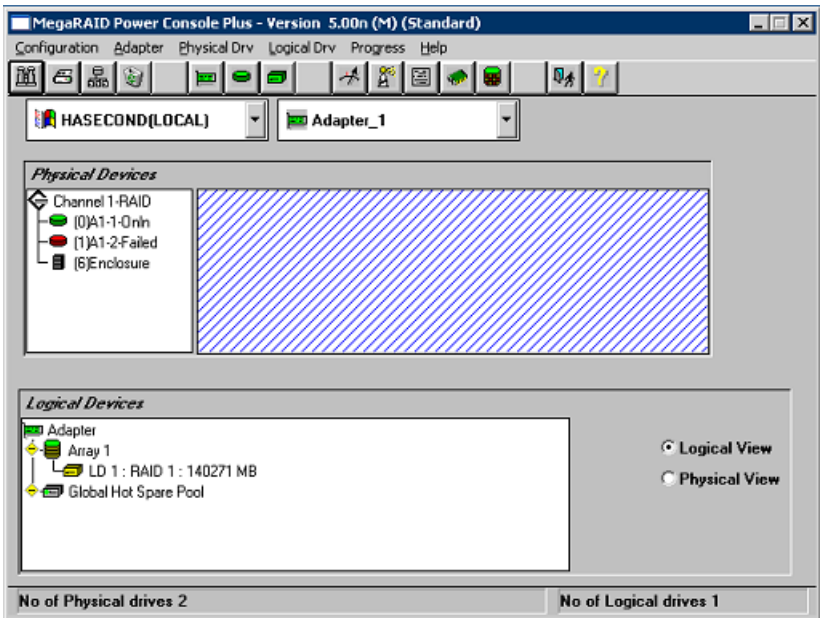


Figure 135: RAID split

9. Perform steps 2-8 on standby CP server.

Synchronize the RAID on a 1005r server after a successful maintenance procedure

1. On the active CP server (without shutting down the server), from Windows, click Start > Programs > Power Console Plus > MegaRAID client.

   Note:
   Ensure that Access Mode > Full Access is selected.

2. Click OK. The MegaRAID Power Console Plus window appears.

3. In the Physical Devices section, right-click the hard disk drive that is marked FAILED. Example: A01-2-Failed.

   Important:

   Do not make the failed drive online at this point, or data corruption can occur. If you failed the wrong drive by mistake, you must select rebuild to bring it back into service.

4. From the right mouse shortcut menu, select Rebuild. When the rebuild is complete, the drive status changes to ONLINE and the icon color changes to green.
5. Repeat steps 1-4 on standby CP server.

Important:

This process can take up to 6 hours. If the server reboots during the rebuild process, the rebuild continues when the server restarts. However, a power down or reboot is not recommended during the rebuild process.

Synchronize the RAID on a 1005r server after an unsuccessful maintenance procedure

1. Power down one of the CP servers.

   Important:

   Do not use the Power Console for the following procedure, or data corruption can occur.

2. Restart the other CP server and enter the Ctrl+M utility when prompted during system bootup.
3. From the Management menu, select Objects and press Enter.
4. Select Objects > Physical Drive and press Enter.
5. Select FAIL Drive for the drive that is online (A01-1-Onln). The drive is displayed as failed.
6. Select the second drive (previously taken offline as the backup drive and marked failed) and make it ONLINE. Ignore the warning message. The second drive is now marked ONLINE and the first drive is marked failed.
7. Exit the utility and press Ctrl+Alt+Delete to reboot the server. The system boots up to the original configuration before the PEP installation.
8. On the CP Server, perform the following steps:

   a. Launch the AutoStart Console.
   b. Start monitoring (to enable automatic failovers). For more information, see Enabling automatic failovers (start monitoring) on page 180.
   c. Bring the resource group online (starting up CallPilot). For more information, see Bringing the CallPilot resource group online on page 176.
   d. Test call processing functionality after the CP server boots into service.

9. Repeat steps 2-7 on the offline CP server.
10. Once both servers are confirmed to be online, open the Windows MegaRAID console and rebuild the failed drive using the same process described in Synchronize the RAID on a 1005r server after a successful maintenance procedure on page 227. The system is now back to its original configuration.

Splitting the RAID on a 1006r server

Ensure that your system is in full working order and the RAID hardware configuration is set up properly. See *1006r Server Maintenance and Diagnostics* (NN44200-709) for details.

Important:

As an added precaution, Avaya recommends that you perform a full system backup prior to performing a RAID-split. For more information about system backups, see the CallPilot Manager online Help.

Split the RAID on a 1006r server

1. On the active CP server, launch the RAID Web Console. Select Start > Programs > RAID Web Console 2 > StartupUI
2. Enter the same credentials used for Windows login and ensure Full Access is selected from the Login Mode drop-down list.
3. Ensure all drives are in an Online state.
4. Right-click on the first drive and select Make Drive Offline.

   A message appears advising that marking the online drive Offline results in changes.
5. Ignore the first warning message. Click Confirm and Yes

   A message appears recommending that data is backed up prior to performing this operation.
6. Click Confirm and Yes.

   At this point, the RAID is split and the backup drive marked as Offline is no longer written to. See Figure 136: RAID split on page 230.

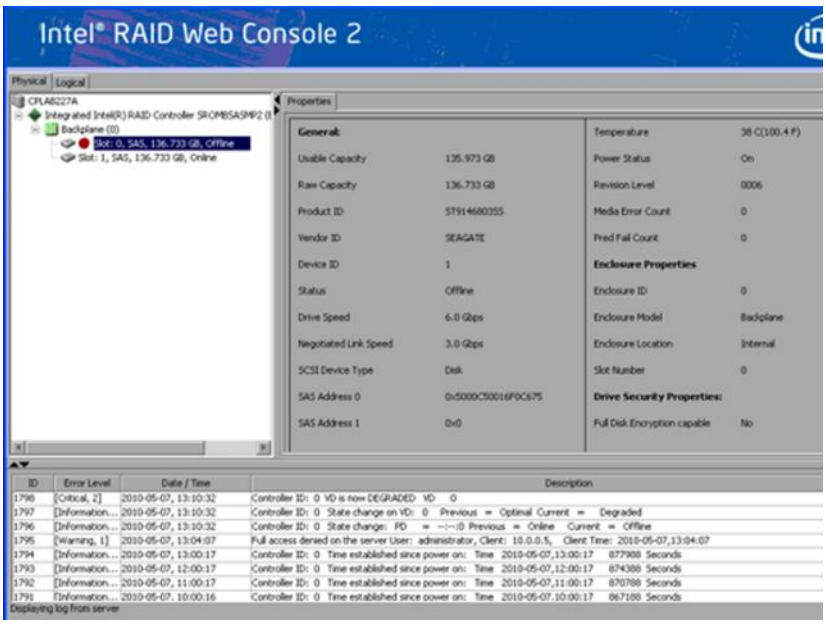


Figure 136: RAID split

7. Perform steps 1-5 on the standby CP server.

Synchronize the RAID on a 1006r server after a successful maintenance procedure

1. On the active CP server (without shutting down the server), from Windows, click Start > Programs > RAID Web Console 2 > StartupUI.
2. Enter Windows login credentials ensure Full Access is selected from the Login Mode drop-down list.
3. Click OK. The RAID Web Console window appears.
4. From the Physical tab, right-click the hard disk drive that is marked Offline and select Rebuild.

   Note:

   You can monitor the rebuild process by opening the Windows RAID application.

   When the rebuild is complete, the drive status changes to ONLINE and the icon color changes to green.

   Important:

   Do not make the failed drive online at this point, or data corruption can occur. If you failed the wrong drive by mistake, you must select Rebuild to bring it back into service.

5. Repeat steps 1-4 on standby CP server.

Important:

This process can take up to one hour. If the server reboots during the rebuild process, the rebuild continues when the server restarts. However, a power down or reboot is not recommended during the rebuild process.

Synchronize the RAID on a 1006r server after an unsuccessful maintenance procedure

Important:

Do not use the RAID Web Console for the following procedure or data corruption can occur.

1. Restart the other CP server and enter the Ctrl+G utility when prompted during system bootup.
2. Select Physical View/Physical Drive then the Make Drive Offline radio button, and click Go for the first drive.
3. Ignore the warning message and click Yes.
4. Click Home

   The drive is now displayed as Offline.
5. Select the second drive (previously taken offline as the backup drive and marked failed) and make it ONLINE. Ignore the warning message. The second drive is now marked ONLINE and the first drive is marked Offline.
6. Exit the CTRL+G utility and press Ctrl+Alt+Delete to reboot the server. The system boots up to the original configuration before the maintenance procedure.
7. After the system is fully operational, open the RAID Web Console and rebuild the drive marked Offline using the same process described in Synchronize the RAID on a 1006r server after a successful maintenance procedure on page 230.

CallPilot Manager, Channel Monitor

The status of channels in Channel Monitor is specific to each CallPilot node in a High Availability pair, and is not synchronized between the nodes. In addition, the status is saved to each node's independent data, which can create unexpected conditions during Resource Group operations, such as bringing the CallPilot Resource Group online, relocating the CallPilot Resource Group (manual failover), and after system defined automatic failovers.

For example, if all channels are stopped on the active CallPilot node during a maintenance activity, such as during a Feature Expansion procedure, the channel status is saved to the node's independent data (not synchronized between nodes).

When the Resource Group is brought online or relocated via a failover to a CallPilot node, the channels will be enabled or disabled depending on the information in the node's independent data, which was saved from the last status change when the node was in service. Channels

can be enabled through Channel Monitor in CallPilot Manager if necessary. The status change (enabled) will be saved to the node's independent data.

Chapter 7: Upgrades, migrations, and feature expansion

In this chapter

Introduction on page 233

Feature Expansion: Adding the High Availability feature to an existing CallPilot 5.0 1005r or 1006r server on page 237

Note:
The screen shots displayed in this chapter are from a 1005r server. The various screens will look slightly different if you are working with a pair of 1006r servers.

Introduction

For the High Availability feature, there are minimal differences between the upgrade and platform migration procedures and the new system installation procedure. The main differences are:

- You must restore data from a backup as part of the upgrade or platform migration.
- You must restore data on both of the servers in the pair when performing the upgrade. Restoring the data is required to ensure that all of the registry settings in the backup (for example, the LDAP search base) are restored correctly.
- You must modify and add settings in Configuration Wizard (for example, NIC card settings).

Scenario 1: If you are upgrading or migrating to Avaya CallPilot® 5.0 1005r or 1006r server and are adding the High Availability feature, do the following:

1. Follow the instructions in the Avaya *CallPilot Upgrade and Platform Migration Guide* (NN44200-400) to upgrade or migrate your server to a CallPilot 1005r or 1006r server running CallPilot 5.0.

Note:

Do not enable the High Availability feature when running the Configuration Wizard.

2. Follow the instructions outlined in Feature Expansion: Adding the High Availability feature to an existing CallPilot 5.0 1005r or 1006r server on page 237 to introduce a second 1005r or 1006r server and to configure the two servers as a High Availability pair.

Scenario 2: If you have a CallPilot 5.0 1005r or 1006r server and are adding the High Availability feature, follow the instructions outlined in Feature Expansion: Adding the High Availability feature to an existing CallPilot 5.0 1005r or 1006r server on page 237 to introduce a second server and configure the two identical servers as a High Availability pair.

After you make any changes to a High Availability configuration, the changes must be transparent to the end users, including any existing CallPilot Reporter, CallPilot Manager, Desktop, My CallPilot and Application Builder installations, as well as the switch. To ensure this transparency, the ELAN IP address, CLAN IP address, and host name used by the original CallPilot server must be used as the new Managed (virtual) IP address for the pair of High Availability servers. Because the Managed IP addresses and host name are visible to the outside world, by reusing the current IP addresses and host name, the changes to the server configuration are invisible to the applications. New ELAN IP address, CLAN IP address, and host names are required for both the original CallPilot server and the new CallPilot server. All IP address and host name changes must be made before you import the AutoStart definition file in order for the software to work correctly.

If you have an existing CallPilot 5.0 1005r or 1006r server (running in a non-High Availability configuration) a feature expansion can be performed to add the High Availability feature to the server, however, a second 1005 or 1006r server (running CallPilot 5.0 with the High Availability feature) is required to complete the High Availability system.

Note:

The High Availability pair must consist of the same server type. A mixture of server types is not supported. For example, a High Availability pair can not consist of a 1005r and a 1006r.

Note:

Application Builder is a graphical program that you use to create CallPilot applications that callers access as dialable services. Application Builder is installed on a customer provided PC. In the past (non-HA configuration) we have been able to access Application Builder over a remote TCP/IP connection utilizing RRAS. In the HA environment each 1005r or 1006r server requires its own unique host name, ELAN IP address, and CLAN IP address. In addition, the pair of servers are assigned a Managed (or virtual) host name, Managed ELAN IP address, and Managed CLAN IP address to make the pair of servers look like a single CallPilot server to the end clients. This new architecture does not make it possible to access application builder over a TCP/IP connection.

The procedure is the same as the new system installation procedure documented in Install and configure the High Availability pair on page 35, with the following exception.

Important:

Before installing the AutoStart software on the existing server, new IP addresses (CLAN and ELAN) and a new host name must be assigned to the existing CallPilot 1005r or 1006r server.

Providing a new host name and IP addresses is required to reuse the existing host name and IP addresses as the Managed host name and IP addresses. As a result, any existing users or applications can continue to access the 1005r or 1006r server without requiring configuration changes.

Guidelines

This section provides a basic overview of the tasks required to perform an upgrade or migration. Read this list and then proceed to the *CallPilot Upgrade and Platform Migration Guide* (NN44200-400) for detailed procedures.

1. On your current system (pre-release 5.0) take note of all networking information: host name, CLAN IP address, ELAN IP address, installed PEPs/SU, and installed languages.

   The networking information (host name and IP addresses) is required when entering in the Managed CLAN host name, Managed CLAN IP address, and Managed ELAN IP. (Estimated time: 10 minutes)

2. Install the CallPilot 5.0 Upgrade Wizard on the pre-release 5.0 system, which will be upgraded or migrated. (Estimated time: 15 minutes)

3. Run the CallPilot Upgrade Wizard.

   During the Upgrade Wizard you are asked to perform a full backup. If a backup is done to disk (that is, backed up to a network location), then it is possible to restore both CP1 and CP2 at the same time, which saves time to be in service. (Estimated time: 40 to 160 minutes depending on system and database size)

4. Upgrade only—Once the Upgrade Wizard is completed and a full back up is performed, install the CallPilot 1005r or 1006r Release 5 image on CP1. The second 1005r (CP2) comes preinstalled with Release 5.0 from the factory. Log on to the CP1 and CP2 servers using the default login user name and password (administrator / Bvw250). (Estimated time: 40 minutes)

   Migration and Upgrade—The CallPilot 1005r or 1006r Release 5.0 image comes preinstalled at factory. Log on to both CP1 and CP2 system using default login user name and password (administrator / Bvw250) (Estimated time: 0 minutes)

5. On both CallPilot servers (CP1 and CP2), configure new computer names and IP addresses for the CLAN. The computer names and IP addresses are new as the current CLAN host names and IP addresses are reused as the Managed CLAN host name and IP address for the High Availability pair. Otherwise, proceed to next step.

(This would be required in order to perform a system restore from disk [network drive]). (Estimated time: 10 minutes)

6. Run the CallPilot Setup Wizard on CP1 and CP2. (Estimated time: 30 minutes per server; includes PEP installation)
7. When prompted to perform a restore, select Yes. Both CP1 and CP2 can be restored at the same time if you are restoring from a disk (that is, a network location). Otherwise, CP1 must be completely restored before CP2 can be restored. (Estimated time: 180 minutes per server)
8. Run the Configuration Wizard on CP1. Do not enable High Availability during network configuration (ensure that the High Availability mode check box is not selected). Restart CP1 when prompted. (Estimated time: 40 minutes)

   If you are performing the restore from tape, CP2 can begin the restore at this point.
9. On CP1, you can begin testing to ensure voice services and channels are properly working. (Estimated time: 120 minutes)
10. Run the Configuration Wizard on CP2. Do not enable High Availability during network configuration (ensure that the High Availability mode check box is not selected). Restart CP2 when prompted. (Estimated time: 40 minutes)
11. If testing was satisfactory on CP1, run the Configuration Wizard again on CP1 and enable the High Availability feature, add the new network parameters, and restart when prompted. (Estimated time: 10 minutes)

    Note:

    To do this, you can use the CallPilot Individual Feature Configuration [Express Mode] and select Network Interface Card Configuration check box.
12. Run the Configuration Wizard again on CP2 and enable the High Availability feature, add the new network parameters, and restart when prompted. (Estimated time: 10 minutes)

    Note:

    To do this, you can use the CallPilot Individual Feature Configuration [Express Mode] and select Network Interface Card Configuration check box.
13. Run Stage 1 of the High Availability Configuration Wizard. For the Managed CLAN host name, Managed CLAN IP address, and Managed ELAN IP address, use the host name and IP addresses that you noted in item 1 (that is, the host name and IP addresses from the pre-release 5.0 system). (Estimated time: 5 minutes)
14. On CP1, install the EMC AutoStart software and add the administrator account of CP2. (Estimated time: 15 minutes)
15. Install the EMC AutoStart software on CP2. (Estimated time: 10 minutes)
16. Configure the EMC AutoStart software on CP1. All the configuration is done from CP1. (Estimated time: 30 minutes)

17. Run Stage 2 of the High Availability Configuration Wizard. (Estimated time: 5 minutes)
18. Complete the EMC AutoStart configuration. (Estimated time: 5 minutes)
19. Bring the CallPilot resource group online. (Estimated time: 10 minutes)
20. Bring the CP1 and CP2 resource groups online. (Estimated time: 5 minutes)
21. Test the system. (Estimated time: 120 minutes)
22. Create the CallPilot Report connections. (Estimated time: 20 minutes)
23. If required, join the Windows domain. (Estimated time: 30 minutes)

Feature Expansion: Adding the High Availability feature to an existing CallPilot 5.0 1005r or 1006r server

A CallPilot High Availability system consists of either two 1005r or two 1006r servers that work as peers. At any time, one server is active while the other server is in standby mode.

If you have a CallPilot 5.0 1005r or 1006r server (running in a non-High Availability configuration), a feature expansion can be performed to add the High Availability feature to the server. However, a second 1005r or 1006r server (running CallPilot 5.0 with the High Availability feature) is required to complete the High Availability system.

Note:

The High Availability pair must consist of the same server type. A mixture of server types is not supported. For example, a High Availability pair can not consist of a 1005r and a 1006r.

Use the procedures in this section to do the following:

- Add a second 1005r or 1006r server running CallPilot 5.0 to an existing 1005r or 1006r server, respectively, running CallPilot 5.0.
- Configure the two servers as a High Availability pair.

For the purposes of this section, the servers are referred to as CallPilot server 1 (CP1) and CallPilot server 2 (CP2) where:

- CP1 is the existing 1005r or 1006r server. (CP1 must be running CallPilot 5.0 or must have been upgraded or migrated to run CallPilot 5.0.)
- CP2 is the new 1005r or 1006r server that is being added (a new server that has CallPilot 5.0 installed from the factory).

Feature expansion task list

The following table outlines the tasks and procedures that must be completed to add the High Availability feature. Ensure that you complete each task in the ordered presented.

Table 12: Task List: High Availability feature expansion

Task	Estimated time	Procedures
Prepare the switch	60 minutes	See Preparing the switch on page 239
Install the new 1005r or 1006r server (CP2)	210 minutes	See Install the new 1005r or 1006r server (CP2) on page 239
Record the current server configuration from CP1	5 minutes	See Recording the current server configuration (CP1) on page 240
Run the Upgrade Wizard on the existing 1005r or 1006r server (CP1)	160 minutes depending on system and database size	See Running the Upgrade Wizard on CP1 on page 241
Prepare the new 1005r or 1006r server (CP2)	10 minutes	See Prepare the new 1005r or 1006r server (CP2) on page 244
Run the Setup Wizard on the new 1005r or 1006r server (CP2)	210 minutes (includes restore time)	See Running the Setup Wizard on CP2 on page 245
Configure CP1 using the CallPilot Configuration Wizard	40 minutes	See Configuring CP1 using the Configuration Wizard on page 249
Configure CP2 using the CallPilot Configuration Wizard	40 minutes	See Configuring the replacement server using the Configuration Wizard on page 252
Complete the High Availability feature configuration	215 minutes	See Completing the High Availability feature configuration on page 257

Prepare the switch

The switch configuration must be completed before the High Availability feature can be implemented.

Preparing the switch

1. Configure the Meridian 1 or Avaya Communication Server 1000 switch.

   For detailed information, see the following:

   - *Meridian 1 and CallPilot Server Configuration* (NN44200-302)
   - *Communication Server 1000 and CallPilot Server Configuration* (NN44200-312)

   Note:
   Both High Availability servers must use the same Control Directory Number (CDN).

   Note:
   Server CP2 requires dedicated MGate cards in the switch to function correctly. Both the number of MGate cards and the switch configuration must be the same as for the existing CallPilot server CP1.

2. Prepare the switch by adding additional MGate cards as required.
3. Program the switch as necessary.

Install the new 1005r or 1006r server (CP2)

A second server is required to complete the High Availability pair. The following procedure assumes that this 1005r or 1006r server has come from the factory with CallPilot 5.0 and the High Availability feature installed.

Installing the new server (CP2)

1. Refer to the following documents to perform the steps outlined in this procedure.

   - 1005r Server Hardware Installation (NN44200-308). or 1006r Server Hardware Installation (NN44200-320)
   - Installation and Configuration Task List (NN44200-306)

2. Unpack the server.
3. Install CP2 in the same rack as CP1.

   Ensure that the two servers are close enough so that they can be connected by the crossover LAN cables for the HB1, HB2, and MIRROR connections. The cables must be long enough to connect the two servers.

   Important:
   Do not connect the HB1, HB2, and MIRROR crossover LAN cables at this time.

4. Connect the peripheral equipment to both servers.

The peripheral equipment includes the monitor, keyboard, and mouse.

5. Power on the CP2 server.

   Result: The server starts and the Windows 2003 Mini-Setup runs. During the Windows 2003 Mini-Setup, the server automatically restarts twice.

Record the current 1005r or 1006r server configuration (CP1)

To ensure that end users can access the pair of High Availability servers and that they do not require any changes to their systems, the following information for the server (CP1) must be recorded and then reused as the managed networking parameters:

- existing computer name
- ELAN IP address
- CLAN IP address
- installed PEPs and SUs
- installed languages

Recording the current server configuration (CP1)

1. Record the current computer name.

   The computer name will be used as the Managed computer name of the High Availability pair.

2. Record the current ELAN IP address.

   The ELAN IP address will be used as the Managed ELAN IP address of the High Availability pair.

3. Record the current CLAN IP address.

   The CLAN IP address will be used as the Managed CLAN IP address of the High Availability pair.

4. Record the IDs of any PEPs and SUs that are installed on the current server.

   The same PEPs and SUs must be installed on both servers in the High Availability pair.

5. Record the languages that are installed on the current server.

   The same languages must be installed on both servers in the High Availability pair.

Run the Upgrade Wizard on the existing server (CP1)

The Upgrade Wizard must be run on the existing 1005r or 1006r server (CP1) to generate a backup that can be restored on the new 1005r or 1006r server CP2.

For Scenario 1, you do not have to perform the following procedure because a backup was created when you ran the Upgrade Wizard during your upgrade or migration process.

For Scenario 2, you must complete the following procedure.

Running the Upgrade Wizard on CP1

1. Launch the CallPilot 5.0 Upgrade Wizard by clicking **Start > Programs > CallPilot > Upgrade Wizard**.

   Note:
   While the CallPilot 5.0 Upgrade Wizard runs, all screen information is written to the log file in the following folder: `D:\Nortel\Data\UpgradeWizard.log`

   Result: The **CallPilot 5.0 Upgrade Wizard - Welcome** screen appears.
2. On the CallPilot 5.0 Upgrade Wizard - Welcome screen, click **Next**.

   Result: The **Platform Validity Check** screen appears.
3. Wait while the CallPilot 5.0 Upgrade Wizard analyzes your platform.

   Result: The **Platform Validity Check** screen displays which software and hardware are currently on the system, and evaluates the status of each item.
4. Click **Next** to continue.

   Result: If all components meet the minimum requirements, the **Data Validation – Ready to Validate Data** window appears
5. Click **Next** to validate your data.

   Result: The **Data Validity Check** screen appears. A process bar shows how much of the data has been validated.
6. Wait while the CallPilot 5.0 Upgrade Wizard checks the data.

   Result: The result of the Data Validity check is displayed in the **Data Validity Check** window.
7. Click **Next**.

   Result: The **Data Validation Complete** screen appears.
8. Click **Next**.

   Result: The **Serial Number and Key Code** screen appears.

You need your CallPilot 5.0 keycode, serial number, and image CDs or DVDs to proceed.

9. Click **Next** to verify your CallPilot keycode.

   Result: The **Feature Verification** screen appears. The **Keycode Validation** result is displayed at the bottom of the window.

10. Check your installed features against the screen list.

    If a feature is missing from your new keycode, contact your distributor to obtain a new keycode.

11. Click **Next** to verify that your image CD or DVD matches your CallPilot platform.

    Result: The **Image Media** screen appears.

12. Insert the CallPilot 5.0 Image CD or DVD into the CD or DVD drive, and enter **Z:** as the drive letter, and click **Next**.

13. Wait while the wizard checks that the inserted CD or DVD is valid for your platform.

    Note:
    If the CD or DVD is not valid, the wizard blocks the rest of the upgrade process and you must contact your distributor (channel partner) to obtain the correct CD or DVD.

    Result: The **Optional Language CD** validation screen appears.

14. Select the **Skip Language CD Validation** option.

    Important:
    You must use a CallPilot 5.0 Language CD when configuring a CallPilot 5.0 system. An earlier release (pre-5.0 Language CD) cannot be used.

15. Click **Next**.

    Result: The following message appears: “You have selected not to validate the Language CD. It is recommended that the validation is done. Are you sure you want to skip?”.

16. Click **Yes** to continue.

    Result: The **Full System Backup** screen appears.

    Caution:
    ANY MESSAGES RECEIVED AFTER BACKUP BEGINS ARE LOST

    The backup takes from 1 to 3 hours to complete and consumes considerable CPU resources. Any messages that come in while the backup is running are not included in the backup. To avoid losing any user messages, Avaya recommends that you courtesy down the system prior to starting the backup.

17. Select the type of backup medium for your CallPilot data.

    - If you choose to back up to tape:

Important:
This process overwrites the existing data on the tape.

Insert the tape into the tape drive and click **Next** to start the backup immediately. Proceed to the next step.

- If you choose to back up to disk:

  Click **Next** to choose the backup device. The **Full System Backup** screen appears. Click **List Devices**.

  Result: The screen displays the backup devices that are defined on your CallPilot server.

  - If no devices are listed, log on to CallPilot Manager and define your backup devices (**System > Backup/Restore > Maintain and configure backup devices**). Click **List Devices** again. Select the backup device you want to use and click **Next** to start the backup.
  - If the list is populated, select the appropriate backup device and click **Next** to start the backup.

18. When the **Full System Backup - Perform System Backup** screen appears, click **Start Backup**.
19. After the progress bar shows the percentage complete and displays the status, do the following:

IF	THEN
errors occur	• follow the displayed link and examine the log file for errors. • contact your distributor (channel partner) if you need assistance to resolve the errors. • click the **Restart** button to restart the backup process.
no errors occur	• click **Next**.

20. After the backup is complete, eject the tape from the tape drive (if the data was backed up to a tape).

    Important:
    Failure to remove the tape from the drive adds an hour or more to the restore process.

21. Click **Next**.
22. Click **Finish** to close the CallPilot 5.0 Upgrade Wizard.
23. Print or record the IP address information in the file `D:\Nortel\Data\IPCONFIGURATION.txt`.

Note:

You need the IP address information if your backup is on a network drive, or if you are downloading PEPs from the network prior to the restore process. You also need this IP address information to configure your Embedded LAN (ELAN) subnet and Avaya server subnet after the restore process. The IPCONFIGURATION.txt file is saved as part of your backup and is available after the restore.

Prepare the new 1005r or 1006r server (CP2)

The following procedures may be required depending upon your setup configuration.

- Manually change the server name. (The CallPilot Configuration Wizard can also be used to change the server name.)

  For more information, see Manually changing the server name on page 39.

- Manually set the IP parameters. (The CallPilot Configuration Wizard can also be used to set the IP parameters.)

  For more information, see Manually setting the IP parameters on page 40.

  Note:

  The procedures listed in the preceding bullets are performed under the following circumstances:

  a. If you are restoring from a network location. In order to perform a restore the CLAN IP address must first be set.

  b. If you are using a DNS as part of your network solution, then the DNS entries must be manually completed.

- Check the Primary DNS suffix.

- Install antivirus software on both servers. (optional)

  For more information about the antivirus software packages that are approved by Avaya for CallPilot, see the P-2007-0101-Global : CallPilot Support for Anti-Virus Applications bulletin.

Run the Setup Wizard on CP2

Run the Setup Wizard on the new 1005r or 1006r server (CP2), restoring the data from the backup created by the Upgrade Wizard that was run on CP1.

Caution:

Ensure you use the backup created from the CallPilot 5.0 Upgrade Wizard for the following reasons:

1. The backup provides the most current view of the system.
2. The CallPilot 5.0 Upgrade Wizard corrects the data prior to the backup.
3. Using an earlier backup can result in issues encountered during the restore process.
4. The backup from the CallPilot 5.0 Upgrade Wizard includes the CallPilot 5.0 Upgrade Wizard logs so that they can be brought forward to CallPilot 5.0. These logs can be used by Avaya Technical Support to troubleshoot the system.

Running the Setup Wizard on CP2

1. Log on to the new CallPilot 1005r or 1006r server after the Windows Mini-Setup is complete. The default password for the Administrator account is Bvw250.
2. The Setup Wizard automatically launches if you log on to an unconfigured CallPilot server. A CallPilot server, freshly upgraded to CallPilot 5.0, is not configured. You can also launch the Setup Wizard manually by clicking Start > Programs > CallPilot > Setup Wizard.

   Result: The CallPilot Setup Wizard welcome screen appears.

   Note:

   If you exit after a successful restore and before the Setup Wizard is finished, you can continue or restart the Setup Wizard.

   If your backup is on a network drive or you are downloading PEPs from the network, you must restore your network settings:

   a. Specify the IP address and subnet mask for the Avaya server subnet. Do not change your computer name unless necessary.
   b. Specify the gateway for the Avaya server subnet (CLAN).
   c. Restart the system (if prompted by Windows).
   d. Log on to the CallPilot server. The default password for the Administrator account is set to Bvw250.

   If your backup is on tape, continue to the next step.

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

   Result: The Service Update (SU) / PEP Installation screen appears.

   Important:

   If you downloaded PEPs, close the wizard, install the PEPs, and restart if required. When the system is in service, restart the wizard and select No on the Installing SU/PEP screen. If your PEPs are on CD, continue with Step 4.

4. If Service Updates (SUs) or PEPs are available, you must install the same SUs and PEPs that are installed on CP1. Select Yes or No and click Next.
   - If you choose Yes, install SU/PEPs:

     Result: The Installing SU/PEP screen appears.

     i. Install all the required SUs and PEPs.

     Note:
     After you install all the SUs and PEPs, restart (if required).

     ii. If no restart was required, click Next to continue. Otherwise, restart the server.
   - If you choose No, do not install SU/PEPs now:

     Result: The Platform Validity Check screen appears.
5. View the items on the Platform Validity Check screen and click Next.

   Note:
   If your server does not meet the minimum hardware and software requirements for the upgrade, contact your support organization.

   Result: The Telephony Board Validation screen appears.
6. If the system detects an error, an error message appears. You cannot continue with the Setup Wizard. Do the following:

   a. Power off the system.
   b. Install the boards in the correct locations.
   c. Restart the system.
   d. Log on to Windows and restart the Setup Wizard.
   e. Continue to the next step.

   If your board configuration is correct, click Next to continue to the next step.

   Note:
   The following synchronization and disk space checks only pause for display if the checks fail. Results of the checks are written to the setup log.
7. The Setup Wizard performs a disk space check. There must be enough free disk space to restore your backed up data.

IF the disk	THEN
does not have enough free space	• the Checking Free Disk Space screen appears. • free up space on drive D by removing unnecessary files.

IF the disk	THEN
	• follow the link on the screen and use the instructions to free up enough space, and then click Next. • the wizard performs another check and if there is still not enough space, the Checking Free Disk Space screen reappears. • If there still is not enough free disk space, exit the wizard and call your support organization.
has enough free space	• the Setup Wizard continues. **Note:** Results of the disk space check are written to the Setup Wizard log.

Important:

The data restoration takes from 1 to 3 hours to complete.

Only use the backup created by the CallPilot 5.0 Upgrade Wizard.

8. On the Selecting Upgrade of the CallPilot screen, choose Yes to continue with the restore process. Do not choose No.

   Result: The Restore Medium Selection screen appears.

9. Choose the medium on which your backup is stored.

   - If you choose to restore from disk:

     Result: The Choose Remote Disk screen appears.

     i. Find the remote disk to restore from and click on it.

     ii. Click Next to continue.

   - If you choose to restore from tape:

     i. Make sure the tape is firmly in the tape drive and click Next. (If a tape is already in the drive, remove it and reinsert it. Otherwise, a tape list can take up to two hours.)

        Result: The List Backups screen appears.

     ii. Click List Backups to view a list of valid backups on your backup medium.

     iii. The available backups appear in the List of Backups table.

     iv. Select the backup that you want to use for the restore and click Next.

        Result: The Performing Restore screen appears. The CallPilot services are shut down and the Wizard automatically starts the

restore operation. The progress bar shows the percentage complete and the number of errors.

10. Determine if the restoration was successful.

IF the restoration	THEN
was not successful	• review the log files. • Click Retry to start the restoration again. • If you are still not successful, contact your support organization.
was successful	• click Next to continue.

Result: The Ready to Upgrade Database screen appears.

11. Click Next to start the database upgrade.

The warning screens for the Unsupported SMTP authentication option and the Unsupported IMAP authentication option can appear (same screens as in the Upgrade Wizard). Click Next through those screens and the database upgrade starts.

Result: The database upgrade starts and the Upgrading Data screen appears.

IF the database upgrade is	THEN
not successful	• click Upgrade Database to try again. **Note:** If subsequent attempts to upgrade the database are not successful, contact your support organization.
successful	• the Setup Wizard continues.

12. Click Next to complete the Setup Wizard.

Result: The Finished screen appears.

13. Read the information displayed on the Finished screen and click Finish.

Result: A screen appears warning you that the system restarts automatically.

14. Click OK.

Result: The system restarts.

Configure CP1 using the Configuration Wizard

Configuring CP1 using the Configuration Wizard

1. On the existing CallPilot 1005r or 1006r server (CP1), log on to CallPilot Manager:
   a. After the Windows log on screen appears, log on with the current password.
   b. Launch Internet Explorer.
   c. Enter http://<server name or IP address>/cpmgr in the URL address box.

      Result: The CallPilot Manager Logon Web page appears.
   d. Log on using your existing CallPilot logon information. Enter information into the following:
      - Mailbox Number—Enter your existing mailbox number (000000).
      - Password—Enter your existing password for mailbox 000000.
      - Server—Specify the name or the IP address of the CallPilot server that you want to configure. (The server name may have changed during the upgrade or platform migration.)

      Note:
      When you launch Internet Explorer, you may see a box that says "M/S IE Enhanced Security config is currently enabled on your server. This advanced level of security reduces risk." Avaya recommends that you do not lower the security level. Avaya also recommends that you do not select the check box to not show the message again. If you do lower the security level and you try to access a Web site off the server, it may be blocked by the security setting. You do not receive a warning but a blank screen appears.
   e. Click Login.

      Result: The system may prompt you to change the password for the Administrator mailbox.
   f. If prompted, do not change the password.

      Result: The main CallPilot Manager screen appears.
2. Click the Configuration Wizard icon.

   Result: A dialog box appears, prompting you to choose either an Express or Standard setup.
3. Select CallPilot System Configuration (Standard Mode).
4. Click OK.

Result: The Configuration Wizard: Welcome screen appears.

Note:

Because the CallPilot system is not yet configured, an error dialog box can appear while you run the Configuration Wizard. Disregard the error message by closing the dialog box, and continue the configuration procedure.

5. On the Welcome screen, click Next.

   Result: The Keycode and serial number screen appears.

6. If you have a new CallPilot 5.0 keycode with the High Availability feature included, enter the serial number and new keycode.

   If your CallPilot 5.0 keycode includes the High Availability feature (but High Availability is not yet enabled), click Next.

   Result: The Feature Verification screen appears.

7. Ensure that the details on the Feature Verification screen match your expectations and click Next.

   Note:

   If a feature is missing or is not what you expected, acquire a new keycode from your Avaya distributor.

   Result: The Server Information screen appears.

8. On the Server Information screen, enter the new host name in the Computer Name field.

   Important:

   The computer names of the High Availability servers must contain only alphanumeric characters. Nonalphanumeric characters (such as a hyphen [-]) are not supported.

   Note:

   You must change the computer name of CP1 so that the current name can be reused as the Managed computer name for the High Availability pair.

9. Click Next.

   Result: The Password Information screen appears.

10. Select Leave the Password Unchanged.
11. Click Next.

    Result: The Multimedia Allocation screen appears.

12. Verify the number of MPB boards and, if applicable, DSP cards, and ensure that they match the hardware installed in the CallPilot server.
13. Change the Port Allocations as required.
14. Click Next.

Result: The Switch Information screen appears.

15. Verify the CDN configuration.

    If you need to make changes, do the following:

    a. Click New to add a new CDN.

       Result: The system prompts you for the CDN and the name of the application to dedicate to the CDN.

    b. Specify the CDN, choose the application, and then click OK.

       Result: The system returns you to the CDN Information page.

16. Click Next.

    Result: The Language Source Directory screen appears.

17. Select the Skip Language CD Validation option.

18. Click Next.

    Result: The CallPilot Local Area Network Interface screen appears.

19. On the CallPilot Local Area Network Interface screen, do the following:

    a. Make note of the current ELAN and CLAN IP addresses.

       Note:
       These ELAN and CLAN IP address values from the existing CallPilot 1005r or 1006r server (CP1) will be reused as the Managed ELAN/CLAN IP address for the pair of server in the new High Availability configuration.

    b. Change the ELAN and CLAN IP address values to the new values.

    c. Select the High Availability mode check box.

       Note:
       To enable High Availability, a proper keycode is required and the High Availability Mode check box must be selected.

    d. Enter IP information for the HB1, HB2, and MIRROR network interface cards.

       The following table shows the suggested default values for HB1, HB2, and MIRROR on CP1. If you do not use these suggested values, ensure that you use your new values throughout the configuration.

Network Interface Card (NIC)	IP Address	Subnet Mask
Heartbeat 1 (HB1)	192.0.0.10	255.255.255.0
Heartbeat 2 (HB2)	194.0.0.10	255.255.255.0
MIRROR	193.0.0.10	255.255.255.0

20. Click Next.

Result: The Ready to Configure screen appears.

21. Click Finish.

    Result: A dialog box prompts you to confirm the configuration.

22. Click OK to configure CallPilot.

    Result: The configuration is applied to the server. This task can take from 5 to 10 minutes to complete, depending on the number of languages installed and the number of programmed DSP cards. The Configuration Wizard displays progress information.

    After the configuration is applied to the server, a dialog box reminds you to restart the server for the configuration to take effect.

23. Click OK to dismiss the dialog box.

    Result: The system returns you to the main CallPilot Manager screen.

24. Log off CallPilot Manager and close the Web browser.
25. Restart CP1.

Configuring the replacement server using the Configuration Wizard

Important:

If you must go back into the Configuration Wizard at any time to correct any entries, note that the Database, LDAP, and AOS services must be started to gain access to CallPIlot Manager. The D:\Nortel\HA folder contains a file called stat_svr.bat that automatically starts any necessary services. This script can be run to start the required services.

Important:

Ensure that the dongle is installed on the replacement server.

Configuring the replacement server using the Configuration Wizard

Time required: 20 minutes (assuming one language is installed).

1. Launch the Internet Explorer Web browser on the replacement server.
2. In the address field, enter the following URL to start CallPilot Manager: http://localhost/cpmgr.

   Result: The CallPilot Manager Logon Web page appears.

3. Log on to CallPilot Manager using the administrator mailbox and default password created from the CallPilot Setup Wizard:.

   a. Under the User area, enter the following:

      i. The administrator mailbox number is 000000.

ii. The default password is 124578.

b. Under the Server area, enter the localhost in the Server field.

4. Click Login.

   Result: Change User Password window appears.

5. Change the password for 000000 administrator mailbox if necessary by doing the following:

   a. Enter the Current Password.

   b. Enter the New Password.

   c. Reenter the new password in New Password Re-entry field.

   d. Click Save.

      Result: Welcome to CallPilot Manager page appears.

6. Click Configuration Wizard.

   Result: Configuration Wizard: Welcome page appears.

7. Click Next.

   Result: The Keycode and serial number page appears.

8. Enter the following:

   a. In the Serial number field, enter the serial number of the dongle assigned to the CallPilot server. The serial number entered for the replacement server must be the same as the serial number entered for the existing server.

   b. In the Keycode field, enter the High Availability enabled keycode assigned to the CallPilot server. The keycode entered for the replacement server must be the same as the keycode entered for the existing server.

9. Click Next.

   Result: The Feature Verification page appears.

10. Ensure that all parameters are correct and that the High Availability feature is set to Mirroring.

11. Click Next.

    Result: The Server Information page appears.

12. On the Server Information page, do the following:

    a. In the Computer Name field enter the CallPilot server name.

    b. In the Time Zone field, select the correct time zone.

    c. Under Dialog Information, enter the Area Code and Country Code.

    d. Enter LDAP search base. For example, dc=nortel,dc=ca.

Note:

All values on the Server Information page for the replacement server must be the same as for the existing server. Use Table 4: High Availability system checklist on page 23 that you completed for both nodes.

13. Click Next option.

    Result: The Password Information page appears and Change the password option is selected.

14. On the Password Information page, do the following:

    a. In New Password field, enter the new password. The new password entered for the replacement server must be the same as the password used on the existing server.

    b. In Confirm the new password field, reenter the new password. The new password entered for the replacement server must be the same as the password used on the existing server.

    c. Click Next.

       Result: A warning message appears.

15. Click Ok to dismiss the warning message.

    Result: Password Information page reappears.

16. Click Next.

    Result: The Multimedia Allocation page appears.

17. Configure the MPB96 settings.

18. Click Next.

    Result: M1 Switch Information page appears.

19. Configure the switch information:

    a. Select the Switch Type. Switch Type must be the same for both nodes.

    b. Enter the Switch Customer Number. Switch Customer Number must be the same for both nodes.

    c. Enter the Switch IP Address. Switch IP Address must be the same for both nodes. See the Table 4: High Availability system checklist on page 23 containing the information for both nodes.

    d. Provision the channels as follows:

       Note:

       To automatically provision a number of channels you can enter the information for one channel, select the number of channels required, and then click Fill. The Configuration Wizard automatically datafills the channels, and increments the TNs, ACD Position ID, and SCN.

Note:
The number of TNs configured on both nodes must be the same.

Note:
To obtain switch-provisioning information, see the completed Table 4: High Availability system checklist on page 23.

i. Select a channel.

   Result: The Channel Detail window appears.

ii. Enter the TN, ACD Position ID, and SCN.

iii. Ensure that Channel Allocation is set to Multimedia.

iv. Click Ok.

   Result: The Meridian 1 Switch Information window appears again.

v. Continue the provisioning of channels until complete.

20. Click Next.

    Result: The Meridian 1 CDN Information page appears.

21. Click New to add a new CDN.

    Result: The CDN Details page appears.

    Important:
    The CDNs must be the same on both nodes.

22. On the CDN Details page, do the folllowing:

    a. In the CDN field, enter the new CDN.

    b. Select the Application Name (Voice Messaging or Multimedia Messaging).

    c. Click Ok.

       Result: The new CDN is added and CDN information page reappears.

23. Click Next.

    Result: The Language Source Directory page appears.

24. Insert the CallPilot 5.0 Language CD in the CD/DVD drive on the replacement server.

    Important:
    You must use a CallPilot 5.0 Language CD. Language CDs from previous CallPilot releases are not compatible with CallPilot 5.0. The Configuration Wizard checks the version of the Language CD and blocks the use of the CD if it is not a CallPilot 5.0 CD.

25. On the Language Source Directory Select page, do the following:

a. Select the Install Language option.

b. In the Language CD Location field, enter the directory location of the Language disk or file. Typically, CallPilot uses drive Z (therefore, enter Z:).

26. Click Next.

    Result: The Language Installation page appears.

27. On the Language Installation page, do the following:.

    a. Select Languages and Automated Speech recognition to be installed.

    b. Select Primary and Secondary Languages.

Note:
The Secondary Language is optional.

Important:
The same languages must be installed on both nodes. Ensure that the Primary and Secondary languages are also the same on both nodes.

28. Click Next.

    Result: The CallPilot Local Area Network Interface page appears.

29. On the CallPilot Local Area Network Interface page, do the following:

    a. Select the network interface card from the drop-down list.

       Result: The MAC addres, IP address, and Subnet mask values are updated for the network interface card.

    b. Change the ELAN and CLAN IP information (IP address and Subnet Mask).

    c. Select the High Availability mode check box to display the High Availability Network Interfaces.

       Note:
       To enable High Availability, a proper keycode is required and the High Availability Mode check box must be selected. The keycode has the ability to enable High Availability; however, the feature does not have to be enabled and can be done at a later date.

    d. Enter IP information for the HB1, HB2, and MIRROR network interface cards.

       The following table shows the suggested default values for HB1, HB2, and MIRROR on both servers. If you do not use these suggested values, ensure that you use your new values throughout the configuration.

Network Interface Card (NIC)	CP#1 IP	CP#2 IP	Subnet Mask
Heartbeat 1 (HB1)	192.0.0.10	192.0.0.11	255.255.255.0

Network Interface Card (NIC)	CP#1 IP	CP#2 IP	Subnet Mask
Heartbeat 2 (HB2)	194.0.0.10	194.0.0.11	255.255.255.0
MIRROR	193.0.0.10	193.0.0.11	255.255.255.0

30. Click Next.

    Result: The Ready to Configure page appears.

31. Click Finish to start process.

    Result: The system starts the configuration process and Progress Information page appears.

32. After the process is complete, a dialog box reminds you to restart the server for the configuration to take effect.

33. Click OK to dismiss the dialog box. Restart the replacement server.

Complete the High Availability configuration process

Use the following procedure to guide you through the remainder of the High Availability configuration process.

Completing the High Availability feature configuration

1. Connect the LAN.

   For more information, see Connect and verify LAN connections on page 52 and complete the following procedures:

   - Connecting and verifying LAN connections on page 52
   - Modifying the hosts file on page 55 (optional)
   - Testing the host name resolution on page 57

2. Check the configuration of CP1 and CP2.

   For more information, see Running Stage 1 of the High Availability Configuration Wizard to check CP1 and CP2 configuration on page 58.

3. Install the AutoStart Software on CP1.

   For more information, see Installing the AutoStart Agent and Console software on CP1 on page 62.

4. Add the replacement server Administrator account to the AutoStart Console.

   For more information, see Add the node 2 administrator account to the AutoStart Console on node 1 on page 70.

5. Install the AutoStart software on CP2.

For more information, see Installing the AutoStart Agent and Console software on CP2 on page 72.

6. To configure the AutoStart software, do the following:

   a. Configure the AutoStart software.

      For more information, see Configure the AutoStart software on page 81.

      Warning:
      You must wait for both servers under Domains > [AutoStart_Domain] > Nodes to appear green before making any changes in the AutoStart Console. Failure to do so can result in the loss of configured information for verification links upon the next restart.

      i. Modify the AutoStart Domain and Verification links.

         For more information, see Modifying the AutoStart Domain and Verification links on page 81.

      ii. Add the Remote Mirroring Host for the new 1005r or 1006r server (CP2).

         For more information, see Adding the Remote Mirroring Host for CP2 on page 84.

   b. Generate the AutoStart Definition File.

      For more information, see Generating the AutoStart Definition File on page 86.

   c. Import the AutoStart Definition File.

      For more information, see Importing the AutoStart definition file on page 88.

   d. Add the Windows administrator account password for the AutoStart Utility Processes.

      For more information, see Adding the Windows administrator account password for the AutoStart Utility Processes on page 89.

7. Bring the Resource Groups online.

   For more information, see Bring the Resource Groups online on page 92.

   a. Bring the CallPilot Resource Group online on CP1.

      For more information, see Bringing the CallPilot Resource Group online on CP1 on page 93.

   b. Bring the CallPilot_[CP1] and CallPilot_[CP2] Resources Groups online.

      For more information, see Bringing the Resource Groups CallPilot_[CP1] and CallPilot_[CP2] online on page 95.

8. Create the CallPilot Reporter connections. For more information, see Creating the CallPilot Reporter connection on page 99.
9. If required, add the servers to a Windows domain. See Joining a Windows domain on page 99.

Index

A

automatic failover 32, 179
AutoStart software . .13, 62, 81, 88, 89, 153, 154, 160, 164, 183, 192, 195
  configuring 81
  definition file 88, 164
  installing 62
  licence administration 160
  maintaining 153
  notification settings 154
  reinstall 183, 195
  stand-alone PC 183
  uninstall 183, 192
  updates 183, 195
  Utility Processes 89

B

backup 203

C

CallPilot Reporter 98
channel capacity 141
Configuration Wizard 42
connections 10, 21, 52
  CLAN 52
  ELAN 52
  HB1 ....10, 21, 52
  HB2 ....10, 21, 52
  mirror 10, 21, 52
customer service 7

D

definition file 164
  export 164
  import 164
distributor 7
documentation 7

F

failover 14, 31, 161, 179, 181
  automatic 179
  manual 181
  status 161
feature expansion 233, 237

H

High availability 14
High Availability 19, 22, 35, 58, 81, 106, 233, 237
  Configuration Wizard 58, 81
    Stage 1 58
    Stage 2 58
  feature expansion 233, 237
  installing 35
  maintaining 106
  planning 19
  system checklist 22

L

LAN connections 52

M

maintainence 106, 113, 115, 117, 120
  languages 117
  media allocation 113
  network interface cards 120
  network settings 120
  server information 106
  switch configuration 115
manual failover 33, 181
migration 233
monitoring 179
  starting 179
  stopping 179

N

networking settings 121, 126
  local 121
  managed 126

P

PEP 195

planning 19, 21, 22, 25, 27
facility 25
hardware requirements 27
High Availability configuration 22
management 19
network 21
switch 25

R

remote support 200
reseller 7
resource group 92, 175
restore 203, 208

S

server 161, 209
reimage 209
replace 209
status 161
software licenses 133
status 161
failover 161
HB1 161
HB2 161
mirror 161
server 161
support 195
switch 172
IP address change 172

T

training 7

U

upgrade 233, 235
guidelines 235
utility processes 131
password change 131