Avaya Communication Server 1000 Linux Platform Base and Applications Installation and Commissioning

Release 7.6
NN43001-315
Issue 06.08
June 2016

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 in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of 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 or on the express behalf of 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 websites 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 Avaya hardware and software. 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 website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

“Hosted Service” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. 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 CHANNEL PARTNER; 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”).

License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya’s prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”).

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, 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.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER’S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya’s security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, 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, Hosted Service(s) 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.

Contents

Chapter 1: New in this Release 11
Features 11
Other changes 11
Revision history 12
Chapter 2: Customer service 16
Navigation 16
Getting technical documentation 16
Getting product training 16
Getting help from a distributor or reseller 16
Getting technical support from the Avaya Web site 17
Chapter 3: Introduction 18
Navigation 18
Conventions 19
Supported hardware platforms 20
Linux Base applications installation and commissioning task flow 21
Communication Server 1000 task flow 23
Upgrade path 25
Release 5.0 or 5.5 to Release 7.5 or later 25
Release 6.0 or 7.0 to Release 7.5 or later 25
Chapter 4: Fundamentals 26
Navigation 26
Linux platform overview 26
Linux Base key features 26
Linux Operating System and Distribution 27
Co-resident Call Server and Signaling Server 27
Security server configuration 29
Network and firewall 29
Syslog and log rotation 30
Software reliability 30
Linux security hardening 32
Patching 32
Centralized authentication 32
User accounts and access control 33
SNMP 35
Disaster recovery 35
Avaya UCM overview 36
Description 36
Deployment Manager 42
Deployment View 43

Web browser 44
Turning off the compatibility mode 44
Software loads 44
Supported configurations 45
Backup and restore application data 47
6.0 Deployment Targets 49
System upgrade 49
NFS/system upgrade versus a local installation 49
Element Manager 49
Chapter 5: New Linux Base installation 51
Navigation 51
Prerequisites 51
Installing a new Linux base 55
Chapter 6: Deployment Manager—New system installation and commissioning 68
Navigation 68
Installation workflow 68
Primary security server configuration 69
Configuring the primary security server 70
Deployment Manager—Server preconfiguration 74
Preconfiguring process using Deployment View 74
Logging on to Unified Communications Management 77
Accessing Deployment Manager 77
Software loads 78
Deployment View 81
Deployment Actions 103
Backups 108
6.0 Deployment Targets 108
Prerequisites 108
Deploy 108
Deploying application software to a Call Server 109
Undeploying application software 110
Backing up existing system data files 110
Restoring system data 112
NFS based new installation 113
Installation workflow using NFS 113
NFS based remote installation topology 114
Prerequisites 115
Installing the servers (NFS-based new installation) 116
Chapter 7: Upgrade Linux base 119
Navigation 119
Upgrade Linux base manually 119
Upgrade Linux base using Deployment Manager 123
Chapter 8: Upgrade Avaya Communication Server 1000 system Linux installation 124

Navigation 124
Upgrading a backup or member server from Release 6.0 or later 125
Accessing the Local Deployment Manager 129
Configuring a Server pre-loaded with Avaya Linux base 130
Chapter 9: Avaya Aura® MS 7.6 installation 133
Navigation 134
Prerequisites 134
AMS 7.6 installation process 135
Installing Avaya Aura® MS 7.6 by formatting preexisting administration partition 136
Installing Avaya Aura® MS without formatting preexisting administration partition 138
Chapter 10: Avaya Aura® MS upgrade and MAS 7.0 migration 140
Navigation 141
Prerequisites for upgrade 141
Upgrade overview 142
Avaya Aura® MS upgrade and MAS 7.0 data migration process 142
Upgrading Avaya Aura® MS and migrating MAS 7.0 data 143
Migrating Avaya Aura® MS 7.0 data from CLI 146
Amsupgrade tool 147
Deployment Manager 147
CS 1000 Avaya Aura® MS 7.6 Patching 148
Avaya Aura® MS 7.6 EM access 149
Avaya Aura® MS Element Manager login options 151
Avaya Aura® MS Element Manager Role Based Access Control (RBAC) 151
Configuring the default admin password and enabling Avaya Aura® MS RBAC 152
Avaya Aura® MS Element Manager RBAC with System Manager 153
Using the hostconfig tool 154
Adding System Manager roles 154
Content Store data replication between clusters 155
Changing Avaya Aura® MS server IP address and host name 156
License server 157
Avaya Aura® MS 7.6 EM certificate management 157
Get Certificates from System Manager 157
Import System Manager Certificates into AMS Element Manager 159
Media port management 160
Chapter 11: Base Manager 161
Navigation 161
Accessing Base Manager through UCM 162
Accessing Base Manager through local logon 164
Deploying software in local login mode 165
Undeploying software in local login mode 166
Rebooting the server 166
Base system configuration using Base Manager 167
Editing network identity for a Member server 167

DNS and Hosts ... 170
Adding a route entry ... 174
Deleting a route entry ... 174
Configuring Explicit Congestion Notification ... 176
Date and time configuration ... 177
Configuring NTP transfer mode ... 182
Configuring the clock source for a primary server ... 183
Configuring the clock source for a secondary server ... 185
Configuring a server that is not a clock server ... 187
Regenerating SSH Keys for a UCM Member server ... 188
Software maintenance using Base Manager ... 190
Managing application status ... 190
View and export logs using Base Manager ... 191
Viewing application logs ... 192
Exporting application logs ... 193
Chapter 12: Disaster recovery ... 196
Navigation ... 196
Prerequisites ... 196
Performing disaster recovery for Avaya Linux Base ... 196
UCM considerations for disaster recovery ... 200
Changing Linux Base passwords ... 201
Appendix A: Hardware platforms ... 204
Navigation ... 204
Configuring the privilege level for Windows Vista or Windows 7 ... 205
Creating a bootable RMD for Linux Base installations ... 205
Hardware installation checklist ... 209
CP PM card ... 211
Determining CP PM disk size ... 211
Determining CP PM memory size ... 212
BIOS methods ... 213
CP PM Signaling Server ... 217
Connecting a CP PM Signaling Server ... 218
Changing the baud rate on a CP PM Signaling Server ... 219
Installation in a CS 1000E system ... 221
Connecting a CP PM Signaling Server to the ELAN and TLAN subnets of a CS 1000E system. 221
Connecting a CP PM Signaling Server to the ELAN and TLAN subnets of a CS 1000M system. 222
CP DC card ... 223
Determining CP DC memory size ... 223
CP MG card ... 223
Determining CP MG memory size ... 224
Dell R300 server ... 224
Configuring the COM1 serial port on a Dell R300 server ... 225
Setting the BIOS password for the Dell R300 server ... 228

Configuring RAID settings 231
HP DL320 G4 server 231
HP DL320 G4 BIOS settings 233
Connecting an HP DL320 G4 Signaling Server 238
HP DL360 G7 server 239
Front panel components 239
Back panel components 241
ROM-Based setup utility interface 241
Connecting an HP DL360 G7 Signaling Server 243
HP DL360p G8 server 244
Front view of HP DL360p G8 Server 245
Rear view of HP DL360p G8 Server 246
Configuring the BIOS serial console 246
Configuring the baud rate 247
Connecting an HP DL360p G8 signaling server 247
HP DL360 G9 server 248
Front view of HP DL360 G9 Server 249
Rear view of HP DL360 G9 Server 249
Internal view of HP DL360 G9 Server 251
Configuring the BIOS serial console 252
Configuring the baud rate 252
Connecting an HP DL360 G9 signaling server 252
IBM x306m server 253
IBM x306m BIOS settings 255
Connecting an IBM X306m server 258
Changing the baud rate on an IBM X306m Signaling Server 259
IBM x3350 server 261
Configuring COM port settings for the IBM x3350 server 263
Setting the BIOS password for the IBM x3350 server 267
Appendix B: Installation times 270
Average installation times by media type 270
Linux Base and application deployment—average installation time 271
Appendix C: Avaya Aura® Media Server 272
Checklist for adding a new maintenance release for Avaya Aura® MS 272
Checklist for upgrading a stand-alone MAS 273
Quick Fix Engineering Avaya Aura® MS patches 273
Appendix D: Avaya Linux Base CLI commands 275
Appendix E: Troubleshooting 283
Deployment errors 283
Linux Base installation errors 291
Log file 292
Backup security server configuration error 292

Appendix F: Network configuration for Secure File Transfer Protocol (SFTP) data backup 293
Network configuration 293
SFTP logon 293
SFTP network configuration requirements 294
Appendix G: Change the FQDN of a Primary or Backup Security Server 295
Changing the FQDN of a Primary Security Server 295
Changing the FQDN of a Backup Security Server 296
Appendix H: Passthrough end user license agreement 298

Chapter 1: New in this Release

The following sections detail what is new in the *Linux Platform Base and Applications Installation and Commissioning, NN43001-315* for Avaya Communication Server 1000 Release 7.6.

- Features on page 11
- Other changes on page 11

Features

There are no feature changes made to this document for Release 7.6.

Other changes

The following changes related to Avaya Aura® MS 7.6 have been made for this release:

- Deployment manager cannot be used to install Avaya Aura® MS 7.6 but, will support existing Avaya Aura® MS 7.0 installation. For more information, see *Deployment Manager* in *Avaya Aura® MS upgrade and MAS 7.0 migration*.
- With Avaya Aura® MS 7.6, UCM domain is no longer supported; there is no hyperlink to the Avaya Aura® MS Element Manager from CS 1000 UCM. To accessElement Manager, use one of the following URLs:

  http://<ams7.6 server ip:8080>/em OR http://<ams7.6 FQDN:8080>/em
- Role Based Access Control is available for Avaya Aura® MS Element Manager. For more information about accessing Avaya Aura® MS 7.6 EM, see *Avaya Aura® MS 7.6 EM access*.
- In Avaya Aura® MS 7.6, the patch manager is no longer available. Use the CLI for all patching, including Linux Base patching. You can now install multiple patches with the amspatch command. For more information, see *CS 1000 Avaya Aura® MS 7.6 patching*.
- Media Port Management feature is available with Avaya Aura® MS 7.6. See *Media port management*.

Revision history

June 2016	Standard 06.08. This document is up-issued to include information about the supported web browsers and HP DL360 G9 server.
September 2015	Standard 06.07. This document is up-issued to include updates related to Avaya Aura® MS.
November 2014	Standard 06.06. This document is up-issued to include updated descriptions for the **`sysbackup`** and **`sysrestore`** commands.
June 2014	Standard 06.05. This document is up-issued to include updates regarding Avaya Aura® MS 7.6.
November 2013	Standard 06.04. This document is up-issued to include updates regarding Common Server R2. Added the Mozilla Firefox browser support.
April 2013	Standard 06.03. This document is up-issued to include updates to the section Prerequisites on page 51 .
April 2013	Standard 06.02. This document is up-issued to support Avaya Communication Server 1000 Release 7.6. Notes have been added to the procedures Installing a new Linux Base on page 55 and Upgrading Linux base manually on page 120.
March 2013	Standard 06.01. This document is up-issued to support Avaya Communication Server 1000 Release 7.6.
August 2012	Standard 05.22. This document is up-issued to update IPv6 information in the section Prerequisites on page 51.
April 2012	Standard 05.21. This document is up-issued for changes to the Deployment Manager and Linux Base applications and commissioning task flow sections.
April 2012	Standard 05.20. This document is up-issued to support the removal of Gryphon tool content.
February 2012	Standard 05.19. This document is up-issued for changes in technical content; a note is added to the section Deleting a Network Service on page 93.
January 2012	Standard 05.18. This document is up-issued for changes to the section Editing network identity for a Member server on page 167.
January 2012	Standard 05.17. This document is up-issued to provide information about UCM and disaster recovery.
December 2011	Standard 05.16. This document is up-issued to include a list of supported platforms in the Upgrade Linux Base section.
November 2011	Standard 05.15. This document is up-issued to reflect changes in technical content to the Base Manager section.

Table continues…

October 2011	Standard 05.14. This document is up-issued to support the removal of content for outdated features, hardware, and system types.
September 2011	Standard 05.13. This document is up-issued to reflect changes in technical content for product codes for CP PM components.
September 2011	Standard 05.12 This document is up-issued to support Avaya Communication Server 1000 Release 7.5. Added a note to the Editing network identity procedure.
August 2011	Standard 05.11. This document is up-issued to support Avaya Communication Server 1000 Release 7.5. Changes made to provide clarification on using Deployment Manager on the Primary Security server rather than logging on to the local server.
August 2011	Standard 05.10. This document is up-issued to support Avaya Communication Server 1000 Release 7.5.
August 2011	Standard 05.09. This document is up-issued to support Avaya Communication Server 1000 Release 7.5. Changes were made to add document references, and examples.
June 2011	Standard 05.08. This document is up-issued to include updates to the Troubleshooting section.
June 2011	Standard 05.07. This document is up-issued to update references to Avaya Common Server (HP DL360–G7).
May 2011	Standard 05.06. This document is up-issued to support Avaya Communication Server 1000 Release 7.5.
February 2011	Standard 05.05. This document is up-issued to support Avaya Communication Server 1000 Release 7.5. Updated the COTS3 HP DL360 G7 server content.
February 2011	Standard 05.04. This document is up-issued to support Avaya Communication Server 1000 Release 7.5. Added the COTS3 HP DL360 G7 server.
January 2011	Standard 05.03. This document is up-issued to support Avaya Communication Server 1000 Release 7.5. Added a prerequisite on avoiding a session timeout when adding a software load from a client machine in the Deployment Manager section for new installation and commissioning. References to pre-loaded CP PM configurations have been removed. Changes to keycode validation.
November 2010	Standard 05.02. This document is published to support Avaya Communication Server 1000 Release 7.5.
November 2010	Standard 05.01. This document is up-issued to support Avaya Communication Server 1000 Release 7.5.
September 2010	Standard 04.03. This document is up-issued to support Communication Server 1000 Release 7.0. Updated Deployment View and Deployment Actions content. Changed title of New CS 1000 system installation and commissioning to Deployment Manager—New system installation and commissioning and

Table continues…

	moved the Deployment Manager chapter to a subsection of the Preconfiguring (staging) deployment targets section.
June 2010	Standard 04.02. This document is up-issued to support Avaya Communication Server 1000 Release 7.0. Changes made to the media types for adding a software load and NFS prerequisites.
June 2010	Standard 04.01. This document is up-issued to support Avaya Communication Server 1000 Release 7.0.
July 2009	Standard 03.08. This document is up-issued to include revised information for Disaster recovery on page 196.
July 2009	Standard 03.07. This document is up-issued to support Communication Server 1000 Release 6.0.
June 2009	Standard 03.06. This document is up-issued to support Communication Server 1000 Release 6.0.
June 2009	Standard 03.05. This document is up-issued to support Communication Server 1000 Release 6.0.
May 2009	Standard 03.04. This document is up-issued to support Communication Server 1000 Release 6.0.
May 2009	Standard 03.03. This document is up-issued to support Communication Server 1000 Release 6.0.
May 2009	Standard 03.02. This document is up-issued to support Communication Server 1000 Release 6.0.
April 2009	Standard 03.01. This document is up-issued to support Communication Server 1000 Release 6.0.
May 2008	Standard 02.08. This document is up-issued to update information in the Upgrading Linux base procedures.
April 2008	Standard 02.07. This document is up-issued to add information to the procedure Installing the Primary Security Service and Network Routing Service and added UCM Upgrade Procedures 5.00 GA to 5.50.12 to Task Flow chapter.
April 2008	Standard 02.06. This document is up-issued to add lab trial information.
February 2008	Standard 02.05. This document is up-issued to include references to host configuration scripts found in *Unified Communications Management Common Services Fundamentals , NN43001-116*.
February 2008	Standard 02.04. This document is up-issued to support changes in technical content, including the addition of task flow diagrams for the installation and upgrade of the Linux base and applications.
January 15, 2008	Standard 02.03. This document is up-issued for changes in technical content. New screen captures have been included and an installation and upgrade task flow section has been added.
December 2007	Standard 02.02. This document is up-issued for changes in technical content.

Table continues…

December 2007	Standard 02.01. This document is up-issued to support Communication Server 1000 Release 5.5. This document contains new information on CLI commands, an upgrade procedure, firewall ports, and alarms. Screen captures for the Linux base installation procedure are updated.
November 2007	Standard 01.04. This document is up-issued for changes in technical content.
September 2007	Standard 01.03. This document is up-issued to address changes in technical content for Release 5.0.
June 2007	Standard 01.02. This document is up-issued to remove the Confidential statement.
May 2007	Standard 01.01. This document is issued to support Communication Server 1000 Release 5.0.

Chapter 2: Customer service

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

Navigation

- Getting technical documentation on page 16
- Getting product training on page 16
- Getting help from a distributor or reseller on page 16
- Getting technical support from the Avaya Web site on page 17

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, go to www.avaya.com/support. From this Web site, locate the Training 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 3: Introduction

This document is intended to guide you through the various stages of planning your network and upgrading your servers using Deployment Manager on the Primary security server (Deployment Server) for an end-to-end installation and configuration of Linux Base and applications to your target servers. The preconfiguration capability of Deployment Manager allows you to stage the deployment (or upgrade) of your telephony solution and perform the actual installation and deployment to the target servers on your own time line. Deployment Manager can also enable remote Linux Base installation and upgrades for Release 6.0 and later systems, thereby reducing the need for physical access to your target servers.

The following are the various stages.

- Planning process: identify the network configuration requirements of your target servers
- Identify your Primary security server: perform a fresh Linux Base installation or upgrade
- Preconfiguration process: stage your servers for a logical deployment or upgrade
- Identify pre-Release 6.0 systems for a physical upgrade
- Committing your servers: your servers have now been upgraded with the latest Linux Base and applications are deployed.

After you have read the Introduction and Fundamentals chapters, install or upgrade Linux Base on your Primary Security server Upgrade Linux base on page 119 or New Linux Base installation on page 51 and then proceed to Deployment Manager—New system installation and commissioning on page 68.

Navigation

- Fundamentals on page 26
- New Linux Base installation on page 51
- Deployment Manager—New system installation and commissioning on page 68
- Upgrade Linux base on page 119
- Upgrade Avaya Communication Server 1000 system Linux installation on page 124
- Base Manager on page 161
- Disaster recovery on page 196
- Hardware platforms on page 204
- Installation times on page 270

- Avaya Aura Media Server on page 272
- Avaya Linux Base CLI commands on page 275
- Troubleshooting on page 283
- Network configuration for Secure File Transfer Protocol (SFTP) data backup on page 293
- Passthrough end user license agreement on page 298

Conventions

In this document, the term System refers generically to the following:

- Avaya Communication Server 1000E (Avaya CS 1000E)
- Avaya Communication Server 1000M (Avaya CS 1000M)
- Meridian 1

In this document, the term Server refers generically to the following hardware platforms:

- Call Processor Pentium IV (CP PIV) card
- Common Processor Pentium Mobile (CP PM) card
- Common Processor Media Gateway (CP MG) card
- Common Processor Dual Core (CP DC) card
- Commercial off-the-shelf (COTS) servers
  - IBM x360m server (COTS1)
  - HP DL320 G4 server (COTS1)
  - IBM x3350 server (COTS2)
  - Dell R300 server (COTS2)
  - HP DL360 G7 server (Avaya Common Server)
  - HP DL360 G8 server (Avaya Common Server R2)
  - - HP DL360 G9 (Avaya Common Server R3)

  In this document, the term COTS refers generically to all COTS servers. The terms COTS1, COTS2, and Common Server (Common Server R1) refer to the specific servers in the previous list.

In this document, the term Media Controller refers generically to the following cards:

- Media Gateway Controller (MGC) card (NTDW60 and NTDW98)
- Media Gateway Extended Peripheral Equipment Controller (MG XPEC) card (NTDW20)
- Common Processor Media Gateway (CP MG) card (NTDW56 and NTDW59)

In this document, the term Media Gateway refers generically to the following cards:

- Option 11C Mini Chassis (NTDK91) and Expander chassis (NTDK92) - legacy hardware
- Option 11C Cabinet (NTAK11) - legacy hardware
- Expander chassis (NTDK92) - legacy hardware
- MG 1000E Chassis (NTDU14) and Expander chassis (NTDU15)
- MG 1010 Chassis (NTC310)
- IPE module (NT8D37) with MG XPEC card (NTDW20)

Supported hardware platforms

The following table shows the supported roles for common hardware platforms.

Table 1: Hardware platform supported roles

Hardware Platform	VxWorks Server	Linux Server	Co-res CS and SS	Gateway Controller
CP PIV	yes (see Note 2.)	no	no	no
CP PM	yes	yes	yes	no
CP DC	no	yes	yes	no
CP MG	no	no (see Note 1.)	yes (see Note 1.)	yes (see Note 1.)
MGC	no	no	no	yes
MG XPEC	no	no	no	yes
COTS1	no	yes	no	no
COTS2	no	yes	yes	no
Common Server	no	yes	yes	no
Common Server R2	no	yes	yes	no
Common Server R3	no	yes	no	no
Note 1: The CP MG card functions as the Co-res CS and SS and the Gateway Controller while occupying slot 0 in a Media Gateway. Note 2: HS supports the CP PIV for only the VxWorks Call Servers for HA groups.				

Linux Platform Base and Applications can run on the following hardware platforms:

- CP PM card
- CP DC card
- CP MG card
- COTS Servers
  - IBM x306m

  - HP DL320 G4
  - IBM x3350
  - Dell R300
- Common Server
  - HP DL360 G7
  - HP DL360 G8
  - HP DL360 G9

The Avaya CS 1000 Linux Base system provides a Linux server platform for applications on a Server. The platform supports Session Initiation Protocol Network Redirect Server (SIP NRS), Avaya Unified Communications Management (UCM), traditional Signaling Server applications, SIP Line Gateway Applications, and deployment of the Co-resident Call Server and Signaling Server applications.

Call Server hardware platforms that support the CS 1000E High Availability configuration are supported in the CS 1000 High Scalability configuration. This includes the CP PM for the Call Server software running under the VxWorks operating system and the CP PM and COTS servers that support the Signaling Server applications, including the NRS.

Linux Base applications installation and commissioning task flow

The following task flow provides a high-level task flow for the installation and commissioning of Linux Base and applications on a Server. The task flow depicts the recommended sequence of events and provides a reference to the relevant technical document for each event.

Each box in the task flow represents a stage in the Linux Base installation and commissioning process. The stages are as follows:

- Plan your system
- Identify (gather) parameters for all Servers
- Install and commission the Primary security server (Deployment Server)
- Install and deploy target servers
- Configure and provision applications (for example, Subscriber Manager)

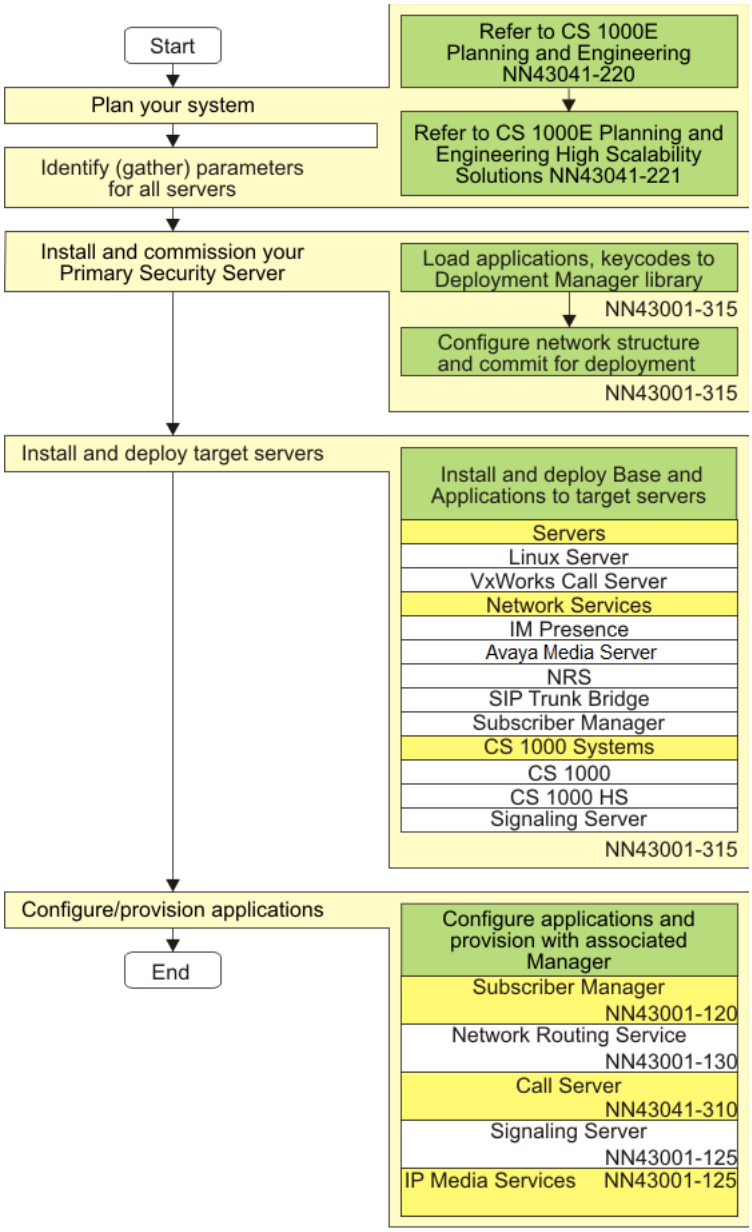


Figure 1: High-level task flow

The following technical documents are referenced in the preceding task flow diagram:

- *Avaya Communication Server 1000E Planning and Engineering, NN43041-220*
- *Avaya Communication Server 1000E High Scalability Planning and Engineering , NN43041-221*
- *Avaya Linux Platform Base and Applications Installation and Commissioning, NN43001-315*
- *Avaya Subscriber Manager Fundamentals, NN43001-120*

- *Avaya Signaling Server IP Line Applications Fundamentals, NN43001-125*
- *Avaya Network Routing Service Fundamentals, NN43001-130*
- *Implementing and Administering Avaya Aura® Media Server*
- *Avaya Element Manager System Reference - Administration, NN43001-632*
- *Avaya Security Management Fundamentals, NN43001-604*
- *Avaya Communication Server 1000E Installation and Commissioning, NN43041-310*

Note:

The document *Implementing and Administering Avaya Aura® Media Server* includes information on Avaya Aura® MS capabilities which are NOT supported with the CS 1000. Sections on WebLM Licensing, High Availability, Video Codecs and Diameter Configuration within this document are not applicable to CS 1000 deployments and should not be used for Avaya Aura® MS configuration.

Avaya Aura® Media Server was formerly known as Media Application Server (MAS).

Communication Server 1000 task flow

The following figure provides a high-level task flow for the installation or upgrade of a Communication Server 1000 system. The task flow indicates the recommended sequence of events to follow when configuring a system and provides the technical document number that contains the detailed procedures required for the task.

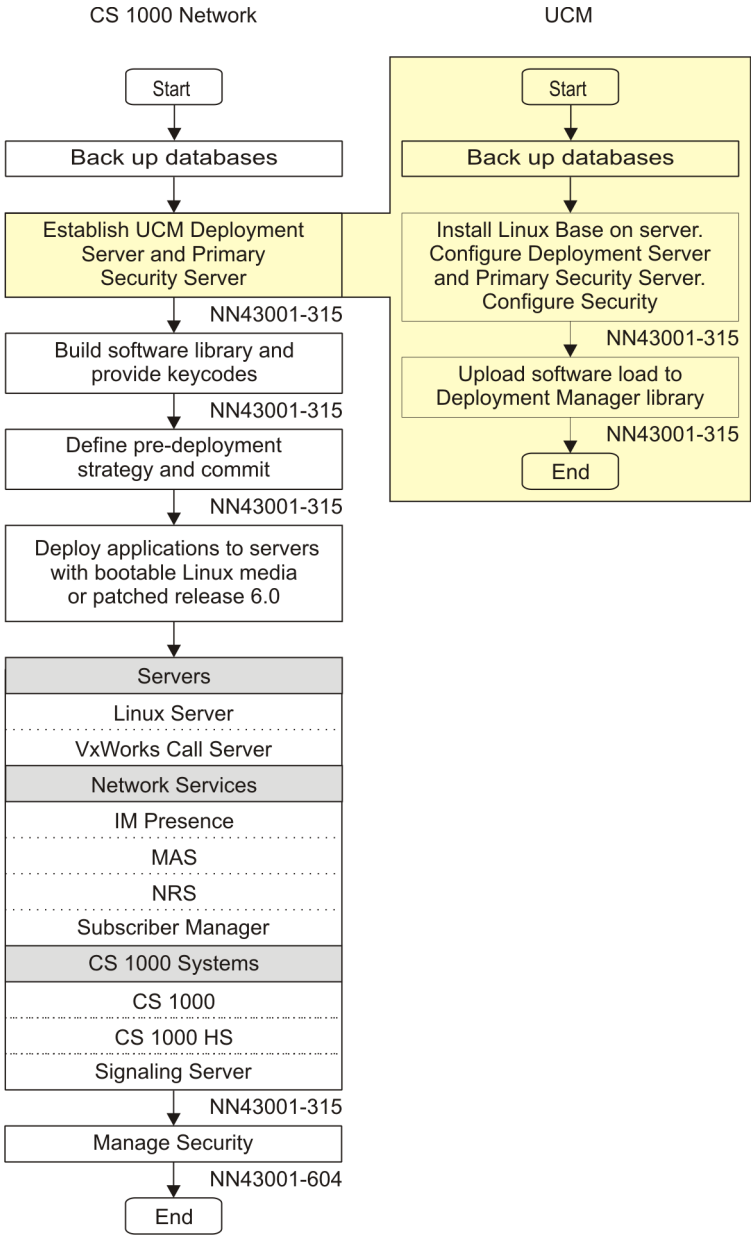


Figure 2: Communication Server 1000 task flow

Note:

For the purposes of this diagram, Linux patching is considered to be part of the Configure Call Server box in the CS 1000 task flow. For more information about Linux patching, see *Avaya Patching Fundamentals, NN43001-407*

Upgrade path

There are two supported upgrade paths.

- Release 5.0 or 5.5 to Release 7.5 or later
- Release 6.0 or 7.0 to Release 7.5 or later

Release 5.0 or 5.5 to Release 7.5 or later

The flow to upgrade from Release 5.0 or 5.5 to Release 7.5 or later requires the following high level steps:

- Backup existing customer data, for example, NRS.
- Perform a CS 1000 Linux base installation or upgrade.
  - If it is a new Linux base installation, see New Linux Base installation on page 51.
  - If it is an upgrade, see Upgrade Linux base on page 119.
- Restore the customer data for the corresponding Management systems, for example, NRSM for NRS. For more information, see *Network Routing Service Fundamentals, NN43001–130*.

For VxWorks Call Server upgrades, see *Avaya Communication Server 1000E Software Upgrades, NN43041–458*.

Release 6.0 or 7.0 to Release 7.5 or later

The flow to upgrade from Release 6.0 or later to Release 7.5 or later requires the following high level steps:

1. Patch all Release 6.0 or later targets to the latest Service Pack (the latest patch contains the migration patch).

   Note:

   If upgrading from Release 6.0 to 7.6, the MPLR30019 patch is required to be loaded prior to upgrading to Release 7.0, 7.5, or 7.6.
2. Backup the Release 6.0 or later data, for example, NRS
3. Upgrade the Primary Security server to Release 7.6
4. Patch the Release 7.6 Primary Security server to the latest Release 7.6 SP (if applicable)
5. Populate the Release 7.6 Deployment View. For more information, see Deployment View on page 43.
6. Run **System Upgrade** from Deployment Manager to automatically upgrade the Linux Servers (Primary Server is not included as it is already upgraded).

Chapter 4: Fundamentals

This chapter provides an overview about basic information and concepts necessary to successfully install and configure the Linux Base.

Navigation

- Linux platform overview on page 26
- Avaya UCM overview on page 36
- Deployment Manager on page 42
- Software loads on page 44
- Supported configurations on page 45
- Backup and restore application data on page 47
- 6.0 Deployment Targets on page 49
- NFS system upgrade versus a local installation on page 49
- Element Manager on page 49

Linux platform overview

This section provides an overview about basic information and concepts necessary to successfully install and configure the Linux Base.

Linux Base key features

The following are the Linux Base features:

- Linux operating system and distribution
- Firewall
- Software reliability
- Linux security hardening

- Patching
- User accounts and access control
- Software installation and delivery
- System upgrades
- Debugging
- Logging
- Disaster recovery
- Network Time Protocol (NTP)

Linux Operating System and Distribution

The selected distribution is Red Hat Linux 5. This distribution is built on a 2.6.18 kernel, and supports many Open Source Development Lab (OSDL) Carrier Grade Linux (CGL) features.

Red Hat Linux 5 (update 1) supports Linux kernel version 2.6.18 and the following applications:

- Avaya Unified Communications Management (UCM)
- Simple Network Management Protocol (SNMP)
- Deployment Manager (DM)
- Signaling Server (SS)
- Network Routing Service (NRS)
- Call Server (CS)
- Session Initiation Protocol Line (SIPL)
- Element Manager (EM)
- Subscriber Manager (SubM)

Co-resident Call Server and Signaling Server

The Avaya Communication Server 1000 (Avaya CS 1000) Linux Base Co-resident Call Server and Signaling Server (Co-res CS and SS) can run the Call Server software, the Signaling Server software, and the System Management software on the same hardware platform. The Co-res CS and SS can run on various hardware platforms. For more information, see Supported hardware platforms on page 20.

The Signaling Server software on the Co-res CS and SS refers to a suite of CS 1000 software applications which includes:

- Line Telephony Proxy Server (LTPS)
- Virtual Trunk (VTRK) includes H.323 Gateway or SIP Gateway

- NRS includes SIP Proxy Server (SPS), SIP Redirect Server (SRS), H.323 Gatekeeper, Network Connect Server (NCS), Network Routing Service Manager
- Personal Directory (PD) includes RL, CL, and Unicode Name Directory
- UCM Common Services
  - Security Server
  - Element Manager (EM), including Cluster Manager/IP Telephony node
  - Deployment Manager
  - Base Manager
  - Patching Manager
  - Subscriber Manager
  - SIP Line

You need not deploy all the preceding software applications on the Server. For example, you can install and configure a Co-res CS and SS to run only the Call Server, LTPS, VTRK, UCM Security Server, and EM software. However, the Co-res CS and SS must have the Call Server and at least one Signaling Server application installed. A stand alone Call Server is not supported on the Linux based Servers.

Note:

A Server running Signaling Server and/or UCM applications without a Call Server is not referred to as a Co-res CS and SS.

Upgrade paths

The following upgrade paths are supported for CS 1000 systems:

- CS 1000 Release 6.0 or earlier CP PM based CS 1000E Standard Availability (SA) Call Server to a CS 1000 Release 7.5 or later Co-resident Call Server and Signaling Server
- CS 1000 Release 6.0 or earlier CS 1000E Signaling Server to CS 1000 Release 7.5 or later Co-resident Call Server and Signaling Server
- Option 11C, CS 1000M, or CS 1000S Call Server to CS 1000 Release 7.5 or later Co-resident Call Server and Signaling Server
- Option 11C, CS 1000M, or CS 1000S Call Server to CS 1000 Release 7.5 or later Co-resident Call Server and Signaling Server
- Option 11C Call Server to CS 1000 Release 7.5 or later CS 1000E TDM system.
- CS 1000M Call Server to CS 1000 Release 7.5 or later Co-resident Call Server and Signaling Server

Note:

If you upgrade from a non-CP PM based CS 1000E Call Server, you must replace your old Call Server hardware with a supported Server and upgrade the software.

For more information about the CS 1000 Co-res CS and SS, see *Avaya Co-resident Call Server and Signaling Server Fundamentals,* NN43001-509.

Security server configuration

A Linux Base server can be assigned one of three security roles: Primary, Backup, or Member.

A network requires one primary security server. The backup security service is optional. One backup security server and one or more member servers can exist for each UCM security domain.

The primary security server must be configured; it provides basic security features such as user administration including password changes, the ability to configure different authorization levels, and the enforcement of security policies.

The backup security server is an optional server that you can configure to perform authentication and authorization when the primary security server is unavailable.

For a more details about UCM configuration of primary, backup, and member servers, see *Avaya Unified Communications Management Common Services Fundamentals, NN43001-116*. For more information about security management, see *Avaya Security Management Fundamentals, NN43001-604*.

Network and firewall

All applications operate behind a network firewall. The firewall starts on system boot, which invokes the Linux iptables facility to load the firewall configuration.

Each Linux server supports at least two Ethernet ports; one for ELAN subnet connectivity and another for TLAN subnet connectivity. By convention, the TLAN is open to the network, while the ELAN is reachable only within the subnet. The Linux application selects the Ethernet port to use. The firewall protects both ports. For a list of Linux Base open firewall ports see Table 2: Linux Base open firewall ports on page 29. For a definition of ELAN and TLAN, see Network configuration on page 293.

Use the command line interface (CLI) command **`basefirewallconfig`** to configure the network firewall. For a list of Avaya Linux Base CLI commands see Avaya Linux Base CLI commands on page 275.

Table 2: Linux Base open firewall ports

Protocol	Port number or range
TCP	22
UDP	22
UDP	53 (to configured DNS servers only)

Table continues…

Protocol	Port number or range
UDP	123
UDP	500
UDP	514
TCP	2100
UDP	33434—33524
RPC	111

Note:

The port numbers in Table 2: Linux Base open firewall ports on page 29 apply only to the Linux Base. Linux applications can require different ports. For a list of ports opened for the application, see the appropriate application document.

Syslog and log rotation

Syslog

Syslog provides application logging. The log files are stored in the /var/log/avaya directory. The log file partition is 10 percent of your hard drive disk space. To increase the performance, the SYNC option is turned off for all application logs. Log files must be readable and writable when logged on using the admin2 account.

Log rotation

The log rotation mechanism is enabled for all application log files. Use log rotation to ease the administration of systems that generate large numbers of log files and provide automatic rotation, compression, removal, and mailing of log files. The log files can be configured for rotation on a daily, weekly, or monthly basis or when the log file reaches a predefined limit. For more information, see the logrotate MAN pages on your Linux Base.

Software reliability

Software monitoring

Avaya uses a third-party application package to monitor the important daemon services automatically initiated at startup. If a malfunction occurs, you can see actions such as, alert, start, stop, and restart.

The following system parameters are monitored: memory, CPU, and device space usage. If a parameter exceeds a warning threshold a message appears and an SNMP trap is generated. Table 3: Warning and Critical thresholds on page 31 shows the warning and critical thresholds.

Table 3: Warning and Critical thresholds

System Resource	Warning Clear	Warning Set	Critical Clear	Critical Set
Memory usage	—	—	90%	95%
CPU usage	—	—	90%	95%
/boot (/dev/sda1) Size: 100 MB. Critical.	70%	75%	80%	85%
admin (/dev/sda2) Size: 4 GB.	80%	85%	85%	90%
/ (/dev/sda6) Size: 4 GB.	80%	85%	85%	90%
/opt (/dev/sda7) Size: 8 GB. Not critical.	80%	85%	90%	95%
/home (/dev/sda8) Size: 4 GB. Not critical.	80%	85%	90%	95%
/tmp (/dev/sda9) Size: 20 GB. Critical.	80%	85%	85%	90%
/var (/dev/sda10) Size: 30 GB. Critical.	80%	85%	85%	90%

Figure 3: Critical Set alarm example on page 31 shows an example of a Critical Set alarm. Figure 4: Critical Clear alarm example on page 31 shows an example of a Critical Clear alarm message.

Note:

If critical alarms persist, contact your Avaya technical support.

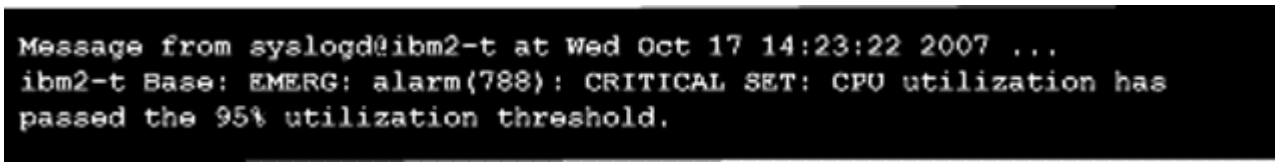


Figure 3: Critical Set alarm example

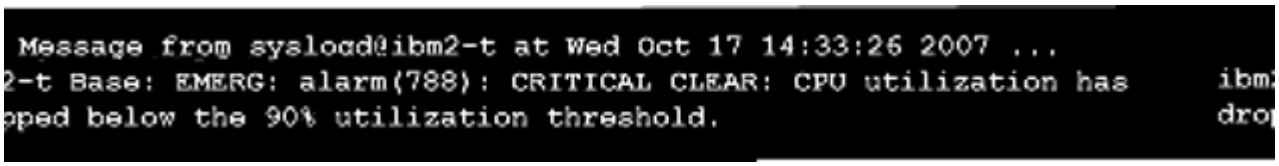


Figure 4: Critical Clear alarm example

Hardware watchdog

Servers running Linux Base offer a hardware watchdog. The watchdog is a hardware component of each server which includes a count-down timer that is programmed during the server startup. If the timer reaches zero, the watchdog unconditionally restarts the server (reboots the Linux operating

system). The watchdog timer duration is five minutes. A program running as part of the Linux Base continually resets the timer on a periodic basis. The software program and hardware timer work together to effect a systematic recovery of the server in the unlikely event it enters a halted or suspended state (also known as: hung, frozen, or dead). In this case, the software component also halts, and ceases to reset the hardware timer, resulting in an inevitable restart of the server. A server halt can only be the result of an anomalous hardware or software event.

Linux security hardening

Linux security hardening is divided into two categories: basic hardening and enhanced hardening. During the Linux Base installation, the generic Linux Base components are installed, then the basic and enhanced hardening items are applied. The enhanced hardening items are set to default values when they are applied during the installation process.

Basic hardening:

Basic Linux security hardening includes all hardening items that do not affect the performance of Avaya applications. Basic hardening items are on by default and they are not configurable.

Enhanced hardening:

Enhanced hardening items include all hardening items that can affect the performance of Avaya applications, or hardening items that require configuration. Enhanced hardening items that do not affect Avaya applications performance are on by default, enhanced hardening items that affect performance are turned off by default.

For details about Avaya Linux security hardening, see *Avaya Security Management Fundamentals, NN43001-604*.

Patching

Avaya Linux Base uses Patching Manager to perform patching tasks. You can use Patching Manager on the primary security server to remotely deploy patches from a central location to other Linux servers in the same security domain using the Central Patching Manager. You can also install patches locally. You can access Local patching from the Base Manager of each element, using the Local Patching Manager.

For more information about Avaya Linux patching, see *Avaya Patching Fundamentals , NN43001-407*.

Centralized authentication

UCM provides a centralized, GUI-based interface for individual account administration for the CS 1000 network. When a user logs on to a Linux server CLI they receive a prompt for user name and password. First, the user name and password are authenticated locally. If authentication fails, the user name and password is encrypted and sent to the centralized UCM security server through the

RADIUS protocol for verification. UCM acts as a RADIUS server to provide authentication for RADIUS clients. If the user is defined in the UCM database then access is granted to the proper Linux shell with the roles defined in the UCM database. For more information about UCM role creation, see *Avaya Unified Communications Management Common Services Fundamentals, NN43001-116*.

User accounts and access control

User accounts and access control methods are managed by native Linux user account management (root and admin2) and tools such as RADIUS and PAM for the UCM managed accounts.

Linux Base includes the following accounts:

- root (as Linux default)

  Note:

  Avaya does not recommend logging on using the root account unless you are explicitly directed to do so. All base maintenance and debug actions must be performed using the admin2 account.

  Note:

  You can log on directly as root through the COM1 console, or through a keyboard and video monitor (KVM).

  Caution:

  Do not change your KVM terminal. If you switch the KVM terminal, logon can fail if you log on directly as root.

  Important:

  If you log on to the COM1 port, make sure you turn off **Caps Lock** before you log on.

- admin2: The user account for the basic Linux Base operations as well as for base manager. For a list of CLI commands that can be invoked by admin2, see Avaya Linux Base CLI commands on page 275.
- System UCM accounts: These accounts are governed by UCM policies; for information about UCM password policies, see *Avaya Unified Communications Management Common Services Fundamentals, NN43001-116*.

Note:

If you log in and your account remains inactive for 15 minutes, you are automatically logged out.

Note:

System Linux Base accounts that make three successive incorrect logon attempts are locked for one hour. System UCM accounts making successive incorrect logins are locked based on the policy settings defined in UCM.

Note:

For SSH/telnet/rlogin/web access, the address must be entered in IPv4 format. IPv6 is not supported.

Passwords

The following regulations govern the use of passwords:

Password policy

The password for the root account expires after three months, but the root account does not expire.

Note:

A warning that the password will expire is given by the system when logging into the server during last seven days before it expires. After the password for the account has expired, the password must be changed the next time the account is used to log into the server. The password for the admin2 account never expires, but it is still recommended that the password be changed at a regular schedule, based on your security requirements.

- A new password must differ from the previous three passwords.

UCM password rules for Admin are different than the System UCM accounts. For more information, see *Avaya Unified Communications Management Common Services Fundamentals, NN43001-116*.

Password creation guidelines

Passwords must meet the following criteria:

- Passwords must contain both uppercase letters, lowercase letters, numeric characters, and special characters.
- In addition to letters, passwords must use digits (0 to 9) and special characters (@#$%^*()_+|~-=\`{}[]:";'&<>?,./!).
- The password must contain at least eight alphanumeric characters.
- The password cannot be a word in the English language as defined in the Linux Pluggable Authentication Module (PAM) module.
- Passwords cannot use discernible character patterns such as abcdef or 123123.
- Passwords cannot use the backward spelling of a word.
- Passwords cannot be an English language word (as defined in the Linux PAM module) preceded or followed by a digit. For example, 1secret or secret1.
- You can change your password by using the **`passwd`** CLI command.

For more information about changing lost or forgotten passwords, see Changing Linux Base passwords on page 201.

SNMP

Linux Base supports standard server type Management Information Base (MIB) II MIBs. For information about the configuration of SNMP on Linux Base, see *Avaya Communication Server 1000 Fault Management — SNMP, NN43001-719*.

Disaster recovery

Important:

If you are attempting to recover a server that has been upgraded from Communication Server 1000 Release 6.0 or later and does not have the latest backup data (either USB or SFTP), perform a backup data restore during the Linux Base installation. Performing a restore ensures a graceful reregistration to the UCM Security Domain and UCM Deployment Manager. For more information, see Performing disaster recovery for Avaya Linux Base on page 196.

Hardware faults can occur that require disaster recovery. Recovery occurs in two steps. First, restore the Linux Base (including operating system and Base applications), and then restore the Avaya applications.

A file backup and restore option supports the base disaster recovery.

During a system backup, information for the following applications (if installed) is backed up and is restorable when the applications are reinstalled:

Note:

The list of backed up Base and Avaya applications is comprised of applications successfully installed prior to the backup. This list contains common applications; your installation can contain applications not listed here.

- Base configuration data
- UCM

  UCM backs up the following data:

  - Data pertaining to Element Registry
  - Certificate Authority (if the server is the primary UCM server); certificates and jboss keystore.
  - User and Emergency accounts. If Subscriber Manager is installed, subscriber accounts are also backed up.
  - Configuration files
  - SSH keys
- SNMP
- DM

- SS
- NRS
- CS
  - Data from the last EDD is backed up.
- SIPL
- EM
- SubM
- Intrasystem Signaling Security Solution (ISSS)

Disaster recovery does not back up Avaya logs; however, UCM backs up security logs.

Application-configured system data:

You can configure values for routes using Adding a route entry on page 174. You can add or delete host records using DNS and Hosts on page 170, and firewall rules using the CLI commands **`routeconfig`**, **`hostconfig`**, and **`basefirewallconfig`**. These values are application-configured system data. Application-configured system data is backed up as part of the system data backup.

For more information about disaster recovery prerequisites and procedures, see Disaster recovery on page 196.

Avaya UCM overview

The following section contains an overview and references about Avaya Unified Communications Management (Avaya UCM) security configuration.

Description

UCM is a collection of system management tools. UCM provides a consistent methodology and interface to perform system management tasks. System management tools are Web-based system management solutions supported by the UCM framework.

Installed on every Avaya Linux Base operating system is a Web server with extended security features that forms the basis for UCM and provides the following key features:

- Central element registry for all elements
- Authorization and authentication functionality
- Single sign on across application and hardware platforms
- PKI management
- RADIUS support

- External authentication support

Note:

Support terminals not connected to the DNS domain must modify their local host files to gain initial access to UCM. For more information about managing local host files, see *Avaya Unified Communications Management Common Services Fundamentals, NN43001-116*.

The following overview shows UCM on an Avaya Linux Base system.

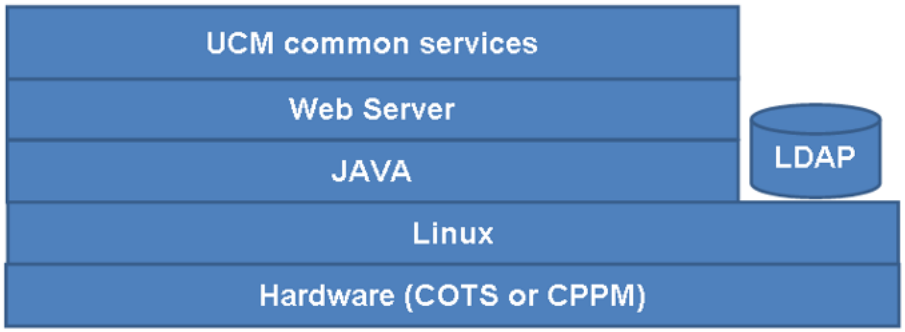


Figure 5: UCM overview

You can configure UCM in one of the following ways:

- Primary security server
- Backup security server
- Member security server

Every security domain must have one primary security server. The security domain can have one or no backup servers; additional servers are member servers.

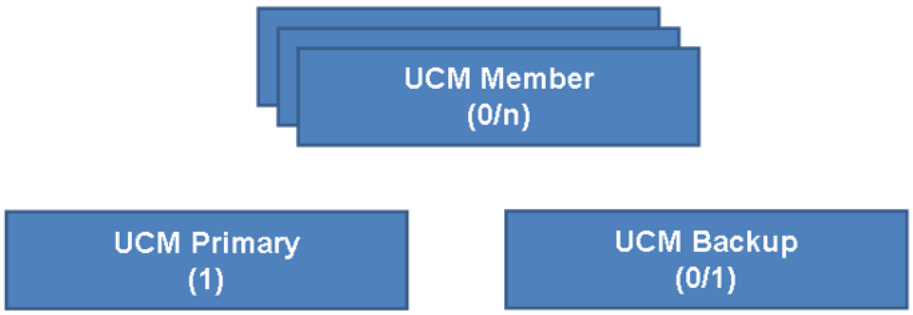


Figure 6: UCM server configurations

UCM framework is installed and runs on all CS 1000 Linux platforms (CP PM and COTS). Management applications are packaged as Web Archive (WAR) files and loaded into the UCM framework.

CS 1000 management applications are auto-deployed, other applications are deployed as required.

- Auto-deployed to the UCM server
  - Base Manager: Provides local Web management for Linux Base. Supports IPv6.
  - Deployment Manager: Provides a one-step Linux Base and application installation or upgrade across all preconfigured servers. Deployment Manager is installed on the Primary security server. Deployment Manager is accessible locally on the target server.
  - Patching Manager: Provides Web-based patch delivery. Patching Manager is centrally accessible from the primary security server or locally on the target server.
  - IPSec Manager: Provides centralized Web-based IPSec management.
  - SNMP: Provides centralized Web-based fault management.
- User deployed
  - Element Manager: Provides traditional CS 1000 Web-based management, including Call Server overlay support. Support IPv6.
  - Network Routing Service Manager
  - Subscriber Manager
  - Signaling Server (virtual trunks, Terminal Proxy Server)
  - SIP Line

The following figure shows application deployment on UCM servers.

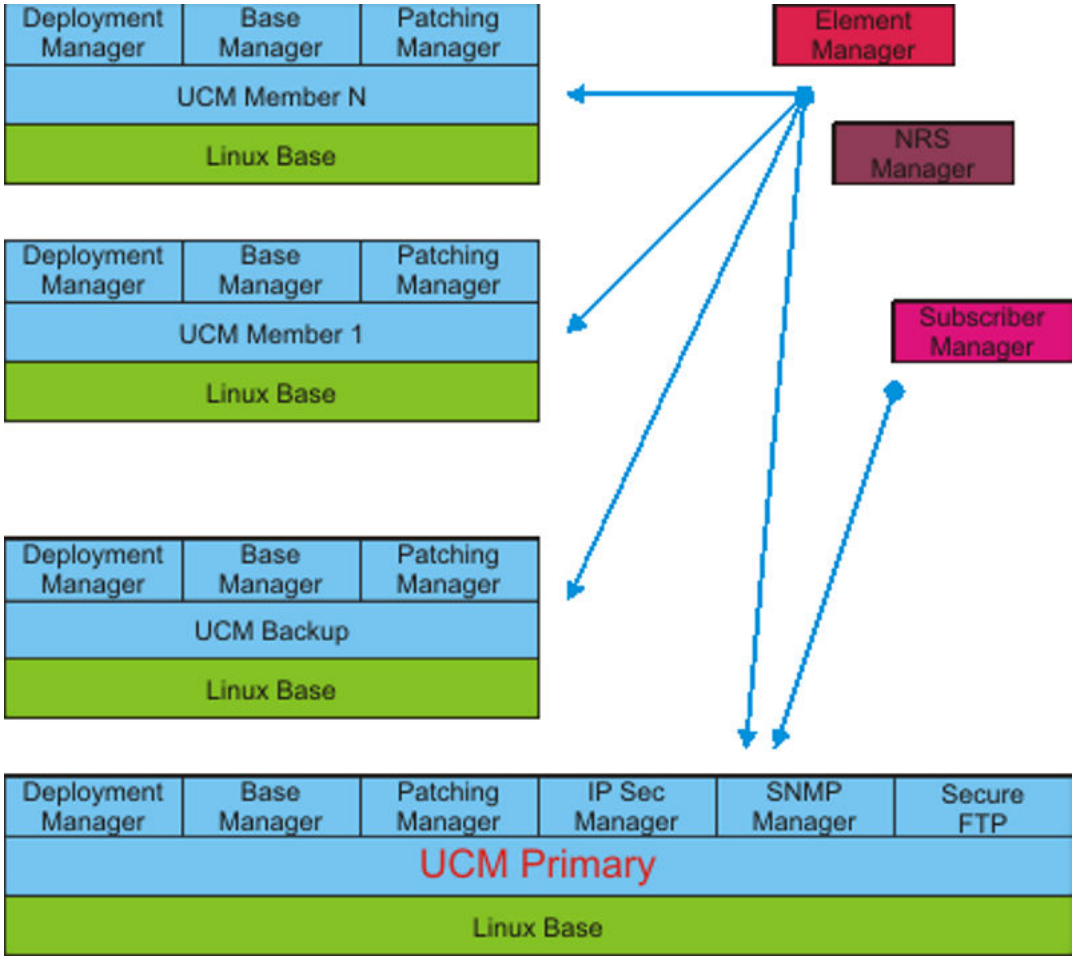


Figure 7: UCM application deployment

The following figure provides an example of system management components deployed in a typical installation. Network and engineering analysis determines the location of the UCM primary and backup servers. Typically EM is deployed physically close to the Call Server it manages.

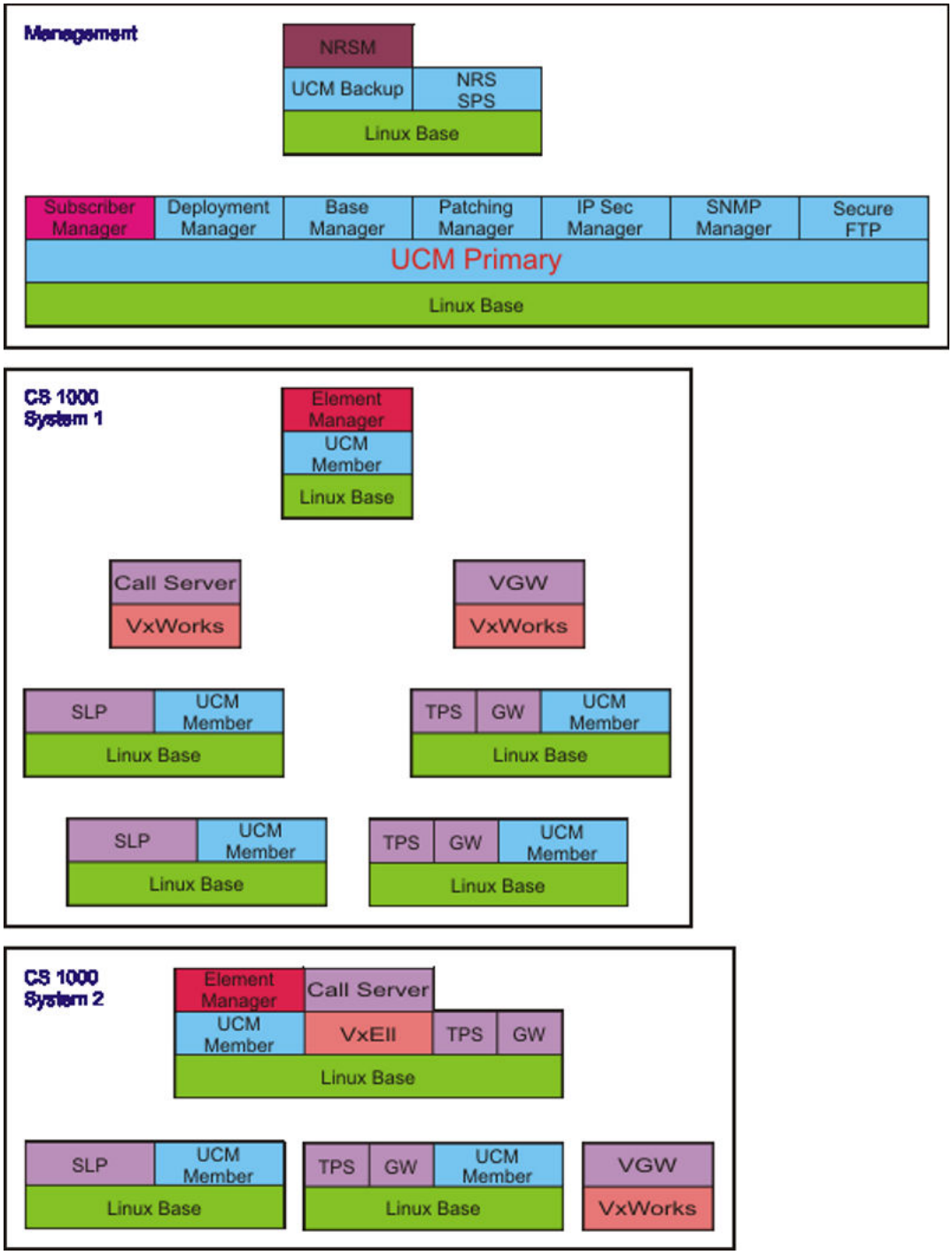


Figure 8: Physical deployment of UCM

The UCM Graphical User Interface (GUI) is shown in the following figure.

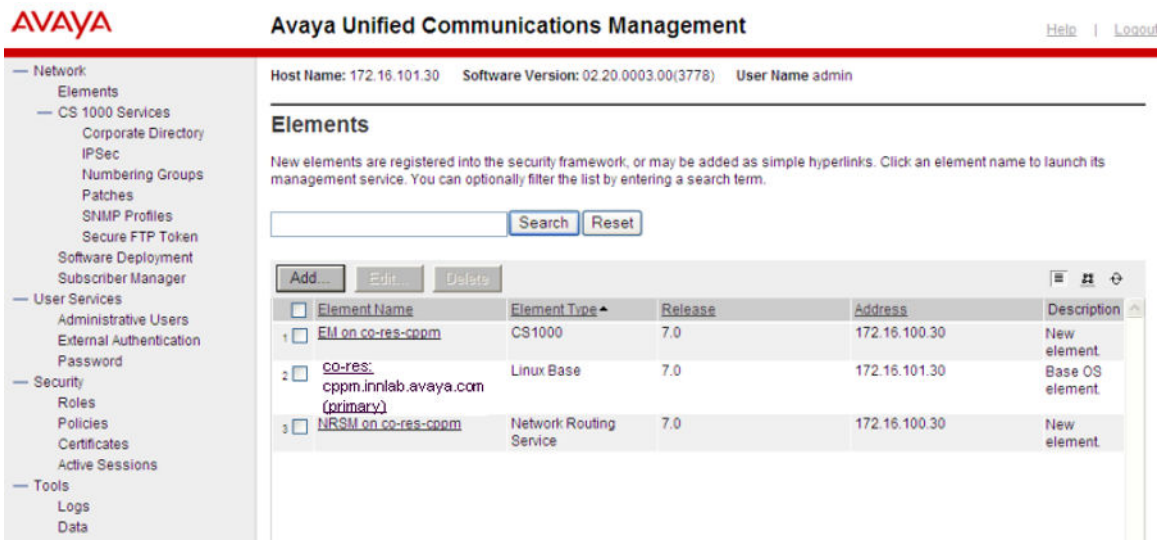


Figure 9: UCM graphical view

The following figure illustrates the three levels of UCM management.

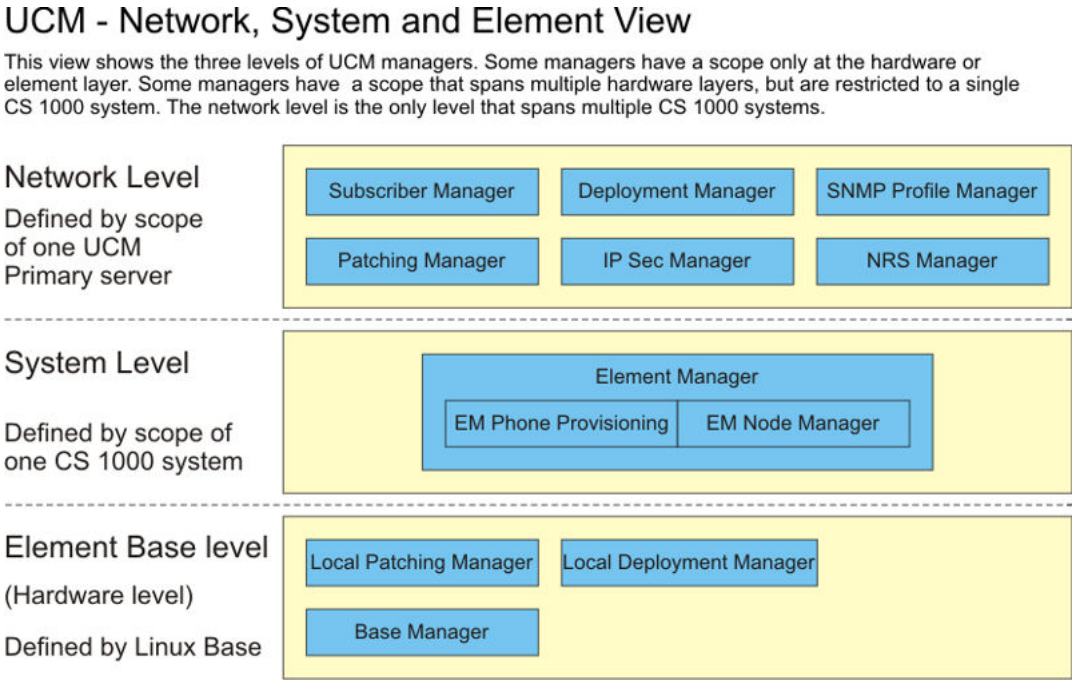


Figure 10: UCM management levels

For detailed information about the components, features, and benefits of Unified Communications Management, see *Avaya Unified Communications Management Common Services Fundamentals, NN43001-116*.

Deployment Manager

Use Deployment Manager on the Primary security server for an end-to-end installation and configuration of Linux base and applications. Deployment Manager provides a simplified and unified solution that enables network installation of Linux base on target servers. The Primary security server is the Deployment Server.

Install the Linux base on the Primary security server (Deployment Server) using a local Linux base installation media. Upgrade Linux base on the Member and Backup servers over the network using Network File System (NFS). For more information, see NFS system upgrade versus a local installation on page 49.

Use UCM Deployment Manager to select groups for predeployed applications prior to joining the domain. After preconfiguration, commit predeployed applications for deployment. You can then deploy application groups to Servers. If the Server is not running Release 6.0, you can physically deploy using the bootable media. For more information about the end-to-end installation and configuration procedures, see Deployment Manager—Server preconfiguration on page 74. For more information about upgrading existing servers, see Upgrade Avaya Communication Server 1000 system Linux installation on page 124.

After installation and configuration is complete:

- Linux base is installed
- Base applications are installed during the first restart of the computer
- UCM is deployed and security configuration is complete
- The application combination is determined and deployed
- Applications are active

There are two different types of Linux base deployments.

- Linux base operating system is already installed
- Linux base operating system is not installed

For more information about the different deployment procedures, see Deployment View on page 43.

Important:

You must install and configure VxWorks elements manually. Deployment Manager cannot be used to perform installation and configuration of VxWorks elements.

Note:

AMS 7.6 no longer uses the Deployment Manager but is bundled inside the Red Hat installation image. AMS 7.6 is installed automatically with the Red Hat Enterprise Linux and LinuxBase install. For more details see *AMS 7.6 Installation*.

From UCM, you can click Software Deployment to reach the UCM Deployment Manager. The following links are available.

-
- Software loads on page 44
- Backup and restore application data on page 47

- 6.0 Deployment Targets on page 49

Deployment View

This section describes how to add servers, Network Services, and Avaya CS 1000 systems, and commit the software for deployment.

Note:

If you are using Deployment Manager on your Deployment Server as your unified solution for end-to-end installation and configuration of Linux Base and applications, you must use the process as described in Preconfiguring process using Deployment View on page 74.

From UCM, you can access the Deployment View page by clicking Software Deployment, UCM Deployment Manager. For an overview of the Deployment View page, see Deployment View on page 43.

From Deployment View, you can access the following:

- Servers on page 82
- Network Services on page 90
- CS 1000 systems on page 93

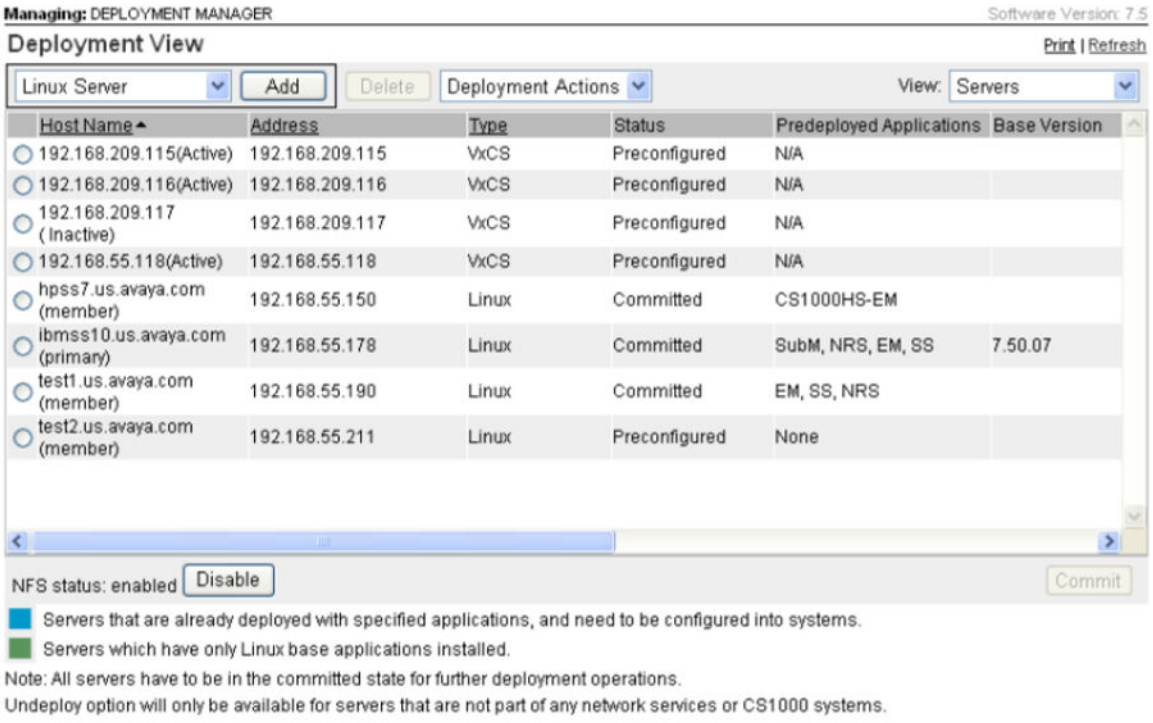


Figure 11: Deployment View page

Web browser

Deployment Manager supports specific web browsers. For information about supported browsers, see *Unified Communication Management Fundamentals, NN43001-116*.

Turning off the compatibility mode

You might not be able to view the status of some operations on Web pages using Internet Explorer because Internet Explorer imposes a time-out limit for the server to return the data. To correct this problem, you must install the patch for Internet Explorer from the website of Microsoft at http://support.microsoft.com/kb/181050%20.

About this task

Some features might not work as expected on Internet Explorer version 8 or later if the compatibility mode is turned on. Therefore, you must turn off the compatibility mode.

Procedure

1. On the menu, click **Tools** > **Compatibility View Setting**.
2. On the Compatibility View Settings dialog box, clear all check boxes that are already selected.
3. Ensure that the **Websites you've added to Compatibility View** field does not contain the address of the System Manager server and UCM primary, secondary, or member server.

Software loads

There are three load types for CS 1000 Linux applications.

- CS 1000 load: avaya-cs1000-linux-7xxxx-Pyyy-Mzz.nai
- CS 1000 EL6 load: cs1000-linux-el6-7xxxx-Pyyy-Mzz.nai
- Avaya Aura® MS load: cs1000-linux-mas-700xx-Pyyy-Mzz.nai

The naming convention for the .nai file is cs1000-linux-version and release number-loadware number-deplist.nai

- el6 indicates the Enterprise Linux 6 (Common Server 3) base
- 7xxxx is the version and release number
- Pyyy is the preinstallation loadware number that is part of the nai distribution
- Mzz is the deplist number that is part of the nai distribution
- nai is the extension name (Avaya Application Image)

Downloading the nai file:

Download the nai file for the CS 1000 or the Avaya Aura® MS software load.

1. Go to the Avaya Web site http://www.avaya.com.
2. Navigate to **Support > Downloads**.
3. Enter the Product as Avaya Communication Server 1000and select the Release number from the list (for example, 7.6x), the click one of found articles that contain the required software load file for the server platform, for example, **Communication Server 1000 Software Downloads – Release 7.6x**.
4. On the appeared page click the software load file, for example, cs 1000-linuxbase–7.65.16.23.iso, 7.6.x.

You can download the application load files directly to the hard drive of the client PC, or you can copy the application load file to a CD, DVD, compact flash (CF), or USB device and then attach the storage medium to the client PC and upload the application load file. Deployment Manager provides the functionality to transfer the application load file from the client PC to the server hard disk.

For central deployment, you must upload the application load file to Deployment Manager, which deploys the software to other servers in the security domain. Local deployment requires that you upload the software load to each target server. The primary security server can then deploy the software applications to other servers in the same security domain.

For Deployment over NFS, the LinuxBase `.iso` load is required to be present on Deployment server. By default, one load is already present on any set up CS1000 Linux server – those from which it was installed. To perform NFS installation and Deployment of server that has different base system type (for example, EL6 based server from non-EL6 based server) it is required to upload the corresponding `.iso` load file first.

Note:

`iso` uploads are not available on CP PM hardware platform.

For more information about installing the load files, see Adding a software load from the Deployment Server on page 78.

Supported configurations

The following list shows the possible application options supported in Deployment Manager:

Predeployed applications	Supported configurations
SS	SS
EM	EM
NRS	NRS
SubM	SubM
CS	CS

Table continues…

Predeployed applications	Supported configurations
CS 1000HS-EM	CS 1000-EM
BRIDGE	BRIDGE
SS, EM	SS_EM
SS, NRS	NRS+SS
SS, SubM	SS_SubM
SS, CS	CS+SS
EM, SubM	SS_EM_SubM
EM, NRS	NRS+SS_EM
EM, CS	CS+SS+EM
NRS, SubM	NRS+SS_SubM
NRS, CS	CS+SS_NRS
SubM, CS	CS+SS_SubM
SS, EM, NRS	NRS+SS_EM
SS, EM, SubM	SS_EM_SubM
SS, EM, CS	CS+SS+EM
SS, NRS, SubM	NRS+SS_SubM
SS, NRS, CS	CS+SS_NRS
SS, SubM, CS	CS+SS_SubM
EM, NRS, SubM	NRS+SS_EM_SubM
EM, NRS, CS	CS+SS+NRS+EM
EM, SubM, CS	CS+SS+EM_SubM
NRS, SubM, CS	CS+SS_NRS_SubM
SS, EM, NRS, SubM	NRS+SS_EM_SubM
SS, EM, NRS, CS	SS+SS+NRS+EM
SS, EM, SubM, CS	CS+SS+EM_SubM
SS, NRS, SubM, CS	CS+SS_NRS_SubM
EM, NRS, SubM, CS	CS+SS+NRS+EM_SubM
SS, EM, NRS, SubM, CS	CS+SS+NRS+EM_SubM

The preceding list shows the applications that are supported in standalone or non-dedicated mode. All other applications, such as Avaya Aura® MS, are supported as standalone only. You can only deploy a standalone application on a member server; otherwise it is not a standalone deployment.

Note:

All configurations that include CS application are not supported on Common Server 3 platform.

Backup and restore application data

In order to retain application data values, you must perform a data backup prior to an installation or upgrade. The type of data backed up is dependent on the applications/manager running on the server. For example:

- UCM data backup always includes Linux Base system settings and parameters. Subscriber accounts are a part of UCM data backup.
- If the server is a primary security server, the backup includes UCM data.
- If the Avaya Aura® MS application is deployed on the server, the backup (Avaya Aura® MS uses Element Manager to backup Avaya Aura® MS data) includes Avaya Aura® MS data.

Note:

For information about data backup using Avaya Aura® MS Element Manager, see the Avaya Aura® MS documentation *Media Server Administration and Security, NN44471-600*.

Other backups can include NRS, Subscriber Manager, CS 1000, CS 1000 HS, and Signaling Server/PD.

After the application installation or upgrade is complete, you can restore application data from the backup you created.

The following actions are performed during a system restore:

- All applications are stopped (including Web applications).
- Configuration and provisioning data for pre-installed applications and for previously deployed applications is restored.
- All applications are restarted except for Base Operating System configuration (such as IP addresses and DNS).

Figure 12: Application data backup and restore on page 48 provides a high-level overview of application data backup and restore processes.

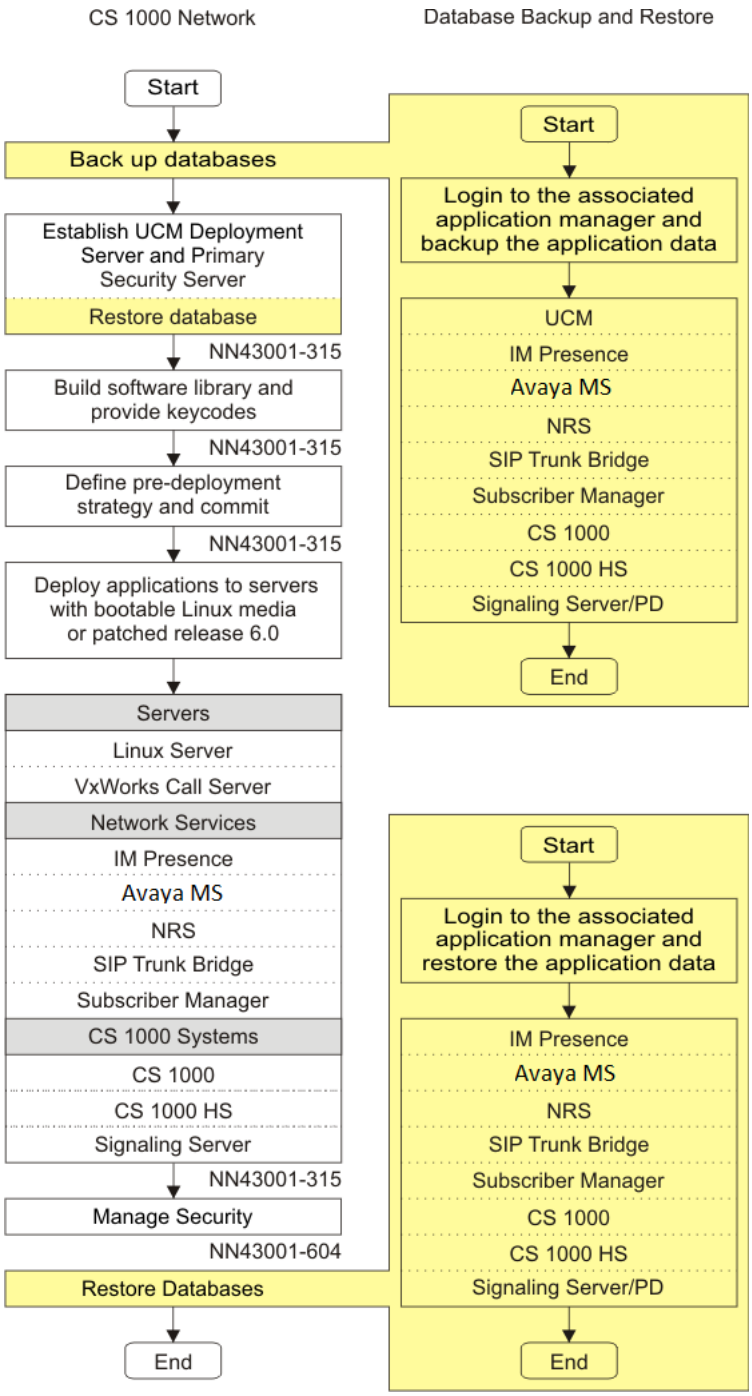


Figure 12: Application data backup and restore

6.0 Deployment Targets

6.0 Deployment Targets can be reached from the UCM Deployment Manager navigation tree. It is available for sites that are supporting a mixed release environment and for those sites that are using a phased approach for upgrading to a later software release. For CS 1000 systems running Release 6.0, you can continue to access the 6.0 Deployment Targets link to manage and deploy application software and for system data backup and restore. For more information, see 6.0 Deployment Targets on page 108.

System upgrade

A system upgrade includes a reinstallation of Linux Base and applications with your system data restored. For more information, see Upgrading a backup or member server from Release 6.0 or later on page 125.

NFS/system upgrade versus a local installation

In scenarios where there is not enough network bandwidth, such as a slow WAN connection between the Deployment Manager server and the desired target server, the recommended approach is to perform a local installation. For procedures on performing a local installation, see Installing a new Linux base on page 55.

Element Manager

When configuring your Communication Server 1000 High Scalability (HS) system in Deployment Manager, there are two lists for Element Manager. The first list includes all the Linux servers that can be selected for deployment with the CS 1000HS-EM application. The second list (for Alternate Element Manager) contains a default value of Not Configured and shows the Linux servers from the first list except for the server that was selected in the first list.

Upon finishing the configuration for Element Manager and Alternate Element Manager, the configured servers (or just Element Manager if that is the only one configured) become members of a UCM group with the type xemGroup. The main Element Manager server is made the leader for this group. This group is made a member to the multicore cluster group.

A file is created with the IP addresses of the main Element Manager server and the Alternate Element Manager server which includes whether it is configured as standalone or redundant mode. This file is transferred to the Target Server during the deployment and is read by the monitoring process.

There are one or two CS 1000 elements created in UCM depending on the number of servers. For example, if the Element Manager server has FQDN1 and the Alternate Element Manager server has FQDN2, then the managementURL field for the two links is https://FQDN1/…/xemWeb/index.jsp and https://FQDN2/…/xemWeb/index.jsp.

The monitoring process internally changes the managementURL to point to the active server. In this example, the managementURL of the second server is also changed to https://FQDN1/…/xemWeb/index.jsp. If for any reason the main element management server changes from the first server to the other then the management URL of both servers is changed to https://FQDN2/…/xemWeb/index.jsp. The following figure shows the CS 1000HS-EM screen from the UCM elements page.

For more information about Element Manager for HS, see *Avaya CS 1000E High Scalability Installation and Commissioning , NN43041-312*. For more information about configuring a CS 1000 High Scalability system, see Defining a new CS 1000 High Scalability system on page 97.

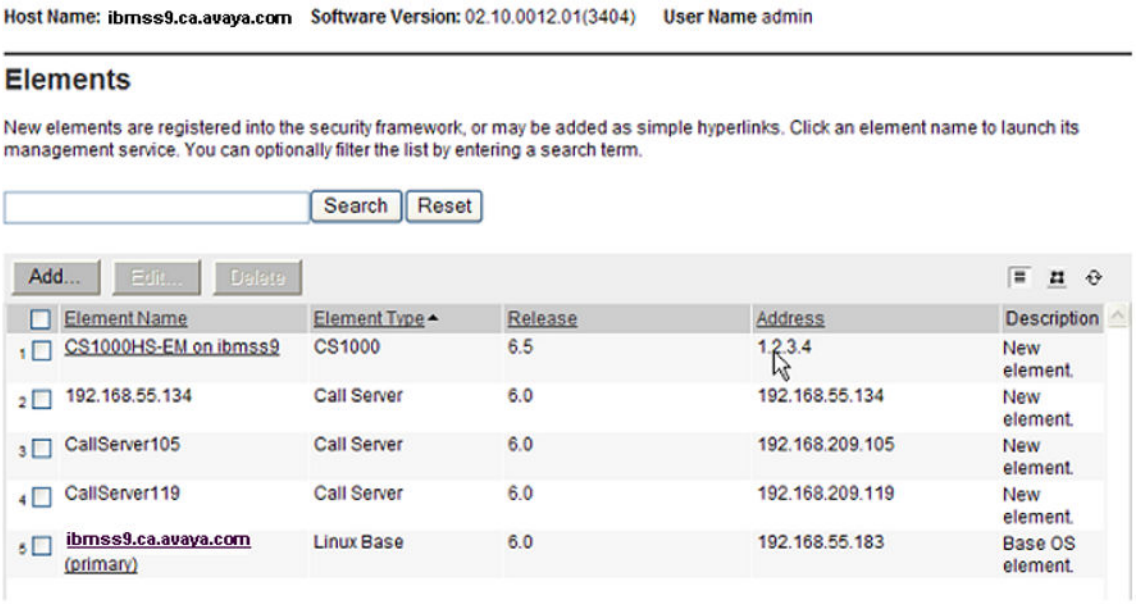


Figure 13: CS 1000HS-EM screen

Chapter 5: New Linux Base installation

The chapter includes a new Linux Base installation. You can install the Linux Base using a local Linux Base installation media or over the network. The following procedures are recommended for a Primary security server installation and, if necessary, you can also use the procedures for an offline installation of the Member and Backup servers. However, the recommended approach for installing Linux Base on the Member and Backup servers is using NFS, see Installing the servers (NFS-based new installation) on page 116.

Note:

If you are installing Linux Base on HP DL360 G7, G8 or G9 server, you must download the corresponding updated Linux Base installation image.

Navigation

- Prerequisites on page 51
- Installing a new Linux base on page 55

Prerequisites

The server must meet the following requirements:

- The hard drive size must be at least 40 GB.
  - If you are installing Linux Base on an existing VxWorks CP PM Signaling Server, use the command **`diskSizeShow`** to check the hard drive size. For information about upgrading the CP PM hard drive, see procedure for Replacing the hard drive on a CP PM Signaling Server in *Avaya Circuit Card Reference, NN43001-311*.
- The CP PM card BIOS must be Release 18 or higher to support Linux Base on a CP PM version 1 card. Linux Base is required for Co-resident Call Server and Signaling Server (Co-res CS and SS) applications.
- The compact flash card must have a capacity of at least 2 GB for CP PM servers. For CP MG and CP DC, USB 2.0 is the only media supported. CP PM supports Compact Flash and COTS supports only CD/DVD-ROM. USB 1.0 and 1.1 flash devices are not supported.

Note:

The N0220961 USB memory stick is supported for Avaya Communication Server 1000. Not all USB memory sticks are supported.

- If you are installing Linux Base on an existing VxWorks CP PM Signaling Server, use the command **`memSizeShow`** to check the memory size. For information about upgrading the memory capacity of a CP PM Signaling Server, see procedure for Upgrading the CP PM memory in *Avaya Circuit Card Reference, NN43001-311*
- You must create a bootable media device using the mkbootrmd.bat tool every time a bootable software load is copied to the media. For information about creating a bootable media device, see Creating a bootable RMD for Linux Base installations on page 205.

Before you install the Linux Base, you must gather the following customer information:

- ELAN IP address
- ELAN gateway IP address
- ELAN netmask
- The host name associated with the TLAN

Note:

Supported Host Name length — The maximum length for the Host Name is 32 characters. The minimum length is 1 character. The first character of the host name must not be a digit.

Supported Host Name characters — The host name you enter must conform to the following:

- A valid host name consists of a text string that can include the alphabetic characters 'a' to 'z', the digits '0' to '9', and the hyphen (-).
- The period (.) is not permitted in the host name because it is reserved for use as a delimiter between domain names.
- No space or tab characters are permitted.
- Hyphen character (-) is not permitted.
- The first character of the Host Name must be an alphabetic character (a to z).

- Domain name

Note:

A Fully Qualified Domain Name (FQDN) consists of a host name, a domain name, and a top-level domain name. For example, the FQDN, kwei.ca.avaya.com, the host name is kwei, the domain name is ca.avaya, and the top-level domain name is .com. The FQDN must contain at least three fields separated by dots. The host name cannot contain dots.

Note:

For security reasons, Internet Explorer does not set cookies for two-letter domains (for example, xx.yy). Therefore, Avaya recommends that you do not configure domain names with less than three letters.

Note:

If you are using a DNS server to resolve the FQDN to an IP address, ensure that you can resolve the FQDN to the expected IP address prior to the installation of the Linux server. For example, attempt to ping the FQDN from a PC that uses the external DNS server, and it should resolve to the expected IP address.

- TLAN IP address
- TLAN gateway IP address
- TLAN netmask
- Timezone
- IP address of the Primary Domain Name Service (DNS) server
- Default system gateway associated with the network interface is TLAN.

Note:

TLAN as the default gateway can be influenced by your deployment decisions about how applications are to be deployed in accordance to your network topology. For a definition of ELAN and TLAN, see Network configuration on page 293.

Note:

The ELAN and TLAN ports on the Co-res CS and SS can be cabled through the Gateway Controller. Even though the ELAN and the TLAN ports can be connected directly to an external Layer 2 switch, it is recommended that the ports be connected to the Gateway Controller to provide ease of cabling and to take advantage of the dual-homing feature provided by the Gateway Controller.

Note:

The CLI command **`routeconfig`** can be used to add routing entries. The choice of routing entries will depend upon the network topology and application deployment. For a list of Avaya Linux Base CLI commands, see Avaya Linux Base CLI commands on page 275.

Warning:

If you are installing Linux Base on a CP PM card and the CP PM card is currently running Signaling Server software from VxWorks, you must either press the faceplate reset button or reseat the card before you begin the Linux Base installation. Failure to do so results in a watchdog reset during installation. This scenario occurs when you issue a reboot -1 from the pdt shell and then proceed directly to the Linux Base installation. Reset the card using the faceplate button to disable the hardware watchdog and allow the installation to complete.

Warning:

Avaya recommends using hardware firewall to avoid DDOS attacks on CPPM and CPMG platforms.

Additional equipment:

You may require the following additional equipment, depending on the installation options that you select.

- PC—you can use a client PC for the following installation tasks:
  - Run a program such as Putty to connect to the Linux server COM1 port. Use of the COM1 port is mandatory for installations on a CP PM server, and optional for installations on a COTS server.
  - Configure UCM primary (Deployment Server), backup, and member servers.
  - Create a bootable media for local installation on a Server (for the Primary (Deployment Server) and on Release 5.5 or earlier systems).
  - Launch Deployment Manager using a Web browser to deploy software.
- Keyboard, video card, and monitor (KVM)—KVM can be used for COTS server Linux Base installation and password recovery.

  Note:

  KVM is no longer mandatory for password recovery; Linux Base also supports COM port password recovery. You can use a USB Keyboard, USB mouse, and a VGA monitor for CP DC card Linux Base installation and password recovery. The CP DC card has a USB and a VGA port on the faceplate.

  Note:

  If you connect to the IBM x3350 server with a terminal for setup, the server does not function with the serial cable that was previously shipped with the ISP 1100 or other COTS platforms. The IBM x3350 server requires the new NTRX26NPE6 9 pin female to 9 pin female null modem cable. For a picture of the null modem cable, see Figure 179: NTRX26NPE6 9 pin female to 9 pin female null modem cable on page 263.
- Ensure the USB security dongle adapter is hidden from plain view.
  - For a Dell R300 server: insert the USB security dongle adapter into an internal USB port (recommended).
  - For an IBM x3350 server: insert the USB security dongle adapter into a rear USB port.
  - For COTS2 and Common Servers: insert the USB security dongle adapter with security dongle into a USB port.
  - Restart the server to ensure the dongle is recognized.

  The following figure shows a USB security dongle and a USB security dongle adapter.

Figure 14: USB Security dongle and adapter

Installing a new Linux base

Install Linux base.

Warning:

If you access the Linux server through the COM port of a client PC, it is possible that garbled characters (such as uuuuuu) can appear during a system restart during the installation. This appearance can make the system seem to hang.

You can resolve the problem by reestablishing the COM port connection from the client PC or work station to the Linux server.

Do not manually restart the system during the upgrade or installation. This can result in hard drive corruption, and forces you to reinstall the system.

1. Insert the Linux base installation media.

   Warning:

   The Linux base DVD should only be inserted in the DVD drive during the Linux base installation on a COTS server (this does not apply to CP PM servers). Normally the DVD auto-ejects after the Linux base installation is complete. If the Linux base DVD is accidentally left in the DVD drive after installation and a system restart occurs, the system will boot into the installation program. This can be interpreted as a hung system. If this occurs, manually eject the DVD and restart the system.

2. Restart the server.

Important:

The boot prompt appears only briefly. You have about eight seconds to respond before it defaults to COM1.

3. For COTS: Watch for the boot prompt during the restart process and proceed to 4 on page 56 in this procedure.

   OR

   For CP DC and CP MG servers, press the F key immediately after the server begins rebooting and proceed to 4 on page 56 in this procedure.

   OR

   For a CP PM server, at the Linux base installer screen, you see ..., at this point press the F key to force the board to boot from the faceplate drive, as shown in the following figure, and proceed to 4 on page 56 in this procedure.

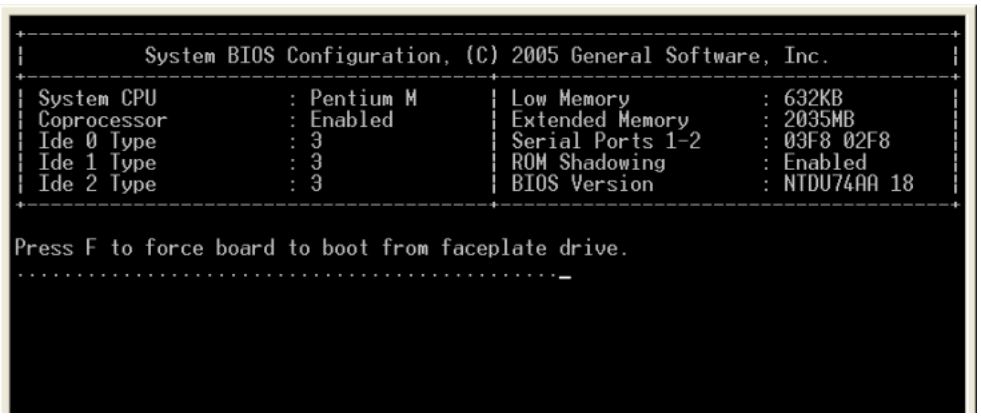


Figure 15: Force board to boot screen

4. Type `com1` to install using a serial console on COM1.

   OR

   Type `kvm` to install using an attached keyboard and video monitor.

   Note:

   Kvm is not a valid option for CP PM servers.

   Important:

   If you log on to the COM1 port, make sure that **Caps Lock** is turned off before you log on.

   The CS 1000 Linux base system installer confirmation screen appears.

5. Type `Y` and press `Enter`, as shown in the following figure.

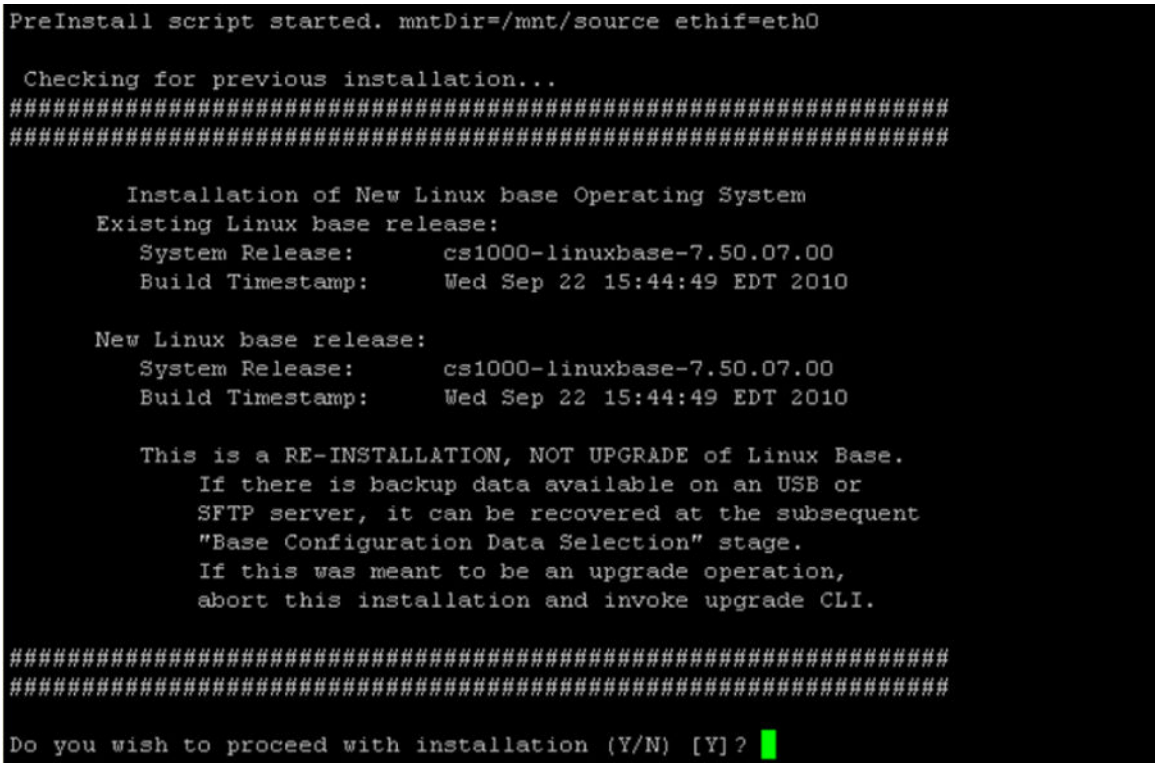


Figure 16: CS 1000 Linux base system installer confirmation screen

The Format all partitions screen appears.

6. Press `Enter` to continue, as shown in the following figure.

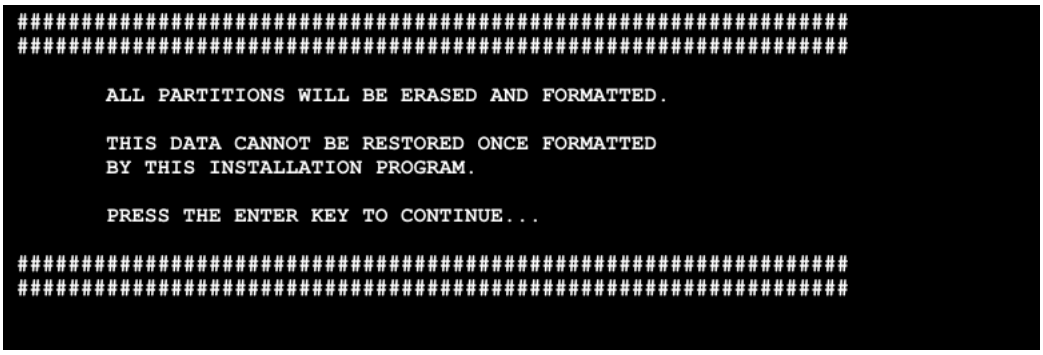


Figure 17: Format all partitions screen

The Base Configuration Data Selection screen appears.

7. Because this is a new installation, type `1` and press `Enter`, as shown in the following figure.

Note:

If you select option 2 or 3, the remainder of the process is the same as the upgrade procedure. Proceed to 9 on page 122 in Upgrade Linux base manually on page 119.

Figure 18: Base Configuration Data Selection screen

The System configuration window appears.

8. Press `Enter` to begin network configuration, as shown in the following figure.

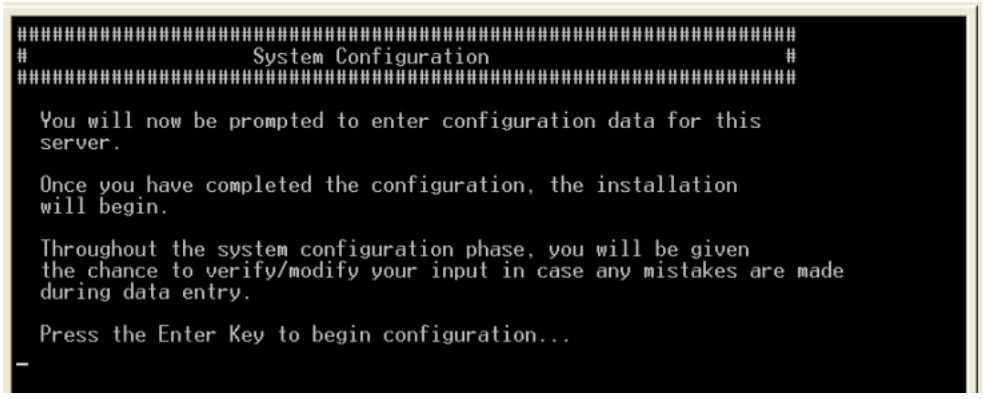


Figure 19: System configuration screen

9. You are prompted to type the following, as shown in the following figure.
   - **ELAN IP Address**
   - **ELAN Netmask**
   - **ELAN Gateway IP Address**
   - **Hostname**

     At the prompt, `Do you wish to configure a Domain Name (Y/N)`, type `Y` as this is a mandatory requirement.
   - **TLAN port Domain Name**

- **TLAN IP Address**
- **TLAN Netmask**
- **TLAN Gateway**

At the prompt, `Do you wish to configure TLAN with IPv6 Addr (Y/N) [N]`, type `Y` to configure TLAN with an IPv6 Address. Default is No.

Press `Enter` to continue.

```
Network Configuration
---------------------
Enter ELAN IP Address: 10.2.115.101
Enter ELAN Netmask: 255.255.255.0
Enter ELAN Gateway IP Address: 10.2.115.1
FQDN (Fully Qualified Domain Name) = Hostname + Domain Name
Enter Hostname: sys219
Do you wish to configure a Domain Name (Y/N) [Y]?
Enter TLAN port Domain Name: canada.com
Enter TLAN IP Address : 10.2.110.201
Enter TLAN Netmask: 255.255.255.0
Enter TLAN Gateway IP Address: 10.2.110.1
Do you wish to configure Tlan with IPv6 Addr (Y/N) [N]?

The Default Gateway will be set to the TLAN Gateway.
Press ENTER to continue.
```

Figure 20: Network Configuration screen

10. On the TimeZone Configuration screen, type the number corresponding to the GMT offset you want to choose, as shown in the following figure.

```
TimeZone Configuration
----------------------
GMT Offset Selection
  1) +00:00                2) +01:00                3) +02:00
  4) +03:00                5) +03:30                6) +04:00
  7) +04:30                8) +05:00                9) +05:30
 10) +05:45               11) +06:00               12) +06:30
 13) +07:00               14) +08:00               15) +09:00
 16) +09:30               17) +10:00               18) +11:00
 19) +12:00               20) +13:00               21) -01:00
 22) -02:00               23) -03:00               24) -03:30
 25) -04:00               26) -04:30               27) -05:00
 28) -06:00               29) -07:00               30) -08:00
 31) -09:00               32) -10:00               33) -11:00
 34) -12:00
Enter GMT Offset (1-34): 27

Select (0,1-3):2
```

Figure 21: TimeZone Configuration screen

For example, to select a time in the United States Eastern time zone, type `28`. The time zone and the corresponding Greenwich Mean Time (GMT) offsets, are shown in the following table.

Table 4: Time zone offsets

Name	Description	Relative to GMT
GMT	Greenwich Mean Time	GMT
UTC	Universal Coordinated Time	GMT
ECT	European Central Time	GMT+1:00
EET	Eastern European Time	GMT+2:00
ART	(Arabic) Egypt Standard Time	GMT+2:00
EAT	Eastern African Time	GMT+3:00
MET	Middle East Time	GMT+3:30
NET	Near East Time	GMT+4:00
PLT	Pakistan Lahore Time	GMT+5:00
IST	India Standard Time	GMT+5:30
BST	Bangladesh Standard Time	GMT+6:00
VST	Vietnam Standard Time	GMT+7:00
CTT	China Taiwan Time	GMT+8:00
JST	Japan Standard Time	GMT+9:00
ACT	Australia Central Time	GMT+9:30
AET	Australia Eastern Time	GMT+10:00
SST	Solomon Standard Time	GMT+11:00
NST	New Zealand Standard Time	GMT+12:00
MIT	Midway Islands Time	GMT-11:00
HST	Hawaii Standard Time	GMT-10:00
AST	Alaska Standard Time	GMT-9:00
PST	Pacific Standard Time	GMT-8:00
PNT	Phoenix Standard Time	GMT-7:00
MST	Mountain Standard Time	GMT-7:00
CST	Central Standard Time	GMT-6:00
EST	Eastern Standard Time	GMT-5:00
IET	Indiana Eastern Standard Time	GMT-5:00
PRT	Puerto Rico and US Virgin Islands Time	GMT-4:00
CNT	Canada Newfoundland Time	GMT-3:30
AGT	Argentina Standard Time	GMT-3:00
BET	Brazil Eastern Time	GMT-3:00
CAT	Central African Time	GMT-1:00

11. On the DST Selection screen, type the number that corresponds to the Daylight Saving Time (DST) value that you want to choose and press `Enter`, as shown in the following figure.

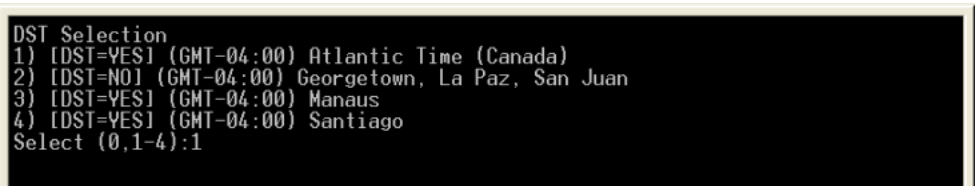


Figure 22: DST Selection screen

12. Review the configuration information on the Network Configuration Validation screen. Type `Y` to confirm the data, and press `Enter`.

    OR

    Type `N` and press `Enter` to reenter the configuration information, as shown in the following figure.

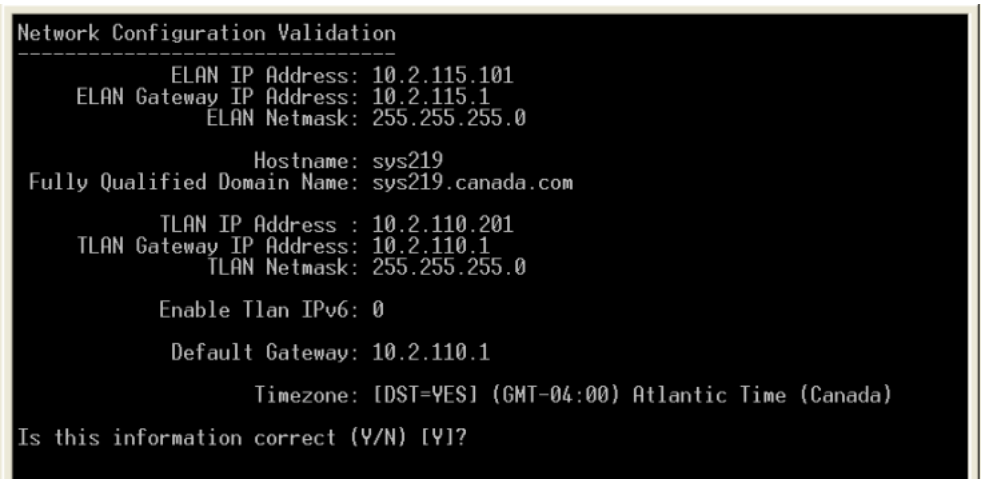


Figure 23: Configuration Validation screen

13. On the Network Time Protocol (NTP) Configuration screen, press `Enter`, as shown in the following figure.

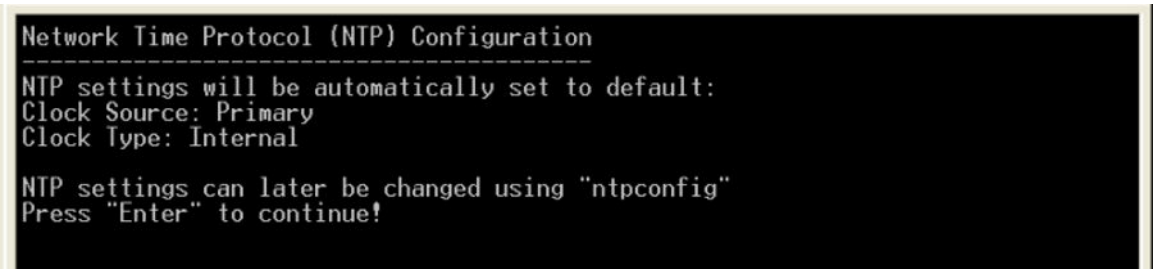


Figure 24: Network Time Protocol (NTP) Configuration screen

Note:

NTP settings can be changed after the installation is complete. To change NTP settings, see Adding a Linux server on page 82. You can also configure NTP settings using the CLI command **`ntpconfig`**.

14. On the, DNS Server configuration screen, type `N` and press `Enter` as you do not want to configure the Primary DNS server IP address if there are no active DNS servers present, as shown in the following figure.

Figure 25: DNS Server Configuration screen

Warning:

Do not configure the DNS IP addresses when no active DNS server is present on the network as you can experience delays in the GUI operations. Use Base Manager to add at a later time.

15. On the DNS Configuration Validation screen, type `Y` and press `Enter` to confirm the configuration.

OR

Type `N` and press `Enter` if the configuration information is not correct.

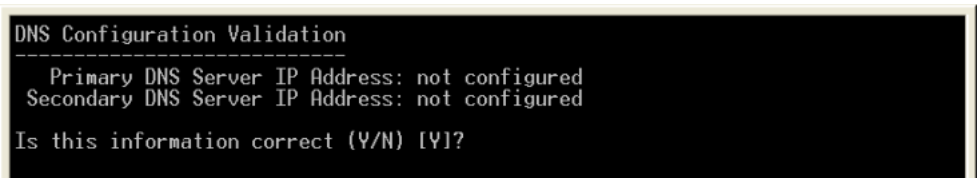


Figure 26: DNS Configuration Validation screen

16. On the Date and Time Configuration screen, type `Y` and press `Enter` to confirm the date and time.

OR

Type `N` and press `Enter` if the configuration information is not correct.

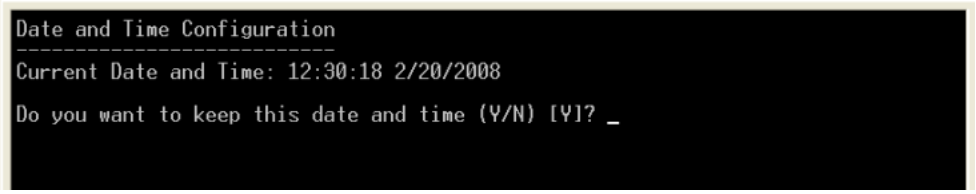


Figure 27: Date and Time Configuration screen

17. On the Password Configuration screen for the local server account, type a root password and retype the root password, as shown in the following figure.

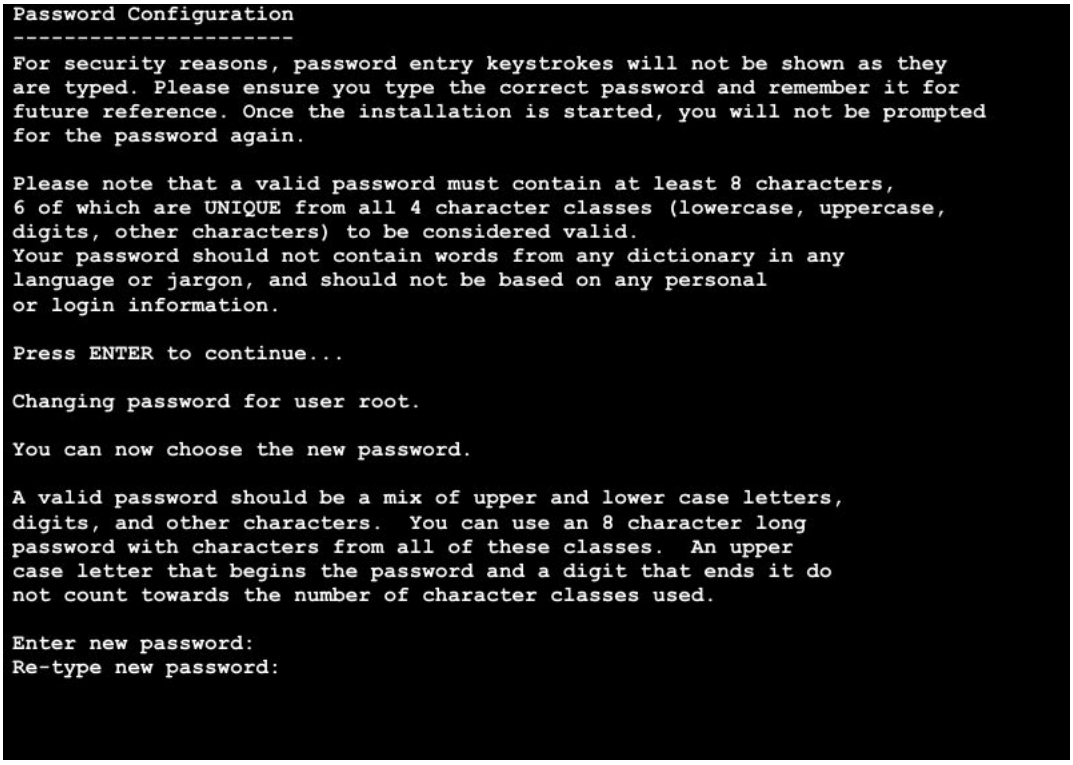


Figure 28: root Password Configuration screen

Note:

For information about passwords, see Password creation guidelines on page 34.

18. On the admin2 Password Configuration screen, type the admin2 password and retype the admin2 password, as shown in the following figure.

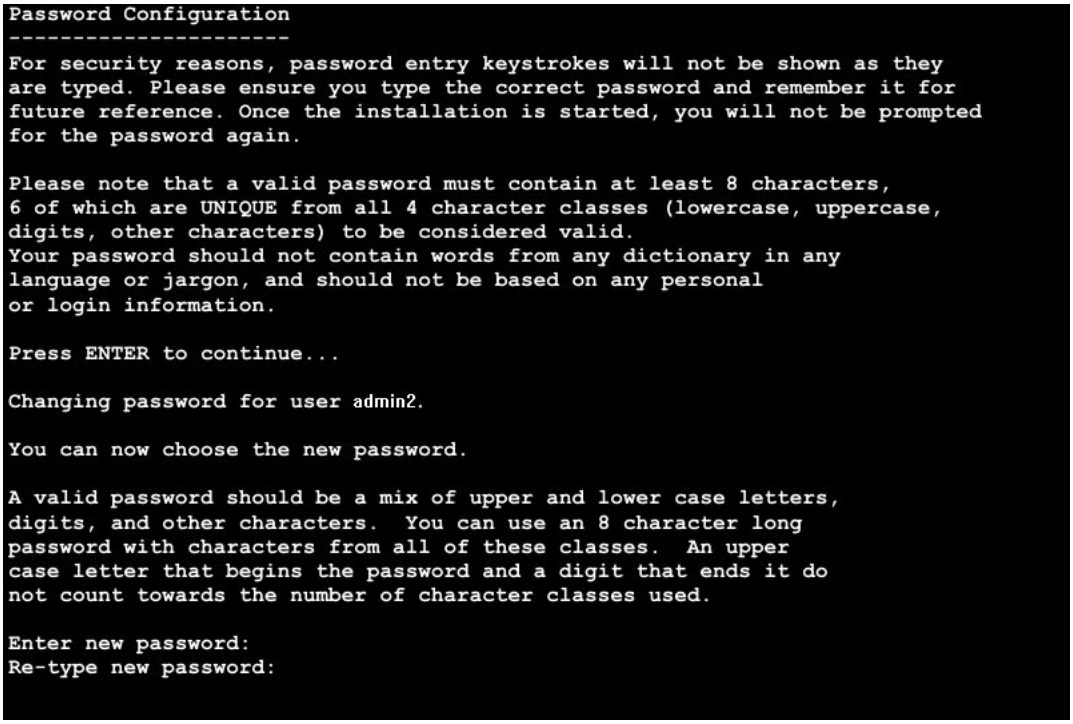


Figure 29: Password Configuration screen

19. On the Deployment Server screen, type `Y` if you wish to configure this system as the Deployment Server (Primary security server)

    OR

    Type `N` for Member and Backup servers, as shown in the following figure. Press `Enter`.

    Continue to the next step to confirm that the Deployment Server is the Primary security server.

20. If you select Y in the previous step, you are prompted to type `Y` at the `Continue configuration as the Deployment Server (Y/N) [N]` prompt, as shown in the following figure.

Figure 30: Deployment Server screen

A pre-installation status screen appears, as shown in the following figure.

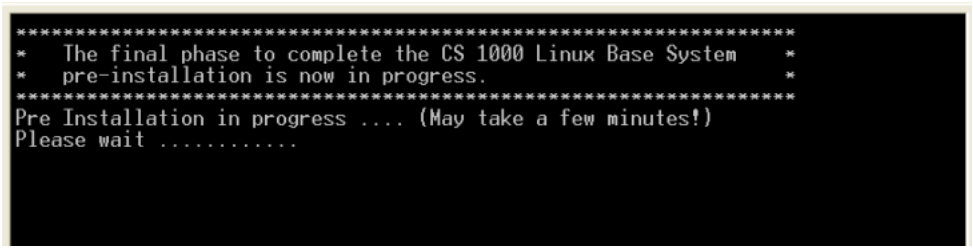


Figure 31: Pre-installation status screen

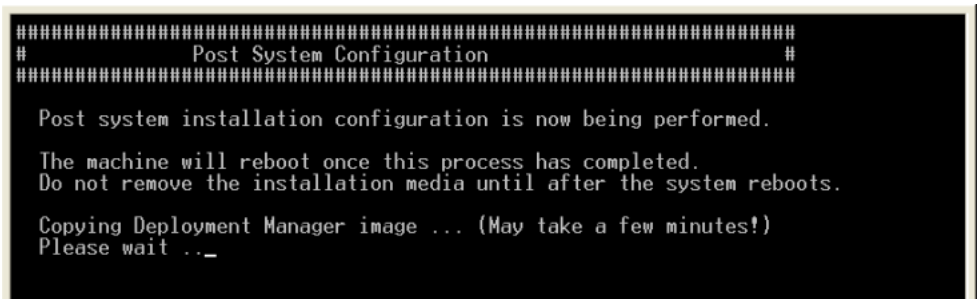


Figure 32: Post System Configuration screen

The Linux Hardening status displays, as shown in the following figure. This indicates that the Linux base installation is finished.

Figure 33: Post Installation Final Phase screen

The system restarts, as shown in the following figure.

Figure 34: System restart screen

Warning:

For COTS servers, make sure that the installation DVD ejects. If the installation DVD does not eject automatically, eject the DVD manually.

21. Remove installation media and insert backup media.
22. For CP PM server cards, do not press F when prompted, as shown in the following figure.

Caution:

Do not press F at this step; otherwise, you are taken back to the installation menu and must perform the procedures again.

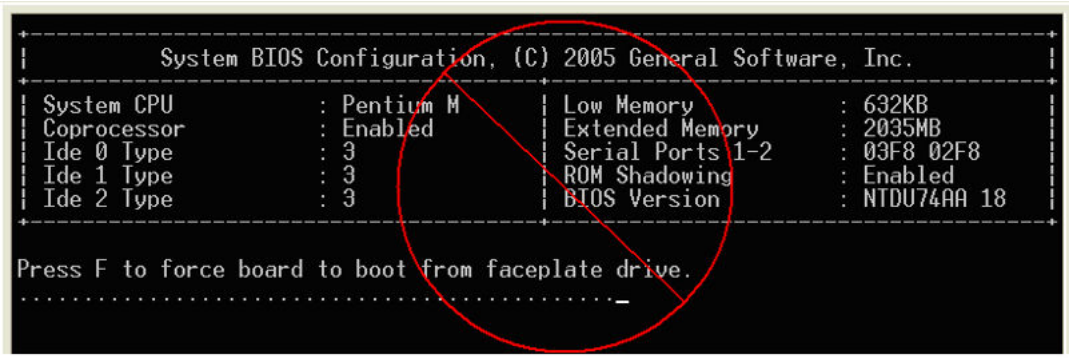


Figure 35: CP PM screen

23. On the Avaya Linux base screen, type the admin2 userid at the login prompt, and type the admin2 password, as shown in the following figure. This can take several minutes before you can proceed to the next step.

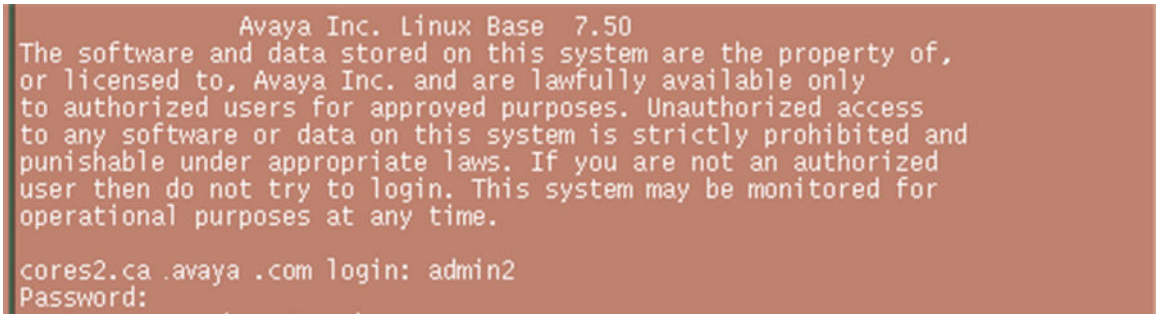


Figure 36: Avaya Linux base screen

24. Start a Web browser to configure the primary security server. For more information about configuring a primary security server, see Configuring the primary security server on page 70.

Chapter 6: Deployment Manager—New system installation and commissioning

This chapter provides the procedures for an end-to-end installation and commissioning of Linux Base and applications. At this stage, Linux Base must be installed on the Primary security server (Deployment Server) but it is not configured.

Navigation

- Installation workflow on page 68
- Primary security server configuration on page 69
- Deployment Manager—Server preconfiguration on page 74
- 6.0 Deployment Targets on page 108
- NFS based new installation on page 113

Installation workflow

The following figure provides an overall workflow for a new Avaya Communication Server 1000 (Avaya CS 1000) system Linux installation and commissioning. The workflow indicates the recommended sequence of events to follow and provides the technical document number for the detailed procedures required for the task.

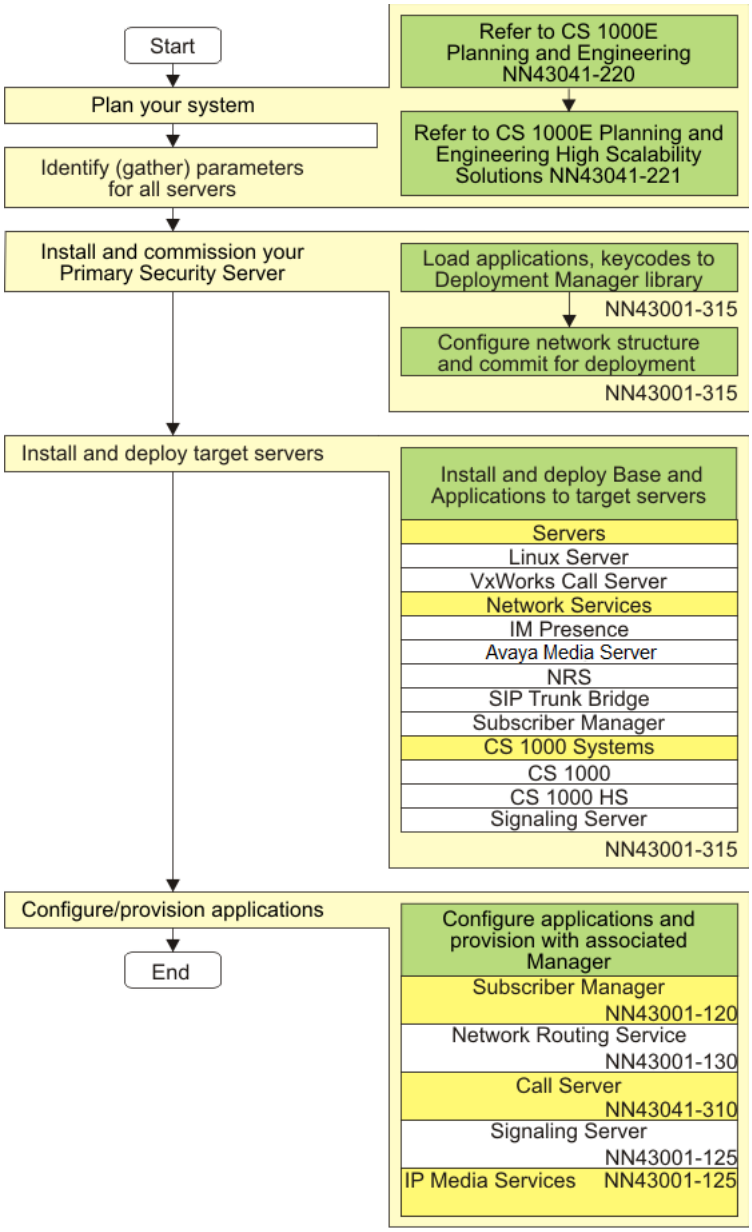


Figure 37: New Linux system installation workflow

Primary security server configuration

This section provides the procedures for configuring the primary security server. For more information about security server configuration, see Configuring the primary security server on page 70 or *Avaya Unified Communications Management Common Services Fundamentals, NN43001-116*.

Configuring the primary security server

Configure the primary security server.

1. In the Web browser Address bar, type `https://<FQDN or IP address>/local-login/` of the primary security server, enter the UserID and password as configured during the Linux Base installation, Password Configuration step and press `Enter`.
2. On the Security Configuration page, select **Full security configuration**, as shown in the following figure.

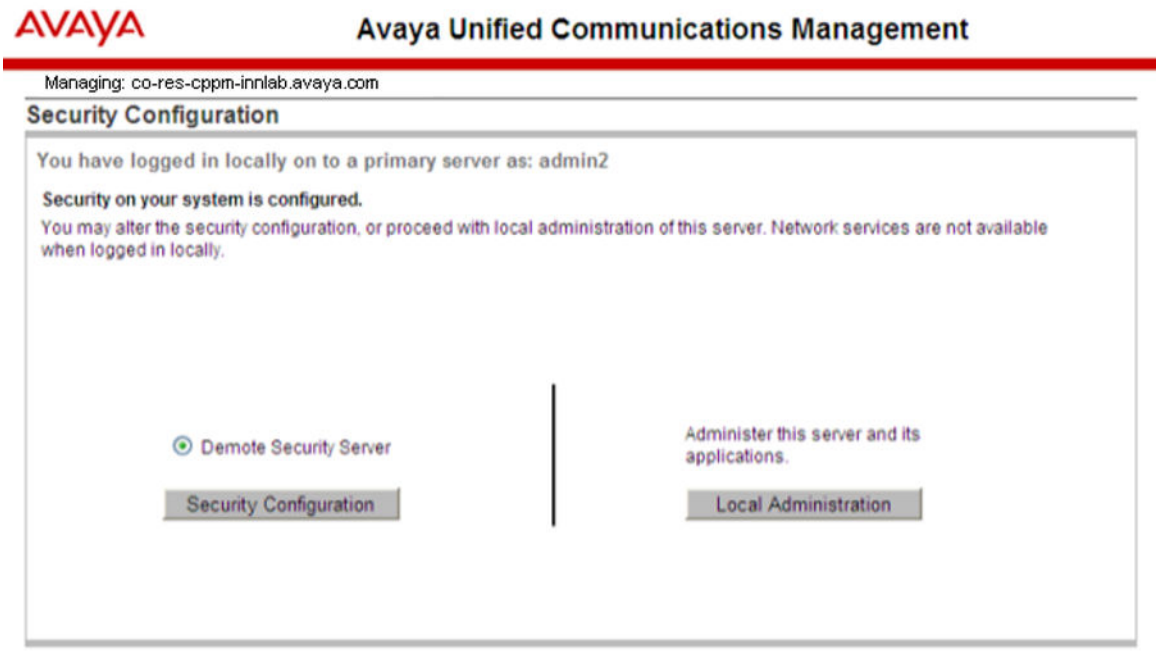
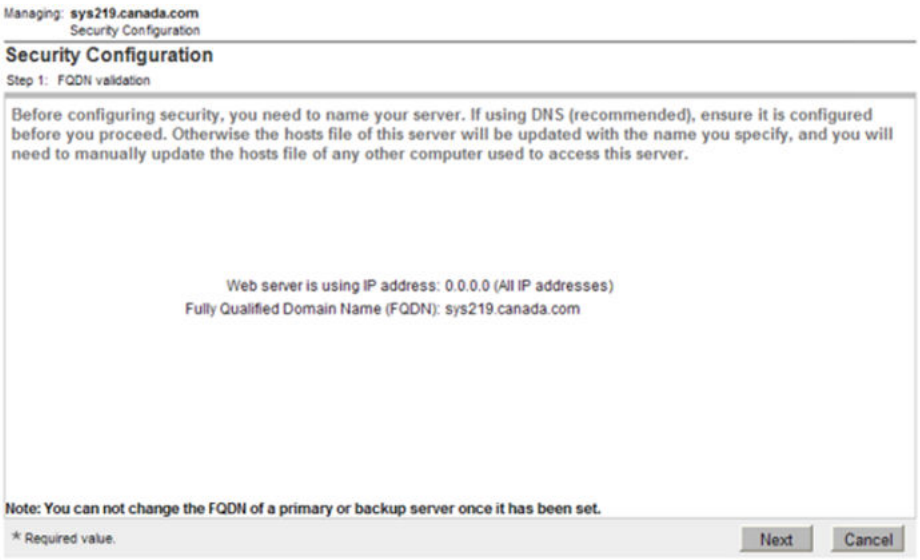


Figure 38: Security configuration page

3. Click **Security Configuration**.

   The FQDN validation page appears, as shown in the following figure.



4. Confirm the IP address and FQDN is correct, and click **Next**.

   Important:

   If using a DNS server, the DNS server must be configured before proceeding.

5. On the **Select server type** page, select **Primary security server**, and click **Next**.

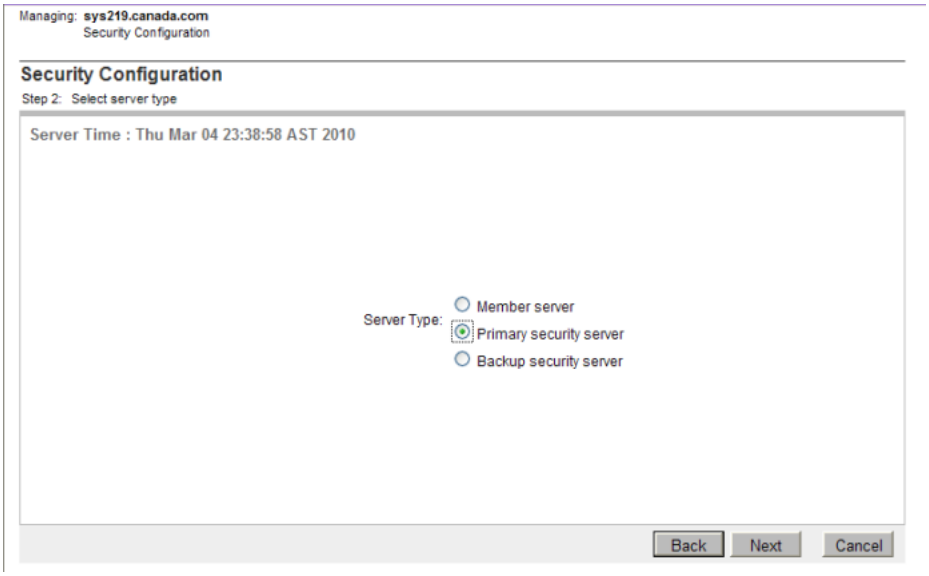


Figure 39: Select server type page

6. On the **Enter server information** page, type the Administrator password for the built-in Admin account, retype the password in the **Confirm Administrator** password field, and click **Next**, as shown in the following figure.

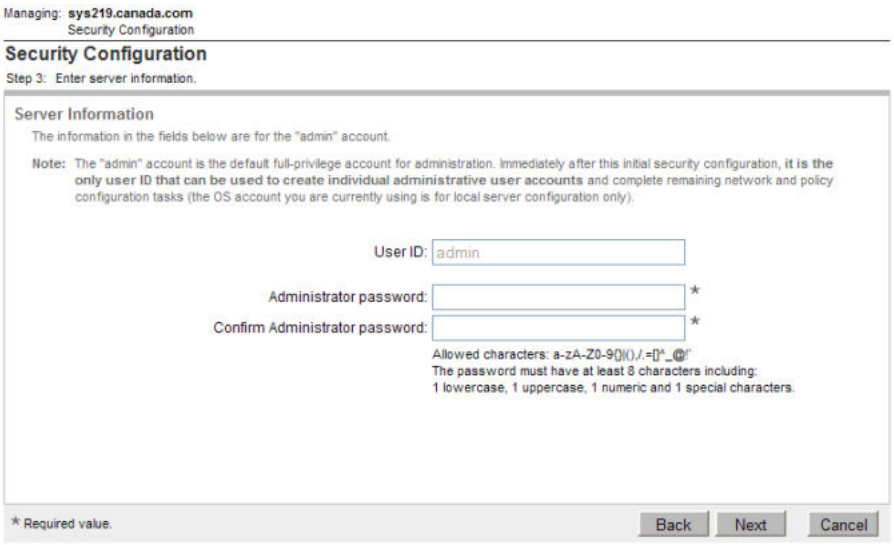


Figure 40: Server Information page

7. On the **Enter Certificate information** page, configure the following values and then click **Finish**.

   Friendly name: Type a string that would be used to identify the certificate, for example, UCM Primary Security Server.

   Bit length: Type a value that represents the number of bits used for encryption. Values can be 1024 and 2048. More CPU is required for processing as the bit value increases.

   Organization: Your company name.

   Organization unit: A division within your company.

   Common name: FQDN of the server. The default is a combination of Windows environment variables Computername and Userdnsdomain. Ensure this field matches the hostname of the system the certificate is on.

   Country/Region: Select a country from the list.

   State/Province: A State/Province where the primary server is located.

   City/Locality: A City/Locality where the primary server is located.

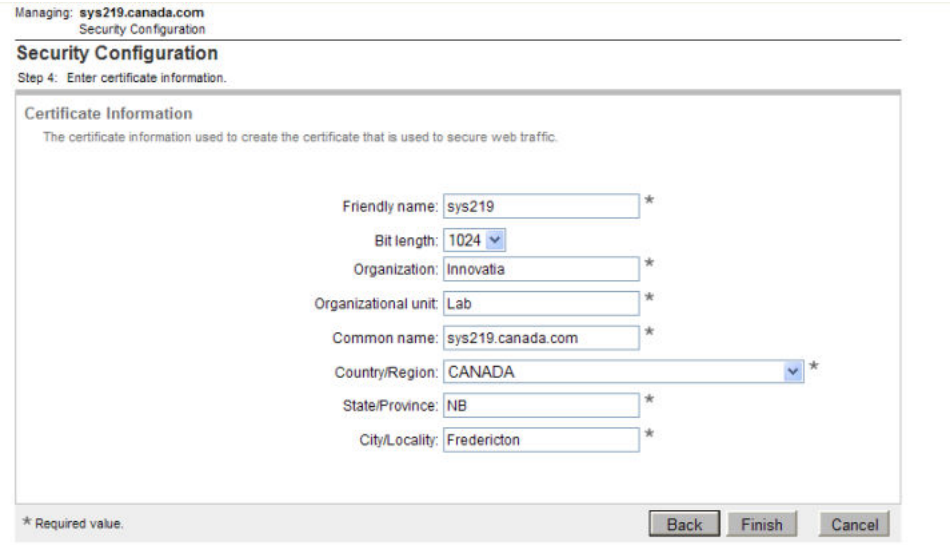


Figure 41: Certificate Information page

8. On the **Security Configuration Progress page**, click **Restart** to restart the Web server and the security configuration changes to take effect.

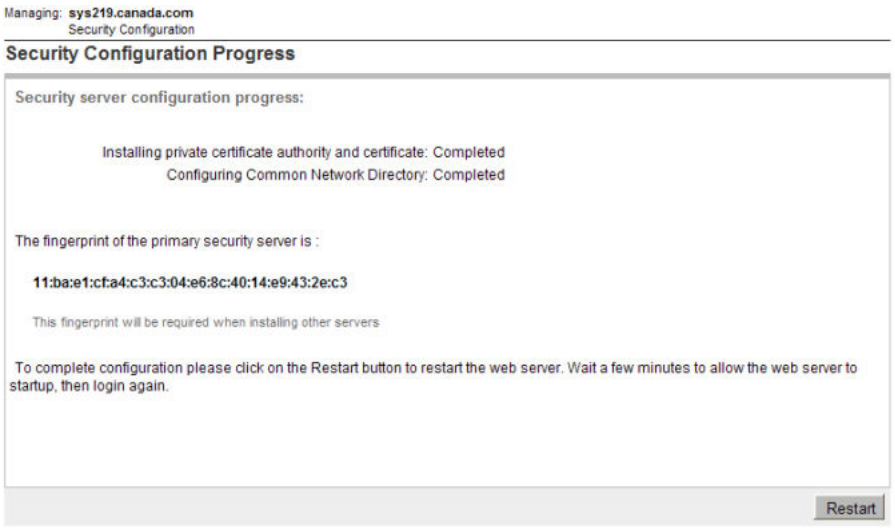


Figure 42: Security Configuration Progress page

The **Restarting the server** Web page appears.

9. Close the Web browser and proceed to Deployment Manager—Server preconfiguration on page 74.

Important:

Wait several minutes after configuring the primary security server before logging on to UCM.

Deployment Manager—Server preconfiguration

You have installed Linux Base on your primary security server (Deployment Server). You can now begin the preconfiguration stage to logically configure the member and backup servers before physically installing the Servers and joining them to the domain. Proceed to Preconfiguring process using Deployment View on page 74.

Prerequisites

- The latest software release of Linux Base must be running on your primary security server (Deployment Server), see Installing a new Linux base on page 55 or Upgrading Linux Base on page 119.
- You must have all the configuration details prepared before you begin preconfiguring the Primary, Member, and Backup servers using Deployment Manager.
- You must be able to log on to UCM. For more information, see Logging on to Unified Communications Management on page 77.

  The primary security server must be configured. For more information, see Configuring the primary security server on page 70.
- Must be able to access Deployment Manager. For more information, see Accessing Deployment Manager on page 77.
- Ensure your hardware is a COTS, CP PM, CP MG, or CP DC.

Preconfiguring process using Deployment View

Use the following procedure to guide you through the process of configuring your member and backup servers. This is the Avaya recommended method.

Note:

Your servers do not have to be physically connected at this stage.

1. Log on to the UCM primary security server with the account that has the NetworkAdministrator role assigned.
2. On the navigation pane, click **Network** > **Software Deployment**.

   The **Deployment View** page appears, as shown in Figure 43: Deployment View commit screen on page 76.
3. On the navigation pane, click **Software Loads**.
4. Select the required .nai files to upload to the deployment server library. For detailed procedures, see Adding a software load from the Client Machine on page 79.

   Important:

   You can upload only one version of each load type. All deployed servers use the same load version.
5. Add the backup and member Linux servers. For detailed procedures, see Adding a Linux server on page 82. If your servers have joined the security domain, proceed to Step 7 on

page 75; otherwise, continue to the next step to add the VxWorks Call Servers to your network.

Important:

The server does not need to be physically installed at this step. The configuration details are only required.

A Linux base element is created in UCM and the element name is visible from the default Deployment View or UCM Elements page.

Important:

On the **Deployment View** page, the Linux base version does not appear under the base Version field and the Status field is identified as Preconfigured. The server is still a logical server at this point. After you physically install the server, the base Version and Status fields show the new version number and Configured status.

6. Add the VxWorks Call Servers to your network, as described in Adding a VxWorks Call Server on page 89 or Adding a VxWorks Call Server for a High Availability system on page 89.

   Note:

   If your VxWorks Call Server has joined the security domain, proceed to the next step.

   An active VxWorks Call Server element appears on the **Deployment View** page. For HA systems, an inactive VxWorks Call Server also appears on the Deployment View page.

   Important:

   The servers are not physically installed or registered to the security domain at this stage.

7. Allocate the servers into the hierarchical groups which determines the application packages required for deployment.

   The servers can be allocated into the following groups:

   - Network Services: for detailed procedures, see the following:
     - Adding a Avaya Aura MS service on page 90
     - Adding a Network Routing Service on page 91
     - Adding a Subscriber Manager service on page 92
   - Avaya CS 1000 systems: for detailed procedures, see the following:
     - Adding a CS 1000 system on page 93
     - Defining a new CS 1000 High Scalability system on page 97

   On the **Deployment View** page, the **Status** field changes from Preconfigured to Predeployed to identify that the server is now part of one or more groups. The Predeployed Applications field shows the applications that correspond to the selected services.

8. On the **Deployment View** page, choose **Servers** from the **View** list, and click **Commit**, as shown in the following figure.

Important:

The Commit button is a system-wide operation. All servers in the Predeployed status are committed.

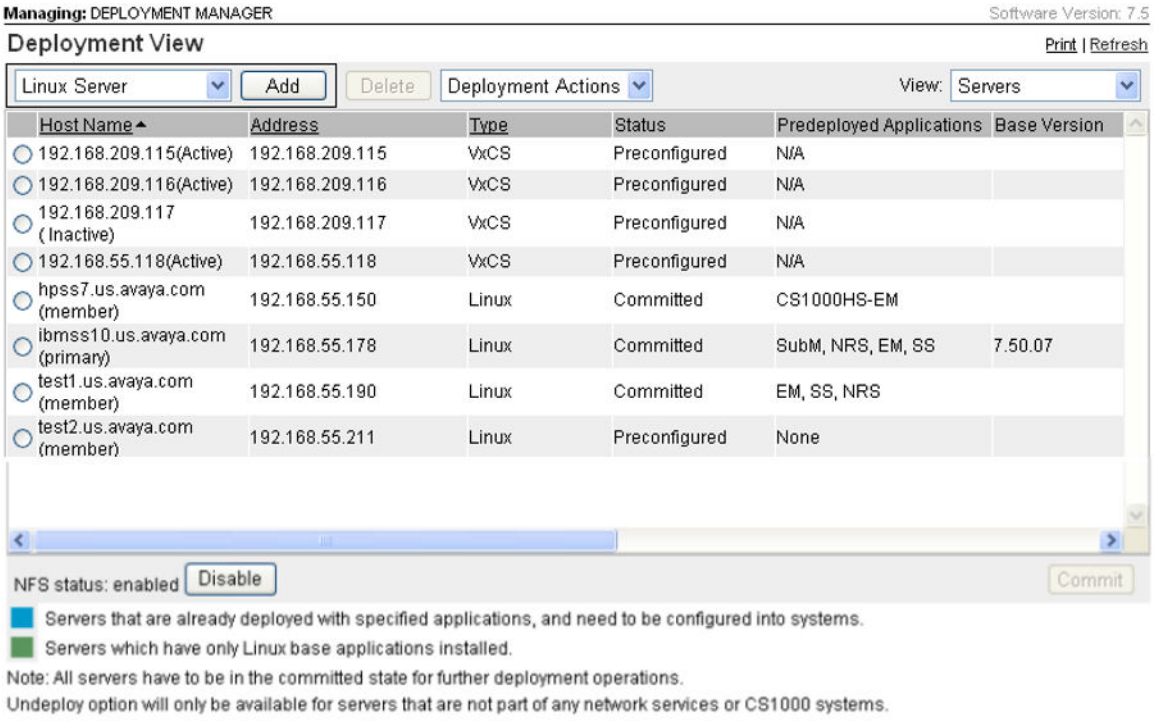


Figure 43: Deployment View commit screen

The Deployment View status is updated to Committed and the Linux servers are now ready for installation and deployment.

9. Install the VxWorks Call Servers and join the security domain, if not already done.

10. You must now physically connect the member and backup servers.

    If Linux base for the backup and member servers is not installed, proceed to NFS based new installation on page 113

    OR

    If Linux base is pre-installed, do the following:

    - Reconfigure the parameters; for more information about reconfiguring parameters, see Configuring a Server pre-loaded with Avaya Linux base on page 130.
    - Configure security; for information about configuring security, see *Unified Communications Management Common Services Fundamentals, NN43001–116*.
    - Proceed to Deploying applications on a Server on page 104.

    OR

    If Linux base is already installed from installation media, then configure security (see *Unified Communications Management Common Services Fundamentals, NN43001–116*) and proceed to Deploying applications on a Server on page 104.

Logging on to Unified Communications Management

Access UCM for application deployment using Deployment Manager.

1. Open the Web browser.
2. Enter one of the following in the Address bar:
   - Fully Qualified Domain Name (FQDN) for the UCM server (preferred). For example, https://<FQDN>.
   - Unified Communications Management (UCM) framework IP address. After you enter the UCM framework IP address, a Web page appears stating that you must access Unified Communications Management by using the FQDN for the UCM server. Click the link on this Web page to use the FQDN for the UCM server.
3. In the **User ID** field, log on using the account with the NetworkAdministrator role (for example, admin).
4. In the **Password** field, enter your password.
5. Click **Log In**.

   The default navigation Web page for UCM appears.

Accessing Deployment Manager

Access Deployment Manager from UCM.

1. Log on to UCM. See Logging on to Unified Communications Management on page 77.
2. In the navigation pane, click **Network**, **Software Deployment**.
3. Validation is performed. If you are logging on for the first time or your credentials have changed, you are prompted for the **Primary Security server user ID** and **Primary Security server password**, as shown in the following figure.

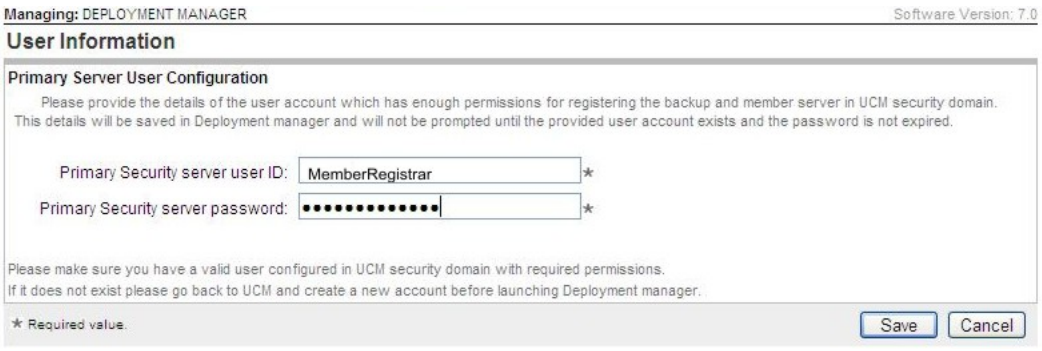


Figure 44: Deployment Manager validation

4. Click **Save**.

Software loads

This section describes how to upload software to Deployment Manager for predeployment. For an overview about software loads, see Software loads on page 44.

Note:

If you are using Deployment Manager on your Deployment Server as your unified solution for end-to-end installation and configuration of Linux Base and applications, you must use the process as described in Preconfiguring process using Deployment View on page 74.

Prerequisites

- Upload the appropriate .nai file (Avaya Communication Server 1000 or Avaya Aura® MS) from the software download site to the server running Deployment Manager.
- Collect your network setup information.
- Must be logged on to the UCM Primary security server using the Admin account. For more information, see Logging on to Unified Communications Management on page 77.
- Must have accessed the Software Deployment section from UCM. For more information, see Accessing Deployment Manager on page 77.
- To avoid a session timeout when adding a software load from a client machine, increase the maximum idle time to 120 minutes on System Manager.
  1. Log on to SMGR, and click **UCM Services**.
  2. On the navigation tree, click **Security > Policies**.
  3. Click the **Session Properties** tab, and click **Edit**.
  4. Change the **Maximum Idle time** to 120, and click **Save**.

Adding a software load from the Deployment Server

Add a software load from the Deployment Server for predeployment.

1. Click **Software Loads** from the **Deployment Manager** navigation tree.

   The Software Loads screen appears, as shown in the following figure.

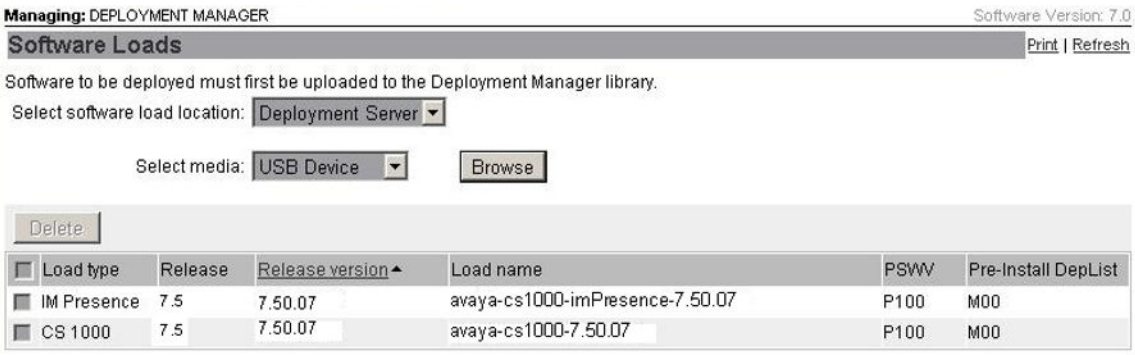


Figure 45: Software Loads screen

2. In the **Select software load location** list, select **Deployment Server**.

3. In the **Select media** list, the choices presented to you are determined by the hardware type for the Deployment Manager.
   - CP DC and CP MG servers: USB Device
   - CP PM: USB and Compact Flash
   - COTS: USB and CD/DVD-ROM
4. Click **Browse** to locate the software load.

   A warning screen appears to ensure that you insert the correct software media on the deployment server or that you upload the correct software to the Deployment Manager Library.
5. Click **Add Load**.

   An upload progress screen appears.
6. The Software Loads screen appears when the upload is complete.

Adding a software load from the Client Machine

Perform the following procedure to add a software load from a client machine.

1. Click **Software Loads** from the **Deployment Manager** navigation tree.

   The Software Loads screen appears, as shown in the following figure.

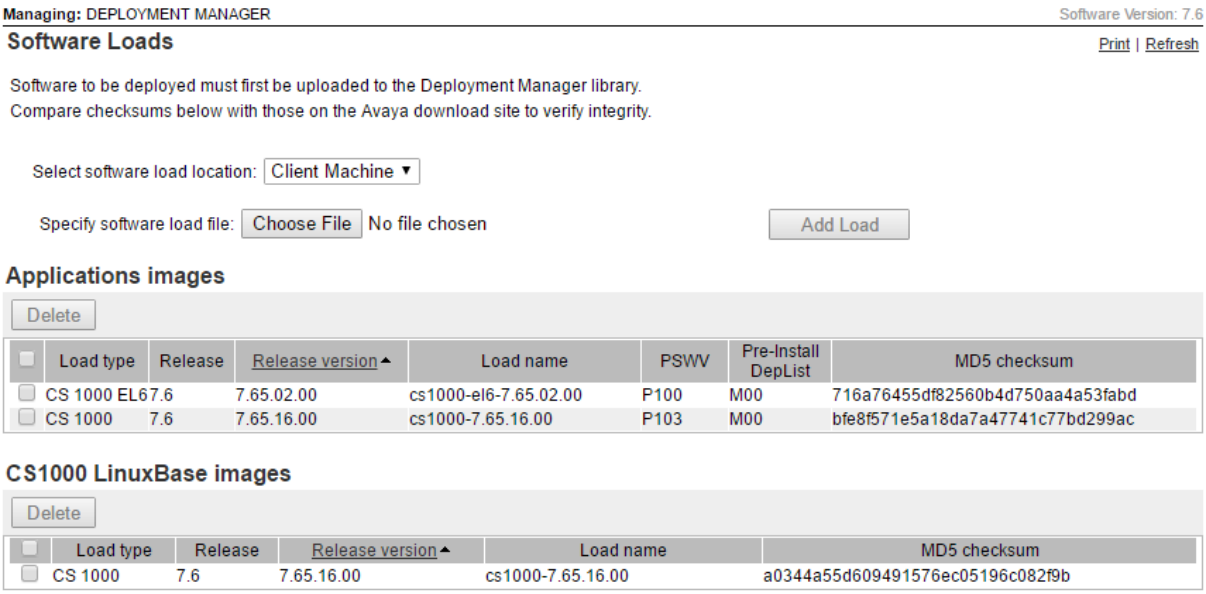


Figure 46: Software Loads screen for Client Machine

2. In the **Select software load location** list, select **Client Machine**.
3. In the **Specify software load file** field, click **Browse** to locate the software load on the client machine.

   The Add Load button is now available.
4. Click **Add Load**.

The upload progress screen appears.

5. The Software Loads screen appears when the upload is complete.

Deleting a software load

Delete a software load.

1. Click **Software Loads** from the **Deployment Manager** navigation tree.

   The Software Loads screen appears, as shown in Figure 45: Software Loads screen on page 78.

2. Select the check box beside the software load to delete.

   The Delete button is now available for you to select.

3. Click **Delete**.

NFS security hardening

Every Primary security server (deployment server) must have the Network File System (NFS) enabled when you deploy the Linux Base and applications to the target servers. By enabling NFS, the server can be an NFS server. Avaya recommends that you disable NFS upon completing the transfer of the Linux Base and application software to the target server. You cannot enable NFS on the member or backup security servers. For information about CLI commands for harden nfs, see Table 19: securityadmin CLI commands on page 279.

Enabling or disabling NFS from Deployment Manager

Enable or disable NFS on the Primary security server. The default state is enabled.

Prerequisites

- Must be able to access Deployment Manager. For more information, see Accessing Deployment Manager on page 77.

Procedure steps

1. On the **Deployment View** page, choose **Servers** from the **View** list.
2. In the **NFS status** section, click **Enable** to enable NFS.

   The NFS status is refreshed to show the status as enabled, as shown in the following figure.

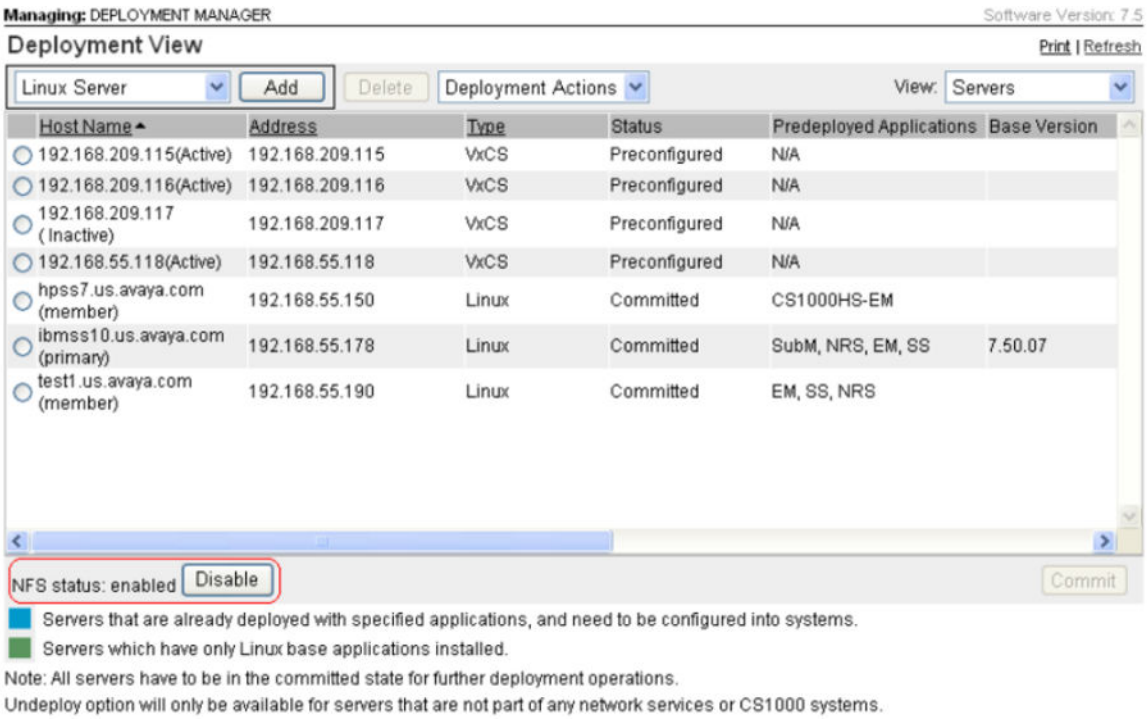


Figure 47: NFS status enabled

OR

Click **Disable** to disable NFS after the Linux Base and applications are deployed to the server.

Important:

The current state of NFS is displayed in the NFS status section on the Deployment View, Servers page.

Deployment View

This section describes how to add servers, Network Services, and Avaya CS 1000 systems, and commit the software for deployment.

Note:

If you are using Deployment Manager on your Deployment Server as your unified solution for end-to-end installation and configuration of Linux Base and applications, you must use the process as described in Preconfiguring process using Deployment View on page 74.

From UCM, you can access the Deployment View page by clicking Software Deployment, UCM Deployment Manager. For an overview of the Deployment View page, see Deployment View on page 43.

From Deployment View, you can access the following:

- Servers on page 82

- Network Services on page 90
- CS 1000 systems on page 93

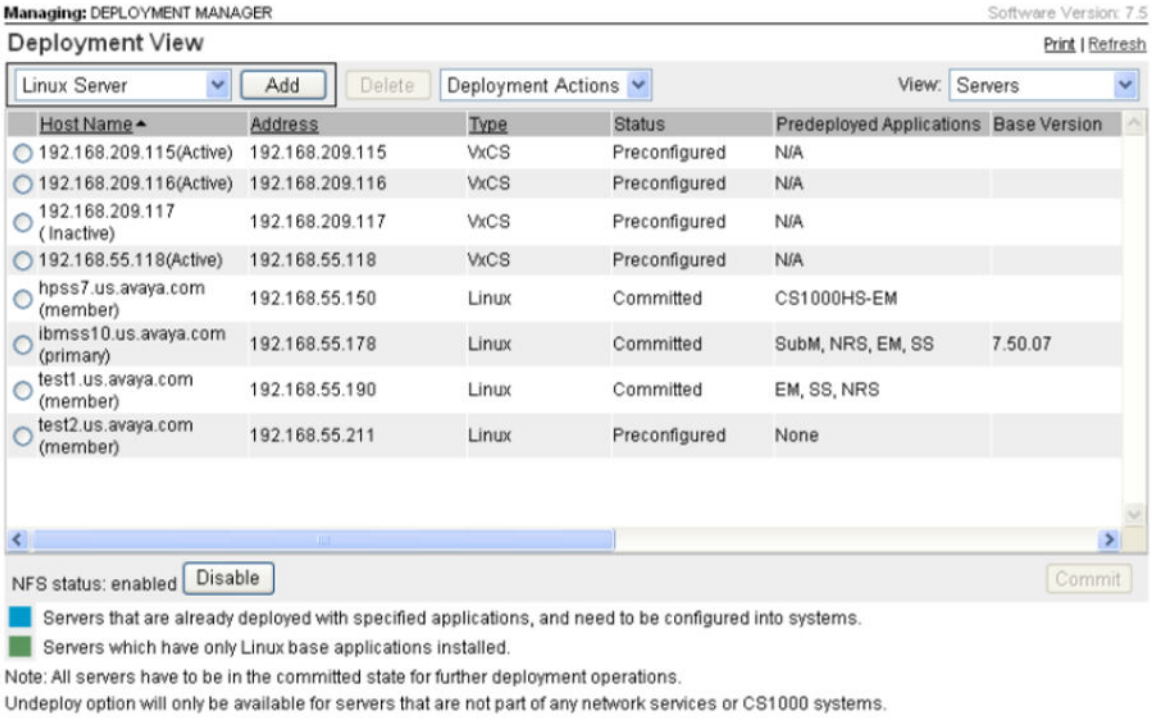


Figure 48: Deployment View page

Servers

This section describes how to add and remove Linux Servers and VxWorks Call Servers.

Navigation:

- Adding a Linux server on page 82
- Configuring the clock source for a Primary server on page 86
- Configuring the clock source for a secondary server on page 87
- Configuring a server that is not a clock server on page 88
- Deleting a Linux server on page 88
- Adding a VxWorks Call Server for a High Availability system on page 89
- Adding a VxWorks Call Server on page 89
- Deleting a VxWorks Call Server on page 89

Adding a Linux server

Add a Linux server to Deployment Manager.

1. On the **Deployment View** page, select **Linux Server** from the list, and click **Add**, as shown in Figure 11: Deployment View page on page 43.

The Enter the network parameters, such as ELAN/TLAN IP addresses, hostname and domain screen appears, as shown in the following figure.

2. In the **Embedded LAN (ELAN)** section, type the IP address, Gateway, and Netmask.

   In the **Fully qualified domain name (FQDN)** section, type the Host name and Domain.

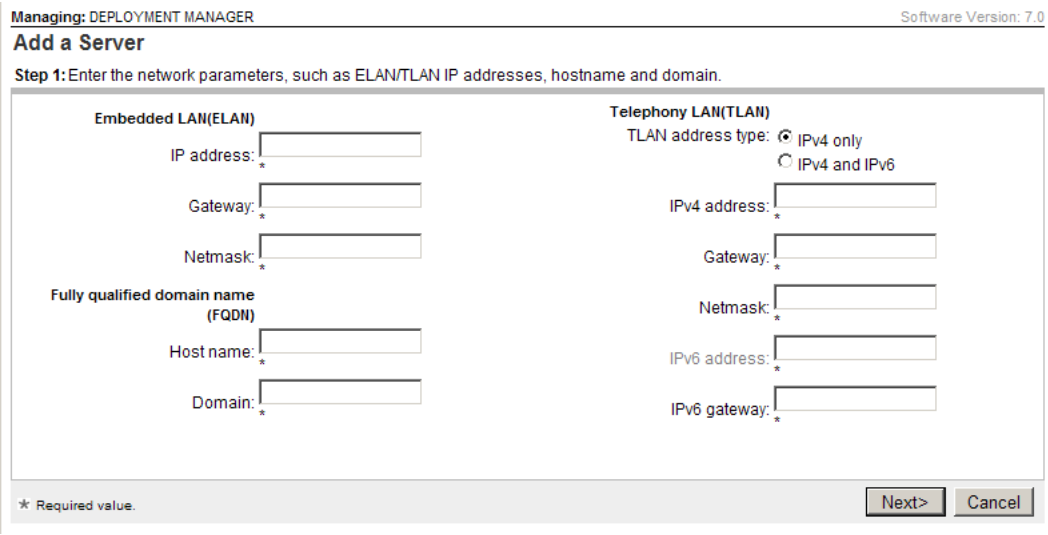


Figure 49: Add a server

3. In the **Telephony LAN (TLAN)** section, select the TLAN address type **IPv4 only**.

   OR

   IPv4 and IPv6.

   If you choose only IPv4, type the IPv4 IP address, Gateway, and Netmask.

   OR

   If IPv4 and IPv6 is chosen, you must also type the IPv6 address and IPv6 gateway, as shown in the previous figure.

4. Click **Next**.

   The Enter the DNS parameters, such as primary/secondary DNS servers IP addresses page appears.

5. In the **Primary** section, type the Primary DNS IP Address .

   In the **Secondary** section, type the Secondary DNS IP Address, and click **Next**.

   The Enter NTP related information and time zone page appears, as shown in the following figure.

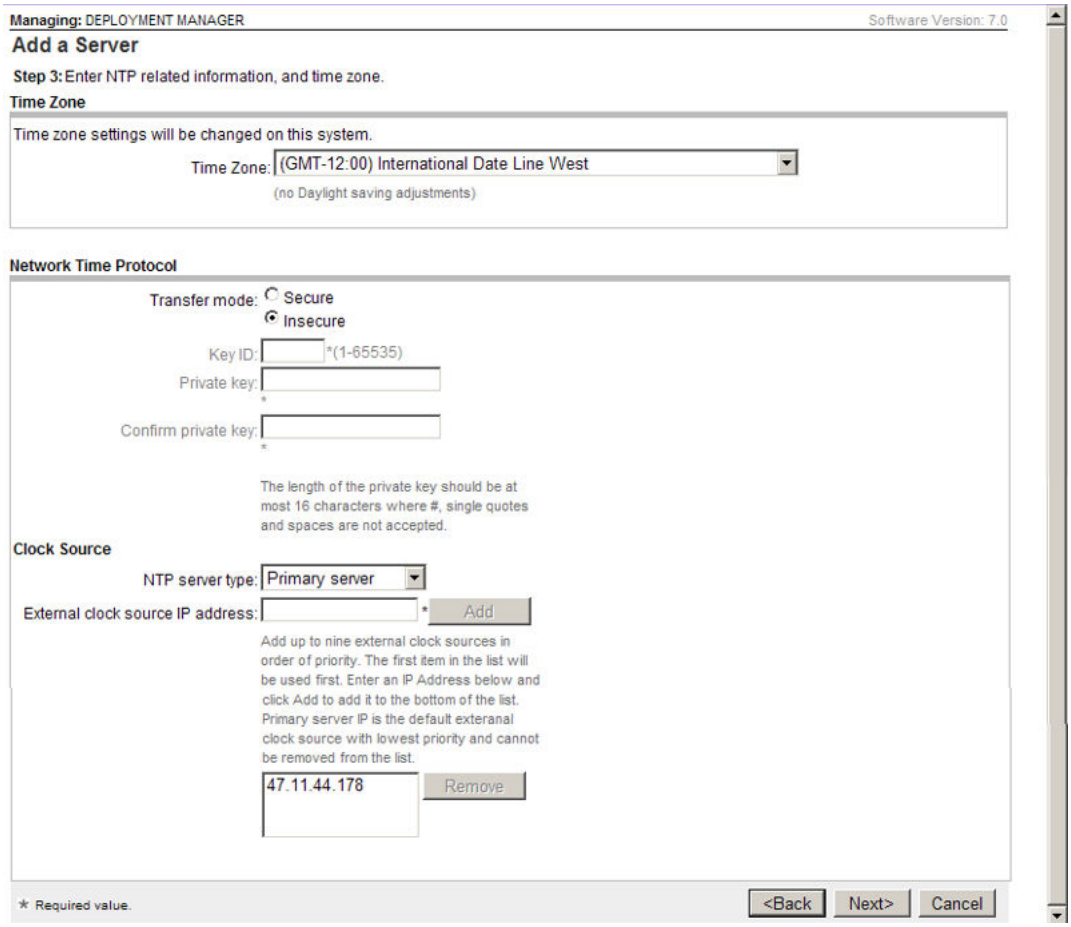


Figure 50: Enter NTP related information page

6. In the **Time Zone** section, choose the time zone setting for this server.
7. In the **Network Time Protocol** section, select the Transfer mode as **Secure** or **Insecure**.

   Important:

   If the Insecure option is selected, the Key ID and Private key fields are dimmed and cannot be changed.
8. If you select the Secure option:

   In the **Key ID** field, enter a value for key ID.

   In the **Private key** field, enter a value for private key.

   In the **Confirm private key** field, enter the private key value again.

   Important:

   The Private key must not exceed 16 characters. The pound (#) symbol, single quotation marks ('), and spaces are not accepted in the string.
9. In the **Clock Source** section, choose one of the following from the **NTP server type** list:

   - Primary server

- Secondary server
- Not a clock server

10. Enter the **External clock source IP Address** and click **Add**.
11. Click **Next**.
12. If you select **Primary server** from the NTP server type list, see Configuring the clock source for a Primary server on page 86.

    If you select **Secondary server** from the NTP server type list, see Configuring the clock source for a secondary server on page 87.

    If you select **Not a clock server** from the NTP server type list, see Configuring a server that is not a clock server on page 88.

    The Enter passwords, hardware type and other base related information page appears.
13. In the **Hardware type** list, choose one of the following:
    - CPDC
    - CPPM
    - Dell R300
    - HP DL320G4
    - HP DL360G7
    - IBM X306M
    - IBM X3350
14. In the **avaya password** field, type the Avaya password and then confirm the password in the **confirm avaya password** field.
15. In the **root password** field, type the root password and then confirm the root password in the **confirm root password** field.
16. Click **Next**.

    The Select server type for the Security Configuration page appears.
17. Click **Member server** or **Backup security server** as the Server Type.
18. Click **Next**.

    The Verify primary security server fingerprint page appears, as shown in the following figure.

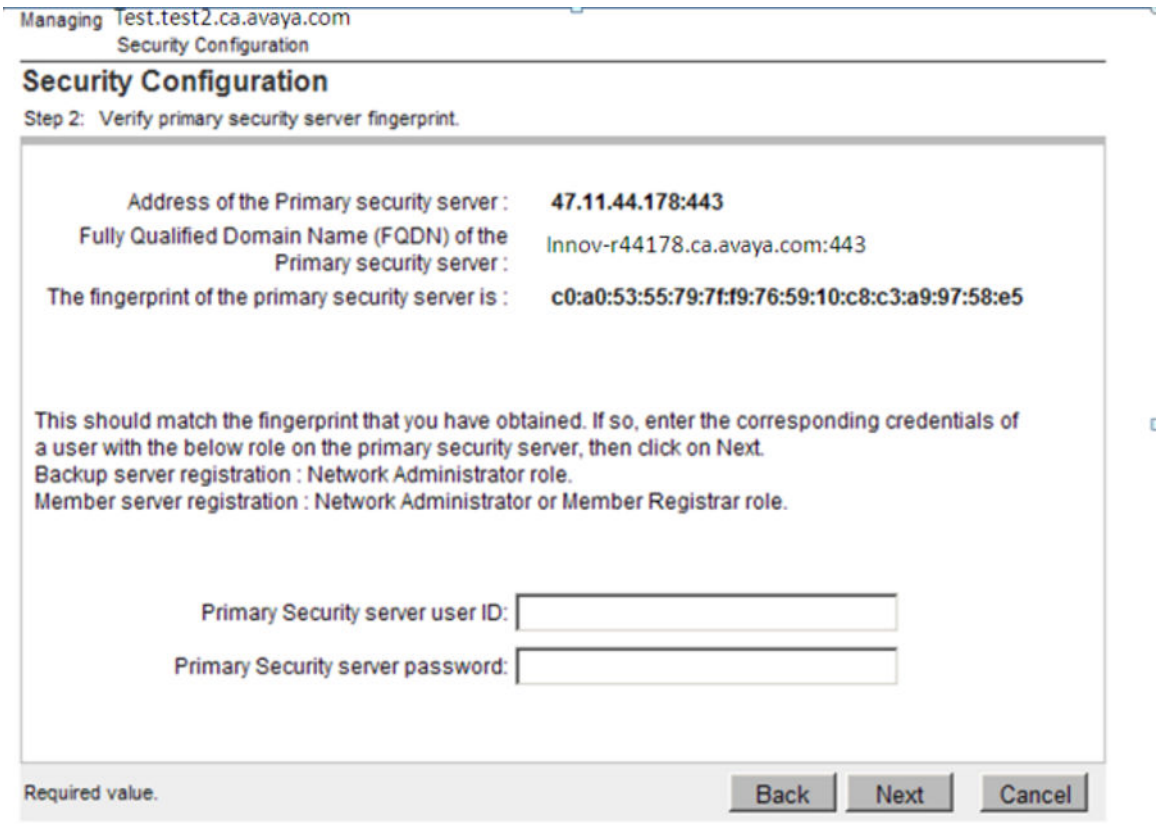


Figure 51: Verify primary security server fingerprint

19. Type the **Primary Security server user ID** and **Primary Security server password**.

    Important:

    The primary security server user ID and password is requested only for the first server configured. If you add additional servers, the values are filled in automatically.

20. Click **Next**.

    The Enter certificate information page appears.

21. Confirm the Certificate Information, and click **Finish**.

    A Linux Base element is created in UCM and the element name is visible from the default Deployment View and UCM Elements page.

    Important:

    The Linux Base version does not appear in the Base Version field and the Status field is identified as Preconfigured. The server is still a logical server at this point. After you physically install the server, the Base Version and Status fields show the new version number and Configured status.

22. Return to the Preconfiguring process using Deployment View on page 74.

Configuring the clock source for a Primary server

Configure the clock source for a Primary server.

Prerequisites:

You must log on using a role from the systemadmin or timeadmin access groups to perform date and time configuration.

Procedure steps:

1. Perform Steps 1 on page 82 to 9 on page 84 in Adding a Linux server on page 82.
2. In the **Clock Source** section, type an IP address for the external clock source in the **External clock source IP address** field, and click **Add**, as shown in the following figure.

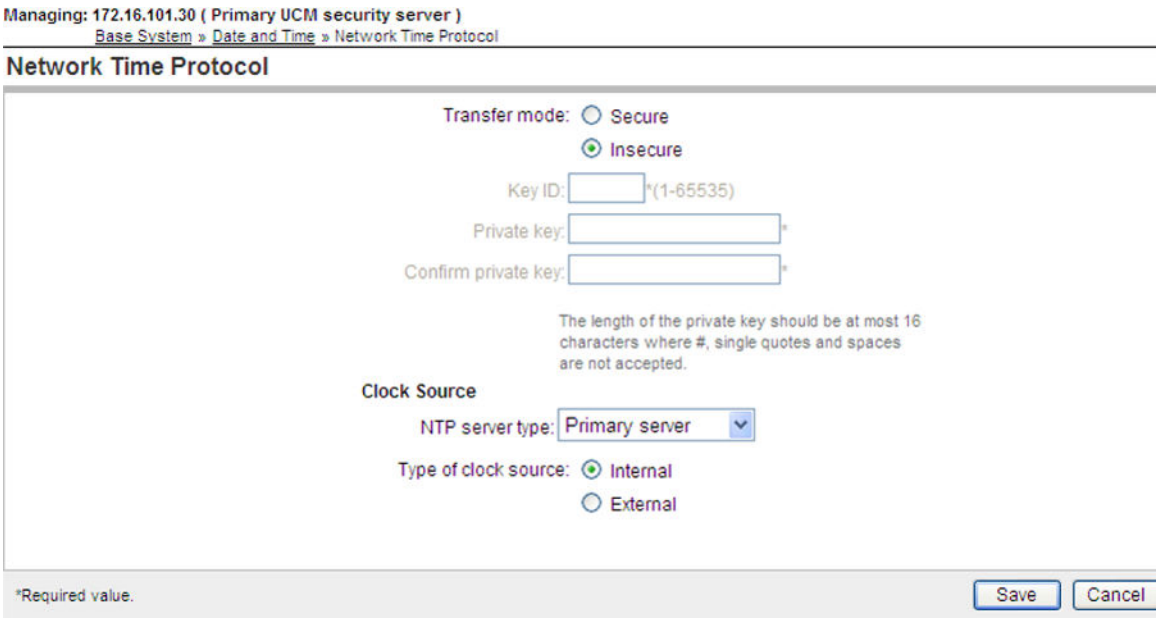


Figure 52: Clock source screen

3. Enter additional external clock sources as required, and click **Add**.

   Important:

   You can add up to 10 external clock sources in order of priority.

4. Click **Next.**
5. Proceed to 13 on page 85 in Adding a Linux server on page 82

Configuring the clock source for a secondary server

Configure the clock source for a secondary server.

1. Perform Steps 1 on page 82 to 9 on page 84 in Adding a Linux server on page 82.

   Upon choosing Secondary Server, the page refreshes to show Primary NTP server IP address.

2. In the **Primary NTP server IP address** field, type a value for the IP address of the Primary NTP server.
3. In the type of clock source field, select **Internal** and proceed to 13 on page 85 in Adding a Linux server on page 82 to continue the configuration.

OR

In the type of clock source list, select **External**.

The Add a Server page is refreshed.

4. Proceed to 13 on page 85 in Adding a Linux server on page 82.

Configuring a server that is not a clock server

Configure a server that is not a clock server.

1. Perform Steps 1 on page 82 to 9 on page 84 in Adding a Linux server on page 82.

   Upon choosing Not a clock server, the page refreshes to show Primary and Secondary NTP server IP address fields.

2. In the **Primary NTP server IP address** field, type a value for the IP address of the Primary NTP server.
3. In the **Secondary NTP server IP address** field, type a value for the IP address of the Secondary NTP server. Use of a Secondary NTP server is optional.
4. Click **Next**.
5. Proceed to Step 13 on page 85 in Adding a Linux server on page 82.

Deleting a Linux server

Delete a Linux server.

Prerequisites

- Ensure the Linux server is not a Primary Security Server.
- Ensure the Linux server is not a member of a group.
- Log on to UCM. See Logging on to Unified Communications Management on page 77.
- Access Deployment Manager. See Accessing Deployment Manager on page 77.

Procedure steps

Important:

You cannot delete the server if it is a Primary Security Server or a member of a group.

1. On the Deployment View page, choose **Servers** from the **View** list on the right of the page.
2. Click the option button beside the Host Name of the server to delete.
3. Click **Delete**.

   A confirmation dialog box appears.

4. Click **Yes** to delete the server.
5. Return to the Preconfiguring process using Deployment View on page 74.

Adding a VxWorks Call Server for a High Availability system

If your VxWorks Call Server is not registered, add a VxWorks Call Server to the Deployment Manager to create an active and inactive VxWorks Call Server for a High Availability system.

1. On the **Deployment View** page, select **VxWorks Call Server** from the list, and click **Add**.

   The Enter Call Server details page appears.

2. Select the **High Availability System** check box.
3. In the **Active call server ELAN IP** field, enter the ELAN IP address for the Active Call Server.
4. In the **Inactive call server ELAN IP** field, enter the ELAN IP address for the Inactive Call Server.
5. Click Finish.

   The Deployment View page appears with the active and inactive VxWorks Call Servers added.

6. Return to the Preconfiguring process using Deployment View on page 74.

Important:

You must register the Call Server after it is up and running.

Adding a VxWorks Call Server

Add an active VxWorks Call Server to the Deployment Manager.

1. On the **Deployment View** page, select **VxWorks Call Serve**r from the list, and click **Add.**

   The Enter Call Server details page appears.

2. In the **Active call server ELAN IP** field, enter the ELAN IP address for the Active Call Server.
3. Click **Finish.**

   The Deployment View page appears with the active VxWorks Call Servers added.

4. Return to the Preconfiguring process using Deployment View on page 74.

Deleting a VxWorks Call Server

Delete a VxWorks server.

Prerequisites

- Ensure the VxWorks server is not a member of a group.
- Ensure the server in not an inactive Call Server of a High Availability (HA) system.
- Log on to UCM. See Logging on to Unified Communications Management on page 77.
- Access Deployment Manager. See Accessing Deployment Manager on page 77.

Procedure steps

1. On the **Deployment View** page, select **Servers** from the **View** list on the right of the page.

2. Click the option button beside the active server to delete.

   Important:

   Deleting the active Call Server for a High Availability system also deletes the inactive Call Server.

3. Click **Delete**.

   A confirmation dialog box appears.

4. Click **Yes** to delete the server.

Network Services

This section contains procedures to view, add, or delete NRS, Avaya Aura® MS, and Subscriber Manager.

Adding a Avaya Aura® MS service

Add Avaya Aura® Media Server as a network service. For more information about Avaya Aura® MS, see the following documents.

- *Installing, Upgrading, and Patching Avaya Aura® Media Server*.
- *Implementing and Administering Avaya Aura® Media Server*
- *Event, Alarms, and Performance Measurement for Avaya Aura® Media Server*

Note:

The document *Implementing and Administering Avaya Aura® Media Server* includes information on Avaya Aura® MS capabilities which are NOT supported with the CS 1000. Sections on WebLM Licensing, High Availability, Video Codecs and Diameter Configuration within this document are not applicable to CS 1000 deployments and should not be used for Avaya Aura® MS configuration.

Prerequisites:

- You must first upload the latest Avaya Aura® MS software load. See Software loads on page 78.
- Ensure your hardware is a COTS2, Common Server, Common Server R2, Common Server R3, or CP DC.

Procedure steps:

1. On the **Deployment View** page, choose **Network Services** from the **View** list.
2. Choose **MAS** from the list, and click **Add**.

   The Enter a name and a description for the service page appears.

3. In the **Name** field, enter a service name.
4. In the **Description** field, enter a description.
5. Click **Next**.

   The Choose the Server for the selected Network Service page appears.

6. In the **Server** field, choose a Server from the list, and click **Next**.

   The Pre-configuration for MAS server page appears.

7. Click **Browse** to choose a keycode file, and click **Validate**.

   OR

   Use Avaya Aura® MS Element Manager to choose a keycode file at a later time.

8. Click **Finish**.

   The Deployment view page appears with a tree view of the MAS server association. The MAS server is now a member of the primary security server.

9. To continue the preconfiguration process, proceed to 7 on page 75 in Preconfiguring process using Deployment View on page 74.

Adding a Network Routing Service

Add a Network Routing Service (NRS) from the Deployment View page.

Prerequisites:

- You must first upload the CS 1000 application software load.

Procedure steps:

1. On the **Deployment View** page, and choose **Network Services** from the **View** list.
2. Choose **NRS** from the list, and click **Add**, as shown in Figure 53: NRS on page 92.

   The Enter a name and a description for the service page appears.

3. In the **Name** field, enter a service name.
4. In the **Description** field, enter a description.
5. Click **Next**.

   The Choose the primary and secondary NRS servers page appears.

6. In the **Primary NRS Server** field, choose a server from the list.
7. In the **Secondary NRS Server** field, choose a server from the list.
8. Click **Finish**.

   The Deployment view page appears with a tree view of the NRS server association. The primary and secondary NRS servers are now members of the NRS group, as shown in the following figure.

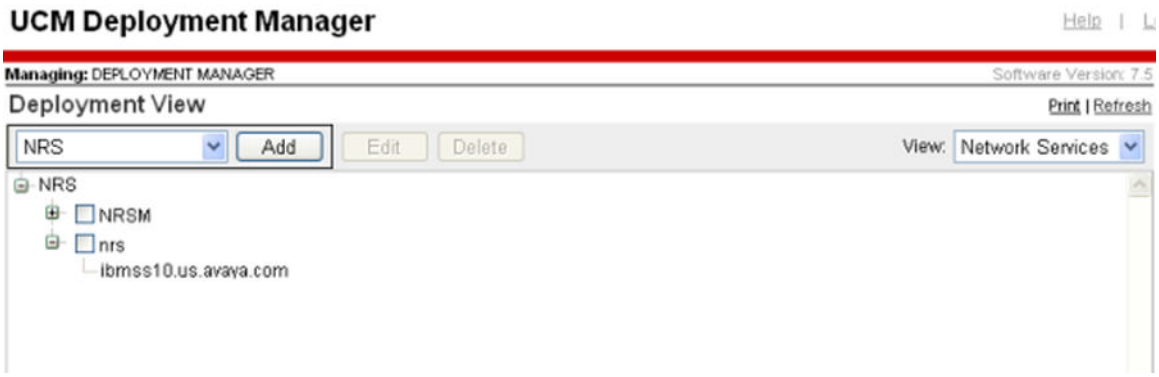


Figure 53: NRS

9. To continue the preconfiguration process, proceed to step 7 in *Preconfiguring Process using Deployment View*in *Linux Platform Base and Applications Installation and Commissioning Avaya Communication Server 1000*.

Adding a Subscriber Manager service

Add a Subscriber Manager service from the Deployment View.

Prerequisites:

- You must first upload the CS 1000 application software load. See Software loads on page 78.

Procedure steps:

1. On the **Deployment View** page, and choose **Network Services** from the **View** list.
2. Choose **Subscriber Manager** from the list, and click **Add**.

   The Enter a name and a description for the service page appears.
3. In the **Name** field, enter a service name.
4. In the **Description** field, enter a description.
5. Click **Next**.

   The Choose the primary server page appears.
6. In the **Name** field, leave the previously entered name or type a new name.
7. In the **Server** field, choose the Primary Security server from the list.
8. Click **Finish**.

   The Subscriber service is available only on the primary security server. The Subscriber group is created with the specified name and the selected server is a member of the group.

   Important:

   The Finish button is dimmed until you select a Primary Server. Allow several seconds for the button to be available to click.
9. To continue the preconfiguration process, proceed to 7 on page 75 in Preconfiguring process using Deployment View on page 74.

Deleting a Network Service

You can delete any Network Service.

Note:

When you add CS 1000 or Network Services groups in Deployment Manager, the tree view of UCM updates. However, if you delete all groups from the UCM tree view it has the following impacts on Deployment Manager:

- If you delete all groups from the UCM Tree view, all groups are removed in Deployment Manager but you cannot undeploy applications.
- If you delete all groups from the UCM Tree view, System Upgrade is available in the Deployment Actions list in Deployment Manager. You can upgrade the system to a new load/release; however, the Avaya applications do not deploy.

1. On the **Deployment View** page, choose **Network Services** from the **View** list.

   The Deployment View page refreshes to show the tree.

2. Expand the tree view by clicking the plus (+) sign.
3. Select the check box beside the server name to delete.

   The Delete button becomes available for you to click. You can select more than one service to delete.

4. Click **Delete**.

   A confirmation dialog box appears.

5. Click **Yes** to delete.
6. To continue the preconfiguration process, proceed to 7 on page 75 in Preconfiguring process using Deployment View on page 74.

CS 1000 systems

The following section contains procedures for viewing, adding, or deleting CS 1000 or CS 1000 High Scalability systems.

Adding a CS 1000 system

Add a CS 1000 system.

Prerequisites:

- Ensure you add all the VxWorks servers required for your CS 1000 system.
- Ensure you add all the Linux servers required for your CS 1000 system.
- Allocate one or two Linux servers to use for Element Manager.

Important:

After the CS 1000 server is created, the allocated Linux servers that run Element Manager cannot be changed. To change an Element Manager role running on a Linux Signaling Server, you must delete the CS 1000 system and recreate it.

Procedure steps:

1. On the Deployment View page, select **CS 1000 systems** from the **View** list, as shown in the following figure.

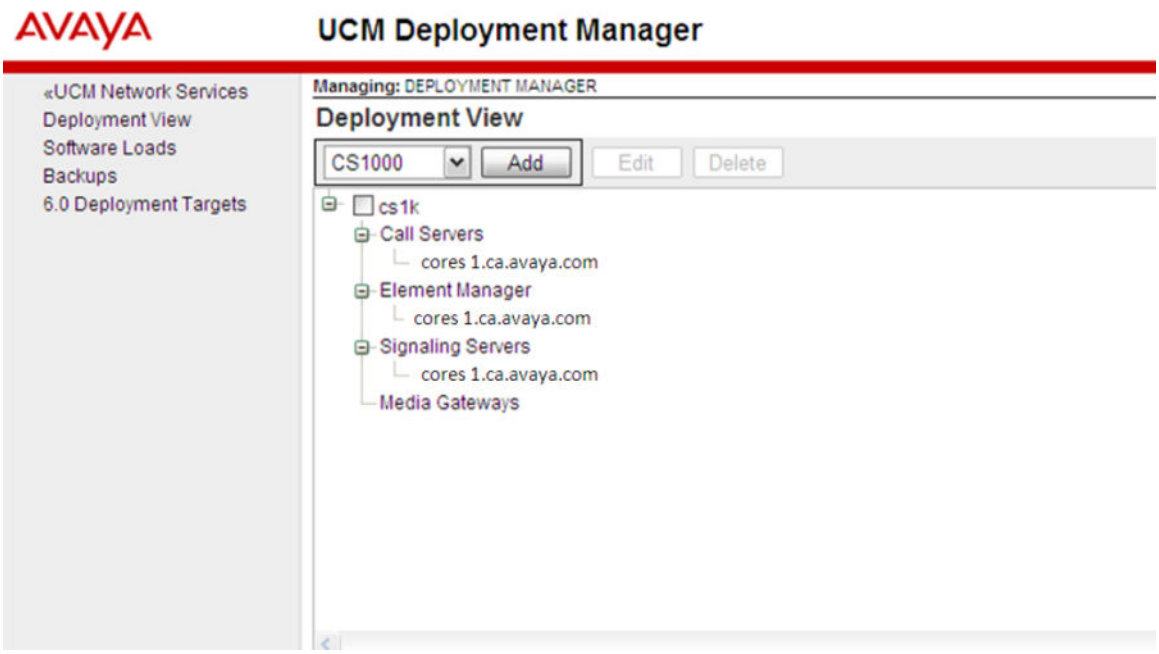


Figure 54: CS 1000 Deployment View screen

2. Select **CS 1000** from the list, and click **Add**.

   The Enter the Call Server Information page appears, as shown in Figure 55: Add a CS 1000 system on page 95.

3. In the **CS 1000 name and description** section, enter the following:

   - **CS 1000 Name:** enter the name for the entire system you are configuring. This name appears on the top level of the hierarchical tree view.
   - **Description:** enter a description.

4. In the **Call Server and Tape ID details** section, enter the following

   - **Call Server:** choose a server name from the list.
   - **Call server tape ID:** enter the tape ID value.

   Important:

   If the selected server is a server that has not joined the security domain at this time, for example, a VXworks server or a Linux server that was just added, you must manually

enter the tape ID. Deployment Manager automatically determines the tape ID of the Call Server application that is deployed on a Linux server when it is chosen as a Call Server.

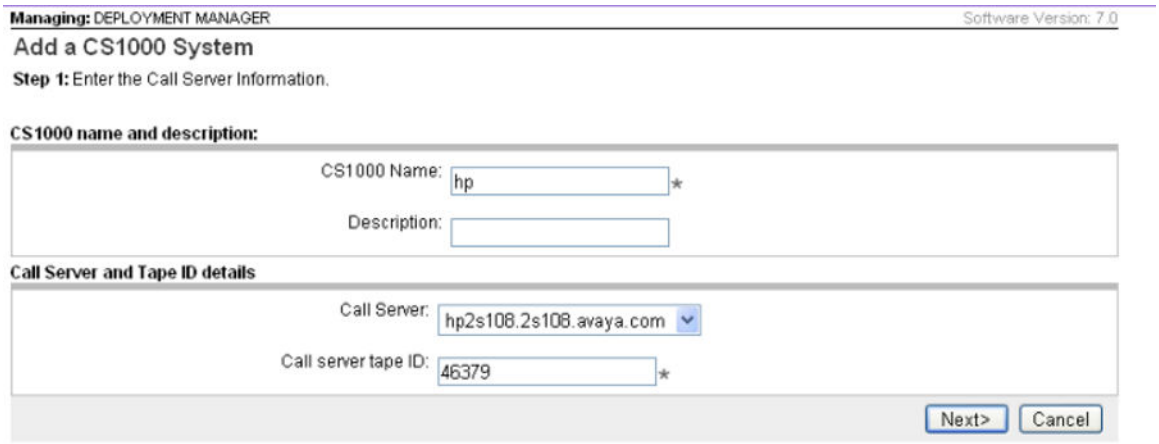


Figure 55: Add a CS 1000 system

5. Click **Next**.

   The Pre-configuration for the Linux call server. Keycode uploading and validation. Language and database selection page appears.

6. In the **Select keycode location** field, select **Client Machine** from the list.

7. In the **Keycode file** field, click **Browse** to obtain the keycode file to upload, and click **Validate** to validate and upload the file.

   Note:

   A 7.5 keycode must be uploaded for 7.0 and 7.5 targets. This keycode is meant for NFS installation.

   The keycode is not validated on the target system; however, minimal prevalidation occurs from the deployment server.

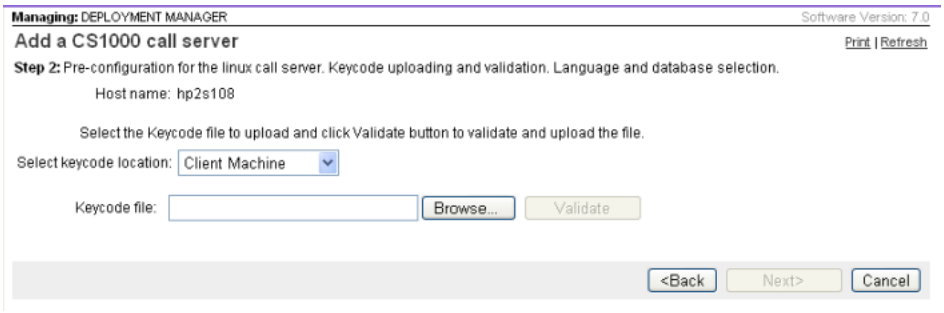


Figure 56: Keycode file screen

8. Click **Next**.

   The page refreshes to show the validation completed and keycode accepted. The language and Database fields appear.

9. In the **Language** field, select a language from the list.
10. In the **Database** field, select one of the following from the list.
    - **Default Database:** This is the prepackaged database that is delivered with the software.
    - **Existing Database**
    - **Customer Database on Client Machine:** The database can be uploaded from any device connected to the client machine.
11. Click **Next**.

    The page refreshes to show the Media field.
12. In the **Media** field, select a medium from the list and click **Browse**.

    The page refreshes to show the Path field.
13. In the **Path** field, select **backup** from the list and click **Upload**.

    The page refreshes to confirm the uploaded database is valid.
14. Click **Next**.
15. In the **CS 1000 Element Manager** field, choose the server to use for Element Manager.
16. In the **Alternate CS 1000 Element Manager** field, choose a server if you want to configure an alternate Element Manager server.

    Note:

    If you choose an Alternate Element Manager server, Deployment Manager installs Element Manager to this server. However, no date synchronization occurs between the two servers.

    On the Deployment View page, the Predeployed Applications field is updated to show Element Manager.
17. In the **Description** field, type a description.
18. In the **Add Signaling Servers** section, choose your Signaling Servers from the list the Linux servers, and click **Add**.

    Important:

    If you add a follower Signaling Server, the ELAN/TLAN subnet must match the leader Signaling Server ELAN/TLAN subnet. If the ELAN/TLAN subnets do not match and the leader Signaling Server is offline, IP Phones cannot reach the IP node of the follower Signaling Server and service is lost.

    On the **Deployment View** page, the Predeployed Applications field is updated to show SS.
19. Click **Finish**.
20. To continue the preconfiguration process, refer step 7 from *Preconfiguring process using Deployment View* in *Linux Platform Base and Applications Installation and Commissioning Avaya Communication Server 1000, NN43001–315*.

Note:

Only the servers that can host a particular application, appear in the list.

Important:

After the CS 1000 group is created, the Signaling Server tree displays all the available Signaling Servers that are added as part of the CS 1000 group. After you add or modify IP Telephony Nodes in Element Manager, a subgroup called Node Group is created or updated with all the node member information. This Node Group appears in Deployment Manager as Node XXXX, where XXXX represents the Node ID of the IP Telephony Node, as shown in Figure 54: CS 1000 Deployment View screen on page 94. After the Signaling Server is part of a Node Group, it is removed from the Signaling Server group to ensure that the same server does not appear in both places. Any servers that belong to the Signaling Server group can be added to any Nodes within that CS 1000 group. When the IP Telephony Node is deleted from Element Manager, all the servers that were part of the Node group go back to the Signaling Server group. These servers are now available to be added to other IP Telephony Nodes.

Defining a new CS 1000 High Scalability system

Add a CS 1000 High Scalability (HS) system. A High Availability (HA) group consists of VxWorks Call Server and a number of Signaling Servers. An HS system consists of multiple HA groups. Each HA group consists of a pair of VxWorks Call Servers and a group of Signaling Servers.

Prerequisites:

- Determine the Linux and VxWorks Call Servers that are to be used for each HA group.
- Identify the Linux servers to use as Signaling Servers and the associated HA group.
- Determine one or two Linux servers to be used for Element Manager HS.

Note:

Element Manager HS is a stand-alone application and must be on a dedicated Linux server. You can allocate a second stand-alone server for redundancy support.

Important:

After the CS 1000 server is created, the allocated Linux server that run Element Manager cannot be changed. To change an Element Manager role running on a Linux Signaling Server, you must delete the CS 1000 system and recreate it.

Procedure steps:

1. On the **Deployment View** page, select **CS 1000 systems** from the list on the right of the page.
2. Select **CS 1000 HS**, and click **Add**.

   The Enter the High Scalability System Information page appears.
3. In the **Name** field, enter the name of the High Scalability server.
4. In the **Description** field, enter a description.
5. Click **Next**.

The Enter the High Scalability System Management Information page appears.

6. In the **CS 1000 Element Manager** field, choose the server to use for Element Manager from the list.
7. In the **Alternate CS 1000 Element Manager** field, choose a server if you want to configure an alternate Element Manager server from the list.
8. In the **Description** field, enter a description.
9. Click **Next**.

   The Add CS 1000 high availability systems page appears.
10. Click **Add** to add a new HA system.

    The Add CS 1000 high availability systems page appears.
11. In the **Call Server** field, choose a server from the list.

    Important:

    You see only the available VxWorks Call Servers. The VxWorks Call Servers that are already defined for other CS 1000 or CS 1000 HS systems do not appear.

    In the **Inactive call server ELAN IP** field, the Inactive Call Server IP address appears.
12. In the **Name** field, type a name for the HA system.
13. In the **Description** field, type a description.
14. In the Choose signaling servers section, choose your Signaling Servers from the list the Linux servers, and click **Add**.
15. Click **Save**.

    On the Deployment View page, the Predeployed Applications field is updated to show SS.
16. Repeat 10 on page 98 to 15 on page 98 in this procedure to add additional HA groups.
17. Click **Finish**.
18. To continue the preconfiguration process, proceed to 7 on page 75 in Preconfiguring process using Deployment View on page 74.

Editing a CS 1000 system

Add or change the Alternate CS 1000 Element Manager and add or delete Signaling Servers.

1. On the **Deployment View** page, select **CS 1000 systems** from the **View** list on the right of the page.
2. Select the check box of the CS 1000 system, and click **Edit**.

   The Call Server information page appears, as shown in the following figure.

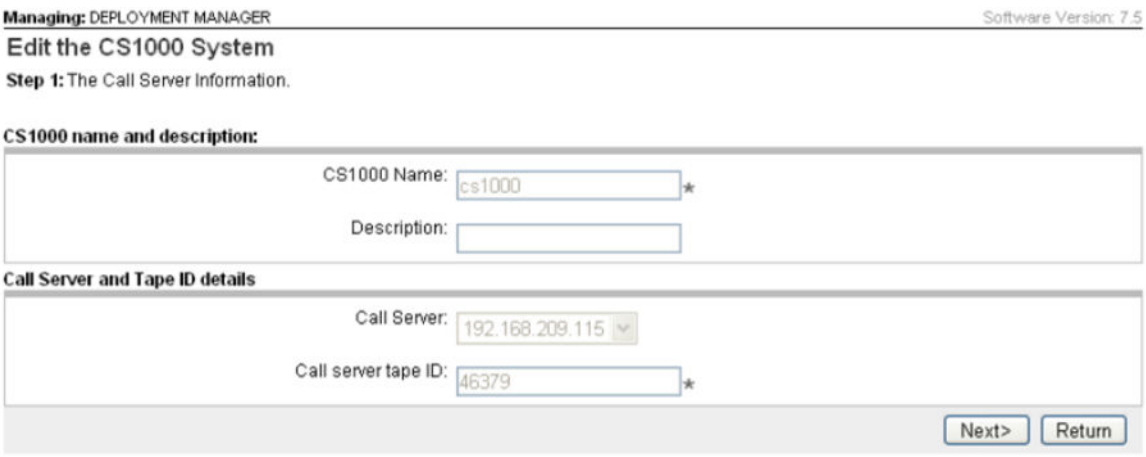


Figure 57: Edit the CS 1000 system

3. Click **Next**.

   The Pre-configuration for the Linux call server. Keycode uploading and validation. Language and database selection screen appears.

4. To upload a different keycode, select **Click here**, as shown in the following figure.

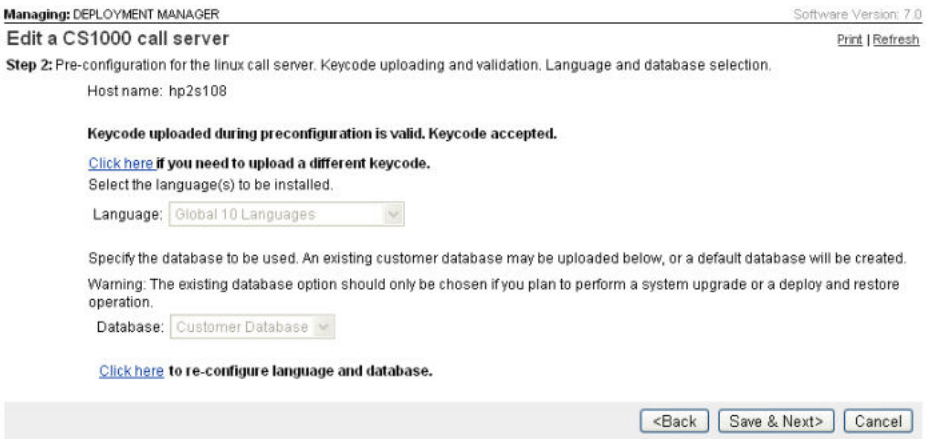


Figure 58: Edit a CS 1000 Call Server screen

5. To change the **Language**, select **Click here**, as shown in the preceding figure.

   The list is no longer dimmed.

6. To change the **Database,** select **Click here**, as shown in the preceding figure. You can choose from **Default Database**, **Existing Database**, **Customer Database on Client Machine**, and **Customer Database on Deployment Server USB**.

   Important:

   The Customer Database list does not show whether it is Customer Database on Deployment Server USB or Customer Database on Client Machine. If you have previously configured one of these and do not want to change this configuration, just click Save & Next to leave your configuration unchanged. However, if you had previously

configured Customer Database on Client Machine and select "Click here", the default selection appears as Customer Database on Deployment Server USB because if you select Customer Database on Client Machine, a tool is started for uploading a new database from the PC. Therefore, if you have already configured Customer Database on Client Machine and do not want to change, just click Save & Next to avoid starting this tool.

7. Click **Save & Next**. Proceed to 8 on page 100 through 10 on page 100 if you chose the Database option as Customer Database on Deployment Server USB; otherwise, skip to 11 on page 100.

   The page refreshes to show the Media field.

8. To change the **Media**, click **Browse**.
9. Click **Browse** to get a list of databases available on the USB device.

   The pages refreshes to show the Path field.

10. To change the **Path**, choose from the list and click **Upload**, as shown in the following figure.

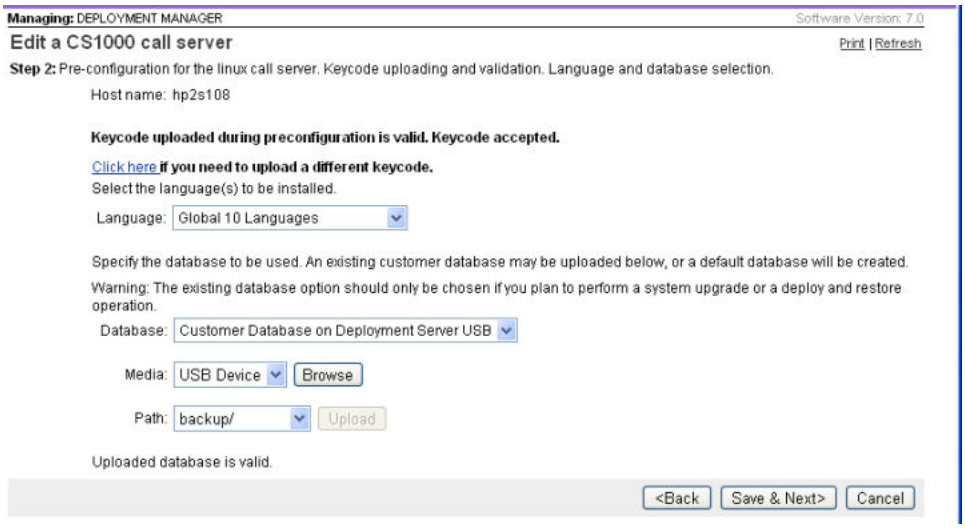


Figure 59: Edit a CS 1000 call server

11. Click **Save & Next**.

    The Select the Alternate CS 1000 Element Manager screen appears. From this screen, you can only select the Alternate CS 1000 Element Manager field if it is not configured and add or remove Signaling Servers.

12. Select an **Alternate CS 1000 Element Manager** from the list to add an Alternate Element Manager or change your selection.
13. In the **Add signaling servers** section, you can **Add** or **Delete** Signaling Servers.

Important:

If you add a follower Signaling Server, the netmask must match the leader Signaling Server netmask. If the netmasks do not match and the leader Signaling Server is offline, IP Phones cannot reach the IP node of the follower Signaling Server and service is lost.

14. Click **Finish**.

Editing a CS 1000 HS system

Edit the CS 1000 HS system and the Alternate CS 1000 HS and add or delete Signaling Servers.

1. On the **Deployment View** page, select **CS 1000 systems** from the **View** list on the right of the page.
2. Select the check box of the CS 1000 HS system, and click **Edit**.

   The Call Server information page appears.
3. Click **Next**.

   The Select the Alternate High Scalability Manager page appears.
4. Select an Alternate CS 1000 Element Manager HS from the list to add an Alternate Element Manager or change your selection.
5. Click **Next**.

   The Add edit, or delete CS 1000 high availability systems page appears.
6. Select a High Availability system and click **Add** , **Edit** , or **Delete**.

   If you select Add or Edit, the Add or Edit existing CS 1000 high availability systems page appears, as shown in the following figure.

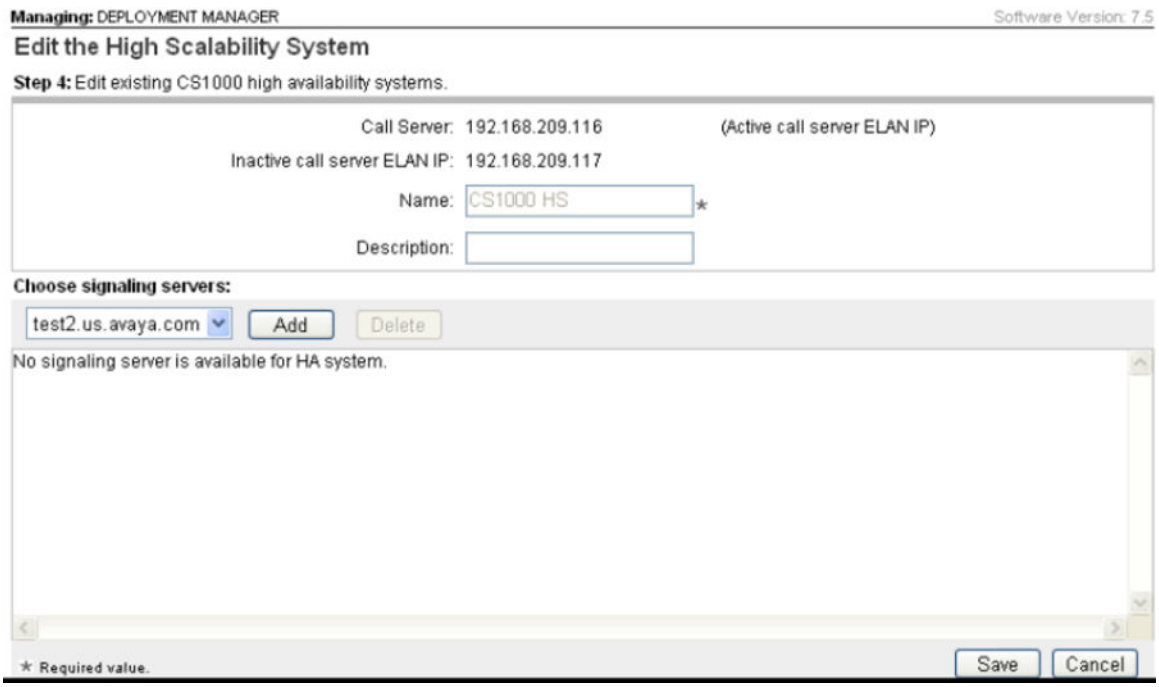


Figure 60: Add or Edit an existing CS 1000 high availability system screen

7. In the **Add signaling servers** section, you can **Add** or **Delete** Signaling Servers.

   Important:

   If you add a follower Signaling Server, the netmask must match the leader Signaling Server netmask. If the netmasks do not match and the leader Signaling Server is offline, IP Phones cannot reach the IP node of the follower Signaling Server and service is lost.

8. Click **Save**.

Deleting a CS 1000 system

Important:

A CS 1000 system that has servers defined under Node xxxx, as described in the Attention box at the end of Adding a CS 1000 system on page 93 cannot be deleted directly from Deployment Manager in the CS 1000 view.

Use the following procedure to delete a CS 1000 system.

Procedure steps:

1. From Element Manager, click **IP Network**, **Nodes: Servers, Media Cards**.
2. Select the check box beside the node to export.
3. Click **Export** and specify the location to export the file.
4. Click **Delete**.

Note:

Avaya recommends deleting the IP Telephony Node during a maintenance window.

5. On the Deployment View page, select **CS 1000 systems** from the **View** list on the right of the page.
6. Select the check box of any CS 1000 system, and click **Delete**.

   The Confirmation window appears.
7. Click **Yes** to delete the selected groups or **No** to cancel.

Note:

The IP Telephony Node is now available to be imported to another CS 1000 system.

Deleting a CS 1000 HS system

The following procedure deletes a CS 1000 HS system. To delete a single HA group, see Deleting a CS 1000 system on page 102

1. From Element Manager, click **IP Network**, **Nodes: Servers, Media Cards**.
2. Select the check box beside the node to export.
3. Click **Export**.
4. Click **Delete**.

Note:

Avaya recommends deleting the IP Telephony Node during a maintenance window.

5. On the Deployment View page, select **CS 1000 systems** from the **View** list on the right of the page.
6. Select the check box of any CS 1000 HS system, and click **Delete**.

   The Confirmation window appears.
7. Click **Yes** to delete the selected groups or **No** to cancel.

Note:

The IP Telephony Node is now available to be imported to another CS 1000 system.

Deployment Actions

This section describes the options available under the Deployment Actions list. This list is context-sensitive so only the actions that are available to select appear in the list.

Note:

If you are using Deployment Manager on your Deployment Server as your unified solution for end-to-end installation and configuration of Linux Base and applications, you must use the process as described in Preconfiguring process using Deployment View on page 74.

The following is a list of the possible actions:

- Deploy: See Deploying applications on a Server on page 104
- Undeploy: See Removing applications on a server on page 106
- Backup: See Performing a backup on page 106
- Restore: See Restoring data on page 106
- System Upgrade: See System upgrade on page 49

Deploying applications on a Server

Choose Deploy when you have completed the predeployment process and the Server is installed with the latest software release of Linux Base. If you are upgrading applications and a backup exists, you can use this procedure to restore your configuration and data.

Prerequisites

The Deployment View status must show the following:

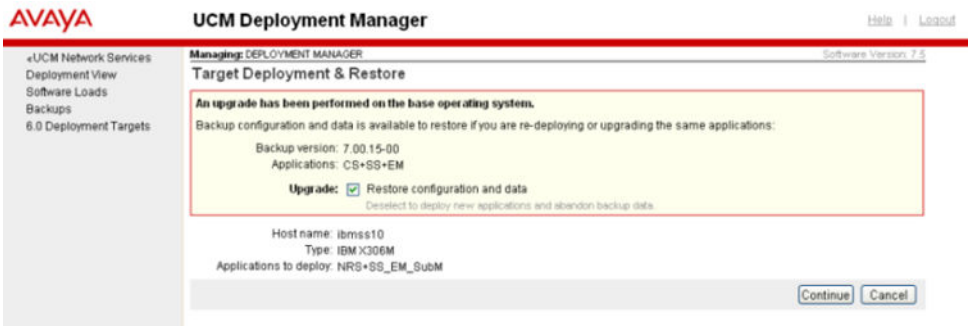
- The **Status** field is in a Committed status. If not, return to Step 8 on page 75 in Preconfiguring process using Deployment View on page 74.
- The **Server Status** field is in the Undeployed status. If the status is in a Deployed state and you want to redeploy, see Removing applications on a server on page 106 to undeploy.
- The Software Load version and Release number must be equal to or greater than the Base version.

Procedure steps

1. On the **Deployment View** page, choose **Servers** from the **View** list.
2. Select the server(s) you want to deploy.
3. From the **Deployment Actions** list, choose **Deploy**.
4. Click **OK** to confirm deployment.

   Note:

   If a backup archive already exists, you are presented with the **Target Deployment & Restore** screen, as shown in the following figure. You have the option to restore your configuration and data. If no previous backup archive exists, the Call Server Preconfiguration details page appears, go to Step 7 on page 105.
5. Select the **Upgrade** check box if you want to restore your configuration and data, as shown in the following figure.



6. Click **Continue** and proceed to Step 10 on page 105.
7. If no previous backup archive exists, the Call Server Preconfiguration details page appears, as shown in the following figure.

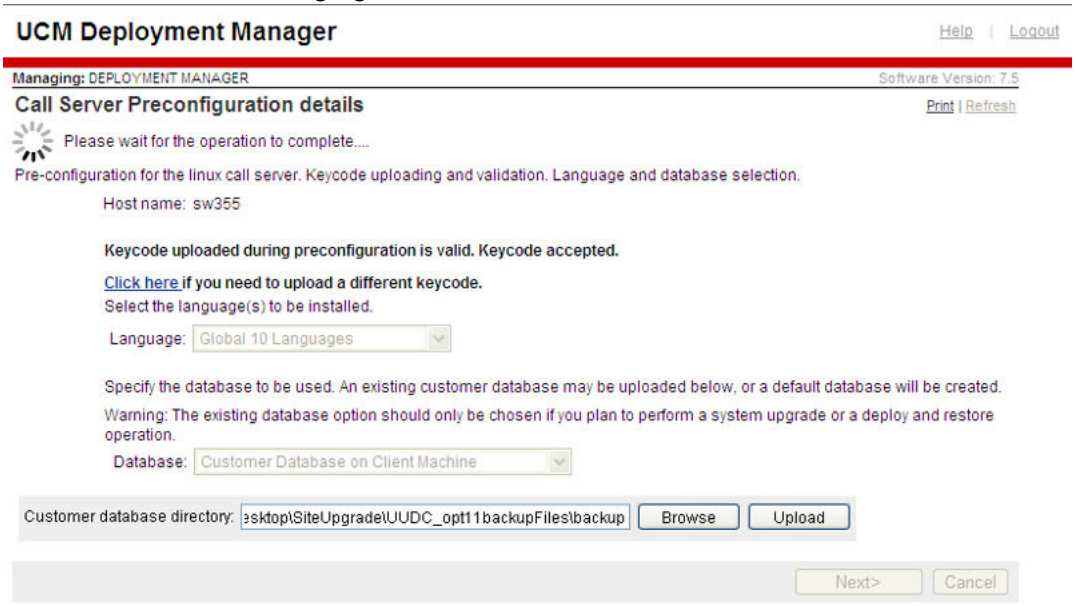


Figure 61: Example of an archive backup

8. Select **Click here** to reconfigure the language and database location, and click **Next**.

   Important:

   The Database field must be defined; otherwise, it uses the Default Database. The Default Database is the prepackaged database that is delivered with the software.

9. In the **Customer database directory** field, click **Browse** to search for the database location, and click **Upload**, as shown in the previous figure.

   Tip:

   The backup folder structure must not be changed; otherwise, it is not recognized by Deployment Manager.

   For example:

   - For backup, the folder structure is: /ARCH_DB/ cust_named_folder/*.rec.
   - For a large system backup, the folder structure is: /backup/single/*.rec.
   - For archive backup, you must navigate to the "cust_named_folder" for upload to Deployment Manager.

10. Click **Return** to return to the Deployment View page. The Deployment View page refreshes to show the applications deployed.

Note:

If you are prompted for keycode validation, you must provide a 7.0 keycode for Release 7.0 and a 7.5 keycode for 7.5 targets.

Removing applications on a server

Remove applications from a previously deployed server (undeploying a server).

Prerequisites

- The server must be removed from all existing groups.
- The Undeploy option is available under the following conditions:
  - The Status field is in a Configured state.
  - The Predeployed Applications field must state N/A.
  - The Base Version field must not be empty.

Procedure steps

1. On the **Deployment View** page, choose **Servers** from the **View** list.
2. Click the option button beside the Host Name of the server from which to remove the applications.
3. From the **Deployment Actions** list, choose **Undeploy**.

Performing a backup

Ensure the latest service pack is applied before performing a backup.

Feature interactions

- Only one backup for each Member server is permitted on the Deployment Server (Primary security server). You must delete the current backup archive before you can perform another backup or choose another backup location.
- There are a maximum of 10 backup archive files allowed on the Deployment Server. You must remove or overwrite an existing backup archive before you can perform another backup.

Note:

For procedures on deleting an existing backup archive, see Backups on page 108

Procedure steps

1. On the Deployment View page, choose **Servers** from the list on the right of the page.
2. Select a server from the list.
3. From the Deployment Actions list, choose **Backup**.
4. In the Select backup location field, choose from the list.
5. Click **Start Backup**.
6. If a backup archive already exists for a target, you are prompted to overwrite the existing backup. Click **OK** to overwrite and **Cancel** to abort the backup operation.

Restoring data

Restore system data.

Prerequisites

The Base version field must not be empty.

Procedure steps

1. On the **Deployment View** page, select **Servers** from the **View** list on the right of the page.
2. Select a server from the list.
3. From the **Deployment Actions** list, choose **Restore**.

   The restore page appears, as shown in the following figure.

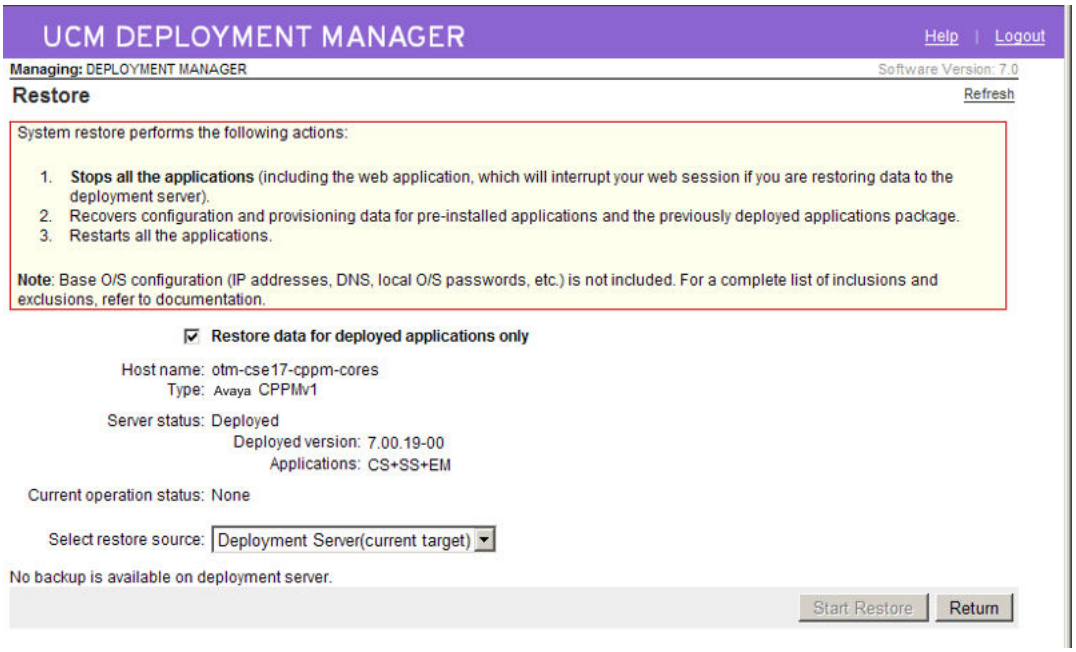


Figure 62: Restore page

4. Select the check box if you want to **Restore data for deployed applications only**.

   OR

   Clear the check box if you want to restore pre-installed applications and deployed applications.

   Note:

   Clear the check box if you want to restore subscriber accounts.

   All elements are stored in the base application and not the deployed application. Hence, elements are not restored when you select the **Restore data for deployed applications only** option.
5. In the **Select restore source**, choose from the list.
6. Click **Start Restore**.

System upgrade

A system upgrade includes a reinstallation of Linux Base and applications with your system data restored. For more information, see Upgrading a backup or member server from Release 6.0 or later on page 125.

Backups

This section describes how to delete existing backup files. You can have a maximum of three backup files for each server and can manage your backups from this link. From UCM, click Software Deployment, Backups.

Deleting an existing backup file

Delete existing backup files on the target server to create space for new backup files.

1. From the Navigation tree, click **Backups**.

   The Backups screen appears.

2. Select the backup file to delete.
3. Click **Delete**.

   The backup file is deleted from the hard drive.

6.0 Deployment Targets

This section is for Release 6.0 systems only. It describes how to manage and deploy application software and backup and restore system data for Release 6.0. For Release 7.0 and later, see Deployment Manager—New system installation and commissioning on page 68.

Important:

Do not use this section for deploying application software for Release 7.0 or later.

Prerequisites

- Must have the Release 6.00.18 software load for your Release 6.0 target servers.

Deploy

For Release 6.0, use Deployment Manager for software application deployment from the primary security server to other Linux servers in the same security domain. The primary security server is the central repository for the software application load and deployment occurs remotely, which eliminates the need to log on to each target server.

Deploying application software to a Call Server

This section, for Release 6.0, describes the procedures for deploying software on an existing configuration or a new configuration for predeployment. You can also use this section to backup and restore.

Prerequisites:

- The target server must be in the Undeployed status.
- Deployment Manager must have a software load that matches the Base version.

Procedure steps:

1. On the **Deployment Manager** page, click **6.0 Deployment Targets**.
2. Click the option button beside the Host Name of the server to deploy.

   Important:

   The Deploy button is not available to select until the target server has a status of Undeployed.

3. Click **Deploy**.

   The Target Deployment page appears, as shown in the following figure.

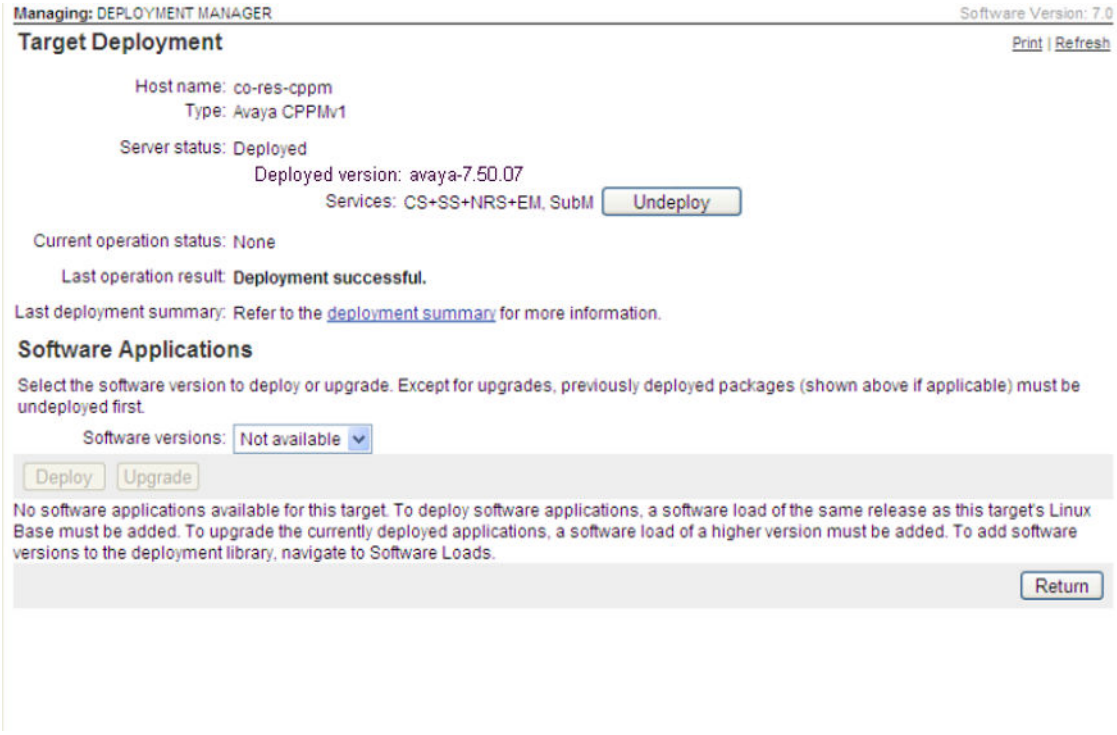


Figure 63: Target Deployment and Software Applications

4. In the **Software versions** field, select the software version from the list.

5. Select the check box beside the Deployment package to deploy and click **Deploy**.

   Important:

   Software applications must be undeployed first.

Undeploying application software

Undeploy previously deployed software packages.

1. On the **Deployment Manager** page, click **6.0 Deployment Targets**.
2. Click the option button beside the Host Name of the server.

   Important:

   The Deploy button is not available to select until the target server has a status of Undeployed.

3. Click **Deploy**.

   The Target Deployment page appears, as shown in Figure 63: Target Deployment and Software Applications on page 109.

4. In the **Software versions** field, select the software version from the list.
5. Select the check box beside the Deployment package to undeploy and click **Undeploy**.

Backing up existing system data files

Backup existing system data files on the target server to free disk space before the backup.

1. On the **Deployment Manager** page, click **6.0 Deployment Targets**.

   The Deployment Targets page appears.

2. Click the option beside the server to remove existing backup files.
3. Click **Backup**.

   The Backup page appears.

4. In the **Select backup location** field, choose a backup location to store the backup data. Select either **Deployment Server** or **SFTP Backup Server** from the list.

   Important:

   Sufficient space must be available on the target server hard drive for the backup file. If space is not available, you must delete a previous backup file before you start. You can store a maximum of three backup files on the target server hard drive; then you must delete a backup file before you add another. For information about deleting backup files from the target server hard drive, see Deleting an existing backup file on page 108.

5. If you choose **Deployment Server** as the backup location, proceed to 11 on page 111 in this procedure.
6. If you choose SFTP Backup Server as the backup location, the Backup screen refreshes with additional Secure File Transfer Protocol (SFTP) fields, as shown in the following figure. Proceed to 7 on page 111 in this procedure.

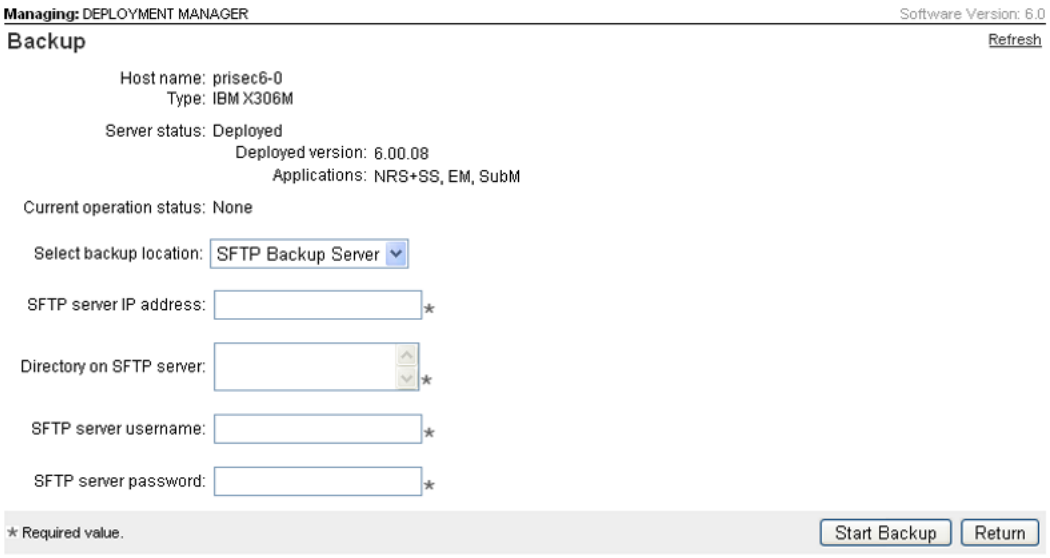


Figure 64: SFTP Backup Server window

7. In the **SFTP server IP address** field, type a value for the SFTP server IP address.
8. In the **Directory on SFTP server** field, type a value for the SFTP server directory.
9. In the **SFTP server username** field, type a value for SFTP server user name.
10. In the **SFTP server password** field, type a value for SFTP server password.
11. Click **Start Backup** to start the backup.

    OR

    Click **Return** to cancel the backup and return to the Deployment Targets screen.

    The Backup screen displays the **Last backup result**, **Last backup time**, and **Last backup name**, as shown in the following figure.

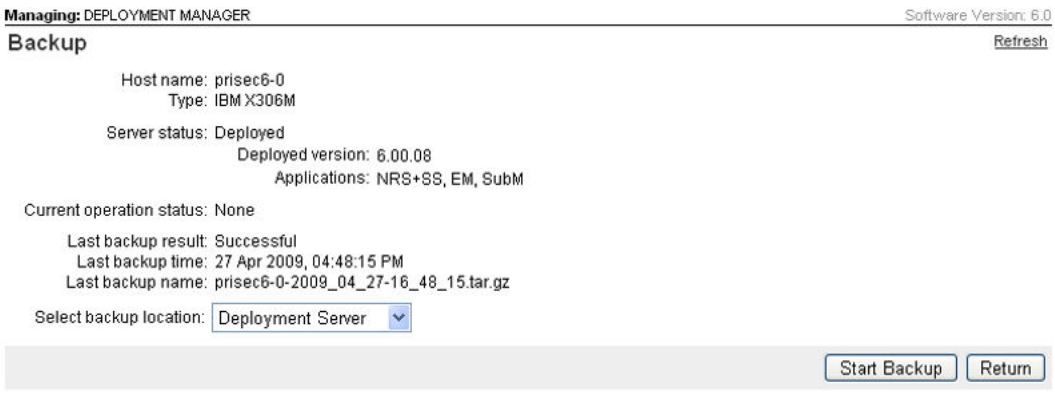


Figure 65: Backup results window

Restoring system data

Restore system data.

1. On the **Deployment Manager** page, click **6.0 Deployment Targets**.

   The Deployment Targets page appears.

2. Click the option button beside the server to restore.
3. Click **Restore**.

   The Restore page appears.

4. In the **Select restore source** field, select the source of the application data backup file from the list.

   If you select **Deployment Server (current target)** as the backup file source, proceed to 5 on page 112 in this procedure.

   If you select **Deployment Server (all targets)** as the backup file source, proceed to 6 on page 112.

   If you select **Client Machine** as the backup file source, proceed to 7 on page 112.

   If you select **SFTP Backup Server** as the backup file source, Proceed to 8 on page 113.

5. Select the backup file from the list of backup files stored on the current target server, and proceed to 12 on page 113.
6. Select the backup file from the list of backup files stored on all targets in the security domain, and proceed to 12 on page 113.
7. Type the backup file name in the **Specify restore file name** field.

   OR

   Click **Browse** to browse to the backup file.

   Proceed to 12 on page 113.

8. In the **SFTP server IP address** field, type a value for the SFTP server IP address.
9. In the **File path of backup on SFTP server** field, type the complete file path for the backup file.

   Note:

   You must enter the complete file path, including the file name.
10. In the **SFTP server username** field, type a value for SFTP server user name.
11. In the **SFTP server password** field, type a value for SFTP server password.
12. Click **Start Restore** to restore the application data.

    OR

    Click **Return** to cancel the restore process and return to the Deployment Targets page.

NFS based new installation

This section describes the recommended approach for installing Linux Base on the member and backup target servers using an Network File System (NFS) based remote installation method.

For Linux Base upgrades or Disaster Recovery procedures, see the following sections:

- Upgrade Linux base on page 119
- Disaster recovery on page 196

Installation workflow using NFS

The following figure shows the workflow for a new Avaya CS 1000 system Linux installation and commissioning using NFS. The flow indicates the recommended sequence of events to follow and provides the technical document number for the detailed procedures required for the task.

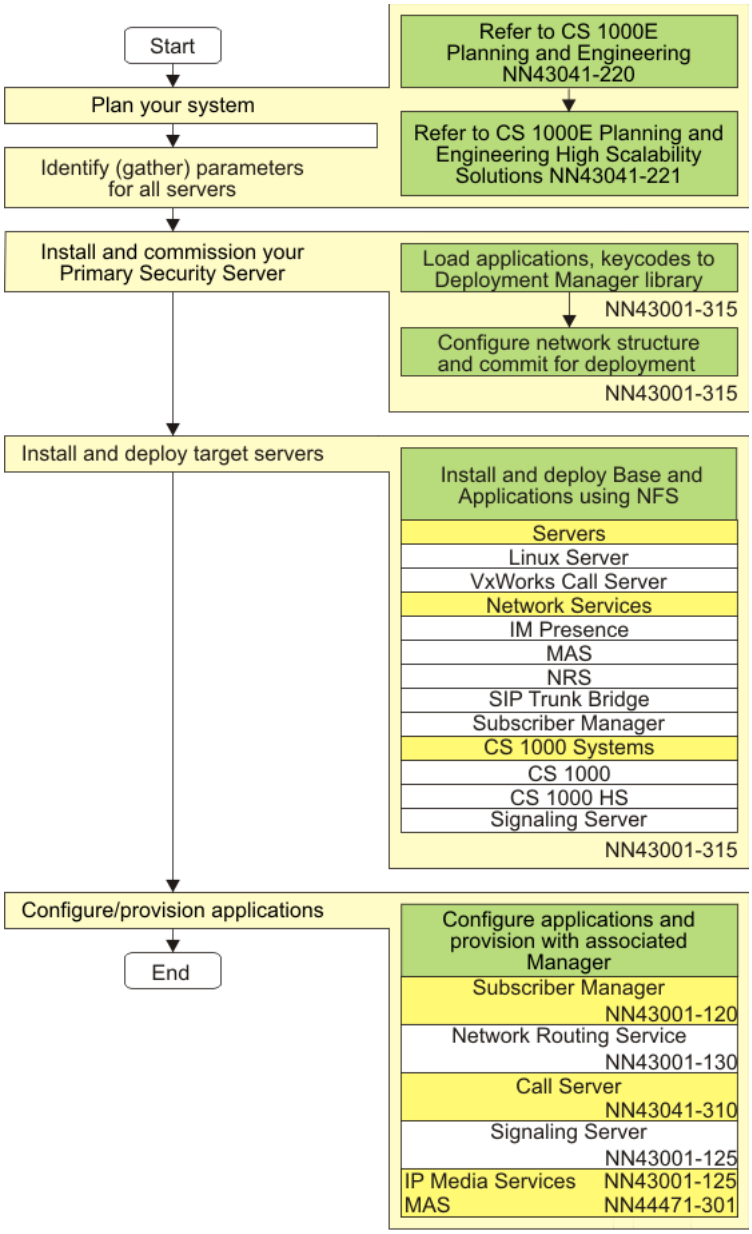


Figure 66: Workflow using NFS

NFS based remote installation topology

The following figure depicts a detailed NFS-based installation. Only the TLAN network interface is supported on the Deployment Server and target servers. In this diagram, TLAN A, B, C, and D are on different subnets in a WAN environment.

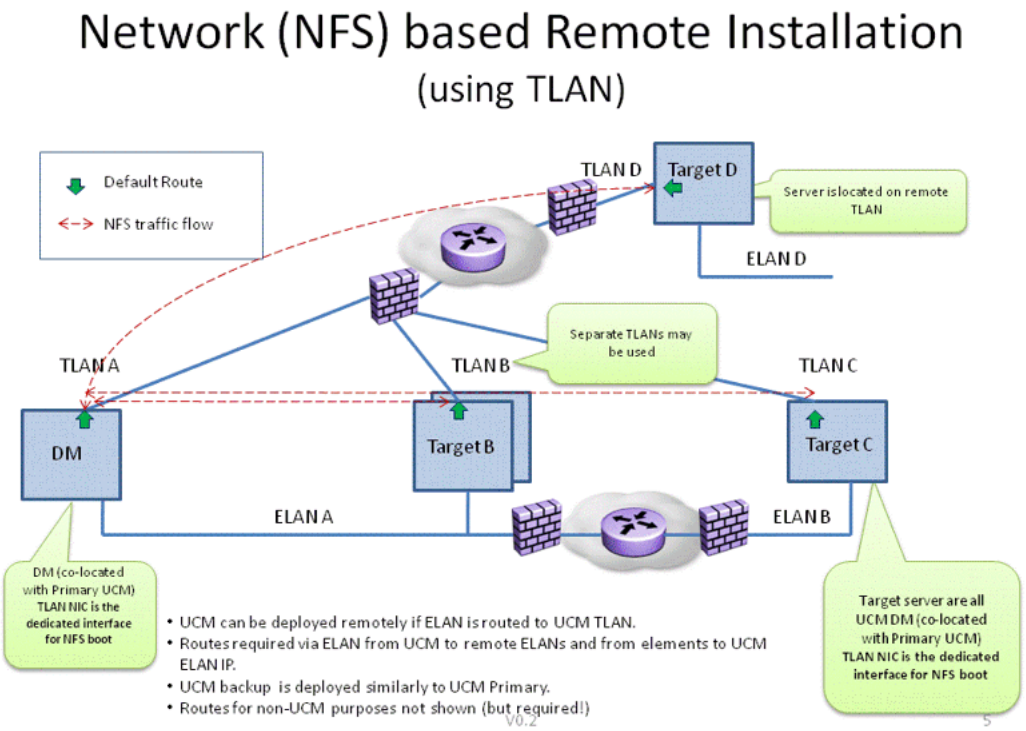


Figure 67: NFS-based remote installation topology (using TLAN)

Prerequisites

- You must connect your terminal to a serial port or kvm (for COTS, CP DC, or CP MG).
- The Deployment Manager must already be commissioned on a server.
- The target servers must be in a Committed status.
- Ensure that the proper TLAN routing on your data network is enabled.
- Ensure NFS service is Enabled from Deployment Manager in the Servers view.

  Note:

  On UCM, a button is available to enable or disable NFS. This option is not available on SMGR.
- Ensure NFS traffic is allowed on your data network.
- On the target servers, ensure the correct IP addresses are provided during the NFS restart process.
- On the target server, ensure the Deployment Server TLAN IP address is provided during the NFS restart process.
- On the target server, ensure the cables for your ELAN/TLAN interfaces are connected.

- If you are installing Linux Base on HP DL360 G7, G8 or G9 server, you must download the corresponding updated Linux Base installation image.
- If Primary security server is System Manager, then the updated image must be uploaded in Deployment Manager.
- If Primary is UCM server, then latest cs1000-linuxbase patch must be installed on this server.

Installing the servers (NFS-based new installation)

Use the following procedure for installing a new Linux Base on your target servers using NFS. For a network topology diagram of NFS, see Figure 67: NFS-based remote installation topology (using TLAN) on page 115.

Important:

Only NFS installation is supported (upgrade is not); therefore, if you configure a CS 1000 server for NFS-based remote installation, you must perform the NFS-based installation before you upgrade the Deployment Server. If you do not install a pre-configured server before you perform a Deployment Server upgrade, you must delete the server on the Deployment View page and re-configure it.

1. Insert the installation media: (DVD, Compact Flash, or USB memory stick) for your specific member server and restart the server.
   - For CP PM servers, insert the compact flash installation media.
   - For CP MG and CP DC, insert the USB 2.0 memory stick.
   - For COTS servers, insert the DVD installation media.

   Note:

   You must have a Compact Flash (CF) card or USB 2.0 memory stick with a capacity of at least 2 GB.

   Note:

   The N0220961 USB memory stick is supported for Avaya Communication Server 1000. Not all USB memory sticks are supported.
2. Restart the server.
3. For COTS: Watch for the boot prompt during the restart process and proceed to 4 on page 117 in this procedure.

   Important:

   The boot prompt appears only briefly. You have about eight seconds to type com1-nfs before it defaults to com1. If you miss the prompt, return to 2 on page 116 above.

   OR

   For CP DC and CP MG servers, press the F key immediately after the server begins rebooting and proceed to 4 on page 117 in this procedure.

OR

For a CP PM server, at the Linux Base installer screen, you see ..., at this point press the F key to force the board to boot from the faceplate drive, as shown in the following figure. Proceed to 4 on page 117 in this procedure.

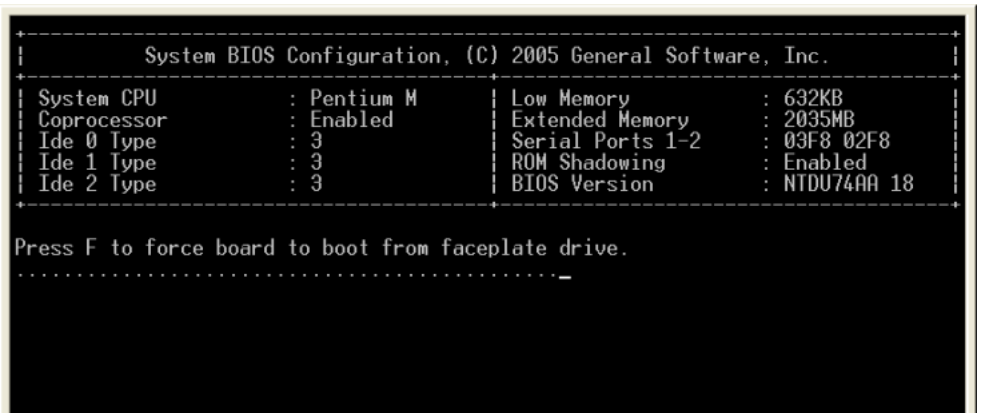


Figure 68: Force board to boot screen

4. At the boot prompt, type `com1-nfs` or `kvm-nfs`.

Note:

Kvm-nfs is not a valid option for CP PM servers.

5. On the Manual IP Configuration page, type the Target Server TLAN IP Address, the TLAN Netmask, the TLAN Gateway address, and the Deployment Server TLAN IP address, as shown in the following figure.

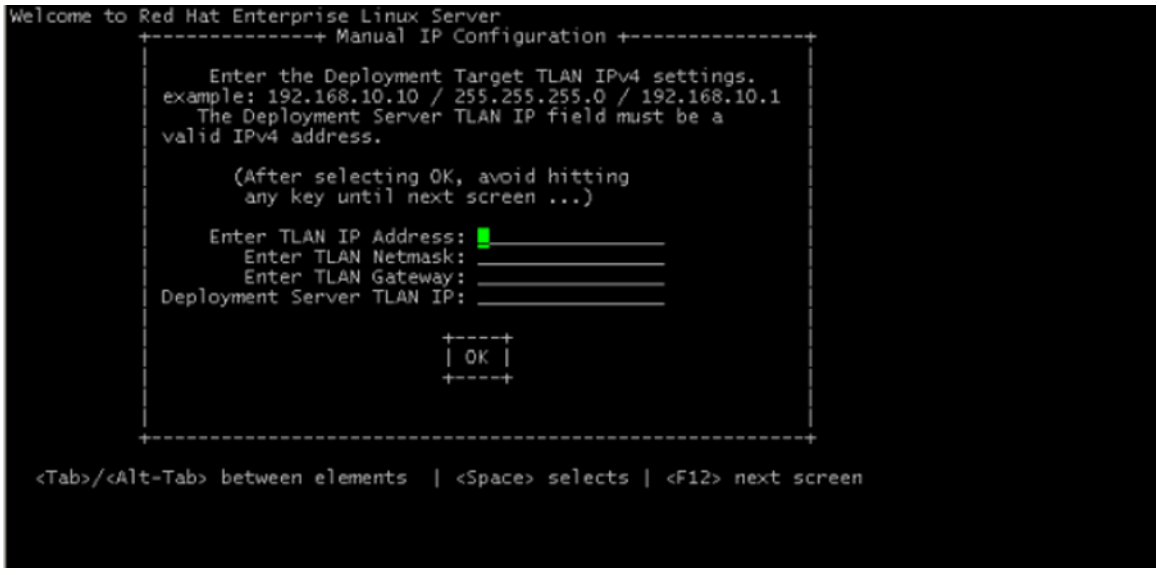


Figure 69: Manual IP configuration screen

6. Select **OK**.

The console displays installation details during the automated process. Upon completion, you receive the logon prompt.

Important:

Expect this procedure to take some time. Upon completion, the member server is installed with the Linux Base, security configured, and the required applications are deployed.

Chapter 7: Upgrade Linux base

This chapter describes the procedures for upgrading Linux Base on the following platforms:

- CP PM
- CP DC
- CP MG
- COTS servers
- Common Server
- Common Server R2
- Common Server R3

Navigation

- Upgrade Linux base manually on page 119
- Upgrade Avaya Linux base using Deployment Manager on page 123

Upgrade Linux base manually

Use the following procedure to perform a manual upgrade of Avaya Linux base.

Prerequisites

- You must create a copy of the keycodes before you perform the upgrade procedure.
- You must be able to log on using the nortel (for Release 7.0 systems) or admin2 (for Release 7.5 or later systems) accounts or any user account with the network administrator role assigned.
- If you are installing Linux Base on HP DL360 G7, G8 or G9 server, you must download the corresponding Linux Base installation image.

Warning:

During an upgrade, the hard drive is formatted and all data is lost. To preserve the data, perform a backup to an external source before you attempt an upgrade.

If the Avaya Aura® MS application is deployed on the server, Avaya Aura® MS must use Element Manager to backup Avaya Aura® MS data. For more information, see Backup and restore application data on page 47

Upgrading Linux base manually

1. Log on to the server using an account with networkadministrator privileges. For example, admin2.
2. At the command prompt, type `upgrade`, as shown in the following figure.

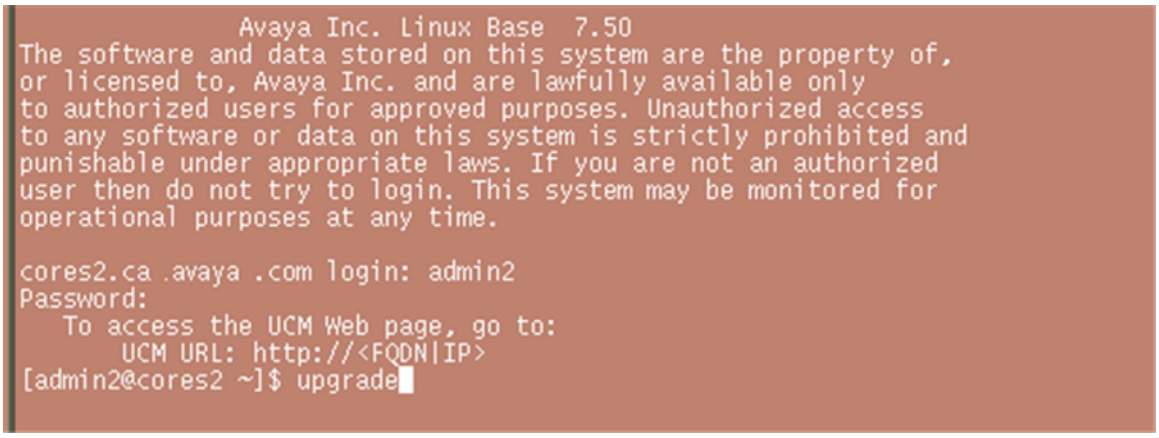


Figure 70: Upgrade

3. Type `Y` at the command prompt to continue the upgrade, as shown in the following figure.

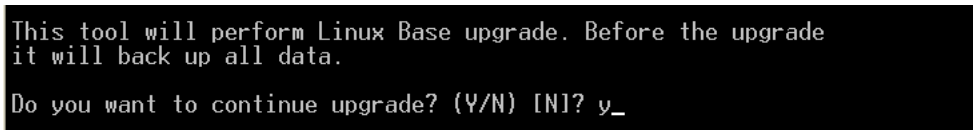


Figure 71: Continue upgrade screen

The tool backs up all system data before upgrading. The system data is saved to the `/admin` partition. Use the option Re-use /admin partition during Linux base installation.

4. Type `Y` at the prompt to backup data to external source (USB/SFTP), as shown in the following figure.

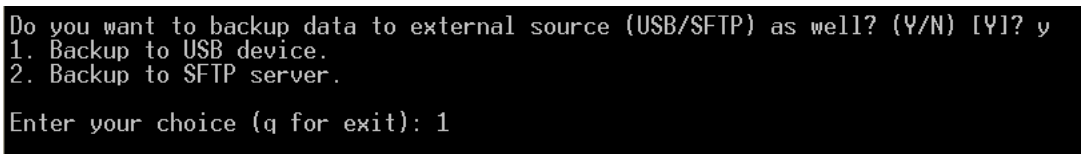


Figure 72: Backup source

Type `1`, if you would like to backup to a USB device or type `2`, if you would like to backup your data to an SFTP server, as shown in the previous figure.

OR

Type `q` to exit and not save the system data to an external source.

5. On the IP address line for the secure FTP server, type a value for secure FTP server IP address.

   On the SFTP login line, type a value for SFTP login.

   On the SFTP password line, type a value for SFTP password.

   On the remote SFTP directory line, type a value for remote SFTP directory.

   Important:

   If you perform SFTP as the admin2 user (non-jailed) then an example of an absolute sftp path is: `/var/opt/avaya/patch`. If you perform SFTP as any other user (jailed) then an example of an absolute sftp path is: `/patch` (assuming that the user is part of the patchadmin group). For users other than admin2 (jailed), the directories available using SFTP depends on what group they belong to.

6. Insert the Linux base upgrade media, and press any key to continue.
7. Type `Y` if you want to proceed with the installation, as shown in the following figure.

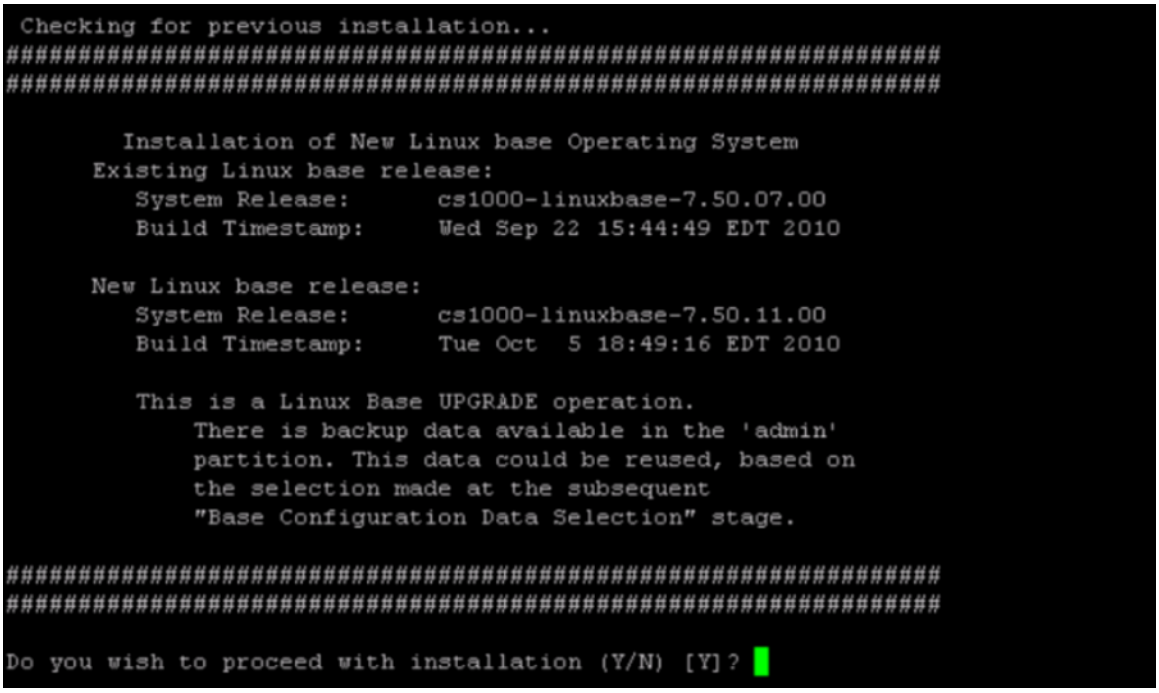


Figure 73: Confirmation screen

You are now prompted to format the administration partition. Only format the partition if you suspect the integrity of the partition has been compromised, for example, a corrupted disk, the local backup information is incorrect, etc.

8. Type `N` if you do not want to format the existing administration partition.

   OR

   Type `Y` if you want to format the existing administration partition, as shown in the following figure.

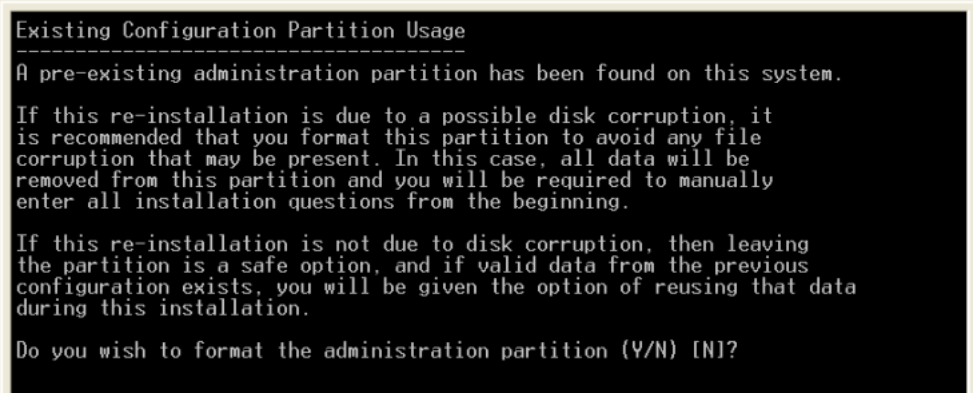


Figure 74: Existing administration partition confirmation screen

The Base Configuration Data Selection screen appears, as shown in the following figure.

9. Type one of the following, as shown in the following figure:
   a. Type `1` to reuse the data from the preexisting configuration file. That data input validation screens are shown for validation.
   b. Type `2` to load previously backed up data from a USB storage device.
   c. Type `3` to load previously backed up data from SFTP server.
   d. Type `4` to ignore the data from the preexisting configuration file. The standard system configuration prompts are presented.

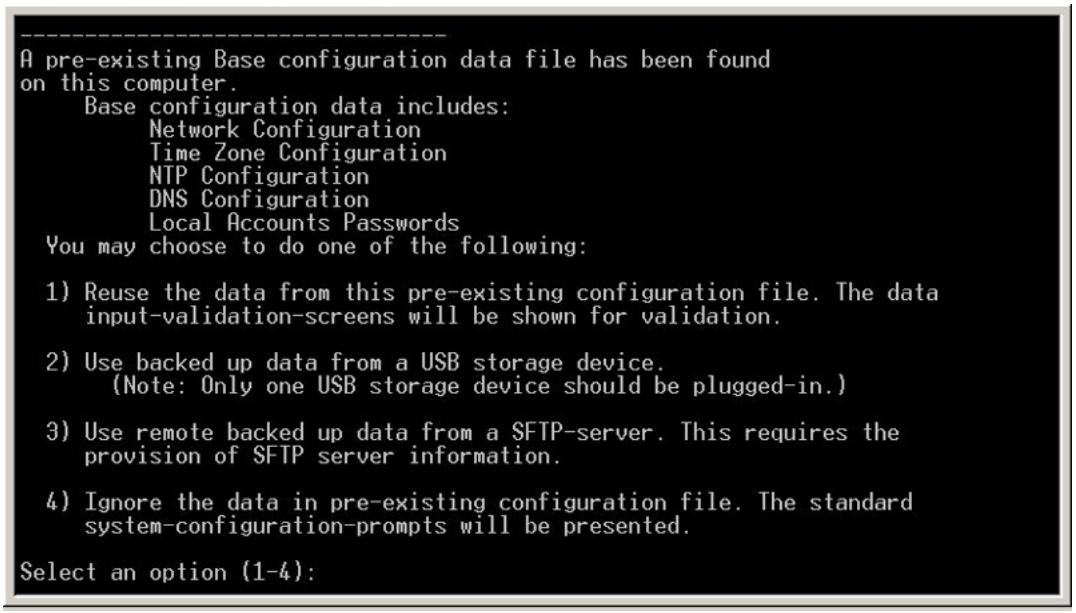


Figure 75: Base configuration data selection screen

10. Proceed to steps 8 through 24 in Installing a new Linux base on page 55 to continue the installation process.

Upgrade Linux base using Deployment Manager

Use the following procedure to perform a Linux base upgrade using Deployment Manager (DM).

Upgrading Linux base using DM

1. Navigate to DM. See Accessing Deployment Manager on page 77.
2. Delete all software loads (.nai files) and Linuxbase image files. See Deleting a software load on page 80.
3. Add the new software loads and Linuxbase image files. See Adding a software load from the Client Machine on page 79.
4. Proceed with the upgrade procedures found in Upgrade Avaya Communication Server 1000 system Linux installation on page 124.

Chapter 8: Upgrade Avaya Communication Server 1000 system Linux installation

This chapter provides the procedures for an end-to-end upgrade of Linux Base and applications. At this stage, Linux Base has been uploaded on the Primary security server (Deployment Server).

Warning:

During an upgrade, the hard drive is formatted and all data is lost. To preserve the data, perform a backup to an external source before you attempt an upgrade.

Warning:

During an upgrade procedure, keycodes for Co-res installations and for installations of Subscriber Manager are lost. You must create a copy of the keycodes before you perform the upgrade procedure.

Warning:

If you access the Linux server through a Terminal Server connected to the COM port, it is possible that garbled characters (such as uuuuuu) can appear during a system restart (for example, during the installation or upgrade procedure). This appearance can make the system seem to hang.

You can resolve the problem by reestablishing the COM1 connection from the client PC or work station to the Linux server.

Do not manually restart the system during the upgrade or installation. This can result in hard drive corruption and forces you to reinstall the system.

Navigation

- Upgrading a backup or member server from Release 6.0 or later on page 125
- Accessing the Local Deployment Manager on page 129

Upgrading a backup or member server from Release 6.0 or later

Upgrade a backup or member server from Release 6.0 or later. A system upgrade includes performing a latest software release installation of Linux Base and applications with your system data restored.

The following figure provides an example workflow for upgrading an Avaya Communication Server 1000 (Avaya CS 1000) system Linux installation and commissioning on a patched Release 6.0 system. The flow indicates the recommended sequence of events to follow and provides the technical document number for the detailed procedures required for the task.

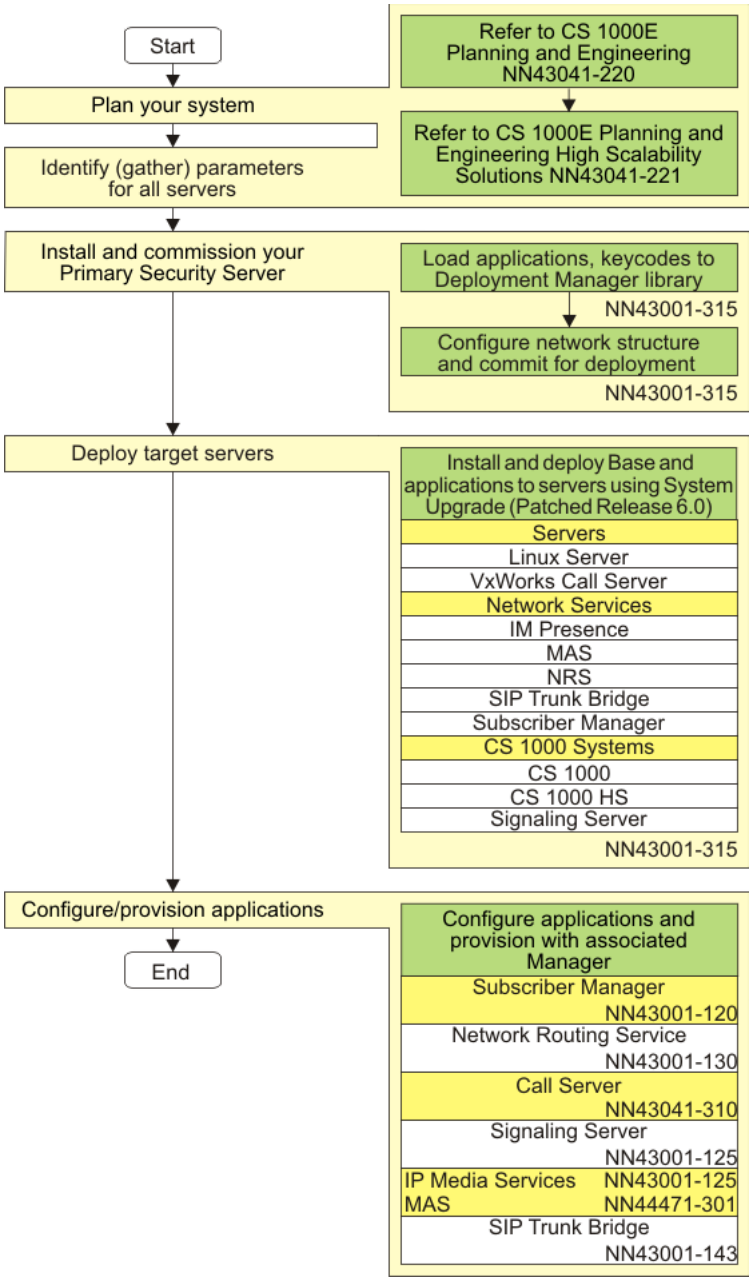


Figure 76: System upgrade patched Release 6.0

Prerequisites:

- The Primary security server (Deployment Server) must already be upgraded to the latest CS 1000 software release. See Upgrade Linux base manually on page 119.
- If the Primary security server is System Manager, CS 1000 Linux base image must be available to perform upgrade. To upload CS 1000 Linux base image in Deployment Manager, select CS 1000 Linux base image and click **Add**. Click **Browse**, choose a Linux Base image for upgrade, and click **Add Image**. After you upload a CS 1000 Linux base image, you can proceed with the System Upgrade.

Note:

If you delete all groups from the UCM Tree view, System Upgrade is available in the Deployment Actions list in Deployment Manager. You can upgrade the system to a new load/release; however, the Avaya applications do not deploy.

Procedure steps:

1. Apply the Service Update (SU) patch for your current software release on the Target Server.
2. Allocate the servers into the hierarchical groups which determines the application packages required for deployment.

   The servers can be allocated into the following groups:

   Important:

   If you are upgrading a previously deployed server and there is a previous configuration or a subset of a supported software configuration, the grouping can only be applied to a supported software configuration. For example, if the previously configured server contained NRS+SS_EM, then this server can be configured for the NRS group, SS group, and you can choose Element Manager. You cannot configure this server as a Call Server. You must also ensure that the server is associated in the same group. For example, if the previously configured server was configured with EM to manage a particular call server, you need to associate this server in the same group as that call server.

   - Network Services: for detailed procedures, see the following:
     - Adding a Avaya Aura MS service on page 90
     - Adding a Network Routing Service on page 91
     - Adding a Subscriber Manager service on page 92
   - Avaya CS 1000 systems: for detailed procedures, see the following:
     - Adding a CS 1000 system on page 93
     - Defining a new CS 1000 High Scalability system on page 97

   On the Deployment view page, the Status field changes from Preconfigured to Predeployed to identify that the server is now part of one or more groups. The Predeployed Applications field shows the applications that correspond to the selected services.
3. If the Primary security server is System Manager, log in to System Manager and click **Communication Server 1000** under the Elements section.

   Note:

   If System Manager is not the Primary security server, proceed to step 5.
4. Click **Software Deployment**.
5. On the Deployment View page, choose **Servers** from the View list, and click **Commit**, as shown in the following figure.

Important:

The **Commit** button is a system wide operation. All servers in the Predeployed status are committed.

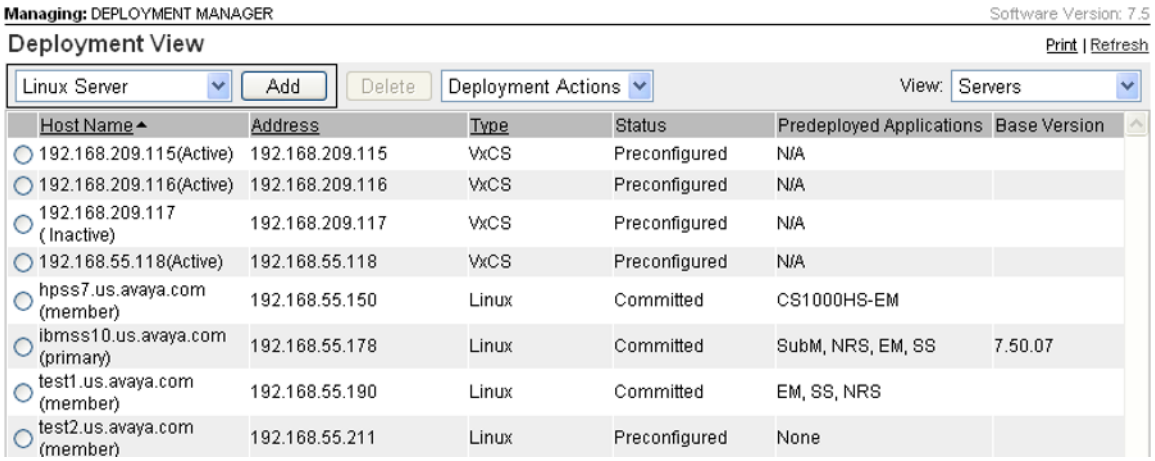


Figure 77: Deployment View commit screen

6. Select the server to upgrade and select **System Upgrade** from the Deployment Actions list

   If required, you can monitor the installation and deployment progress by using a serial port console.

   A message is displayed to confirm whether you want to proceed with the upgrade.

7. Click **OK** to proceed with the upgrade.

   Wait until the system displays None in the **Current operation status** field and Upgrade successful in the **Last operation status** field.

8. You must register the upgraded element using one of the following two options:

   In LD 117, type REGISTER UCMSECURITY SYSTEM FORCE

   OR

   From UCM, select the element to update and click **Edit**.

9. From the Element Details page, click **Edit**.

   The Release page appears.

10. Select Release 7.5 from the list and click **Save**.

Note:

If you are prompted for a keycode validation, you must provide a 7.5 keycode (for Release 7.0 targets).

Accessing the Local Deployment Manager

Application software can be deployed locally on a server. To do this, you must log on to the local server and use the local Deployment Manager to deploy the software. After the server joins the security domain, local deployment information is recognized by Deployment Manager on the Primary Security server (Deployment Server). For information about joining the security domain, see *Unified Communications Management Common Services Fundamentals, NN43001-116*.

Prerequisites:

- Download the appropriate .nai file (Avaya CS 1000 or Avaya Aura® MS) from the software download site to the server running Deployment Manager.

Procedure steps:

1. Log on to the server using the admin2 user ID and password.

   The Security Configuration screen appears, as shown in Figure 78: Security Configuration window on page 129.

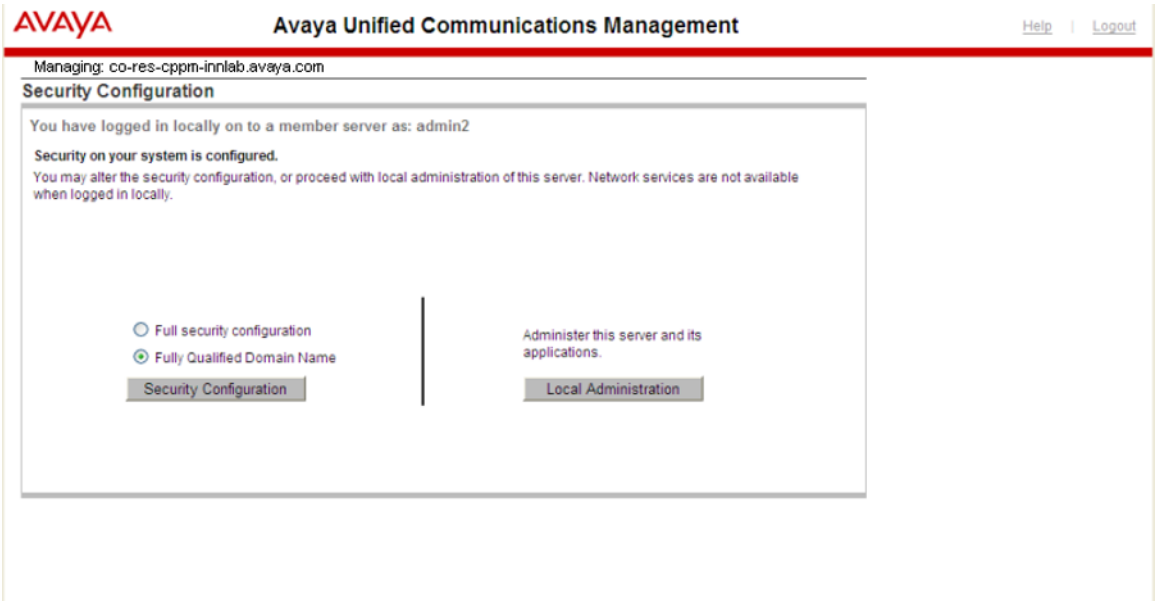


Figure 78: Security Configuration window

2. Click **Local Administration**.

   The screen appears, as shown in Figure 79: Base Manager window on page 130.

Figure 79: Base Manager window

3. In the navigation pane, click **Deployment**.

   The Deployment Manager screen appears, as shown in Figure 80: Deployment Manager window on page 130.

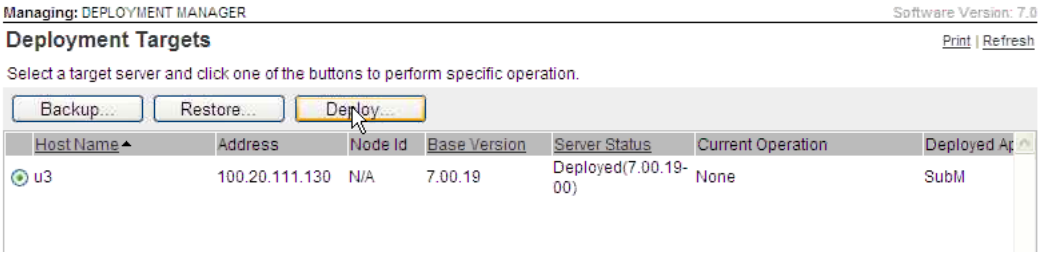


Figure 80: Deployment Manager window

4. Click the button beside the hostname.
5. Click **Deploy**.
6. Click **Upgrade**.
7. To allocate the target servers to a group, proceed to Step 7 on page 75 in Preconfiguring process using Deployment View on page 74.

   Note:

   Servers that are deployed with applications but are not configured into systems are represented in blue in Deployment Manager

Configuring a Server pre-loaded with Avaya Linux base

The Avaya Linux Base image may be pre-loaded on new Servers shipped from the factory; this saves the Linux Base installation time. Currently, CP DC and CP MG hard disks are pre-loaded with

the latest software release. CP PM and Commercial Server hard disks are shipped blank and must be fully installed on-site.

The pre-loaded Server is shipped with some default settings preconfigured, such as:

- The default password for both the root and admin2 user accounts is admin2_Admin2
- The default IP address for the ELAN interface is 192.168.1.3
- The default IP address for the TLAN interface is 192.168.1.2
- The default hostname is: localhost

You are required to start the commissioning of the server by connecting a maintenance terminal to the serial port on the Server for configuration of customer-assigned IP addresses, the FQDN, and other customer settings such as DNS server or time and date.

Perform the following procedure to prepare the server for installation.

1. Connect a maintenance terminal to the server serial port.
2. Log on as admin2 using the default password.
3. Type **passwd** .
4. Change the avaya password. For information about changing passwords, see Changing Linux Base passwords on page 201.
5. Log on as root by typing **su-** and the default password.
6. Type **passwd** .
7. Change the root password. For information about changing passwords, see Changing Linux Base passwords on page 201.
8. Log on as admin2 by typing the **exit** CLI command.

   Note:

   You must be logged on as root.

   OR

   Log on as admin2 by logging on to the COM1 port as nortel and using the newly created password.
9. Type **baseparamsconfig**.

   Warning:

   Do not change the FQDN of the primary or backup security server when you use the baseparamsconfig command.
10. Make appropriate changes to base parameters, such as FQDN or IP settings.
11. Type `Y` to save the base parameters changes.

    The system restarts.
12. Connect the ELAN and TLAN interfaces to the data network.

13. Proceed to step 2 on page 74 in Preconfiguring process using Deployment View on page 74.

Chapter 9: Avaya Aura® MS 7.6 installation

This chapter provides the procedure to install a new Linux Base and AMS 7.6.

Linux Base support for Avaya Aura® MS 7.6

For all Linux servers used for CS 1000, the standard Red Hat Enterprise Linux (RHEL) was customized to add features and content applicable to the CS 1000 environment. These changes are commonly called the CS 1000 Linux Base. As part of the AMS 7.6 upgrade, RHEL version was upgraded from 32 bit release 5.3 to 64 bit release 5.10.

The following features from the Linux Base have changed due to the changes in Avaya Aura® MS along with the RHEL upgrade:

- Base Manager

  Avaya Aura® MS 7.6 onwards, Base Manager will no longer be available. Use the command line interface for all functions previously performed through the Base Manager. These functions include, but are not limited to, network configuration (network identity, DNS, route table) and date and time configuration (NTP, time zone). The command line commands have not changed. For more information on using the CLI commands, refer the relevant CS 1000 documentation or the CLI help utility.

- Patch manager

  Avaya Aura® MS 7.6 onwards, Patch Manager will no longer be available. Use the command line interface for patching Avaya Aura® MS 7.6. See *Avaya Aura® MS 7.6 patching*.

- Security domain

  Avaya Aura® MS 7.6 cannot join the security domain or access any security domain features. This impacts account management, central authentication, and Avaya Aura® MS Element Manager access. Only local accounts can be used to access CLI.

  Account user roles and permissions that were previously set up in UCM will no longer be supported, but, will be replaced with Avaya Aura® MS Element Manager Role Based Access Control (RBAC). For more information, see *Avaya Aura® MS Element Manager Role Based Access Control (RBAC)* and *Avaya Aura® MS Element Manager RBAC with System Manager*.

- CLI commands

  The following CLI commands are no longer supported:

Command	Description
sendSnmpTrap	generates an SNMP trap in Common-MIB format and could be used as a test tool to confirm

Table continues…

	whether traps are being properly sent to the configured destinations No replacement is available for this command.
disableAllTargets	disables all IPSec targets and removes all IPSec data No replacement is available for this command.

All other CLI commands are still supported.

- Avaya Aura® MS 7.6 deployment

  Avaya Aura® MS 7.6 no longer uses the Deployment Manager but is bundled inside the Red Hat installation image. You can install Avaya Aura® MS using a local RHEL and Linux Base installation media. Two types of installation images are provided — DVD image (cs1000-linuxbase-amsx64-7.65.16.xx.iso) and USB image (cs1000-linuxbase-amsx64-7.65.16.xx_cf.zip)

Related links

Navigation on page 134
Prerequisites on page 134
AMS 7.6 installation process on page 135
Installing Avaya Aura MS 7.6 by formatting preexisting administration partition on page 136
Installing Avaya Aura MS without formatting preexisting administration partition on page 138

Navigation

Prerequisites on page 134
AMS 7.6 installation process on page 135
Installing Avaya Aura MS 7.6 by formatting preexisting administration partition on page 136
Installing Avaya Aura MS without formatting preexisting administration partition on page 138

Related links

Avaya Aura MS 7.6 installation on page 133

Prerequisites

The following CS 1000 environments support Avaya Aura® MS 7.6:

- CDPC
- COTS2 servers (IBM x3350, Dell R300)
- Common Server 1 (HP DL360 G7)

- Common Server 2 (HP DL360 G8)
- Common Server 3 (HP DL360 G9)

Prepare appropriate installation media according to the environment on which you want to install Avaya Aura® MS 7.6:

- For COTS2, Common Server 1, Common Server 2, Common Server 3 servers, use DVD
- For CPDC , use USB stick

Keep the following information handy for Linux Base installation:

- ELAN IP address
- ELAN gateway IP address
- ELAN netmask
- host name for the TLAN
- domain name
- TLAN IP address
- TLAN gateway IP address
- TLAN netmask
- Timezone
- IP address of the Primary Domain Name Service (DNS) server
- Default system gateway for the network interface is TLAN

For more information, see *New Linux Base installation.*

Related links

Avaya Aura MS 7.6 installation on page 133

AMS 7.6 installation process

The following figure illustrates the main steps in the AMS 7.6 installation process.

Figure 81: AMS 7.6 installation process

Related links

Avaya Aura MS 7.6 installation on page 133

Installing Avaya Aura® MS 7.6 by formatting preexisting administration partition

Procedure

1. Insert the Avaya Aura® MS installation media into the server.

   Important:

   Use only internal DVD drive for installation from DVD media. External drives are not supported.

   Warning:

   Insert the Linux base DVD in the DVD drive only during Avaya Aura® MS installation. If you accidentally leave the installation DVD in the DVD drive after installation, and the system restarts, the system will boot into the installation program, due to which the system will not respond. To remedy this issue, manually eject the DVD drive and restart the system.

2. Restart the server.
3. Perform one of the following actions:
   - For a COTS or common server, watch for the boot prompt during the restart process and proceed to step 4.
   - For CPDC, press `F` key immediately after the server begins rebooting and proceed to step 4.
4. Perform one of the following actions:
   - To install using an attached keyboard and video monitor, type `kvm`.
   - To install using a serial console on COM1, type `com1`.
5. On the CS 1000 Linux base system installer confirmation screen, type `Y` and press **Enter**.
6. On the Existing Configuration Partition Usage screen, to begin formatting an existing administration partition, type `Y` and press **Enter**.

   The system displays this screen only when it finds an existing administration partition.

```
Existing Configuration Partition Usage
--------------------------------------
A pre-existing administration partition has been found on this system.

If this re-installation is due to a possible disk corruption, it
is recommended that you format this partition to avoid any file
corruption that may be present. In this case, all data will be
removed from this partition and you will be required to manually
enter all installation questions from the beginning.

If this re-installation is not due to disk corruption, then leaving
the partition is a safe option, and if valid data from the previous
configuration exists, you will be given the option of reusing that data
during this installation.

Do you wish to format the administration partition (Y/N) [N]?
```

7. Select an installation option.

   The following options are available if you choose format the administration partition:

Option	Description
1	Install without using any configuration files (normal installation)
2	Load previously backed up data from external USB storage device **Note:** Plug in only one USB storage device.
3	Load previously backed up data from SFTP-server.

8. Enter network parameters (ELAN, TLAN IP addresses, network masks, gateways, and host name) time zone, and daylight saving time parameters.
9. On the Network Configuration Validation screen, validate the displayed information, and type `Y` to confirm.
10. **(Optional)** Change the current system date and system time.
11. Change the passwords for root and admin2 users.
12. The system continues with the installation and restarts automatically.

    Warning:

    For COTS servers, ensure that the installation DVD ejects. If, at the end of the installation, the DVD does not eject automatically, eject it manually.

Result

You have successfully installed Avaya Aura® MS. The system displays a login prompt. You can login using the admin2 account.

Related links

Avaya Aura MS 7.6 installation on page 133

Installing Avaya Aura® MS without formatting preexisting administration partition

Procedure

1. Insert the Avaya Aura® MS installation media into the server.

   Important:

   Use only internal DVD drive for installation from DVD media. External drives are not supported.

   Warning:

   Insert the Linux base DVD in the DVD drive only during Avaya Aura® MS installation. If you accidentally leave the installation DVD in the DVD drive after installation, and the system restarts, the system will boot into the installation program, due to which the system will not respond. To remedy this issue, manually eject the DVD drive and restart the system.

2. Restart the server.
3. Perform one of the following actions:
   - For a COTS or common server, watch for the boot prompt during the restart process and proceed to step 4.
   - For CPDC, press `F` key immediately after the server begins rebooting and proceed to step 4.
4. Perform one of the following actions:
   - To install using an attached keyboard and video monitor, type `kvm`.
   - To install using a serial console on COM1, type `com1`.
5. On the CS 1000 Linux base system installer confirmation screen, type `Y` and press **Enter**.
6. On the Existing Partition Usage screen, to proceed without formatting the existing administration partition, type `N`, and press **Enter**.

   The system displays this screen only when it finds an existing administration partition.

```
Existing Configuration Partition Usage
--------------------------------------
A pre-existing administration partition has been found on this system.

If this re-installation is due to a possible disk corruption, it
is recommended that you format this partition to avoid any file
corruption that may be present. In this case, all data will be
removed from this partition and you will be required to manually
enter all installation questions from the beginning.

If this re-installation is not due to disk corruption, then leaving
the partition is a safe option, and if valid data from the previous
configuration exists, you will be given the option of reusing that data
during this installation.

Do you wish to format the administration partition (Y/N) [N]?
```

7. Select an installation option.

   The following options are available if you choose to continue without formatting the administration partition:

Option	Description
1	Reuse the data from the preexisting configuration file. The system will display data input validation screens for confirmation.
2	Use backed up data from external USB storage device **Note:** Plug in only one USB storage device.
3	Use remote backed up data from an SFTP-server. The system should be able to access SFTP server information during the installation.
4	Ignore the data in the preexisting configuration file. The system will display standard system configuration prompts.

8. Validate the configuration data.
9. Change the passwords for root and admin2 users.
10. The system continues with the installation and restarts automatically.

    Warning:

    For COTS servers, ensure that the installation DVD ejects. If, at the end of the installation, the DVD does not eject automatically, eject it manually.

Result

You have successfully installed Avaya Aura® MS. The system displays a login prompt. You can login using the admin2 account.

Related links

Avaya Aura MS 7.6 installation on page 133

Chapter 10: Avaya Aura® MS upgrade and MAS 7.0 migration

You cannot restore MAS 7.0 backed up data in Avaya Aura® MS 7.6 because a direct upgrade from release 7.0 to 7.6 is not supported. Customers can migrate from MAS 7.0 to Avaya Aura® MS 7.6 by using an upgrade tool that helps transfer customers' database and configuration from 7.0.

The upgrade tool migrates the following data from MAS 7.0 to Avaya Aura® MS 7.6:

- CStore data (provisioned media prompts)
- SIP Configuration (domains, accounts, nodes, routes, and route specific configuration)
- License Server key configuration
- Cluster configuration (server role and replication account user name/password)

A few configurations cannot be migrated with the upgrade utility. Manually configure the following configurations on the new server:

- Provisioned certificates
- Codec configuration
- Media security
- UCM users/roles and passwords

Note:

Avaya Aura® MS 7.6 only supports upgrades from 7.0.0.623.

Perform upgrades only during the maintenance window or at an off peak-usage time.

Related links

Navigation on page 141
Prerequisites for upgrade on page 141
Upgrade overview on page 142
Avaya Aura MS upgrade and MAS 7.0 data migration process on page 142
Upgrading Avaya Aura MS and migrating MAS 7.0 data on page 143
Migrating Avaya Aura MS 7.0 data from CLI on page 146
Deployment Manager on page 147
CS 1000 Avaya Aura MS 7.6 Patching on page 148
Avaya Aura MS 7.6 EM access on page 149
Content Store data replication between clusters on page 155

Changing Avaya Aura MS server IP address and host name on page 156
License server on page 157
Avaya Aura MS 7.6 EM certificate management on page 157
Media port management on page 160

Navigation

Prerequisites for upgrade on page 141
Upgrade overview on page 142
Avaya Aura MS upgrade and MAS 7.0 data migration process on page 142
Upgrading Avaya Aura MS and migrating MAS 7.0 data on page 143
Migrating Avaya Aura MS 7.0 data from CLI on page 146
Deployment Manager on page 147
CS 1000 Avaya Aura MS 7.6 Patching on page 148
Avaya Aura MS 7.6 EM access on page 149
Content Store data replication between clusters on page 155
Changing Avaya Aura MS server IP address and host name on page 156
License server on page 157
Avaya Aura MS 7.6 EM certificate management on page 157
Media port management on page 160

Related links

Avaya Aura MS upgrade and MAS 7.0 migration on page 140

Prerequisites for upgrade

Before beginning an upgrade, ensure that you complete the following:

- Back up Avaya Aura® MS data for all Avaya Aura® MS servers in the cluster. Avaya Aura® MS Element Manager is used to back up Avaya Aura® MS data, including Service Data and manifest file. For more information, see *Implementing and Administering Avaya Aura® Media Server 7.6*.
- Copy two backup files to a USB flash drive or SFTP server to migrate Avaya Aura® MS 7.0 data during installation. The server that is being upgraded should be able to access the SFTP.
- Use the **`sysbackup`** command to back up CS 1000 Linux base for all Avaya Aura® MS servers in the cluster.

Related links

Avaya Aura MS upgrade and MAS 7.0 migration on page 140

Upgrade overview

This section provides a brief overview of the difference in the upgrade procedure for simplex Avaya Aura® MS and load sharing Avaya Aura® MS.

Simplex Avaya Aura® MS upgrade overview

A simplex Avaya Aura® MS is a standalone Avaya Aura® MS that is not part of a cluster.

The system uses the following process to upgrade Avaya Aura® MS:

1. Back up the server data.
2. End active sessions by setting the server through a progression of Pending Lock, Lock, and Stopped states.
3. Perform upgrade procedure.
4. Verify that the system is functional and that there are no unexpected alarms.
5. Back up the new system

N+1 load sharing cluster upgrade overview

With load sharing Avaya Aura® MS installations, you can maintain continuous access to Avaya Aura® MS services during upgrades, by upgrading one cluster server at a time. Either the Primary or Secondary server must remain in service for the cluster to remain operational. Cluster service is lost if the Primary and Secondary servers are out of service at the same time.

The system uses the following process to upgrade N+1 load sharing clusters of Avaya Aura® MS:

1. For the Primary server, perform the procedure to upgrade a simplex Avaya Aura® MS. Wait for any alarms to clear as the server returns to service after the upgrade.
2. For the Standard server, perform the procedure to upgrade a simplex Avaya Aura® MS. Wait for any alarms to clear as the server returns to service after the upgrade.
3. For the Secondary server, perform the procedure to upgrade a simplex Avaya Aura® MS.

Related links

Avaya Aura MS upgrade and MAS 7.0 migration on page 140

Avaya Aura® MS upgrade and MAS 7.0 data migration process

This figure shows the main steps for the Avaya Aura® MS upgrade and MAS 7.0 data migration process.

Figure 82: Avaya Aura® MS upgrade and MAS 7.0 data migration process

Related links

Avaya Aura MS upgrade and MAS 7.0 migration on page 140

Upgrading Avaya Aura® MS and migrating MAS 7.0 data

Procedure

1. Insert the Avaya Aura® MS installation media into the server.

   Important:

   Use only internal DVD drive for installation from DVD media. External drives are not supported.

   Warning:

   Insert the Linux base DVD in the DVD drive only during Avaya Aura® MS installation. If you accidentally leave the installation DVD in the DVD drive after installation, and the system restarts, the system will boot into the installation program, due to which the system will not respond. To remedy this issue, manually eject the DVD drive and restart the system.

2. Restart the server.
3. Perform one of the following actions:
   - For a COTS or common server, watch for the boot prompt during the restart process and proceed to step 4.
   - For CPDC, press `F` key immediately after the server begins rebooting and proceed to step 4.
4. Perform one of the following actions:
   - To install using an attached keyboard and video monitor, type `kvm`.
   - To install using a serial console on COM1, type `com1`.
5. On the CS 1000 Linux base system installer confirmation screen, type `Y` and press **Enter**.
6. On the Existing Configuration Partition Usage screen, perform one of the following:
   - To begin formatting a preexisting administration partition, type `Y` and press **Enter**.

- To continue without formatting the preexisting administration partition, type `N` and press **Enter.**

The system displays this screen only when it finds an existing administration partition.

```
Existing Configuration Partition Usage
--------------------------------------
A pre-existing administration partition has been found on this system.

If this re-installation is due to a possible disk corruption, it
is recommended that you format this partition to avoid any file
corruption that may be present. In this case, all data will be
removed from this partition and you will be required to manually
enter all installation questions from the beginning.

If this re-installation is not due to disk corruption, then leaving
the partition is a safe option, and if valid data from the previous
configuration exists, you will be given the option of reusing that data
during this installation.

Do you wish to format the administration partition (Y/N) [N]?
```

7. Select an installation option.

The following options are available if you choose to format the preexisting administration partition:

Option	Description
1	Install without using any configuration files (normal installation)
2	Load previously backed up data from external USB storage device **Note:** Plug in only one USB storage device.
3	Load previously backed up data from SFTP-server.

The following options are available if you choose to continue without formatting the preexisting administration partition:

Option	Description
1	Reuse the data from the preexisting configuration file. The system will display data input validation screens for confirmation.
2	Use backed up data from external USB storage device **Note:** Plug in only one USB storage device.
3	Use remote backed up data from an SFTP-server. The system should be able to access SFTP server information during the installation.
4	Ignore the data in the preexisting configuration file. The system will display standard system configuration prompts.

Note:

Depending on the option you selected in step 6, the procedure to install Avaya Aura® MS will vary slightly. See *Installing Avaya Aura® MS by formatting preexisting administration partition* and *Installing Avaya Aura® MS without formatting preexisting administration partition*.

8. Enter network parameters (ELAN, TLAN IP addresses, network masks, gateways, host name), time zone, and daylight saving time parameters.

   This step is optional when you install Avaya Aura® MS without formatting the preexisting administration partition.

9. Validate configuration data.
10. **(Optional)** Change the current system date and system time.
11. Change the passwords for root and admin2 users.
12. On the migration of AMS 7.0 database screen, type `Y` and press **Enter**.

    Note:

    You cannot restore Avaya Aura® MS 7.0 data in EM after upgrade. If Avaya Aura® MS 7.0 data migration was not performed during upgrade, it can be performed after upgrade in CLI by using the **`amsupgrade`** tool. For more information, see *Migrating AMS 7.0 data from CLI*.

13. Select a source for Avaya Aura® MS 7.0 backup files.

    The following options are available while selecting a source of data:

Option	Description
1	Use backed up data from amsinfo directory on a USB storage device.
2	Use remote backed up data from an SFTP server.
3	Postpone with recovery and continue installation.

14. Enter network parameters for the current server (ELAN network interface IP addresses, gateway and network masks) and the source for Avaya Aura® MS 7.0 backup files.
15. Validate the network parameters you provided.
16. Select two Avaya Aura® MS 7.0 backup files.
17. The system continues with the Avaya Aura® MS installation and MAS 7.0 data migration. After installation, the system restarts automatically.

    Users can login using admin2 account and apply the required manual configurations. If upgraded server is Primary AMS in cluster, then service is now restored and can start taking calls to minimize customer impact. Similarly, upgrade Secondary AMS server in cluster and then Standard AMS servers in similar manner.

Related links

Avaya Aura MS upgrade and MAS 7.0 migration on page 140

Migrating Avaya Aura® MS 7.0 data from CLI

Before you begin

Important:

Restore system configuration data before the Application data.

Backup data is not portable from one server to another. To replace a server, configure the server with the same IP address, and hostname so that the data is compatible with the server configuration.

Procedure

1. To prevent new sessions from starting on the system, select **EM** > **System Status** > **Element Status**.
2. Select **More Actions** > **Pending Lock**.
3. Click **Confirm**.
4. To check for active sessions on the server, select **EM** > **System Status** > **Monitoring** > **Active Sessions**.

   Wait for the active sessions to end. If you continue before all active sessions end, the system ends the remaining active sessions.
5. To lock Avaya Aura® MS, select **EM** > **System Status** > **Element Status** and then, select **More Actions** > **Pending Lock**.

   This also ends any remaining sessions.
6. Click **Confirm**.
7. After the system ends the sessions, to stop Avaya MS, select **EM** > **System Status** > **Element Status**, and then click **Stop**.
8. Click **Confirm**.
9. Using CLI find the system configuration data backup file.

   The system configuration data backup file name contains Task0_. For example, backupTask0_MyHostname_2014_03_30_0_9_17.zip.
10. To upgrade the system configuration data , type `amsupgrade filename -n`, where *filename* is the syste, configuration data backup file name.
11. Find the application content data backup file.

    The application content data backup file name contains Task1_. For example, backupTask1_MyHostname_2014_04_04_0_9_19.zip.
12. To upgrade the application data, type `amsupgrade filename -n`, where *filename* is the application content data backup file name
13. To start Avaya Aura® MS, select **EM** > **System Status** > **Element Status**, and then click **Start**.

14. Click **Confirm**.

Example

Next steps

Related links

Avaya Aura MS upgrade and MAS 7.0 migration on page 140
Amsupgrade tool on page 147

Amsupgrade tool

The amsupgrade tool is used for Avaya Aura® MS 7.0 data migration.

`amsupgrade` *filename* -noprompt -n -s, where:

Parameter/Variable	Description
filename	Archive file name, optionally including full path, of data to upgrade
-noprompt	Skip confirmation prompt
-n	Do not stop and start Avaya Aura® MS services during upgrade.
-h	Display this help message
-s	Silent mode. Skip prompts and direct output to debug file.

Example

amsupgrade /backup/CONFIG_DATA.zip

amsupgrade /backup/SERVICE_DATA.zip -s

Related links

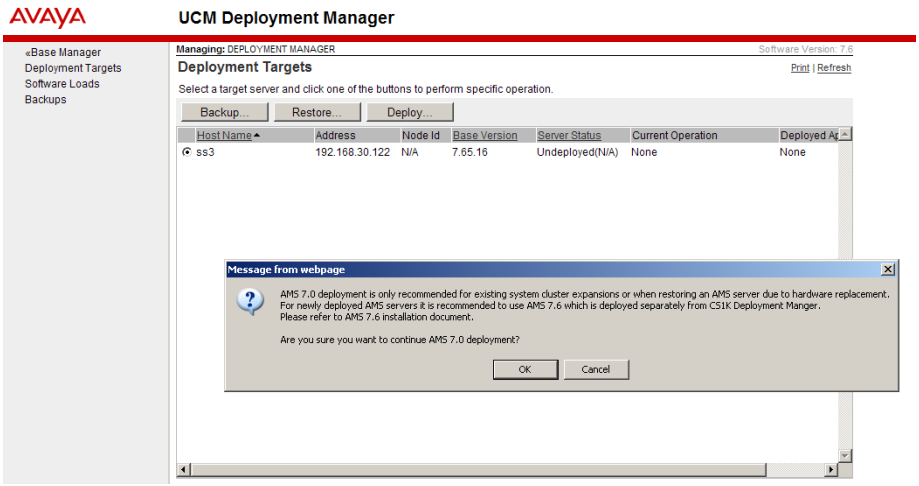
Migrating Avaya Aura MS 7.0 data from CLI on page 146

Deployment Manager

The deployment manager cannot be used to install Avaya Aura® MS 7.6. However, the deployment manager is still available in CS 1000 Release 7.6 to support existing Avaya Aura® MS 7.0 installations.

Existing Avaya Aura® MS 7.0 customers will still be able to expand existing clusters and reinstall hardware using the deployment manager. For all other installations, you must upgrade to Avaya Aura® MS 7.6.

Deployment Manager displays the following warning message during Avaya Aura® MS 7.0 deployment.



Related links

Avaya Aura MS upgrade and MAS 7.0 migration on page 140

CS 1000 Avaya Aura® MS 7.6 Patching

In Avaya Aura® MS 7.6, the patch manager is no longer available. Use the CLI for all patching, including Linux Base patching.

Avaya Aura® MS patches are delivered as Quick Fix Engineering (QFE) patches. You must apply QFE patches in sequential, numerical order because new patches depend on previously installed QFE patches. For example, you must install QFE-platform-7.6.0.230-0001 before you install QFE-platform-7.6.0.230-0002.

Note:

In Avaya Aura® MS 7.0, you can use **maspatch** command to install QFE patches. In AMS 7.6, you must use **amspatch** instead.

This table shows different ways to use the **amspatch** command:

Command	Purpose
amspatch list applied	Check currently applied patches.
amspatch apply all	Apply all patches in the `/opt/nortel/ma/MAS/qfe` directory under the root account
amspatch apply *filepath*	Apply a single patch. For single patch installation both full path or patch name can be used. To use the patch name, the patch must be in the `/opt/nortel/ma/MAS/qfe` directory.

For more information, see *Installing, Upgrading, and Patching Avaya Aura® Media Server 7.6*.

Related links

Avaya Aura MS upgrade and MAS 7.0 migration on page 140

Avaya Aura® MS 7.6 EM access

To access the Avaya Aura® MS EM, use one of the following URLs:

- http://*ams7.6 server ip:8080*/em

  , where *ams7.6 server ip:8080* is the Avaya Aura® MS 7.6 IP address

- http://*ams7.6 FQDN:8080*/em

  , where *ams7.6 FQDN:8080* is the Avaya Aura® MS 7.6 FQDN address

With Avaya Aura® MS 7.6 the UCM domain is no longer supported. There is no hyperlink to the Avaya Aura® MS Element Manager from CS 1000 UCM.

Central Authentication is also no longer supported. To access Avaya Aura® MS 7.6 after installation/upgrade from EM or the command line, use the local user name (admin2) and password that are created during the Avaya Aura® MS 7.6 installation process. Later, you can configure RBAC, or RBAC with SMGR to access Avaya Aura® MS 7.6 from EM using other credentials.

As part of the upgrade to Avaya Aura® MS 7.6, Avaya Aura® MS EM supports specific web browsers. For information about supported browsers, see *Unified Communication Management Fundamentals, NN43001-116*.

For more information on using EM and configuring your browser to use EM, see *Implementing and Administering Avaya Aura® MS 7.6*.

Note:

Custom application and package application are removed out of Avaya Aura® Media Server Element Manager Element Manager Release 7.6. The difference in the Avaya Aura® Media Server 7.0 and Avaya Aura® Media Server 7.6 is illustrated in the images below.

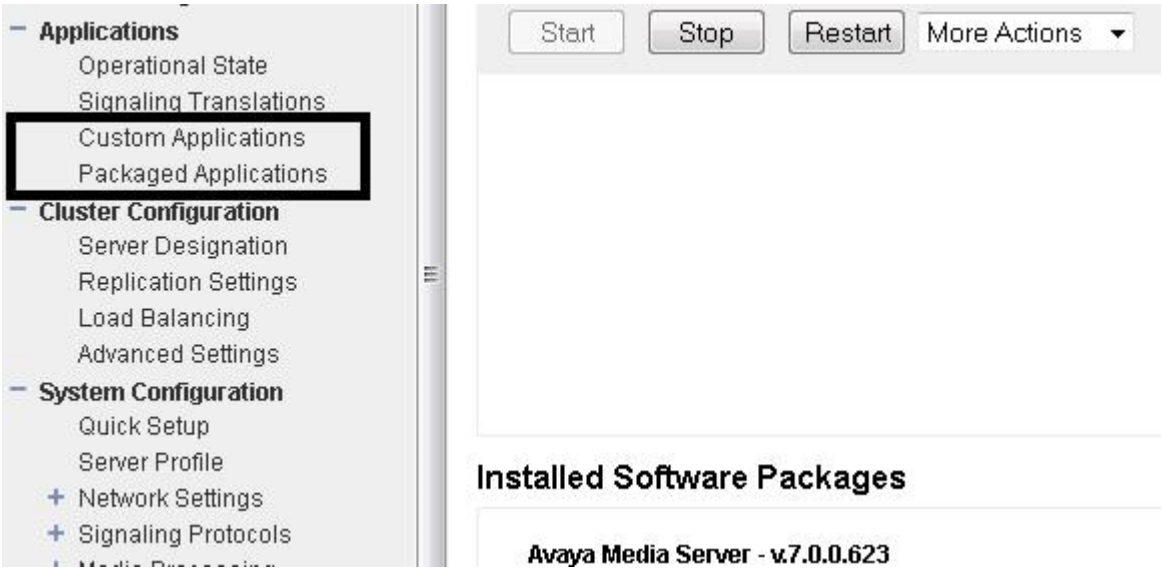


Figure 83: Avaya Aura® Media Server 7.0

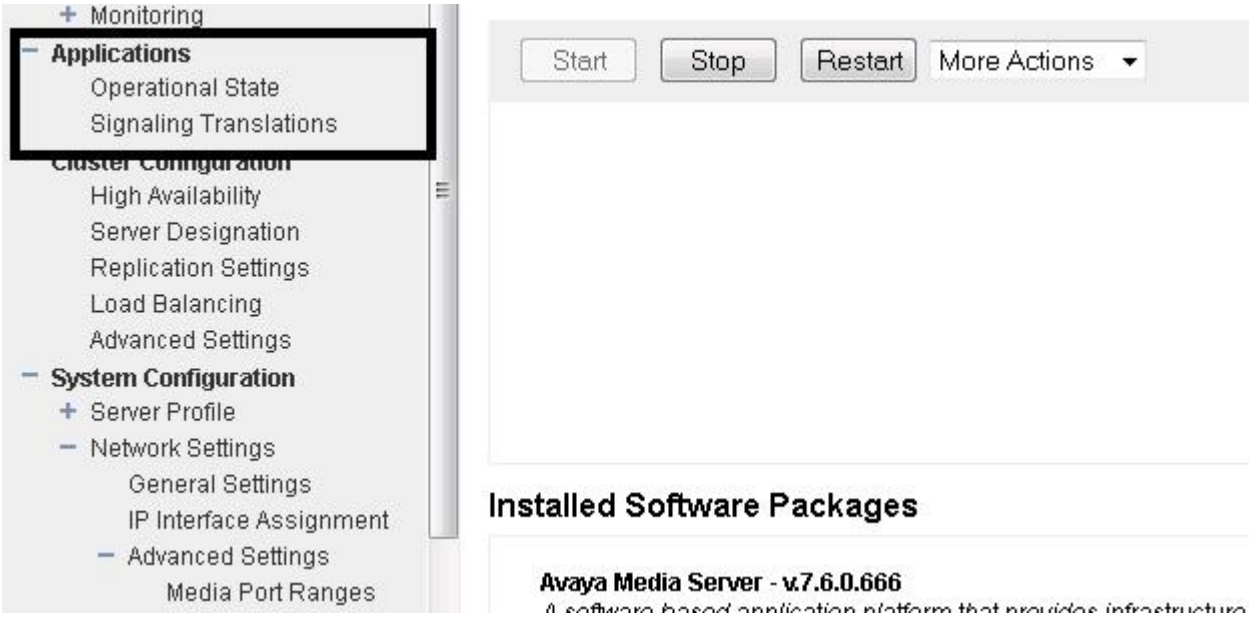


Figure 84: Avaya Aura® Media Server 7.6

Related links

[Avaya Aura MS upgrade and MAS 7.0 migration](#) on page 140
[Avaya Aura MS Element Manager login options](#) on page 151
[Avaya Aura MS Element Manager Role Based Access Control (RBAC)](#) on page 151
[Configuring the default admin password and enabling Avaya Aura MS RBAC](#) on page 152
[Avaya Aura MS Element Manager RBAC with System Manager](#) on page 153
[Using the hostconfig tool](#) on page 154
[Adding System Manager roles](#) on page 154

Avaya Aura® MS Element Manager login options

Avaya Aura® MS Element Manager offers the following options:

Login option	Description
Operating system	This option is the default option after installation, which uses the accounts of the local operating systems – admin2. This option is local and provides no RBAC support. Therefore, users will have access to all Avaya Aura® MS Element Manager tasks.
Avaya Aura® MS (Element Manager)	This option uses the Avaya Aura® MS user database, which is synchronized within the same Avaya Aura® MS cluster. This option is local to the Avaya Aura® MS and offers RBAC support. Because the user data is synchronized within the same Avaya Aura® MS cluster, you can use the same user credential to log in to another Avaya Aura® MS in the same cluster. However, Single Sign-On is not supported. **Important:** The Avaya Aura® MS user database is not synchronized with the database of Linux users. You cannot login to CLI using user accounts created in Avaya Aura® MS Element Manager.
Avaya System Manager	The option uses Avaya System Manager for authentication and authorization. Avaya System Manager is a centralized service provider. Administrators need to configure System Manager parameters and certificates first then enable this option. For the use of Avaya System Manager with Avaya Aura® MS Element Manager, see *AMS EM RBAC with SMGR FD*.

Related links

Avaya Aura MS 7.6 EM access on page 149

Avaya Aura® MS Element Manager Role Based Access Control (RBAC)

Avaya Aura® MS 7.6 is no longer part of the CS 1000 UCM domain; therefore it cannot use any of the configured roles and users from UCM. This functionality has been replaced with Role Based Access Control (RBAC).

RBAC is a common approach to managing system access or resource access for authorized users. You can create and manage roles for each job function. The permissions for specific job functions are assigned to the roles. Users get access permissions to job functions through appropriate role

assignments. Use of RBAC simplifies the management of user access control based on roles of job functions instead of individual permissions.

Avaya Aura® MS Element Manager RBAC implementation is for Avaya Aura® Media Server only. So, the permission set contains only permissions for Avaya Aura® MS Element Manager. Each role will have the same set of Avaya Aura® MS Element Manager permissions. You can configure the permission level of each permission for a role, except the default role.

Avaya Aura® MS Element Manager RBAC support includes one default administrator, with administrator id admin, and one default role called System Administrator. You cannot change or delete the default administrator admin and the default role System Administrator.Avaya Aura® MS Element Manager RBAC implementation is only for Avaya Aura® Media Server. The permission set only affects the permissions for Avaya Aura® MS Element Manager. For mostCS 1000 customers, the default user accounts are sufficient to manage their Avaya Aura® MS installation. However you can define your own users and roles for Avaya Aura® MS.

Each role will have the same set of Avaya Aura® MS Element Manager Permissions. You can configure the permission level for every role, except the default role.

You can use one of the following permission levels:

- Deny: use this permission level to deny access to the associated resource
- View: use this permission level to permit read-only access to the associated resource
- Modify: use this permission level to permit users to access and change the associated resource

Related links

Avaya Aura MS 7.6 EM access on page 149

Configuring the default admin password and enabling Avaya Aura® MS RBAC

Procedure

1. Select **Account Management** > **Administrators** > **Edit Administrator**
2. Select the default administrator, and click **Edit**.
3. Enter a password that meets the password policy requirements, and click **Save**.
4. Select **Account Management** > **Policies**
5. In the **Authentication and authorization source** field, click **Avaya Media Server**.

   For more information about this procedure, see *Implementing and Administering Avaya Aura® Media Server 7.6*.

Related links

Avaya Aura MS 7.6 EM access on page 149

Avaya Aura® MS Element Manager RBAC with System Manager

Avaya Aura® MS Element Manager RBAC is fully integrated with the Avaya System Manager. When Avaya Aura® MS Element Manager uses the Avaya System Manager for authentication (Single Sign-On, SSO) and authorization (RBAC), the users and roles are defined in the System Manager instead of Avaya Aura® MS Element Manager.

System Manager provides centralized RBAC to manage the level of access that the system grants to authorized administrators. RBAC simplifies permission management by assigning permissions to reusable roles instead of individual administrators. The System Manager authentication supports Single Sign-On (SSO).

To use RBAC, you must create roles for each job function, define the permission level for each EM task in a role, and then assign roles that match the job function requirements of each administrator.

System Manager includes one default administrator with the name admin, and with the default role of System Administrator. The default administrator has full access to all levels of Avaya Aura® MS EM tasks. When using System Manager for authentication and authorization, administrators, roles, and permissions can be configured only on System Manager.

If you want to use System Manager with Avaya Aura® MS, you must set up a mutual authentication between the servers. To use System Manager RBAC and SSO, after setting up mutual authentication, you must select Avaya System Manager as the authentication and authorization source.

For System Manager related parameters, you have to set up mutual authentication only on an Avaya Aura® MS Primary server in cluster. Non-Primary Avaya Aura® MS servers get the configuration update from their corresponding Avaya Aura® MS Primary server.

For certificate configuration, you have to set up mutual authentication for any Avaya Aura® MS server in cluster that uses System Manager for RBAC

Important:

To properly use RBAC with Avaya System Manager, you must configure the Fully Qualified Domain Name (FQDN) of System Manager and Avaya Aura® MS servers properly, either in the Domain Name Service (DNS) or the local hosts file. In Avaya Aura® MS server, you can use the **`hostconfig`** tool. For more information, see *Using the hostconfig tool*.

For information about System Manager configuration, please see the corresponding System Manager documentation.

Avaya Aura® MS registers to System Manager RBAC as an element of the type Avaya Aura® Media Server.

Avaya Aura® MS defines the permission levels as follows:

- Deny: use this permission level to deny access to the associated source
- View: use this permission level to permit read-only access to the associated resource
- Modify: use this permission level to permit users to access and change the associated resource

The Avaya Aura® MS element type definition for System Manager contains the permission settings for Avaya Aura® MS Element Manager and the associated default roles. All Avaya Aura® MS permissions with the System Manager default role System Administrator are at the modify level.

If System Manager is configured and enabled but unavailable, administrators can use the login credential of the server operating system (admin2) to go to Avaya Aura® MS Element Manager. In such situations, administrators can use the Avaya Aura® MS Element Manager emergency login URL: https://AMS_SERVER_FQDN:8443/emlogin

For more information, see *Implementing and Administering Avaya Aura® Media Server 7.6*.

Related links

Avaya Aura MS 7.6 EM access on page 149

Using the hostconfig tool

You can use the **hostconfig** tool in the following ways:

hostconfig [-h, --help]

hostconfig [add [-ip *ip*] [-host *hostname*] [-domain *domain*]]

hostconfig [add [-ip *ip*] [-fqdn *fqdn*]]

hostconfig [del [-ip *ip*] [-host *hostname*] [-domain *domain*]]

hostconfig [del [-ip *ip*] [-fqdn *fqdn*]]

hostconfig [del [index number]]

hostconfig [show [-long]]

Related links

Avaya Aura MS 7.6 EM access on page 149

Adding System Manager roles

Procedure

1. Log in to the System Manager with which Avaya Aura® Media Server is associated.
2. In the **Users** section, click the **Administrators** link.
3. On the navigation pane in the Administrative Users page, click the **Roles** link.
4. On the Role Management page, click **Add**.
5. On Add New Role page, enter the role name and role description.
6. After entering data, click **Commit and Continue**.
7. On the Role Details page, click the **Element/Service Permissions** tab.

8. Set permissions by element or resource type and click **Add Mapping**.
9. On the Select Element and/or Network Service to Map to Role page, click the applicable element or service type from the **Element or Resource Type** drop-down menu.
10. Click a specific element or resource instance from the **Element or Resource Instance** drop-down menu and click **Next**.

    Alternatively, to copy all permissions from an existing role, click **Copy All From**. On the Permission Mapping page, select the role to copy from, and click **Copy**.

    Note:

    You should have copy permissions to the role from which you want to copy permission mapping. For example, you cannot copy permissions from the System Administrator role.

    To delete permission mapping to a role, select a mapping name and click **Delete Mapping**.

    To edit permission mapping for a role, click the name link of the permission mapping.
11. On the Role Details page, click the **Assigned Users** tab.
12. Perform one of the following steps:
    - To copy all assignments from an existing role, click **Copy All From**. On Copy User Assignment page, select the role to copy from and click **Copy** button.
    - To add users individually, click **Select Users**. On the Assigned Users page, select the users to which you want to assign the role and click **Commit**.
    - To remove a user from the role, click **Select Users**. On the Assigned Users page, deselect the users to which you do not want to assign the role, and click **Commit**.
13. After permission mapping and user assignment, click **Commit** to save the changes.

    The newly added role appears in the table of roles.

Related links

Avaya Aura MS 7.6 EM access on page 149

Content Store data replication between clusters

With Content Store replication, you can replicate data not only within a cluster, but across clusters. You can migrate the Content Store from one cluster to another.

Content Store replication is a one way data copy from a master cluster to a replica cluster. The master cluster can have up to four directly connected replica clusters. You can create chains of replica clusters, thereby creating hierarchies that scale to greater than four replica clusters in the network. In these cascading hierarchies, intermediate replica clusters act as master clusters for replica clusters further down the hierarchy.

For more information, see *Replication of Content Store data between clusters* in *Implementing and Administering Avaya Aura® Media Server 7.6*.

Note:

The cluster size should be limited to (3+1) which will permit allocation for 3000 licenses.

Related links

Avaya Aura MS upgrade and MAS 7.0 migration on page 140

Changing Avaya Aura® MS server IP address and host name

Before you begin

Stop Avaya Aura® MS before changing the IP address.

About this task

Important:

You must restart the server during IP address change operation.

Procedure

1. Login to CLI using the admin2 account.
2. To change the IP address and host name of the server, use the **`baseparamsconfig`** command.
3. Login to EM using the new ip address in the Element Manager login URL.
4. Click **EM** > **System Configuration** > **Network Settings** > **IP Interface Assignment**.

   Because of the IP address change, **IP Interface Assignment** fields show errors.
5. Select valid IP addresses from the drop-down menus for each field showing Invalid.
6. Click **Save**.
7. Click **Confirm**.

   If this is a Primary server of a master cluster, update the replication clusters, which point to the master cluster, with the new address of this server.
8. On the Primary node in each replication cluster, click **EM** > **Cluster Configuration** > **Replication Settings** > **Master Cluster Primary Node Address**.

Related links

Avaya Aura MS upgrade and MAS 7.0 migration on page 140

License server

License Server provides licensing for both cluster and standalone server configurations. In a cluster, the License Servers reside only on the Primary and Secondary servers in the cluster. All nodes in a cluster share a single license key.

You can check the status of the license server in Avaya Aura® MS EM.

For more information, see *License configuration* in *Implementing and Administering Avaya Aura® Media Server 7.6*.

Related links

Avaya Aura MS upgrade and MAS 7.0 migration on page 140

Avaya Aura® MS 7.6 EM certificate management

Certificates are used to establish a trust relationship between two parties.

In the CS 1000 environment, certificates are used to support SSL, which allows for Web interfacing, and also for TLS, which is used for secure SIP signaling. Certificate authorities provide certificates. Certificates can also be self-signed. A CA is either a private certificate authority or a public certificate authority such as VeriSign or Thawte.

You can go to Certificate Management from **AMS EM** > **Security** > **Certificate Management**. For more information about Certificate management, see *Configuration, Security configuration* in *Implementing and Administering Avaya Media Server 7.6*.

Related links

Avaya Aura MS upgrade and MAS 7.0 migration on page 140

Get Certificates from System Manager

Downloading System Manager Certificate Authority certificate

Procedure

1. Log on to the System Manager that Avaya Aura® Media Server Element Manager will use.
2. In the services section, click the **Security** link.
3. Click **Security** > **Certificates** > **Authority**
4. Click the **Download pem file** link.
5. When prompted, save the System Manager Certificate Authority certificate locally.

   Each Avaya System Manager has its own Certificate Authority certificate. to You might have to start the setup process again while changing the System Manager server.

Related links

Avaya Aura MS 7.6 EM certificate management on page 157

Creating a certificate signed by System Manager

Procedure

1. Log on to the System Manager that the Avaya Aura® MS Element Manager will use.
2. In the **Services** section, click the **Security** link.
3. From the navigation link, go to **Security** > **Certificates** > **Authority**
4. Click **Add End Entity**.
5. On the Add End Entity page, select **INBOUND_OUTBOUND_TLS** from the **End Entity Profile** drop-down menu.
6. Enter a unique user name, such as the server name, to identify the each Avaya Aura® MS server.
7. Enter a password.

   This user name and password will be used to retrieve the End Entity Certificate.
8. Enter the FQDN of the corresponding AMS server in the **Common Name** field.
9. Enter the full name of the state or province in the **State/Province** field.

   Do not use abbreviations.
10. Enter a two-letter country code in the **Country Code** field.
11. Select **ID_CLIENT_SERVER** from the **Certificate Profile** drop-down menu.
12. Select the correct certificate authority from the **CA** field.

    The System Manager default CA is tmdefaultca.
13. Click **Add End Entity** after entering relevant data.
14. Select **Security** > **Certificate** > **Authority**
15. Click **Public Web** at the bottom of the navigation page to access the EJBCA page.
16. On the EJBCA page, click **Create Keystore**.
17. Enter the user name and password that you used while adding the end entity.
18. On the EJBCA Token Certificate Enrollment page, make sure the Certificate profile is **ID_CLIENT_SERVER**.

    You can use either 1024 or 2048 for Key length.
19. Click **OK** to download the certificate for Avaya Aura® MS Element Manager.

Related links

Avaya Aura MS 7.6 EM certificate management on page 157

Import System Manager Certificates into AMS Element Manager

Import System Manager certificate authority Certificate

Procedure

1. Log in to Avaya Aura® MS Element Manager.
2. Go to **Security** > **Certificate Management** > **Trust Store**.
3. Click **Import**.
4. Set **Trust friendly name** and browse to the System Manager CA certificate file from your local computer.
5. Click **Save** to upload and save the certificate into AMS trust store.

Related links

Avaya Aura MS 7.6 EM certificate management on page 157

Import the System Manager-Signed Certificate for Avaya Aura® MS Element Manager

Procedure

1. Log in to Avaya Aura® MS Element Manager.
2. Go to **Security** > **Certificate Management** > **Key Store**.
3. Select the Service profile EM and click **Edit**.
4. On Edit Service Profile page, click **Import**.
5. Enter the password when you create the certificate through EJBCA and browse to the EJBCA-created certificate file from your local computer.
6. T upload and save the certificate for the EM service profile, click **Save**.
7. On Edit Service Profile Confirmation page, click **Confirm** to proceed.

Note:

The Tomcat instance running Avaya Aura® MS Element Manager restarts after the certificate import. You have to close the browser, open another browser, and log back in to Avaya Aura® MS Element Manager again.

Related links

Avaya Aura MS 7.6 EM certificate management on page 157

Media port management

Avaya Aura® MS 7.6, provides Port Management Facility for more effective management of the common port resource pool.

This feature provides:

- Simplified port configuration
- Reduced port footprint
- Support for common high availability port checkpointing
- Elimination of multiple incompatible component-level port management strategies

All Avaya Aura® MS media processors must use the Port Management Facility to minimize the network port footprint of the server.

Avaya Aura® MS EM is used to provide Media Port management. You can use the default port settings if there are no other special requirements

For more information, see *Network settings configuration, Changing media port ranges* in *Implementing and Administering Avaya Aura® Media Server 7.6*.

Related links

Avaya Aura MS upgrade and MAS 7.0 migration on page 140

Chapter 11: Base Manager

This chapter contains information and procedures for managing specific network servers on an individual basis using Base Manager. References to the various Element Manager, Network Routing Service Manager, and Patching Manager documentation are provided. IPv6 is supported for Base Manager.

Use Base Manager to manage the base system in the following functional areas:

- Base System
  - Networking (Network Identity, DNS and Hosts, Route Table).
  - Explicit Congestion Notification
  - Date and Time
  - SSH Keys
- Software
  - Applications
  - Deployment (See Deployment Manager—New system installation and commissioning on page 68)
  - Patches
- Tools
  - Logs

Note:

The server must be part of the security domain before you can perform Base Manager configuration procedures through UCM. For more details about UCM configuration of the primary, backup, and member servers, see *Avaya Unified Communications Management Common Services Fundamentals, NN43001-116*. For more information about security management, see *Avaya Security Management Fundamentals, NN43001-604*.

Navigation

- Accessing Base Manager through UCM on page 162
- Accessing Base Manager through local logon on page 164
- Deploying software in local login mode on page 165
- Undeploying software in local login mode on page 166

- Rebooting the server on page 166
- Base system configuration using Base Manager on page 167
- Regenerating SSH Keys for a UCM Member server on page 188
- Software maintenance using Base Manager on page 190
- View and export logs using Base Manager on page 191

Accessing Base Manager through UCM

Perform the following procedure to access to Base Manager through UCM.

1. Open the Web browser.

   Note:

   For information about supported browsers, logging on to UCM Common Services, logging on to Element Manager, and configuring the UCM Common Services framework, see *Unified Communication Management Fundamentals, NN43001-116*.

2. Enter one of the following in the Address bar, and then press `Enter`:

   - Unified Communications Management (UCM) framework IP address. After you enter the UCM framework IP address, a Web page appears stating that you must access Unified Communications Management by using the Fully Qualified Domain Name (FQDN) for the UCM server. Click the link on this Web page to use the FQDN for the UCM server.
   - FQDN for the UCM server.

3. Click **OK** or **Yes** to accept the security windows that appear.

   The UCM Login Web page appears.

4. In the **User ID** field, enter your user id.
5. In the **Password** field, enter your password.
6. Click **Log In**.

   The UCM default navigation screen appears, as shown in the following figure.

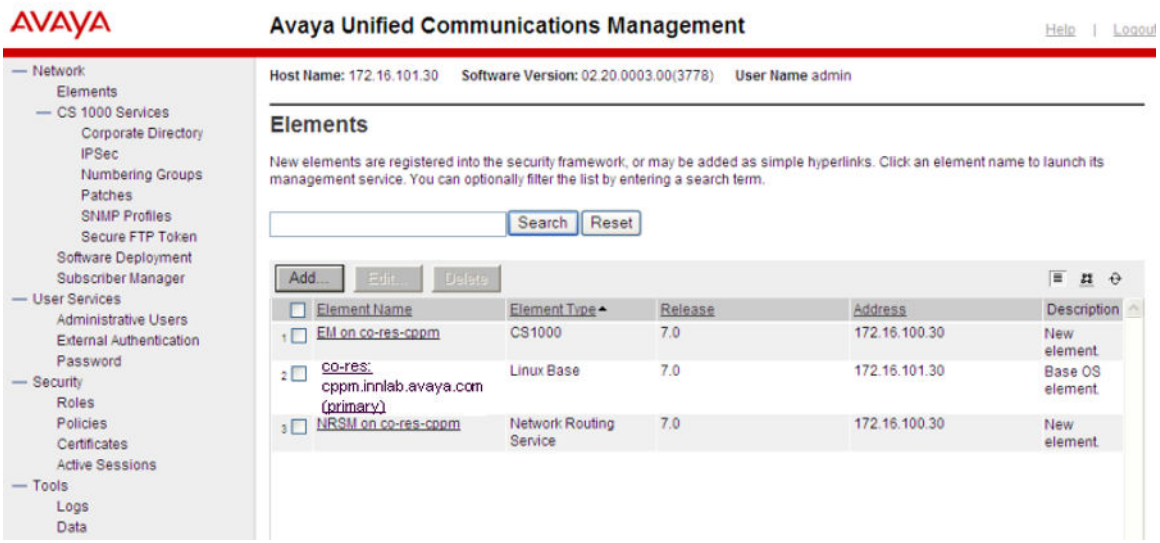


Figure 85: UCM default navigation window

7. On the Elements page of Unified Communications Management, under the **Element Name** column, click on an element of type Linux Base to navigate to Base Manager for that element.

   The Base Overview page appears, as shown in the following figure.

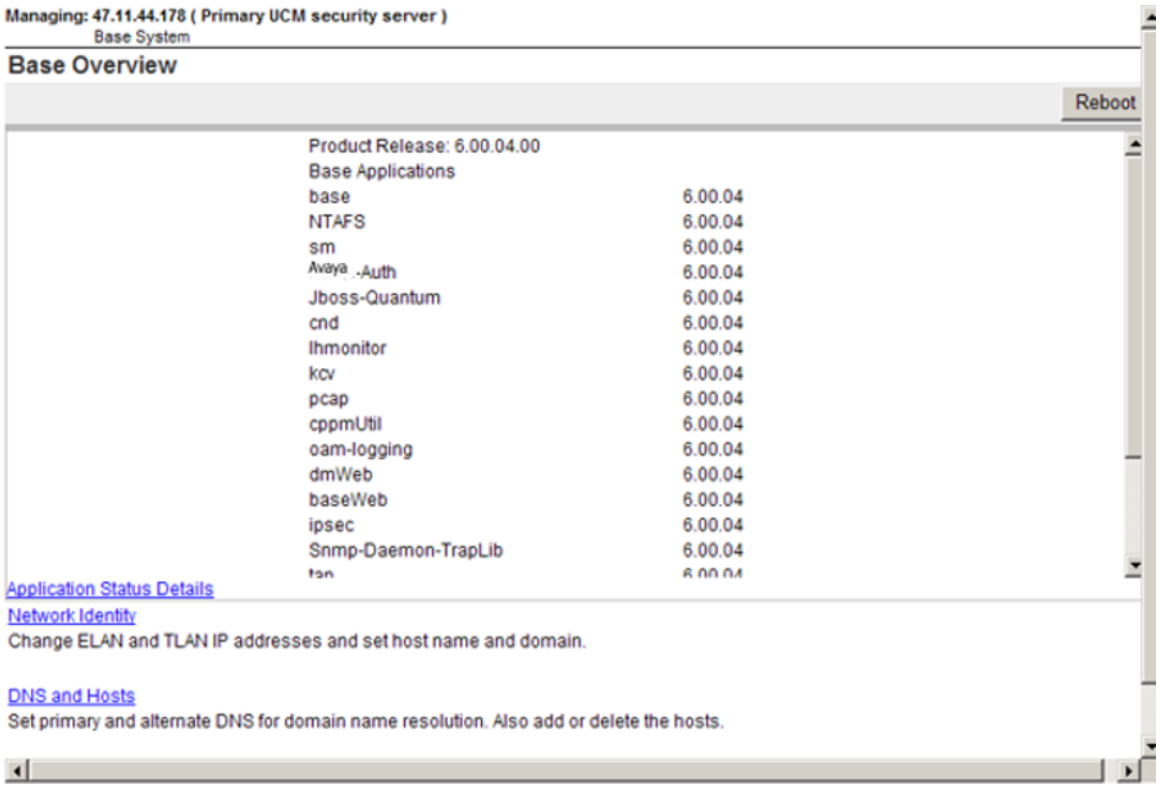


Figure 86: Base Overview window

Accessing Base Manager through local logon

Perform the following procedure to log on to the server locally and access Base Manager.

1. Open the Web browser.

   Note:

   For information about supported browsers, see *Unified Communication Management Fundamentals, NN43001-116*.

2. Enter the following in the Address bar: `http://<FQDN>/local-login`

   The Server logon screen appears, as shown in the following figure.

Figure 87: Server logon window

3. In the **User ID** type, admin2.

   Note:

   You must use the admin2 account to log on to the server locally.

4. In the **Password** field, type the password.
5. Click **Log In**.

   The Security Configuration screen appears, as shown in the following figure.

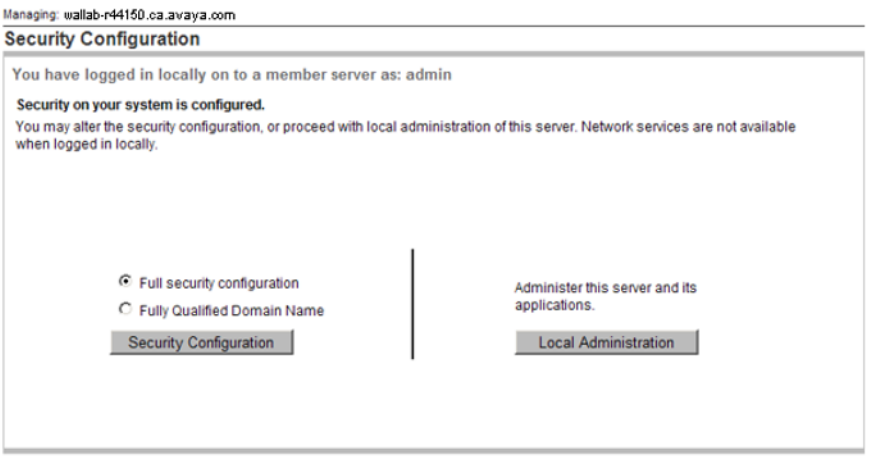


Figure 88: Security Configuration window

6. Click **Local Administration**.

   Base Manager opens and the Base Overview screen appears, as shown in the following figure.

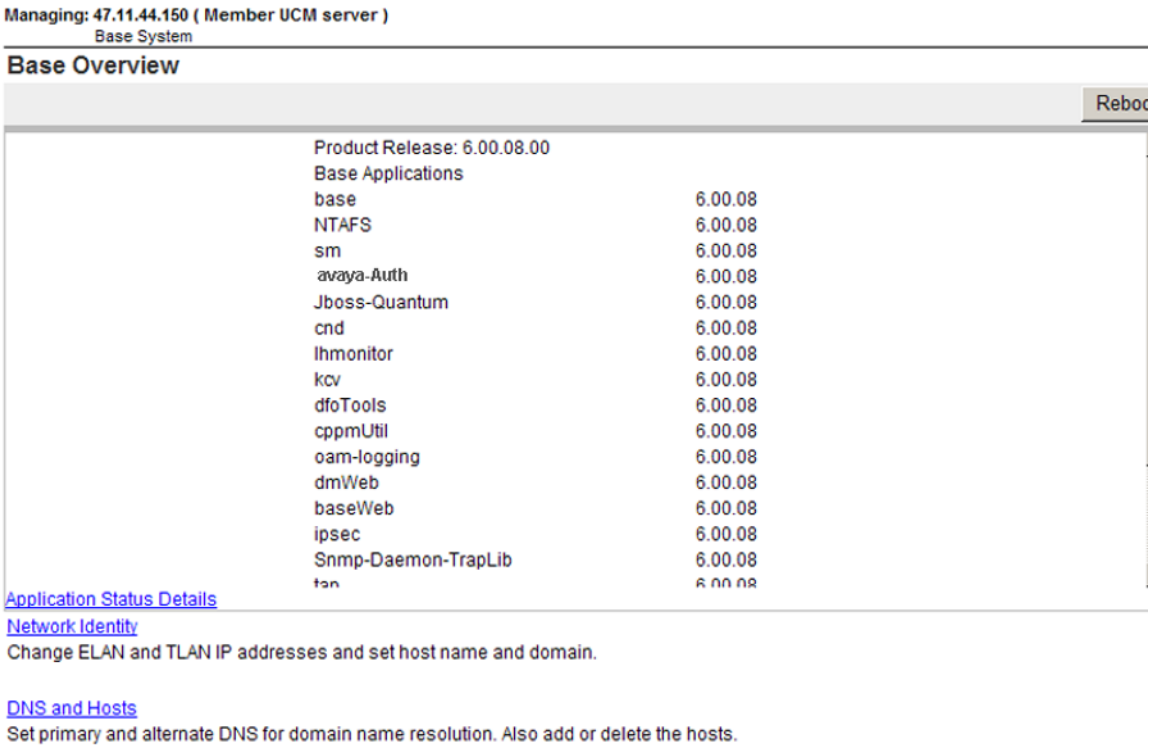


Figure 89: Base Overview window

Deploying software in local login mode

Prerequisite:

- Upload the appropriate .nai file (Avaya Communication Server 1000 or Avaya Aura® MS) from the software download site to the server running the local Deployment Manager. The .nai distribution can be loaded from the local server using a USB or CF device (as appropriate) or from the client PC connected to the server.

Procedure steps:

Use local login to deploy software.

1. Follow the procedures in Accessing Base Manager through local logon on page 164.
2. From the navigation pane, click **Software Deployment**.

   The Deployment Targets page appears.
3. Select the hostname and click **Deploy**.

Note:

Previously deployed software must first be undeployed.

4. Select the check box beside the deployment package you want to **Deploy**.
5. To allocate the target servers to a group, proceed to Step 7 on page 75 in Preconfiguring process using Deployment View on page 74.

Note:

Servers that are deployed with applications but are not configured into systems are represented in blue in Deployment Manager

Undeploying software in local login mode

Prerequisite:

- The application .nai file must first be uploaded.

Procedure steps:

Use the following procedure to undeploy a software package.

1. Follow the procedures in Accessing Base Manager through local logon on page 164.
2. From the navigation pane, click **Software Deployment**.

   The Deployment Targets page appears.
3. Select a hostname and click **Deploy**.
4. Click **Undeploy**.

Rebooting the server

Some procedures require a server reboot for configuration changes to take effect. Perform the following procedures to reboot the server.

1. Log on to UCM and navigate to Base Manager. See Accessing Base Manager through UCM on page 162.
2. Press **Reboot**.

   Note:

   You must have a user role of System Administrator to reboot the server. If you do not have a user role of System Administrator, the Reboot button is not active.

   A confirmation screen appears, as shown in the following figure.

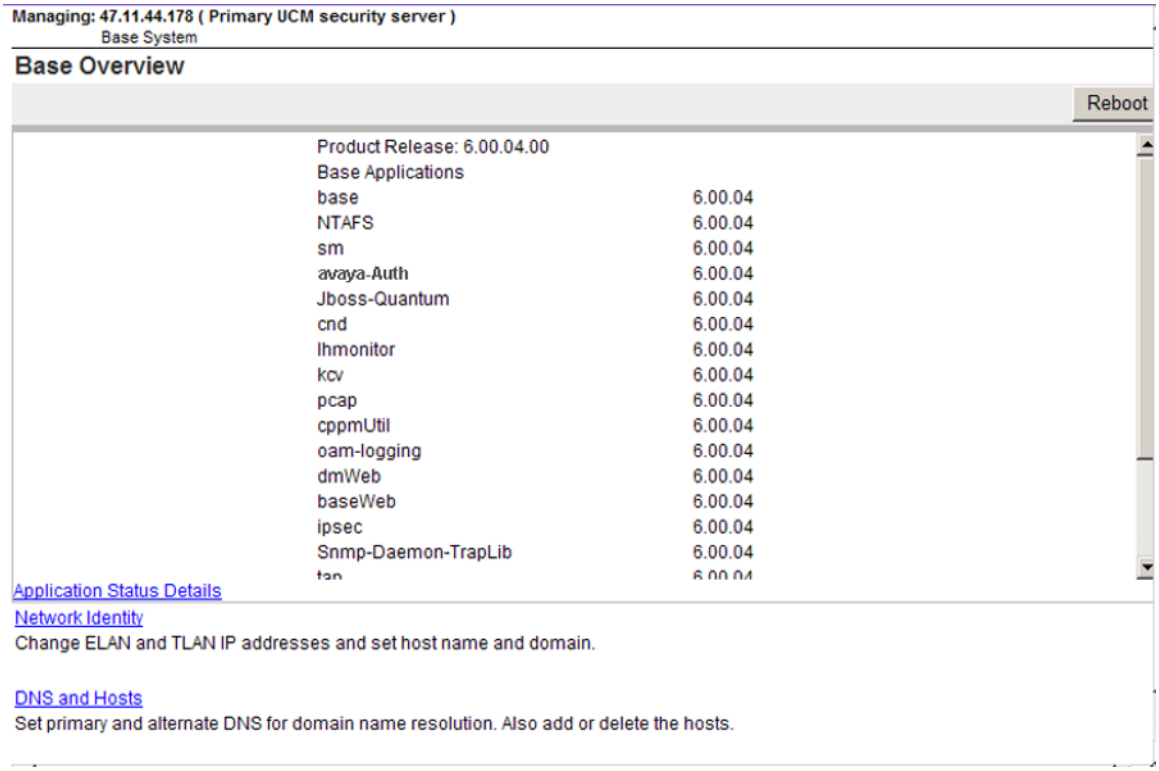


Figure 90: Reboot confirmation window

3. Press **OK** to confirm the server restart.

Base system configuration using Base Manager

You can configure networking values by using Base Manager. You can alter Telephony LAN (TLAN) and Embedded LAN (ELAN) values to edit the network identity, or add or delete hosts. You can add or delete routes to update route tables.

Use Base Manager to configure date and time values. Set system values or configure automatic date and time values using network time servers.

You can also use Base Manager to enable or disable Explicit Congestion Notification (ECN).

Editing network identity for a Member server

Perform the following procedure to manually edit values for ELAN and TLAN.

Important:

You cannot change the FQDN or host name of the primary or backup server using Base Manager. For information about changing FQDN of the primary or backup security servers, see Change the FQDN of a Primary or Backup Security Server on page 295.

Note:

After you edit the network identity, you must manually restart the server for the changes to take effect.

Procedure steps:

1. Log on to UCM and navigate to Base Manager. For details about logging on to UCM and accessing Base Manager, see Accessing Base Manager through UCM on page 162.

   OR

   Log on to the target server locally and navigate to Base Manager. For details about logging on to the target server locally and accessing Base Manager, see Accessing Base Manager through local logon on page 164.

   Note:

   NTP configuration can be done from both Base Manager (BM) and EM. NTP configuration using BM applies to the local Linux server. For that particular server, you can synchronize date and time with the Primary NTP Server after getting the settings from an external NTP source (third party clock source). However, when you apply NTP configuration from EM, you push the same configuration to all members of the security domain. EM transactions override all previous configurations for each Linux server that is a member of the security domain.

2. In the navigation pane, select **Networking**.

   The Networking screen appears, as shown in the following figure.

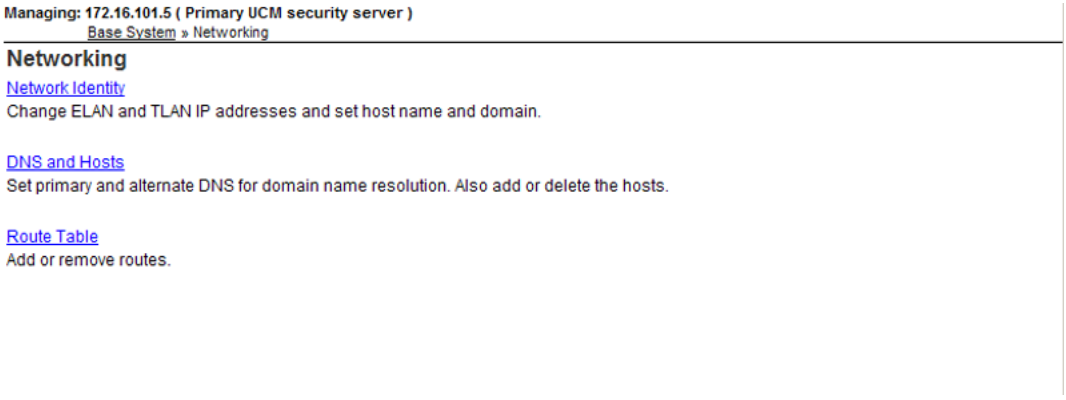


Figure 91: Networking window

3. In the Networking screen, click **Network Identity**.

   The Network Identity screen appears, as shown in the following figure.

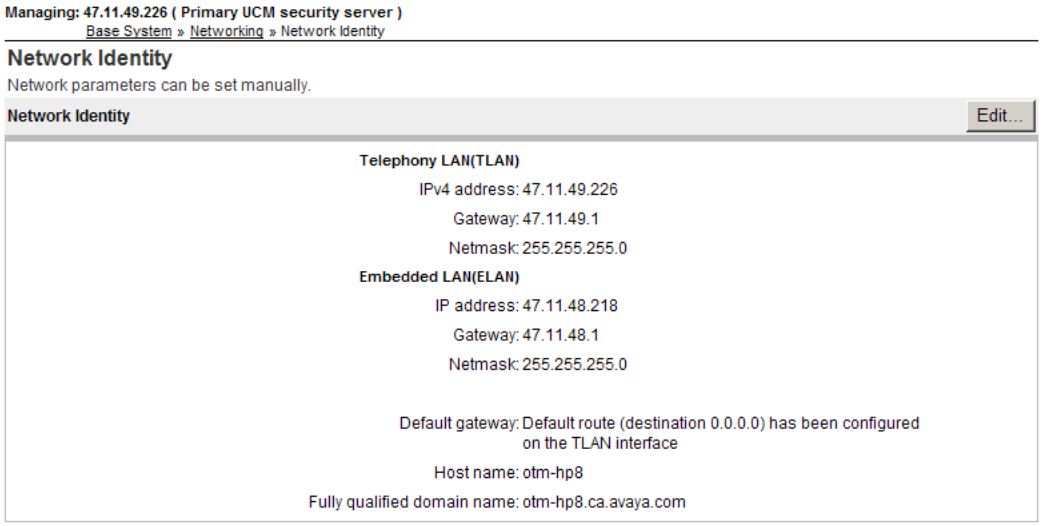


Figure 92: Network Identity window

Note:

If the TLAN IP address is not the default gateway value, a warning appears that indicates that the default gateway value is an IP address other than the TLAN IP address.

4. Click **Edit**.

   The Edit Network Identity screen appears, as shown in the following figure.

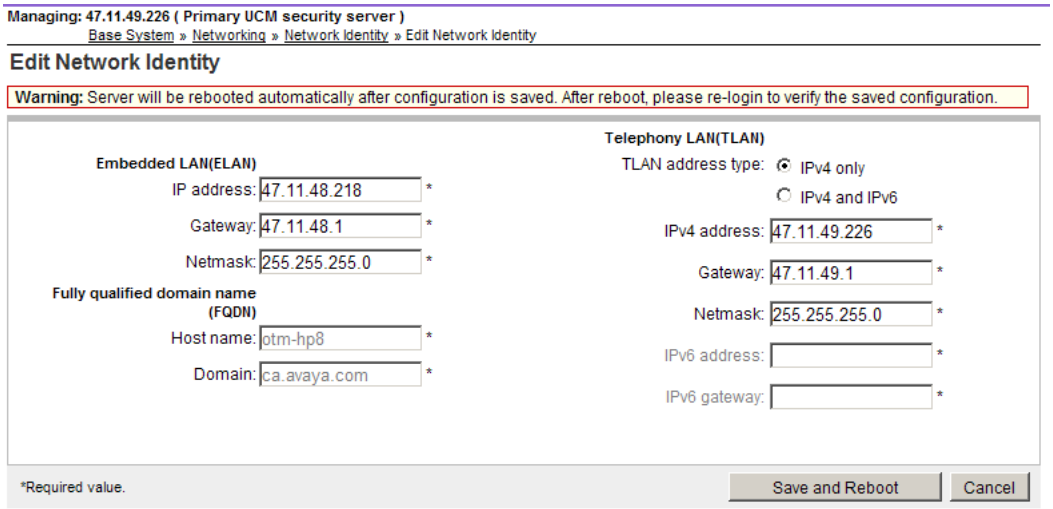


Figure 93: Edit Network Identity window

5. In the **Embedded LAN (ELAN)** section, complete the following:
   - **IP address:** enter a value for the ELAN IP address.
   - **Gateway:** enter a value for ELAN gateway.
   - **Netmask:** enter a value for ELAN netmask.

6. In the **Fully Quality Domain Name (FQDN)** section, complete the following:
   - **Host name:** enter a value for host name.
   - **Domain:** enter a domain value.
7. **Telephony LAN (TLAN)** section, complete the following:
   - **TLAN address type:** click **IPv4 only** or **IPv4 and IPv6**.
   - **IPv4 address:** enter a value.
   - **Gateway** enter a value for TLAN gateway.
   - **Netmask** enter a value for TLAN netmask.

   If you selected IPv4 and IPv6 as the TLAN address type, complete the following two fields:
   - **IPv6 address:** enter a value for the IPv6 address.
   - **IPv6 gateway:** enter a value for the IPv6 gateway.
8. Click **Save and reboot** to save your configuration changes and restart the server. After restarting, log on to verify the saved configuration.

   OR

   Press **Cancel** to discard your changes and return to the Network Identity screen.

DNS and Hosts

Perform the following procedures to add a new host and to remove an existing host.

Adding a host

Perform the following procedure to add a host value to the host table.

1. Log on to UCM and navigate to Base Manager. For details about logging on to UCM and accessing Base Manager, see Accessing Base Manager through UCM on page 162.

   OR

   Log on to the target server locally and navigate to Base Manager. For details about logging on to the target server locally and accessing Base Manager, see Accessing Base Manager through local logon on page 164.
2. In the navigation pane, select **Networking**.

   The Networking screen appears, as shown in the following figure.

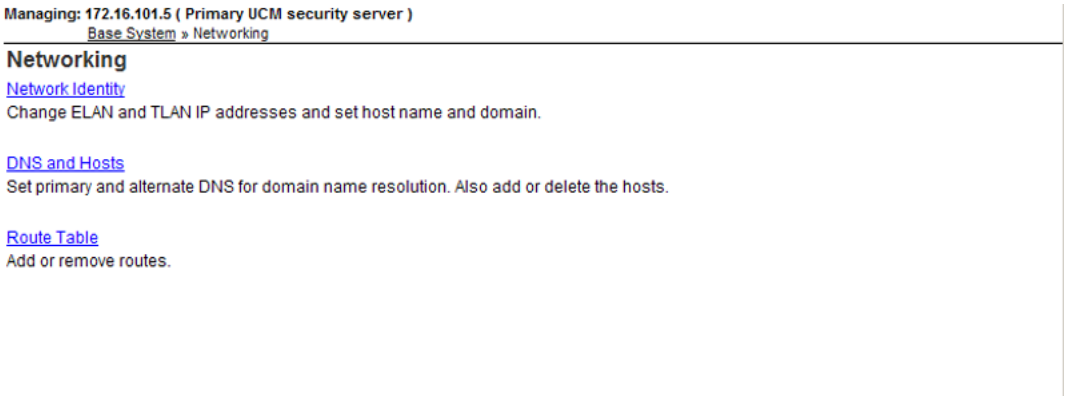


Figure 94: Networking window

3. In the Networking screen, select **DNS and Hosts**.

   The Domain Name Server (DNS) screen appears, as shown in the following figure.

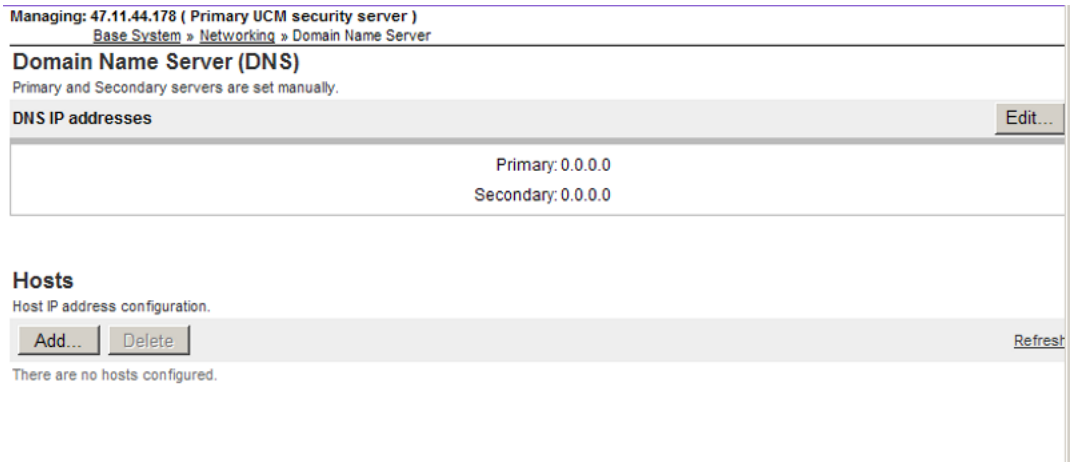


Figure 95: Domain Name Server (DNS) window

4. Click **Add**.

   The New Host screen appears, as shown in the following figure.

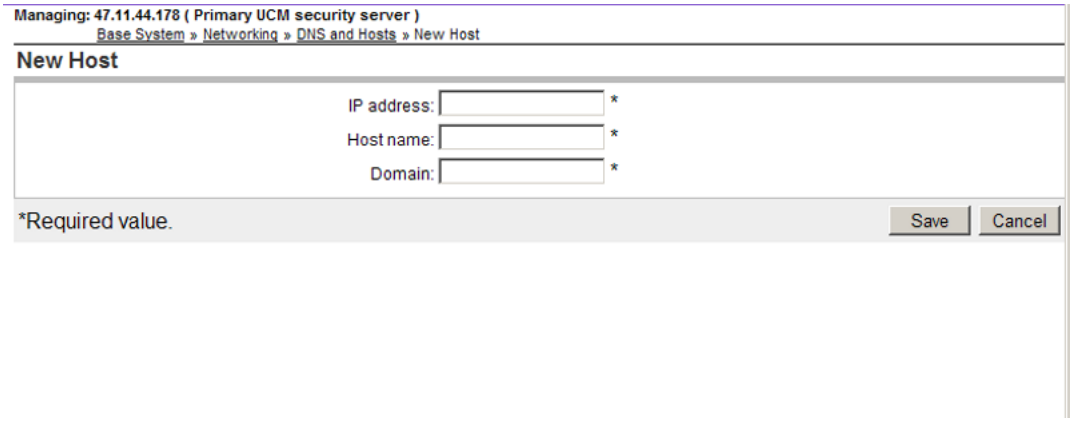


Figure 96: New Host window

5. In the **IP address** field, enter a value for IP address.
6. In the **Host name** field, enter a value for host name.
7. In the **Domain** field, enter a value for Domain.
8. Click **Save**.

   The Domain Name Server (DNS) screen displays the new host, as shown in the following figure.

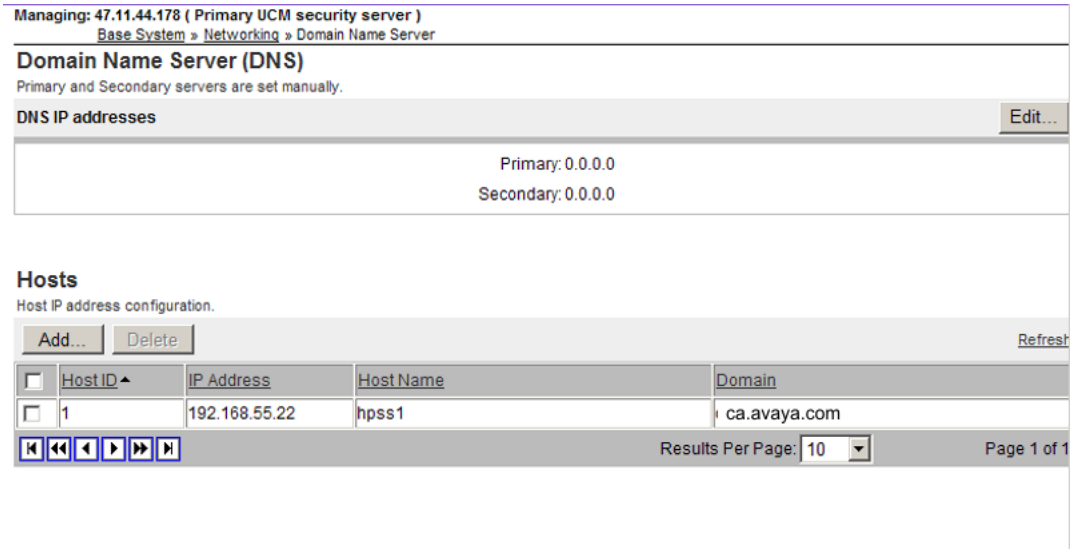


Figure 97: Domain Name Server (DNS) host added

Deleting a host

Perform the following procedure to delete a host value from the host table.

1. Log on to UCM and navigate to Base Manager. For details about logging on to UCM and accessing Base Manager, see Accessing Base Manager through UCM on page 162.

   OR

   Log on to the target server locally and navigate to Base Manager. For details about logging on to the target server locally and accessing Base Manager, see Accessing Base Manager through local logon on page 164.

2. In the navigation pane, select **Networking**.

   The Networking screen appears, as shown in the following figure.

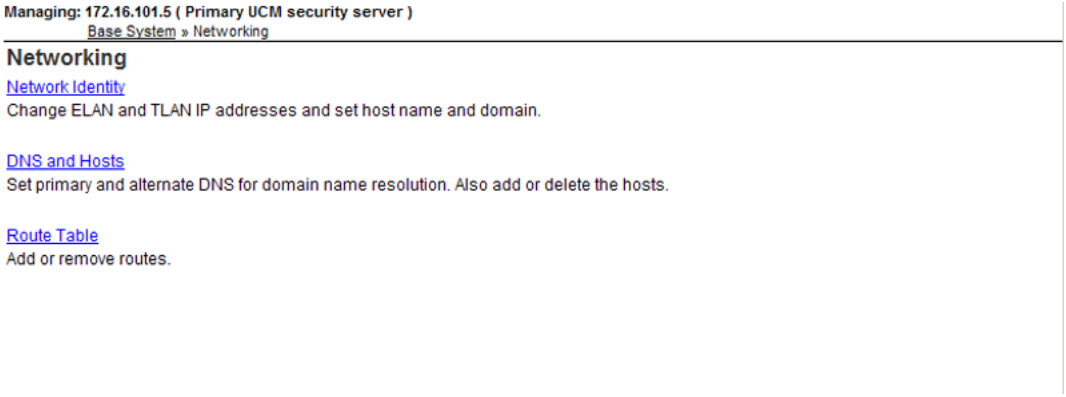


Figure 98: Networking window

3. In the Networking screen, select **DNS and Hosts**.

   The Domain Name Server (DNS) screen appears, as shown in the following figure.

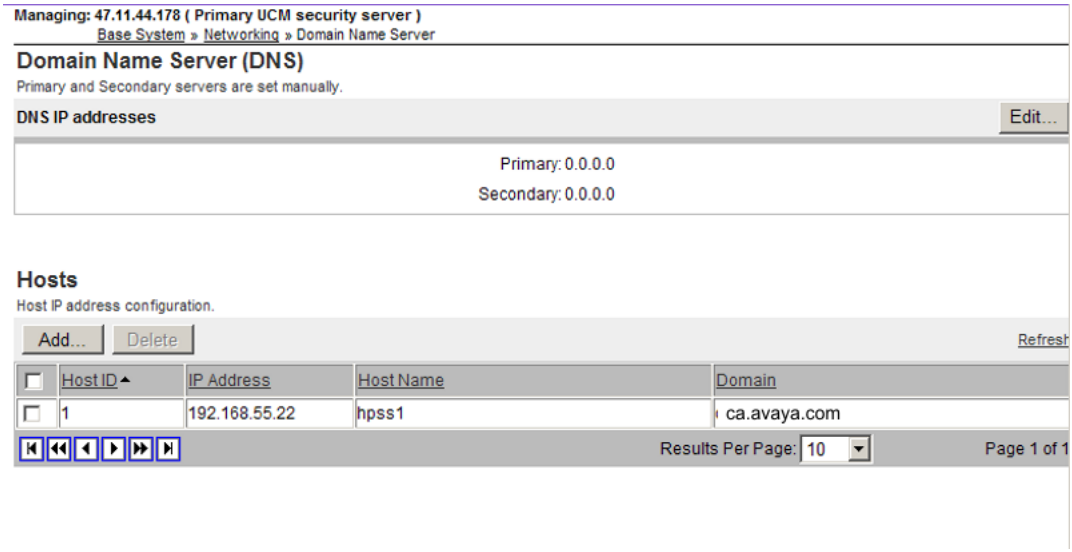


Figure 99: Domain Name Server (DNS) window

4. Select the host that you want to delete.

   The Delete button becomes active.

5. Click **Delete**.

   The Domain Name Server (DNS) screen appears and the host is removed, as shown in the following figure.

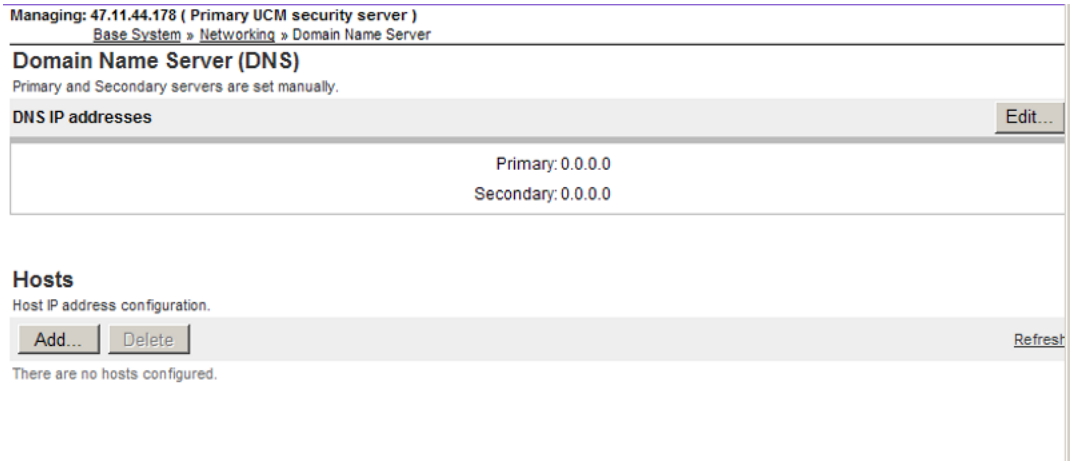


Figure 100: Domain Name Server (DNS) host removed

Adding a route entry

Deleting a route entry

Perform the following to delete an entry from the routing table.

Note:

All routes configured in Base Manager have a Tag value of Manual. Routes with other Tag values are inserted by applications; these routes should only be modified or deleted by configuring the application. Do not use Base Manager to delete a route inserted by an application; this can lead to a malfunction in the application.

Procedure steps:

1. Log on to UCM and navigate to Base Manager. For details about logging on to UCM and accessing Base Manager, see Accessing Base Manager through UCM on page 162.

   OR

   Log on to the target server locally and navigate to Base Manager. For details about logging on to the target server locally and accessing Base Manager, see Accessing Base Manager through local logon on page 164.

2. In the navigation pane, select **Networking**.

   The Networking screen appears, as shown in the following figure.

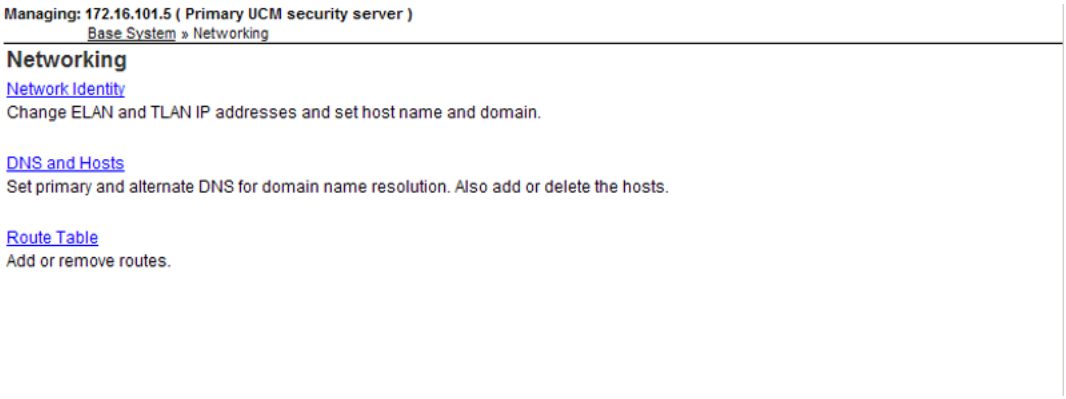


Figure 101: Networking window

3. In the Networking screen, select **Route Table**.

   The Routes screen appears, as shown in the following figure.

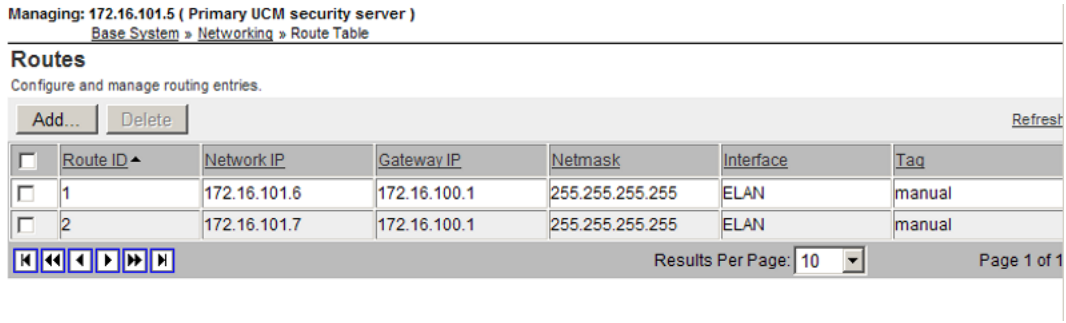


Figure 102: Routes window

4. Select the route that you want to delete.
5. Click **Delete**.

   The Route delete confirmation screen appears, as shown in the following figure.

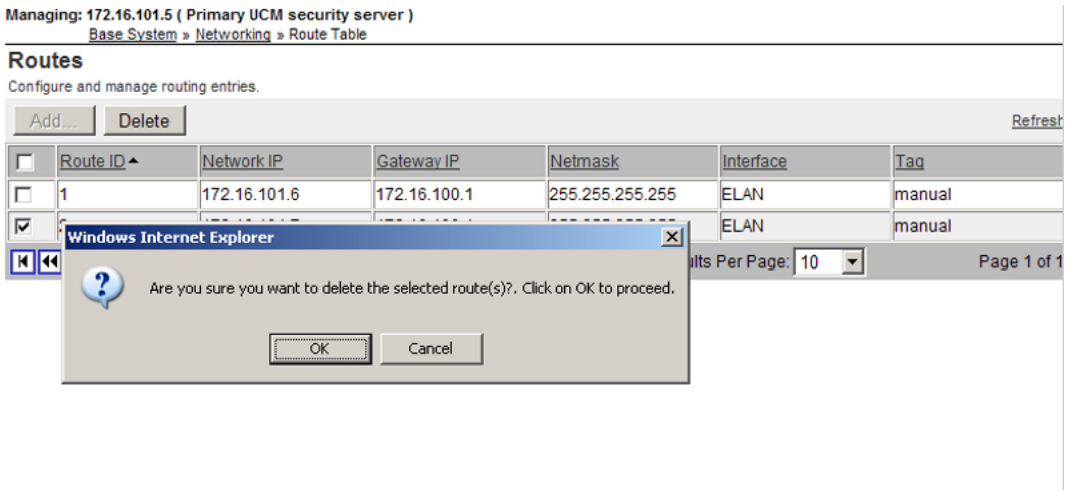


Figure 103: Route delete confirmation window

6. Click **OK**.

   The route is deleted, as shown in the following figure.

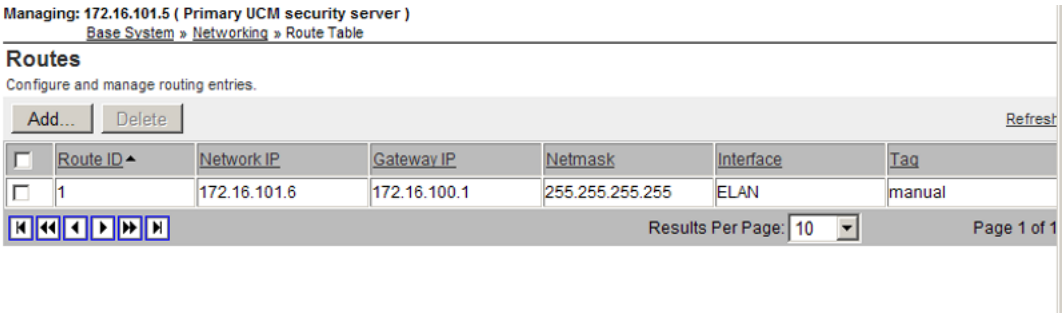


Figure 104: Route deleted window

Configuring Explicit Congestion Notification

Explicit Congestion Notification in the Internet Protocol allows the server and a router to exchange notifications in cases of network congestion. If the data network is relatively poor the Linux server can be given higher priority network routing treatment by enabling the explicit network congestion setting.

Note:

The routers in the network infrastructure must also support the explicit network congestion feature.

Procedure steps:

1. Log on to UCM and navigate to Base Manager. For details about logging on to UCM and accessing Base Manager, see Accessing Base Manager through UCM on page 162.

   OR

   Log on to the target server locally and navigate to Base Manager. For details about logging on to the target server locally and accessing Base Manager, see Accessing Base Manager through local logon on page 164.

2. In the navigation pane, select **Explicit Congestion Notification**.

   The ECN screen appears, as shown in the following figure.

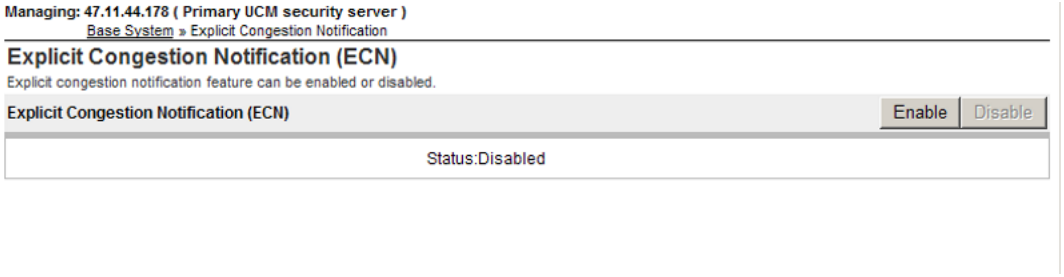


Figure 105: Explicit Congestion Notification window

3. Press **Enable** to enable Explicit Congestion Notification.

   OR

   Press **Disable** to disable Explicit Congestion Notification.

Date and time configuration

The following section contains the procedures to manually configure system date and time value and to synchronize the data and time with network time servers.

The NTP client running on the Linux element obtains time updates by polling an NTP server. The polling interval ranges from 64 to 1024 seconds. After a restart of the element or after NTP synchronization configuration, the initial polling interval is 64 seconds. As the clock stabilizes the interval doubles until it reaches the maximum of 1024 seconds. The polling interval decreases if the clock is not stable; the polling interval increases if the clock cannot be reached. For a newly installed system it can take an additional 15 minutes (approximately) for the clock to stabilize the first time synchronization occurs.

After the clock stabilizes, there can be situations where the NTP clock source time changes. In these situations you can use the Sync Now feature in Base Manager to force an immediate time synchronization, rather than wait as long as 1024 seconds for the next poll to occur.

Configuring system date and time

Prerequisites:

You must log on using a role from the systemadmin or timeadmin access groups to perform date and time configuration.

Note:

Internally there is no way to distinguish the Sync Now request failure caused by initial configuration having just been performed from other rare error conditions (such as NTP software not responding). Any errors from the Sync Now operation are ignored.

Note:

You can configure a maximum of 11 external clock source IP addresses for the primary NTP server; you can configure a maximum of 10 IP addresses for the secondary NTP server.

Procedure steps:

Perform the following procedure to manually configure system values for date and time. If you configure NTP parameters, synchronization is done automatically; you do not need to use the Sync Now feature.

1. Log on to UCM and navigate to Base Manager. For details about logging on to UCM and accessing Base Manager, see Accessing Base Manager through UCM on page 162.

   OR

Log on to the target server locally and navigate to Base Manager. For details about logging on to the target server locally and accessing Base Manager, see Accessing Base Manager through local logon on page 164.

2. In the navigation pane, select **Date and Time**.

   The date and Time screen appears, as shown in the following figure.

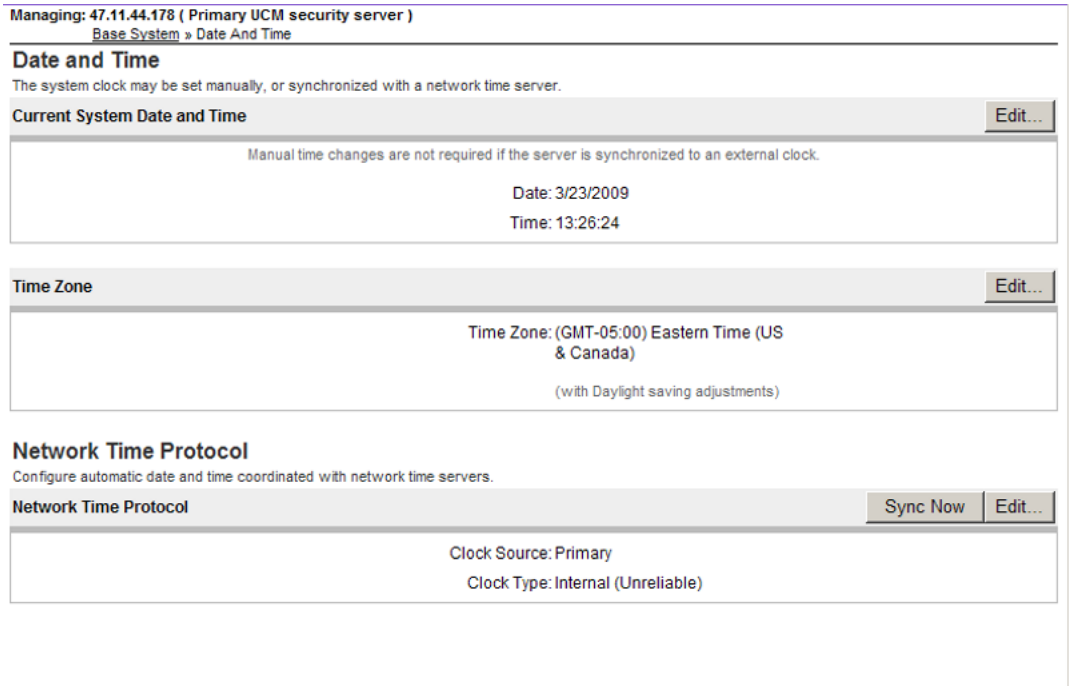


Figure 106: Date and Time window

3. Navigate to the **Current System Date and Time** section.
4. Click **Edit**.

   The Edit Date and Time screen appears, as shown in Figure 107: Edit Date and Time window on page 179.

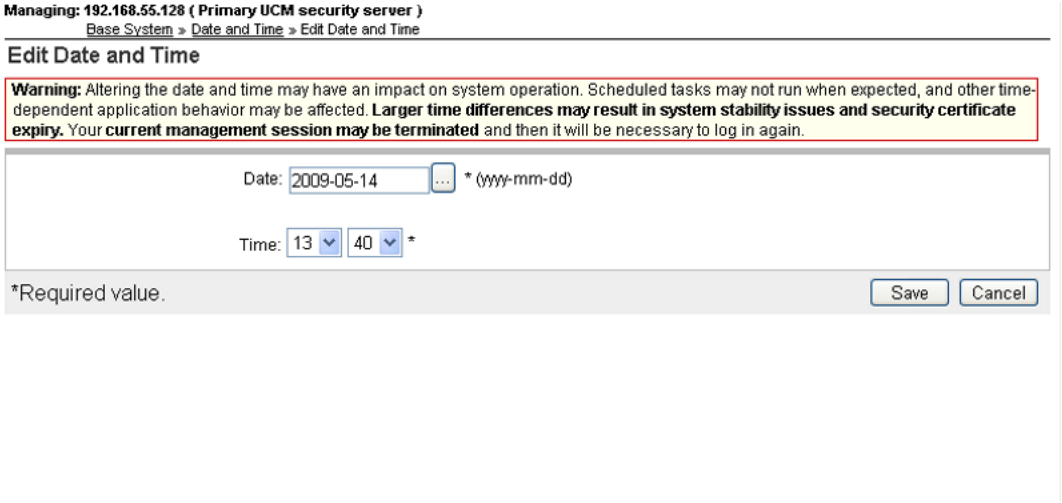


Figure 107: Edit Date and Time window

5. In the **Date** box, enter the date in the format yyyy-mm-dd.

   Warning:

   If you modify the date and time to a future value, your session expires and the initial Base Manager screen displays.

   OR

   Press the Browse (...) button to select the date from a calendar.

6. In the **Time** lists, select values for hours (hh) and minutes (mm).
7. Click **Save** to save your configuration changes.

   OR

   Press **Cancel** to discard your changes and return to the Date and Time screen.

8. Navigate to the **Time Zone** section.
9. Click **Edit**.

   The Time Zone screen appears, as shown in the following figure.

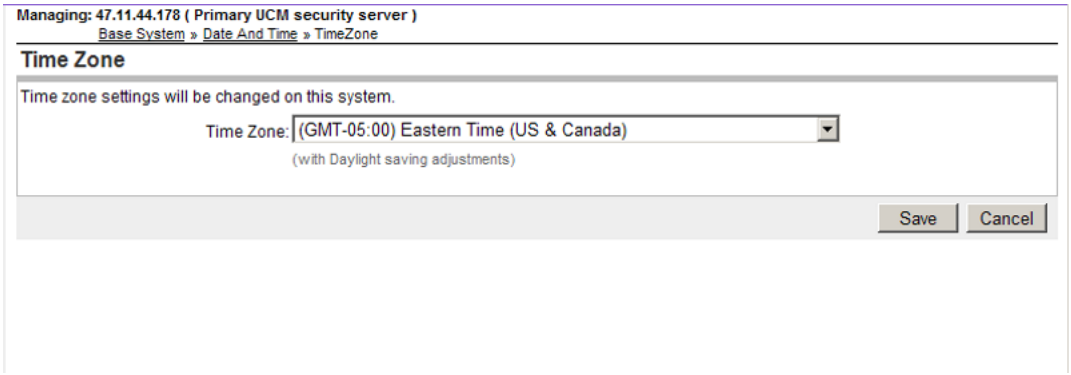


Figure 108: Time Zone screen

10. In the **Time Zone** list, select a value for Time Zone.
11. Click **Save** to save your configuration changes.

    OR

    Press **Cancel** to discard your changes and return to the Date and Time screen.

Synchronizing date and time with network time servers

Prerequisites:

- You must log on using a role from the systemadmin or timeadmin access groups to perform date and time configuration.

Procedure steps:

Perform the following procedure to synchronize system date and time values with network time servers.

1. Log on to UCM and navigate to Base Manager. For details about logging on to UCM and accessing Base Manager, see Accessing Base Manager through UCM on page 162.

   OR

   Log on to the target server locally and navigate to Base Manager. For details about logging on to the target server locally and accessing Base Manager, see Accessing Base Manager through local logon on page 164.
2. In the navigation pane, select **Date and Time**.

   The date and Time screen appears, as shown in Figure 109: Date and Time window on page 181.

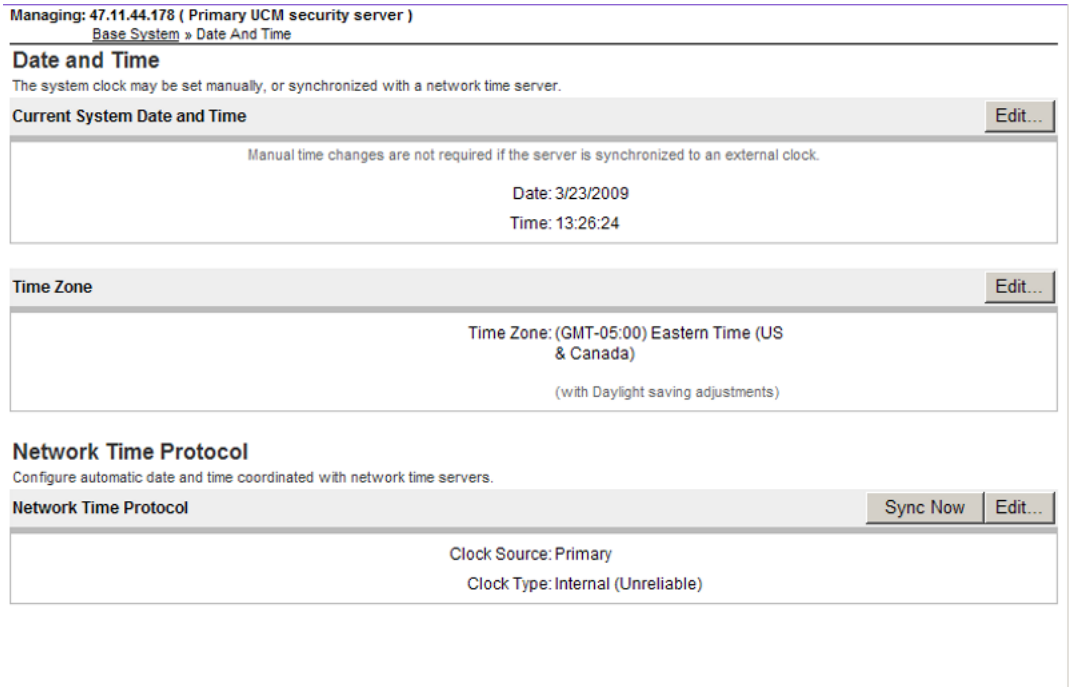


Figure 109: Date and Time window

3. Navigate to the **Network Time Protocol** section.
4. If you want to force an immediate time synchronization with the NTP server click **Sync Now**.

   The time is synchronized with the NTP server and the procedure ends at this point.
5. Click **Edit**.

   The Network Time Protocol screen appears, as shown in Figure 110: Network Time Protocol window on page 182.

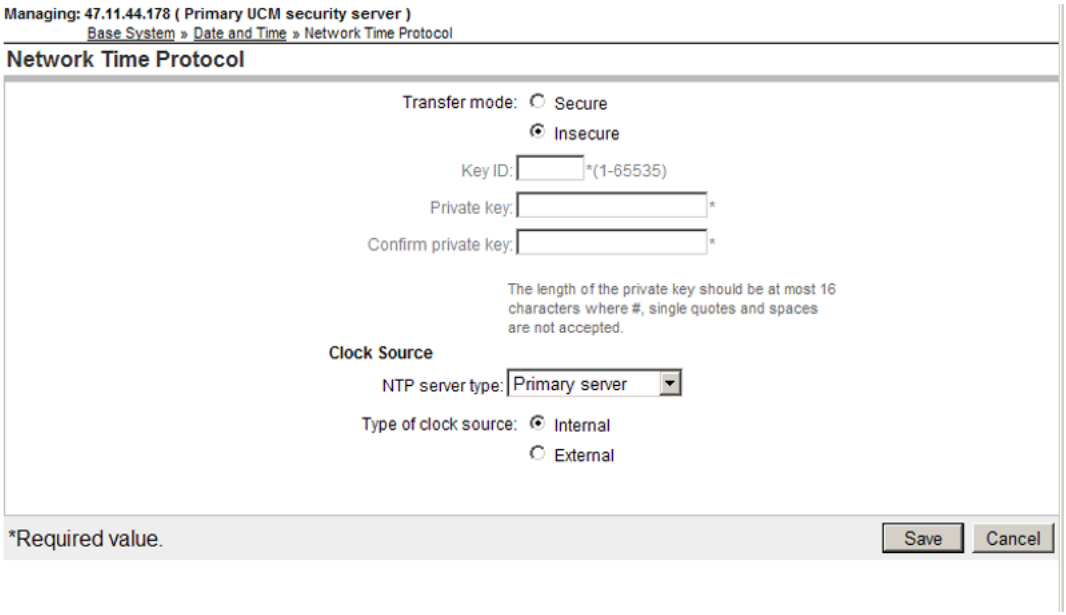


Figure 110: Network Time Protocol window

6. Perform Configuring NTP transfer mode on page 182
7. If you are configuring the clock source for a primary NTP server, perform Configuring the clock source for a primary server on page 183.
8. If you are configuring the clock source for a secondary NTP server, perform Configuring the clock source for a secondary server on page 185.
9. If you are configuring the clock source for a server that is not a clock source, perform Configuring a server that is not a clock server on page 187.

Configuring NTP transfer mode

Configure NTP to operate using a secure or insecure transfer mode. If you choose a secure transfer mode you must also provide a key ID and private key.

Prerequisites:

- You must log on using a role from the systemadmin or timeadmin access groups to perform date and time configuration.

Procedure steps:

1. Navigate to the Transfer mode section.
2. If you want an insecure transfer mode select the **Insecure** option. Proceed to 7 on page 182 in Synchronizing date and time with network time servers on page 180.

   OR

   If you want a secure transfer mode select the **Secure** option.
3. In the **Key ID** field, enter a value for key ID.

4. In the **Private key** field, enter a value for private key.
5. Proceed to 7 on page 182 in Synchronizing date and time with network time servers on page 180.

Configuring the clock source for a primary server

Configure the clock source for a primary server.

Prerequisites

- You must log on using a role from the systemadmin or timeadmin access groups to perform date and time configuration.

Procedure steps

1. Navigate to the Clock Source section.
2. Select **Primary** in the **NTP server type** list.
3. In the type of clock source list, select **Internal**, if you want an internal clock source.
4. In the type of clock source list, select **External**, if you want an external clock source.

   If you select an external clock source, additional fields appear on the screen, as shown in the following figure.

   Note:

   You can use EM to configure a third-party clock source as an external NTP server. If you configure an external NTP server, the Primary NTP server can retrieve date and time values from the external NTP server and distribute or synchronize date and time to other members of the security domain.

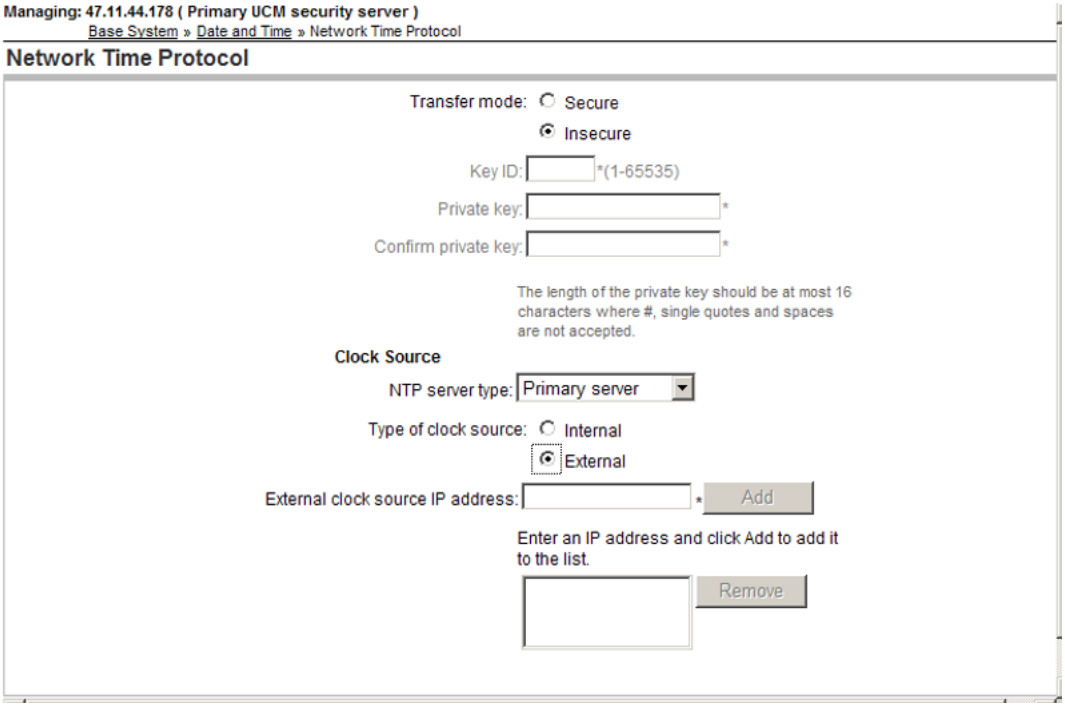


Figure 111: Primary server clock source window

5. In the **External clock source IP address** field, type a value for the external clock source IP address.
6. Click **Add**.

   The value is added to the list of IP addresses, as shown in the following figure.

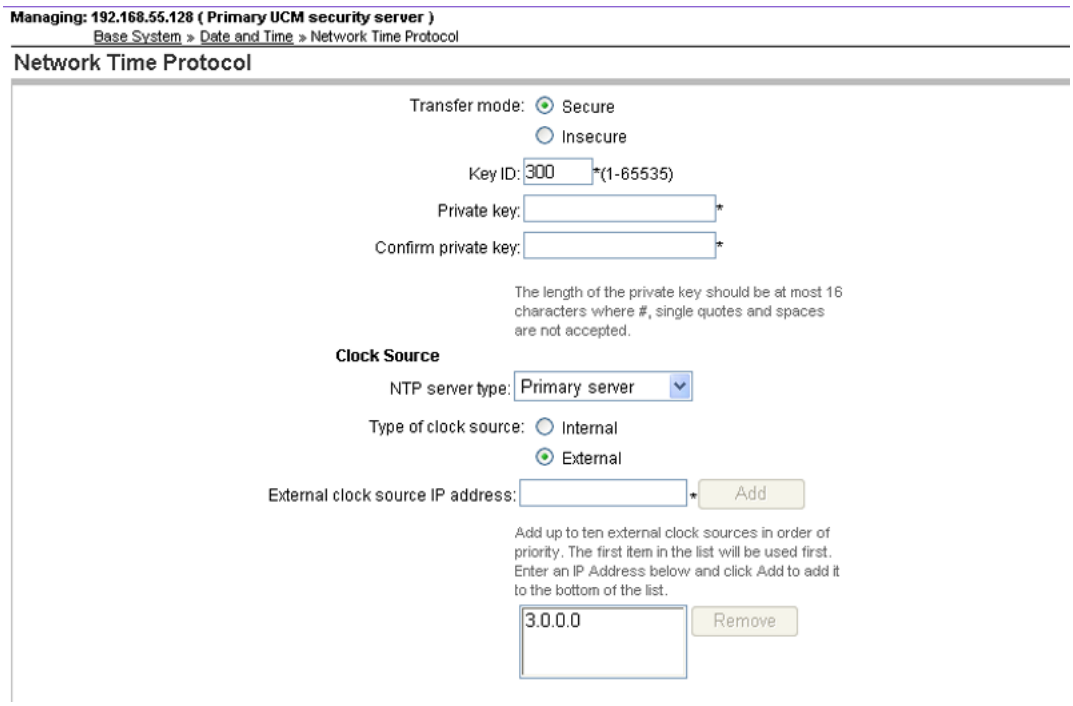


Figure 112: External clock source IP address window

7. If you want to remove a value from the IP address list, highlight the value and click **Remove**.
8. Click **Save** to save the clock source configuration.

   OR

   Click **Cancel** to return to the Date and Time screen.
9. Return to the Preconfiguring process using Deployment View on page 74.

Configuring the clock source for a secondary server

Configure the clock source for a secondary server.

Prerequisites

You must log on using a role from the systemadmin or timeadmin access groups to perform date and time configuration.

Procedure steps

1. Navigate to the Clock Source section.
2. Select **Secondary** in the **NTP server type** list.
3. In the **Primary NTP server IP address** field, type a value for the IP address of the primary NTP server.
4. In the Type of clock source list, select **Internal**. if you want an internal clock source.
5. In the Type of clock source list, select **External**. if you want an external clock source.

If you select an external clock source, additional fields appear on the screen, as shown in the following figure.

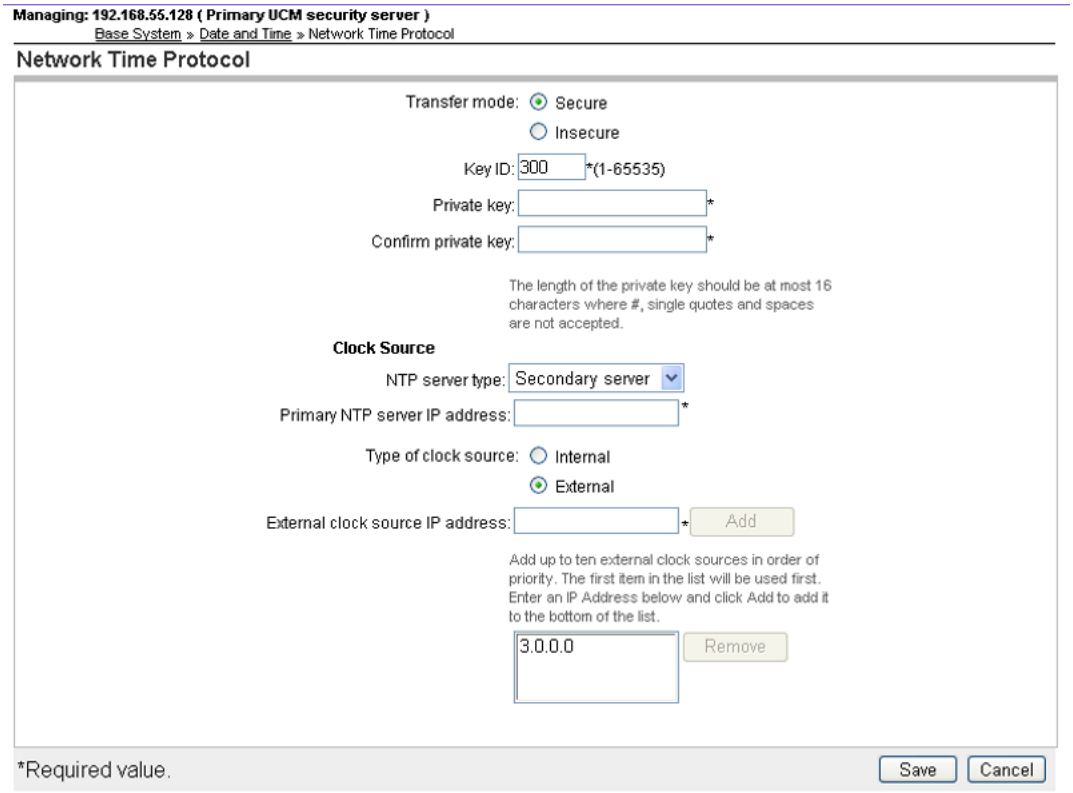


Figure 113: Secondary server clock source window

6. In the **External clock source IP address** field, type a value for the external clock source IP address.
7. Click **Add**.

   The value is added to the list of IP addresses, as shown in the following figure.

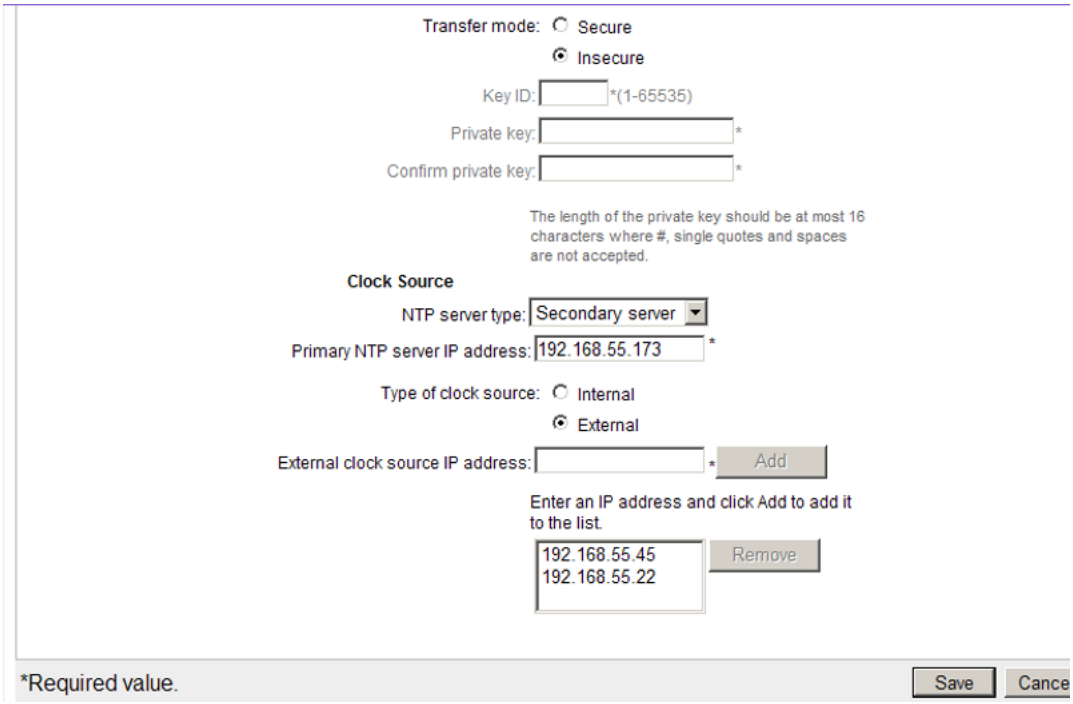


Figure 114: External clock source IP address (secondary server) window

8. If you want to remove a value from the IP address list, highlight the value and click **Remove**.
9. Click **Save** to save the clock source configuration.

   OR

   Click **Cancel** to return to the Date and Time screen.
10. Return to the Preconfiguring process using Deployment View on page 74.

Configuring a server that is not a clock server

Configure the clock source for a server that is not a clock server.

Prerequisites

You must log on using a role from the systemadmin or timeadmin access groups to perform date and time configuration.

Procedure steps

1. Navigate to the Clock Source section.
2. Select **Not a clock server** in the **NTP server type** list.

   The clock source fields appear, as shown in the following figure.

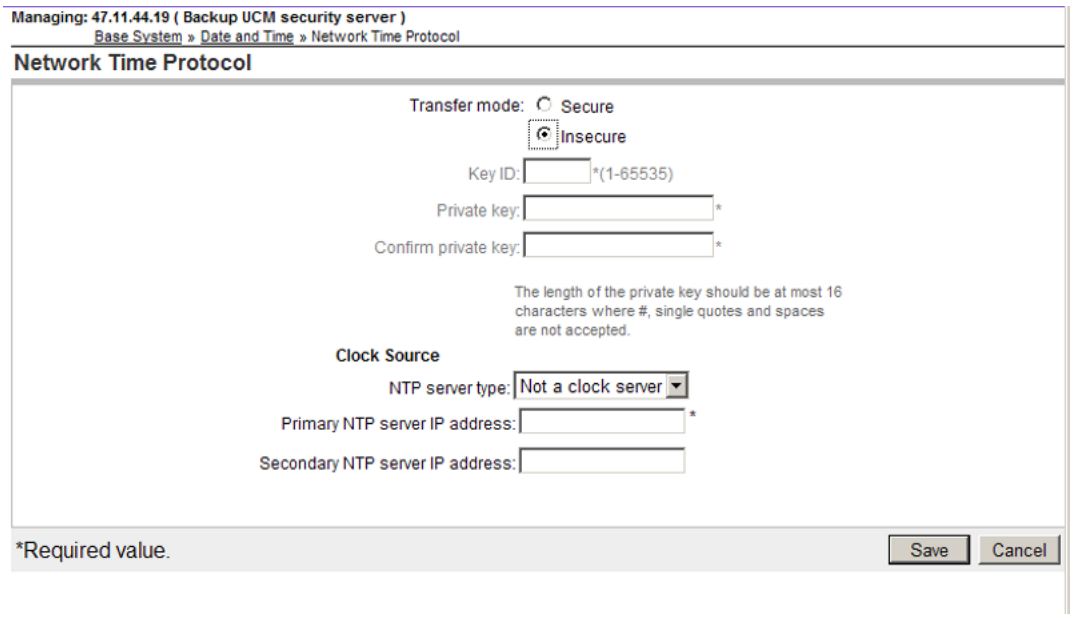


Figure 115: Clock source fields for a server that is not a clock server

3. In the **Primary NTP server IP address** field type a value for the IP address of the primary NTP server.
4. In the **Secondary NTP server IP address** type a value for the IP address of the secondary NTP server.

   Note:

   Use of a secondary NTP server is optional.
5. Click **Save** to save the clock source configuration.

   OR

   Click **Cancel** to return to the Date and Time screen.
6. Return to the Preconfiguring process using Deployment View on page 74.

Regenerating SSH Keys for a UCM Member server

Use Regenerating SSH Keys for a UCM Member server to regenerate the SSH keys for a UCM Member server.

Note:

SSH key regeneration is only available for UCM Member servers. The option to regenerate SSH keys is not available for Primary UCM and Backup UCM servers.

Prerequisites:

- You must log on using a role from the Security Administrator access group to perform SSH key regeneration.

Procedure steps:

1. Log on to UCM and navigate to Base Manager. For details about logging on to UCM and accessing Base Manager, see Accessing Base Manager through UCM on page 162.

   OR

   Log on to the target server locally and navigate to Base Manager. For details about logging on to the target server locally and accessing Base Manager, see Accessing Base Manager through local logon on page 164.

2. In the navigation pane, select **SSH Keys**.

   The SSH Keys page appears, as shown in Figure 116: SSH Keys page on page 189.

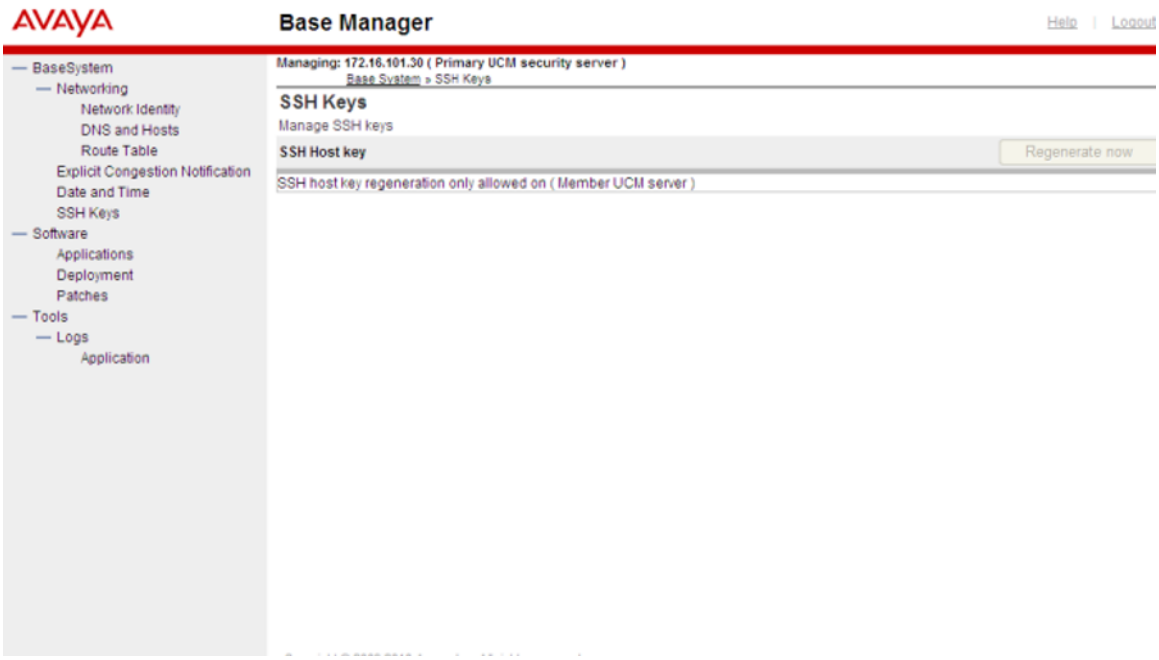


Figure 116: SSH Keys page

3. Click **Regenerate now**.

   The following message displays on the SSH Keys page:

   ```
   The SSH host key has been successfully regenerated.
   ```

   If the regeneration is not successful, the following message displays on the SSH Keys page:

   ```
   SSH host key regeneration failed.
   ```

   If you attempted to regenerate the keys on a server that is not a Member server, the following message displays on the SSH Keys page:

   ```
   SSH host key regeneration only allowed on (Member UCM server).
   ```

Software maintenance using Base Manager

Stopping or restarting applications can impact system operations. It may be desirable to gracefully idle down the system or transfer operations to other redundant devices before stopping or restarting. Restarting or stopping an application can affect other systems, as in the case of network wide virtual office or branch office. Restarting or stopping an application can also cause some applications to issue alarms or generate logs.

There are operational impacts and interactions among applications. Before you stop an application it may be necessary to stop dependent applications. The following table provides a list of interactions among applications.

Table 5: Applications and dependencies

Application	Impact
Base - all	Impacts base and all Avaya applications.
Jboss	Impacts all management applications. **Note:** The web session is disrupted if you restart Jboss.
SNMP	Affects the ability of other applications to send traps.
Database server	Impacts most applications (CS, SS, PD, SIPL, NRS, SubM, EM).
Signaling Server	Impacts TPS, CSV, VTRK, and PD.
Virtual Trunk (VTRK)	Impacts SS applications.
Connection Service (CSV)	Impacts TPS.
Terminal Proxy Server (TPS)	Can be stopped independently.
Personal Directory (PD)	Can be stopped independently.
SIP Proxy server	Can be stopped independently.
Gatekeeper	Can be stopped independently.
Network Connect Server	Can be stopped independently.
Avaya - all	Impacts all higher level applications (all related to call processing).

Managing application status

Perform the following procedure to view the status of installed applications and to start, stop, or restart the applications.

1. Log on to UCM and navigate to Base Manager. For details about logging on to UCM and accessing Base Manager, see Accessing Base Manager through UCM on page 162.

   OR

   Log on to the target server locally and navigate to Base Manager. For details about logging on to the target server locally and accessing Base Manager, see Accessing Base Manager through local logon on page 164.

2. In the navigation pane, select **Software** > **Applications**.

   The **Application Status** screen appears, as shown in the following figure.

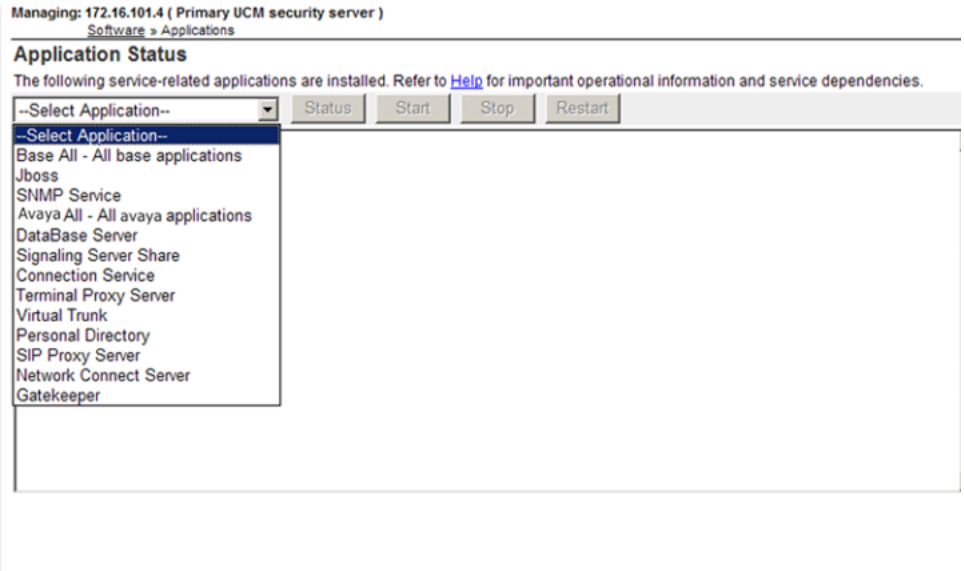


Figure 117: Application Status window

3. Select an application from the application list.

   Note:

   If you select **Base All** you can only perform the status operation. If you select **Jboss** you can only perform status and restart operations. For all other applications status, start, stop, and restart operations are valid.

   Note:

   For start, stop, and restart operations, a confirmation message is displayed when you select the operation.

4. Click **Status** to display the status of the application.
5. Click **Start** to start the application.
6. Click **Stop** to stop the application.
7. Click **Restart** to restart the application.

View and export logs using Base Manager

Base Manager provides access to logs generated by installed applications. You can view the logs or you can export the logs to a file which can be saved locally.

Viewing application logs

1. Log on to UCM and navigate to Base Manager.

   OR

   Log on to the target server locally and navigate to Base Manager.

2. In the navigation pane. select **Tools**,

   The Tools screen appears, as shown in the following figure.

Figure 118: Tools window

3. In the Tools window, click **Logs**.

   The Application Logs screen appears, as shown in the following figure.

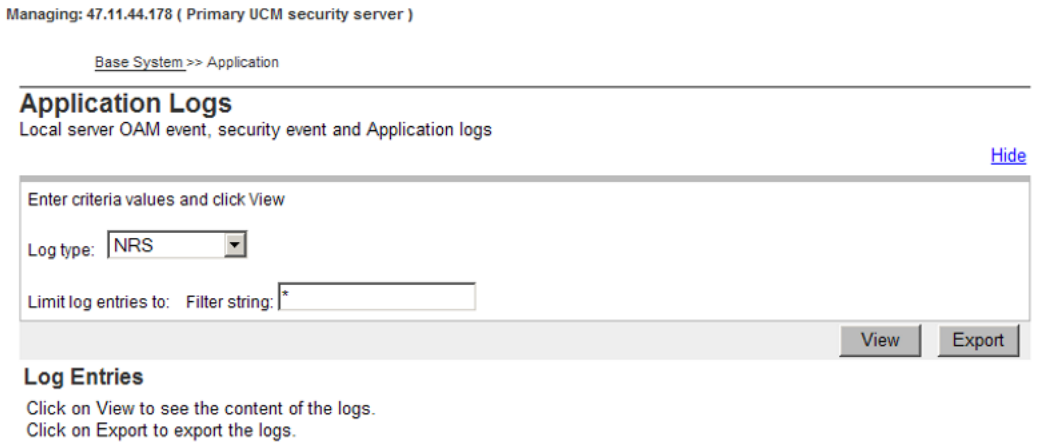


Figure 119: Application Logs window

4. In the **Log type** list, select an application log type.
5. In the **Limit log entries to: Filter string** box, enter a character string to limit the log entry search. If you leave the **Limit log entries to: Filter string** blank, the search returns all log entries.
6. Press **View**.

   The application log entries appear, as shown in the following figure

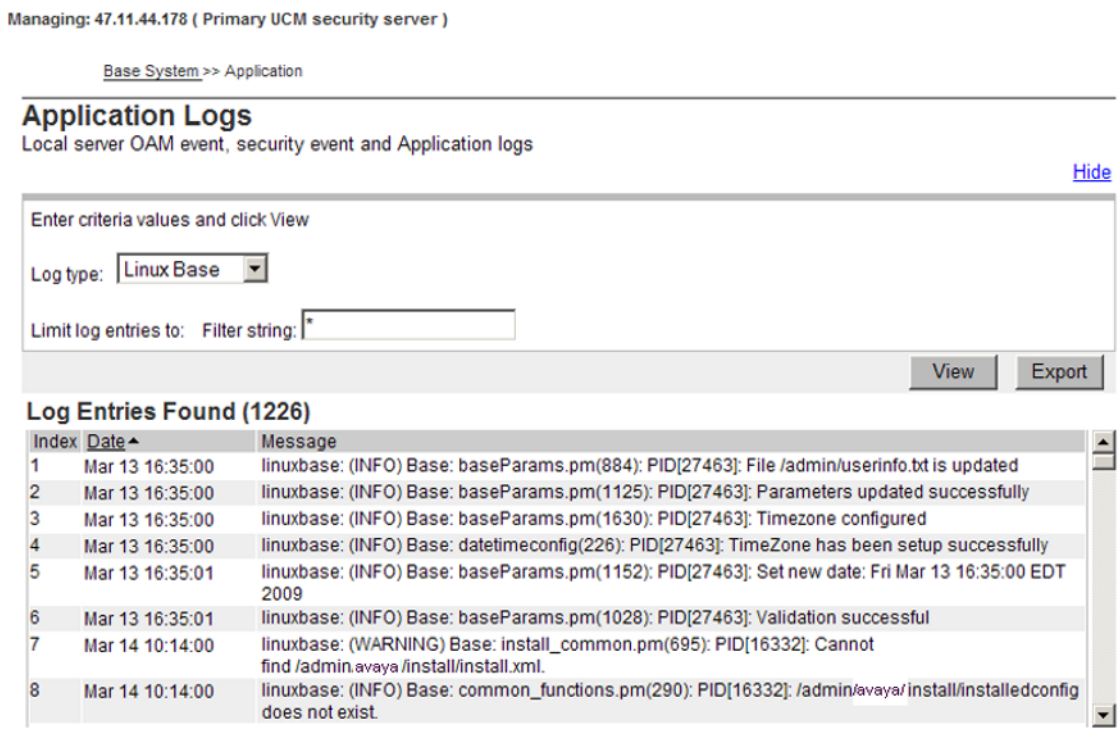


Figure 120: Application Logs - search results window

Exporting application logs

1. Log on to UCM and navigate to Base Manager. For details about logging on to UCM and accessing Base Manager, see Accessing Base Manager through UCM on page 162.

   OR

   Log on to the target server locally and navigate to Base Manager. For details about logging on to the target server locally and accessing Base Manager, see Accessing Base Manager through local logon on page 164.

2. In the navigation pane, select **Tools**, **Logs**, **Application**.

   The Application Logs screen appears, as shown in the following figure.

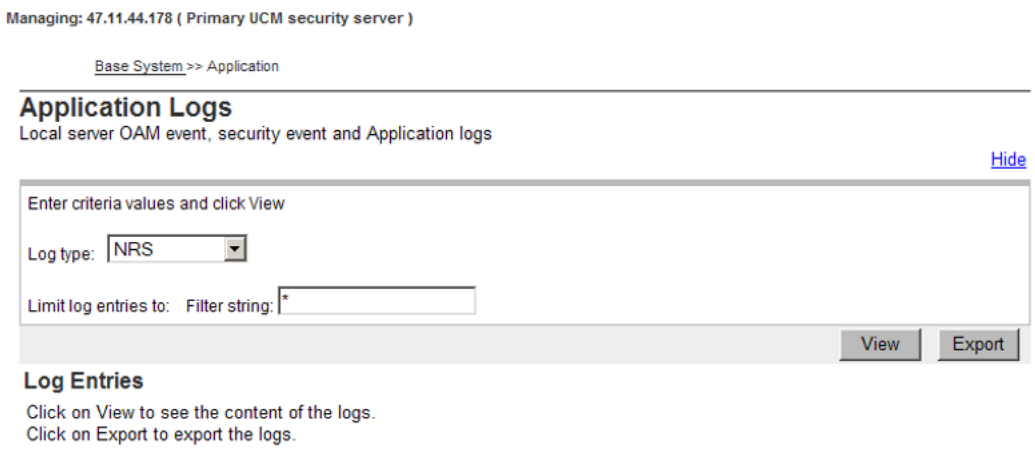


Figure 121: Application Logs window

3. In the **Log type** list, select an application log type.
4. In the **Limit log entries to: Filter string** box, enter a character string to limit the log entry search. If you leave the **Limit log entries to: Filter string** blank, the search returns all log entries.
5. Press **Export**

   . A file download prompt appears, as shown in the following figure.

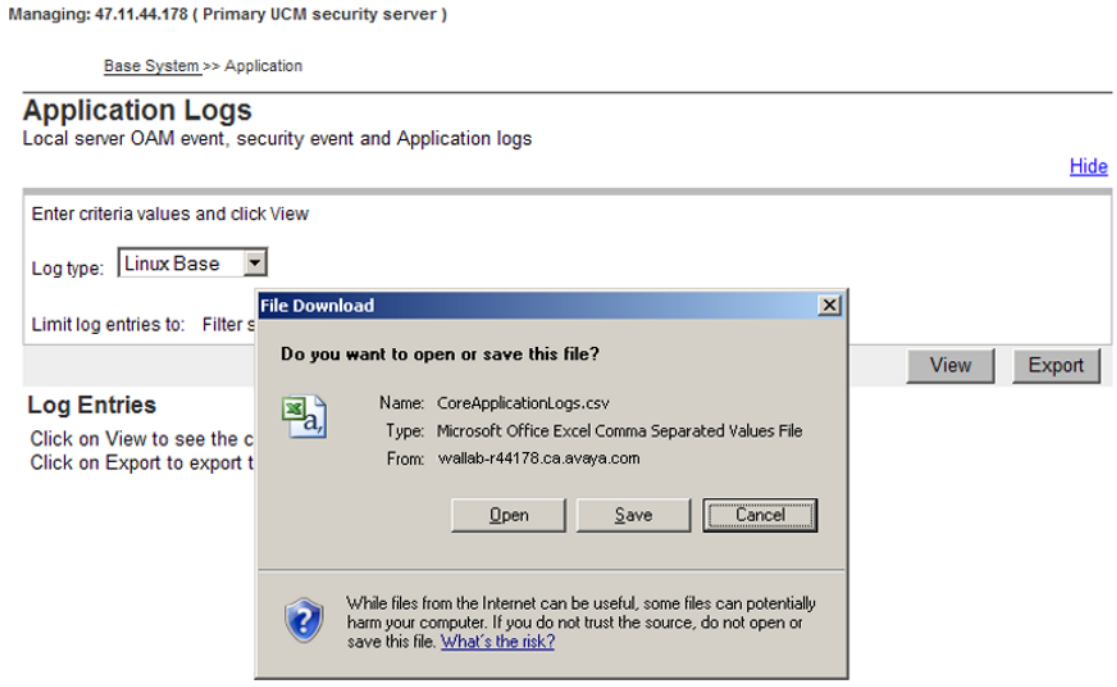


Figure 122: Application Logs - file download prompt window

6. Press **Open** to open a file that contains the application log entries.

   OR

   Press **Save** to save the application logs entries file locally.

Chapter 12: Disaster recovery

This chapter describes the prerequisites and procedures for Avaya Linux system disaster recovery on a Server. For more information about disaster recovery, see Disaster recovery on page 35.

Navigation

- Prerequisites on page 196
- Performing disaster recovery for Avaya Linux Base on page 196
- UCM considerations for disaster recovery on page 200
- Changing Linux Base passwords on page 201

Prerequisites

- You must have a system backup file stored on a USB device or SFTP server. Use Backing up existing system data files on page 110 to perform a system back up to an external SFTP or USB source.
- If a fault occurs in the existing Primary UCM Server and a system backup file is not available, you cannot restore the data; you must perform a fresh installation of a new Primary Server. For more information, see UCM considerations for disaster recovery on page 200.

Performing disaster recovery for Avaya Linux Base

Perform the following procedure to perform disaster recovery for an Avaya Linux Base on a Server.

1. Connect to the Server using the serial console or using the keyboard and video monitor (kvm).
2. Insert the Linux Base installation media. The installation media is either a DVD, USB, or CF card depending on your hardware platform.

Warning:

If using a Linux Base DVD on a COTS server, only insert the DVD in the drive during the Linux Base installation (this does not apply to Server cards). Normally the DVD auto-ejects after the Linux Base installation is complete. If the Linux Base DVD is accidentally left in the DVD drive after installation and a system restart occurs, the system will boot into the installation program. This can be interpreted as a hung system. If this occurs, eject the DVD and restart the system.

3. Restart the server.

Note:

For Server cards, re-seat the card to ensure a successful restart.

When the server boots up, the Avaya Communication Server 1000 (Avaya CS 1000) Linux Base System Installer window appears.

For Server cards, the Avaya CS 1000 Linux Base System Installer window appears, as shown in the following figure.

Figure 123: CS 1000 Linux Base system installer (Server cards)

OR

For COTS servers, the CS 1000 Linux Base System Installer window appears, as shown in the following figure.

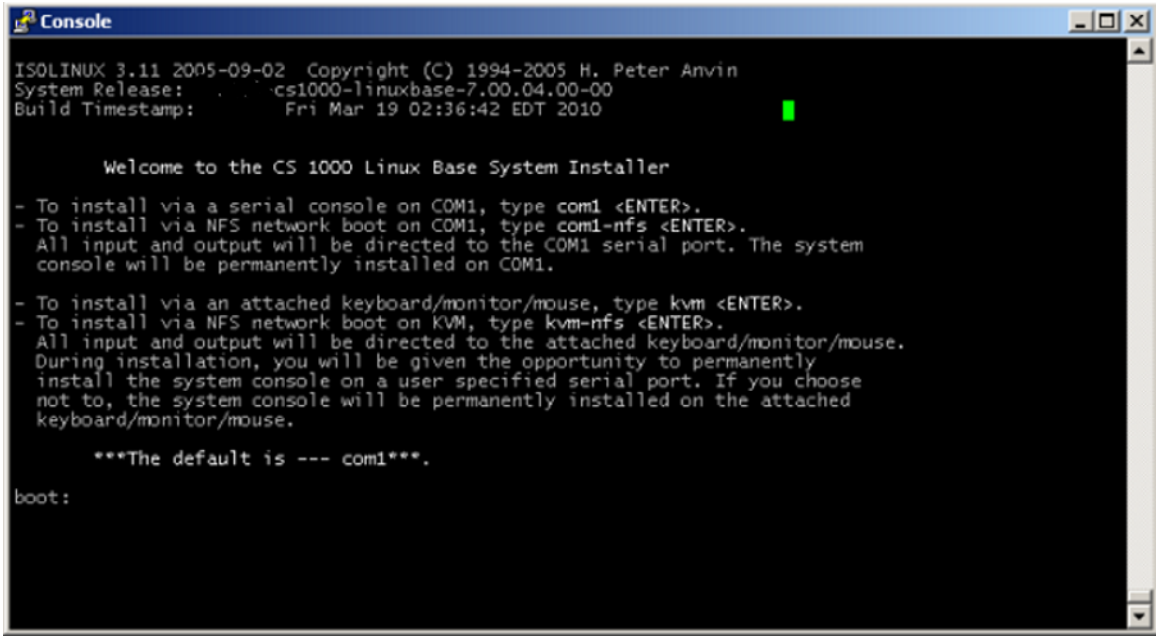


Figure 124: CS 1000 Linux Base system installer (COTS server)

4. Type `com1` or press `Enter` to install using a serial console on COM1.

   OR

   Type `kvm` to install using an attached keyboard and video monitor.

   Warning:

   If you log on to the COM1 port, make sure that **Caps Lock** is turned off before you log on.

   The disaster recovery procedure uses steps in the new and upgrade Linux Base procedures, as referenced in the following steps.

5. If you are attempting a disaster recovery and the following screen appears, the disk is more than likely new, corrupted, or has been formatted. Proceed to follow the procedures in Step 5 on page 56 from Installing a new Linux base on page 55.

Figure 125: CS 1000 Linux Base installer confirmation screen

OR

If you are attempting a disaster recovery and the following screen appears, the disk information is retrievable from the existing /admin partition. If the data stored in the /admin partition is not corrupt and you trust the content, proceed to follow the procedures in Step 8 on page 121 from Upgrade Linux base manually on page 119.

Important:

If you are attempting to recover a server that has been upgraded from Communication Server 1000 Release 6.0 and does not have the latest backup data (either USB or SFTP), perform a backup data restore during the Linux Base installation. Performing a restore ensures a graceful reregistration to the UCM Security Domain and UCM Deployment Manager. During the Linux Base installation, select Option 2 or 3 at the Base Configuration Data Selection screen, as shown in Step 9 on page 122 from Upgrade Linux base manually on page 119.

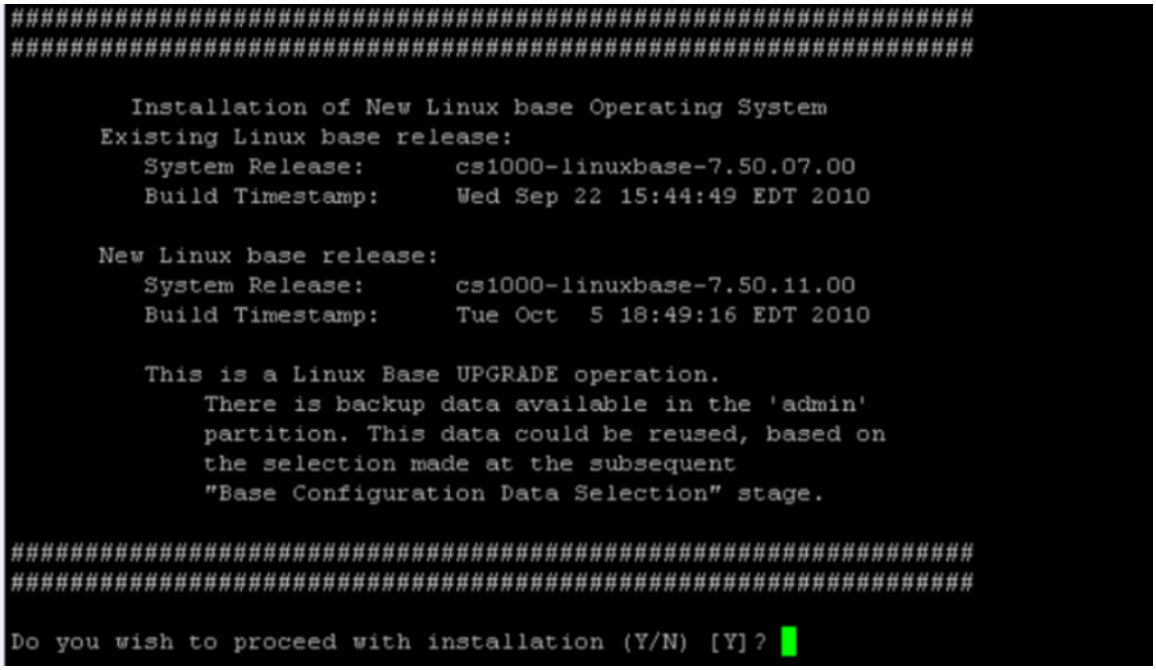


Figure 126: CS 1000 Linux Base system installer confirmation window

Note:

The disaster recovery process is not complete until you perform an application deployment and a patch deployment.

UCM considerations for disaster recovery

If a hardware fault occurs in a Primary UCM Server, there are security domain implications for backup and member servers that impact disaster recovery.

Primary UCM Server replacement

If a fault occurs on the Primary Security Server and a system backup archive is available, then the recovery operation on the new Primary UCM Server restores all Linux base system settings, UCM data, and application data.

- You do not need to rejoin backup or member servers to the security domain because the security domain does not change.
- The FQDN of the new Primary Server must be the same as the FQDN of the damaged Primary Server
- You must perform application deployment and patch deployment on the Primary UCM Server. For information about application deployment, see Deployment Manager—New system installation and commissioning on page 68. For more information about Linux patching, see *Avaya Patching Fundamentals, NN43001-407*.

If a fault occurs on the Primary Security Server and a system backup archive is not available, then the recovery of the Primary Server is not possible. You must perform a new installation of the Linux

base and Avaya applications, deploy and configure applications, perform patch deployment, and re-configure the system settings and security configuration. All member and backup servers must join the new security domain.

•

Backup UCM Server considerations in case of Primary UCM Server replacement

If you restore the Primary UCM Server from a system backup archive, no action is required for the existing Backup UCM Server.

Note:

If the IP address of the Primary Server changes, the backup security server must use the new IP address.

If a fault occurs on the Primary Security Server and a system backup archive is not available, you must perform a new installation. In this case, the security domain is changed and you must either demote the existing backup server to a member server in the new domain, or perform a fresh installation and rejoin the security domain as a backup server. For information about demoting a backup server, see *Unified Communications Management Common Services Fundamentals, NN43001-116*.

Note:

The Backup UCM Server application data can be restored using the command **`sysrestore --deployed_apps`**. This command restores deployed Avaya applications only; it does not restore base applications.

Member UCM Server considerations in case of Primary UCM Server replacement

If you restore the Primary UCM Server from a system backup archive, no action is required for the existing Member UCM Server.

Note:

If the IP address of the Primary Server changes, the member servers must use the new IP address.

If you perform a fresh installation of the Primary UCM Server (there is no backup archive), the member server must join the new security domain.

Changing Linux Base passwords

Perform the following procedure to change the Avaya Linux Base passwords for the root or admin2 accounts.

Prerequisites:

- Ensure you have physical access to the system.
- Ensure you have access to the serial COM port of the Linux server.
- Ensure you have the Linux Base installation media.
  - USB 2.0 memory stick for CP DC and CP MG cards

- DVD for COTS Servers
- RMD for Server cards

Procedure steps:

1. Insert the Linux Base installation media.

   Note:

   If you use COTS3 (HP DL360 G7) platform, you should use LinuxBase Release 7.6 installation DVD. Using 7.5 installation media will result in the error `Cannot define device for / partition`.

2. Restart the system.
3. If you connect to the server through the COM1 console, type `recovery-com1` in the CS 1000 Linux Base system installer screen and press `Enter`.

   OR

   If you connect to the server using a keyboard and video monitor (kvm) type `recovery-kvm` in the CS 1000 Linux Base system installer screen, and press `Enter`.

   Note:

   If you connect to the IBM x3350 server with a terminal for setup, the server does not function with the serial cable that was previously shipped with the ISP 1100 or other COTS platforms. The IBM x3350 server requires the new NTRX26NPE6 9 pin female to 9 pin female null modem cable. For a picture of the null modem cable, see Figure 179: NTRX26NPE6 9 pin female to 9 pin female null modem cable on page 263.

   The Recovery Console menu appears, as shown in the following figure.

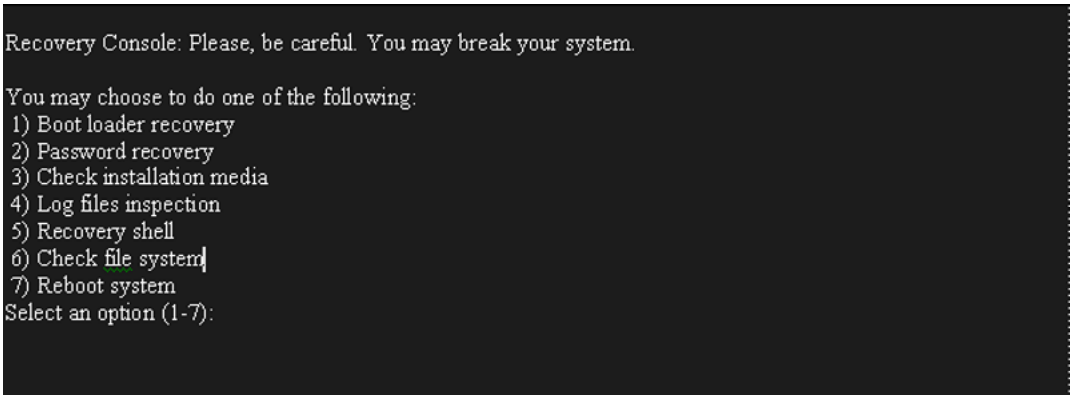


Figure 127: Recovery Console window

4. Select option `2` for password recovery and press `Enter`.

   The Password recovery screen appears, as shown in the following figure.

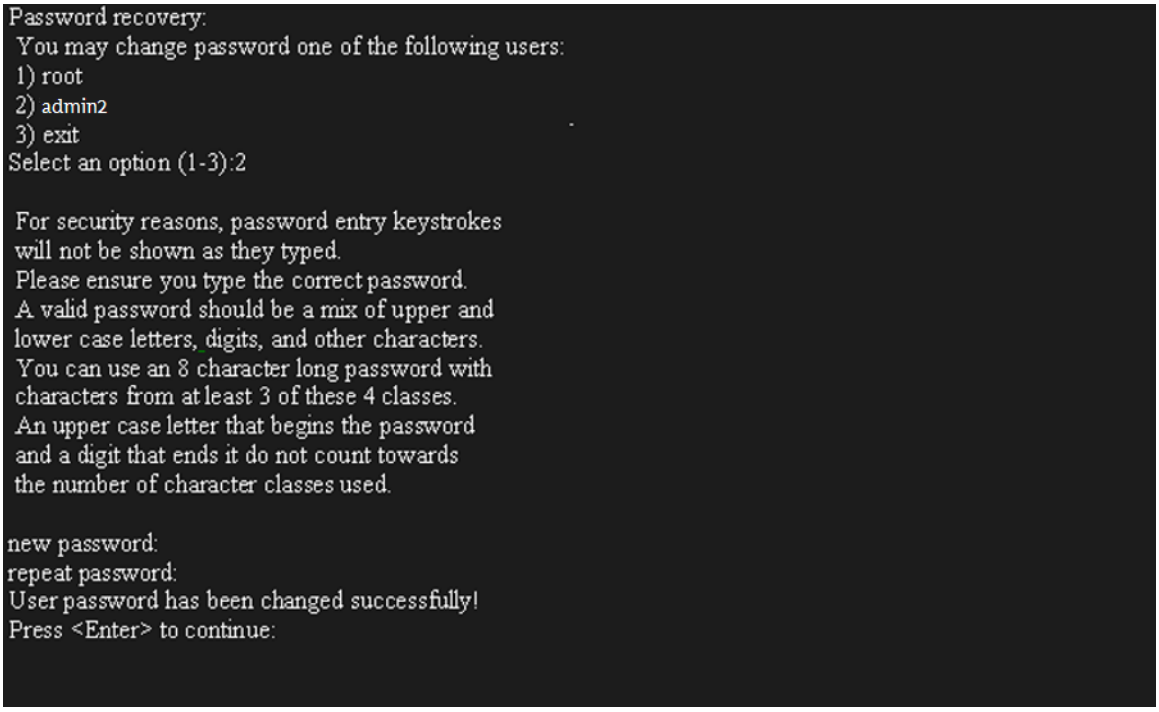


Figure 128: Password recovery window

5. Type the option number for the password that you want to change, and press `Enter`.
6. Enter the new password. For password creation guidelines, see Password creation guidelines on page 34.
7. Reenter the new password.
8. Press `Enter`.

Appendix A: Hardware platforms

The Linux Base is supported on various hardware platforms. For more information on the supported hardware platforms, see Supported hardware platforms on page 20.

Important:

Instructions to install a commercial off-the-shelf (COTS) server is not included in this document. Detailed installation instructions can be found in the documentation shipped with the server.

This section contains general instructions to install a Server. This section also includes instructions to connect all types of servers to the ELAN and TLAN subnets of an Avaya Communication Server 1000 (Avaya CS 1000) system and to connect a maintenance terminal to each type of Server.

Navigation

- Creating a bootable RMD for Linux Base installations on page 205
- Hardware installation checklist on page 209
- CP PM card on page 211
- CP DC card on page 223
- CP MG card on page 223
- Dell R300 server on page 224
- HP DL320 G4 server on page 231
- HP DL360 G7 server on page 239
- HP DL360p G8 server on page 244
- HP DL360 G9 server on page 248
- IBM x306m server on page 253
- IBM x3350 server on page 261

Configuring the privilege level for Windows Vista or Windows 7

If you are using Windows Vista or Windows 7, configure the privilege level to run as administrator prior to creating a bootable RMD for Linux installations

1. Create a temporary folder on your local drive.
2. Open a Web browser window and navigate to http://www.avaya.com.
3. Navigate to **Support** > **Downloads**.
4. Select the Release number from the list, and click the required software load zip file for the server platform, for example **Communication Server 1000 Software Downloads – Release x.x**.

   Note:

   The default release is 7.5.x.
5. Click the **Downloads** tab.
6. Click the software load zip file, for example, cs1000–linuxbase-7.5.017.00_cf.exe.
7. Unzip the files in the software load zip file to the newly created temporary folder. The following folders appear in the temporary folder:
   - baseapps
   - extra
   - license
   - relnotes
   - scripts
   - utilities
8. Open the **utilities** folder.
9. Right-click **syslinux.exe**, and select **Properties**.
10. Click the **Compatibility** tab.
11. In the **Privilege level** section, select the **Run this program as administrator** check box.
12. Click **Apply** and click **OK** to exit the syslinux properties window.
13. You can now proceed to Creating a bootable RMD for Linux Base installations on page 205.

Creating a bootable RMD for Linux Base installations

Linux Base installation requires the following bootable Removable Media Device (RMD):

- CP PM require a Compact Flash (CF) card.

- CP DC and CP MG require a USB memory stick.

Important:

To ensure that the latest boot loader is installed on the media boot sector, use a clean disk and repeat the steps in this procedure for every new software load.

Prerequisites:

- You must have a Compact Flash (CF) card or USB 2.0 memory stick with a capacity of at least 2 GB.
- You must use the correct bootable device for your hardware type:
  - CP PM requires a Compact Flash (CF) card.
  - CP DC and CP MG requires a USB memory stick.

    Note:

    The N0220961 USB memory stick is supported for CS 1000. Not all USB memory sticks are supported.
- If you are using Windows Vista or Windows 7, you must configure the Privilege Level, see Configuring the privilege level for Windows Vista or Windows 7 on page 205.

Procedure steps:

1. Create a temporary folder on your local drive.
2. Open a Web browser window, and go to http://www.avaya.com.
3. Navigate to **Support** > **Downloads**.
4. Select the Release number from the list, and click the required software load zip file for the server platform, for example **Communication Server 1000 Software Downloads – Release x.x**.

   Note:

   The default release is 7.5.x.
5. Click the **Downloads** tab.
6. Click the software load zip file, for example, cs1000–linuxbase-7.5.017.00_cf.exe.
7. Unzip the files in the software load zip file to the newly created temporary folder.

   The following folders appear in the temporary folder:

   - baseapps
   - extra
   - license
   - relnotes
   - scripts
   - utilities

8. Open the **utilities** folder.
9. Double-click the **mkbootrmd.bat** file, and press any key to continue, as shown in the following figure.

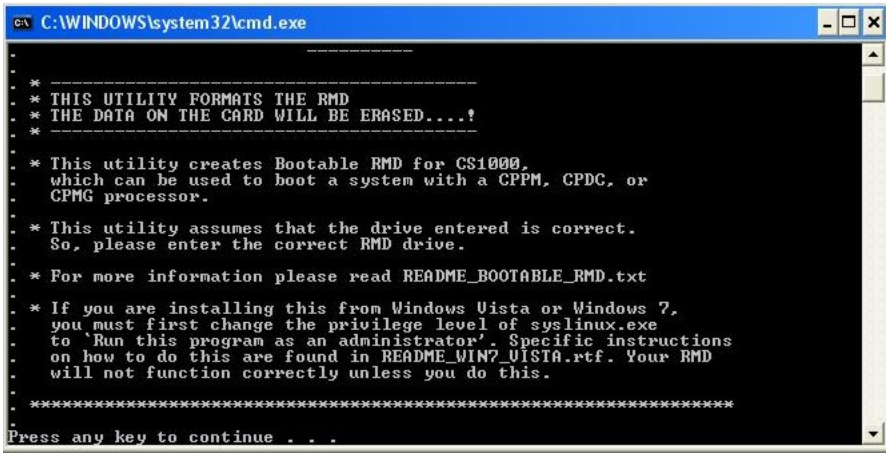


Figure 129: mkbootrmd.bat screen

10. At the prompt, **Please enter the Drive letter of your RMD**, type a drive letter, as shown in the following figure.
11. At the prompt, **Create bootable Compact flash or USB stick**, select either `C` for Compact Flash or `U` for USB device, as shown in the following figure.

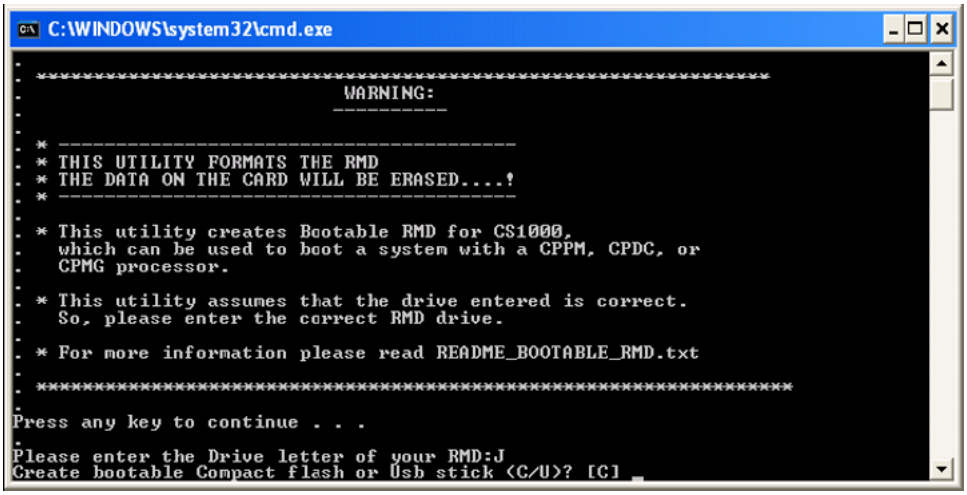


Figure 130: Select bootable media screen

Important:

If the USB memory stick is selected, some additional files are copied to overwrite the files for a Compact Flash installation, the following message appears, Configuring for USB install. The same is also true if the Compact Flash is selected; however, the additional files are copied to overwrite the files for a USB stick.

12. Select `Yes` if you want to proceed.

OR

Select `No` to return to the drive selection screen, or `Abort` to exit the utility without making changes to the selected drive, as shown in the following figure.

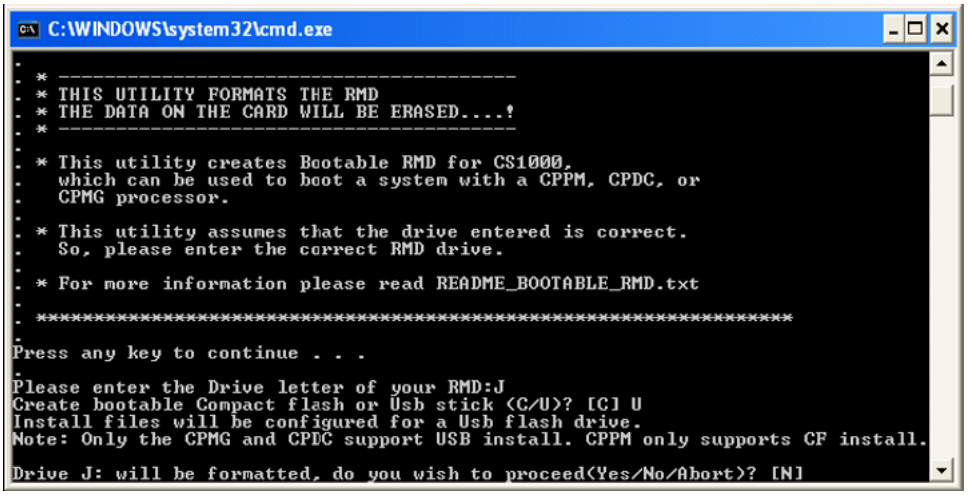


Figure 131: Confirmation screen

Important:

USB 2.0 memory stick is the only media supported for CP MG and CP DC. USB 1.0 and 1.1 are not supported. USB and CF have the same size requirements.

13. Copy the distribution image from the temporary folder to your installation media. You must always reformat your installation media using mkbootrmd.bat before you copy the distribution image from the temporary folder to your installation media.

    Important:

    - Do not unzip the software load zip file directly to the installation media.
    - Do not copy the contents of the temporary folder to the installation media without first running mkbootrmd.bat.
    - Do not copy the contents of the temporary folder to an installation USB if mkbootrmd.bat was most recently run selecting the CF option.
    - Do not copy the contents of the temporary folder to an installation CF if mkbootrmd.bat was most recently run selecting the USB option

Important:

If you do not select the correct bootable device for your hardware type (as described in the preceding Prerequisites), you must repeat the procedures in Creating a bootable RMD for Linux Base installations; otherwise, you receive error messages, as shown in the following table.

Table 6: Error messages when using the incorrect bootable device

Error condition:	Error message:
If a USB is created as a bootable Compact Flash by mistake and com1-nfs install is used on a CP DC or CP MG, and the error message appears on the COM port console.	---------- Networking Device ---------- You have multiple network devices on this system. Which would you like to install through? eth - Intel Corporation Unknown device 5045 eth0 - Intel Corporation Unknown device 5049 eth1 - Intel Corporation Unknown device 5041 OK || Identify || Back
If a USB is created as a bootable Compact Flash by mistake and com1 install is used on a CP DC or CP MG, and the error message appears on the COM port console.	----- Error Downloading kickstart file -------- Unable to download the kickstart file. Please modify the kickstart parameter below or press Cancel to proceed as an interactive installation. hd:hdc1:/ ks_cppm.cfg OK || Cancel
If a Compact Flash is created as a bootable USB by mistake and com1-nfs install is used on a CP PM, the user would see slow message output, a messy display, and the error message appears on the COM port console after IP input.	---- Deployment Target booting error ---- Unable to access files on Deployment Server. Check the connection from the Deployment Server (e.g. ping) If it is reachable from the Deployment Server, check: 1. Does the data network block NFS traffic? 2. Is this target 'Committed' in the Deployment Manager servers view? 3. Is NFS 'enabled' in the Deployment Manager servers view? If it is not reachable from Deployment Server, check: 1. ELAN/TLAN in the Deployment Manager view are not interchanged. 2. Valid IP settings are provided. 3. A valid Deployment Server TLAN IP Address is provided. 4. The physical cable connectivity of your ELAN/TLAN interfaces. 5. Ensure that proper TLAN routing on data network is enabled. Please press OK to proceed to reboot. OK
If a Compact Flash is created as a bootable USB by mistake and com1 install is used on a CP PM, the user would see slow message output, a messy display, and the error message appears on the COM port console after IP input.	------- Error downloading kickstart file ------ Unable to download the kickstart file. Please modify the kickstart parameter below or press Cancel to proceed as an interactive installation. hd:sdb1:/ ks_usb.cfg OK || Cancel

Hardware installation checklist

Before installing a Signaling Server in a CS 1000 system, complete the following checklist.

Warning:

Do not modify or use a supplied AC-power cord if it is not the exact type required in the region where you install and use the Signaling Server. Be sure to replace the cord with the correct type.

Table 7: Installation checklist

Have you:
Received all server equipment and peripherals? For a COTS server: • installation accessories for rack-mounting the server • AC-power cord • a DTE-DTE null modem cable (supplied) • NTE90672: Linux Signaling Server software DVD for COTS servers For an Avaya CS 1000M Server cards (NTDW66 CP PM and NTDW54 CP DC) • CP PM Signaling Server Linux Upgrade kit (CP PM only), which includes - CP PM Hard Drive kit (optional, provided if required) - 2 GB Compact Flash (CF) with Linux software, 2 GB blank CF - CP PM 1 GB DDR SO-DIMM memory upgrade (optional, provided if required; 2 GB memory required) - CP DC 2 x 2 GB memory upgrade (4 GB required for the CP DC card, as of Communication Server Release 7.6) • NTAK19ECE6: 2 port SDI Cable assembly kit • NTDW69AAE5: Large System Cabling kit • a DTE-DTE null modem cable (supplied) **Note:** Save the packaging and packing materials in case you must ship the equipment or peripherals.
Made sure the area meets all environmental requirements?
Checked for all power requirements?
Verify the CP PM hardware meets all required specifications (2GB ram, 40GB hard drive, CP PM BIOS version 18 or higher)?
Checked for correct grounding facilities?
Obtained the following? • screwdrivers • an ECOS 1023 POW-R-MATE or similar type of multimeter • appropriate cable terminating tools • a computer (maintenance terminal) to connect directly to the Signaling Server, with: - teletype terminal (ANSI-W emulation, serial port, 9600 bps) - a Web browser for Element Manager (configure cache settings to check for new Web pages every time the browser is invoked, and to empty the cache when the browser is closed)
Prepare the network data as suggested in *Avaya Converging the Data Network with VoIP, NN43001-260* and *Avaya Communication Server 1000E: Planning and Engineering, NN43041-220* or *Avaya*

Table continues…

Have you:
Communication Server 1000M and Meridian 1: Large System Planning and Engineering, NN43021-220, as appropriate for your Avaya CS 1000 system?
Read all safety instructions in *Avaya Communication Server 1000E Installation and Commissioning, NN43041-310* or *Avaya Communication Server 1000M and Meridian 1 Large System Installation and Commissioning, NN43021-310*, as appropriate for your Avaya CS 1000 system?

CP PM card

The Common Processor Media Card is a Server card that you can deploy as a VxWorks Call Server, a Linux Base Signaling Server, or a Linux Base Co-resident Call Server and Signaling Server (Co-res CS and SS).

The CP PM card is available in multiple variants:

- a single slot card for CS 1000E systems (NTDW61)
- a double-slot card for CS 1000M systems (NTDW66)
- a single slot metal faceplate for CS 1000E systems (NTDW99)

Note:

Co-res CS and SS can only be installed on a NTDW61BAE5 CP PM server.

Avaya Linux Base requires CP PM servers to meet criteria for disk size, memory size, and BIOS version. Perform the following procedures to determine CP PM disk size, CP PM memory size, and CP PM BIOS version, and to upgrade the CP PM BIOS version.

Determining CP PM disk size

Perform the following procedure to determine the CP PM disk size.

1. Connect to the CP PM server remotely by using SSH or locally by using a serial port.

   Important:

   The Avaya NTAK19EC cabling kit is required to connect a maintenance terminal to the serial port of a CP PM or CP DC card as follows.

   - to adapt the 50-pin MDF connector at the back of the CS 1000E Media Gateway or the CS 1000M Universal Equipment Module (UEM) to a 25-pin DB connector
   - a 25-pin to 9-pin straight-through serial cable (not supplied) is required to connect the 25-pin DB connector to a 9-pin serial port on the maintenance terminal

2. Log on to the CP PM server in a systemadmin role.
3. Issue the Linux **`hdparm`** command:

   The disk size appears as shown in the following figure.

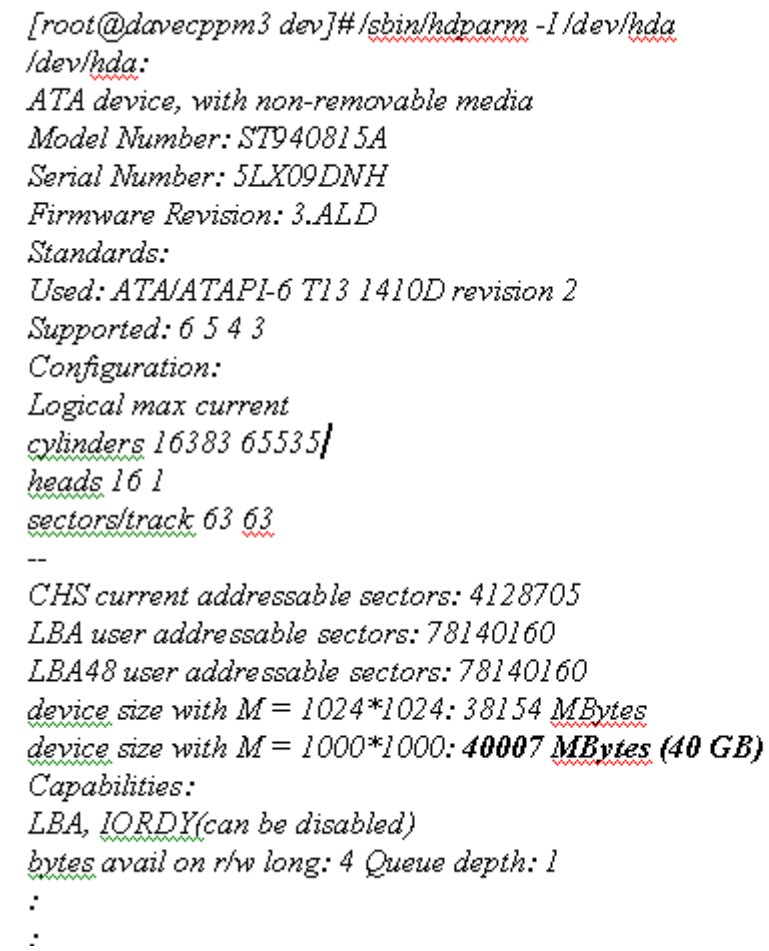


Figure 132: CP PM disk size

Determining CP PM memory size

Perform the following procedure to determine the CP PM memory size.

1. Connect to the CP PM server remotely by using SSH or locally by using a serial port.
2. Log on to the CP PM server.
3. Issue the Linux command to read the /proc/meminfo file.

   The command and results appear in the following figure.

```
[ avaya@ccVxELL_cppm ~]$ cat /proc/meminfo
MemTotal: 1023548 kB <- need to update with 2G nums
MemFree: 841920 kB
Buffers: 28732 kB
Cached: 120380 kB
SwapCached: 0 kB
```

Figure 133: CP PM memory size

BIOS methods

This section provides the procedures for determining and upgrading the CP PM BIOS.

Determining CP PM BIOS Method 1

Determine the CP PM BIOS Method 1.

1. Power up the CP PM hardware.
2. Observe the CP PM BIOS output in the bootup screen, as shown in the following figure.

```
+-------------------------------------------------------------+
| System BIOS Configuration, (C) 2005 General Software, Inc.
+--------------------------+----------------------------------+
| System CPU : Pentium M   | Low Memory      : 632KB          |
| Coprocessor: Enabled     | Extended Memory : 1011MB         |
| Ide 0 Type : 3           | Serial Ports 1-2 : 03F8 02F8     |
| Ide 1 Type : 3           | ROM Shadowing   : Enabled        |
| Ide 2 Type : 3           | BIOS Version    : NIDU74AA18 |
|+-------------------------+----------------------------------+
Press F to force board to boot from faceplate drive.
```

Figure 134: CP PM boot up window

3. If the BIOS needs to be updated, see Upgrading the CP PM BIOS on page 214

Determining CP PM BIOS Method 2

Determine the CP PM BIOS Method 2.

1. Connect to the CP PM server remotely by using SSH or locally by using a serial port.
2. Log on to the CP PM server.

3. Type the Linux command to read the cppmHWInfo.dat file in the /etc/opt/avaya/base folder.

   The BIOS version appears as shown in the following figure.

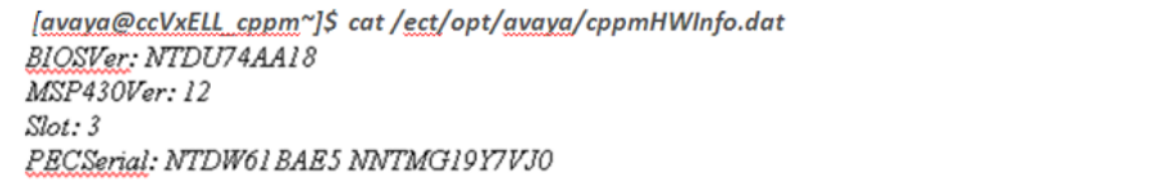


Figure 135: CP PM BIOS version display

Upgrading the CP PM BIOS

Upgrade the BIOS on a CP PM server.

Prerequisites:

- You must have a bootable Removable Media Device (RMD) Compact Flash (CF).

1. Connect to serial port 1 on the CP PM server.
2. Insert the Linux Base installation CF card into the faceplate CF slot.
3. Power on the system.

   Once the initial boot and memory check completes, the CP PM initial boot screen appears.
4. Press the `F` key to boot from the Linux Base installation faceplate CF card.
5. Press ENTER to direct the input and output to COM1.

   The CS 1000 Linux Base system installer (CP PM server) screen appears, as shown in the following figure.

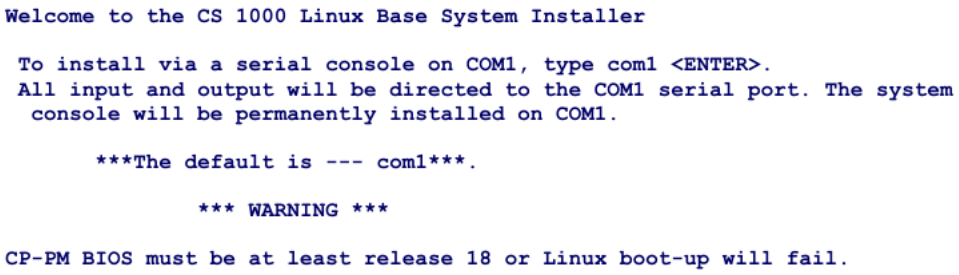


Figure 136: CS 1000 Linux Base system installer (CP PM server)

If the CP PM server BIOS version is lower than 18, the BIOS upgrade screen appears, as shown in the following figure.

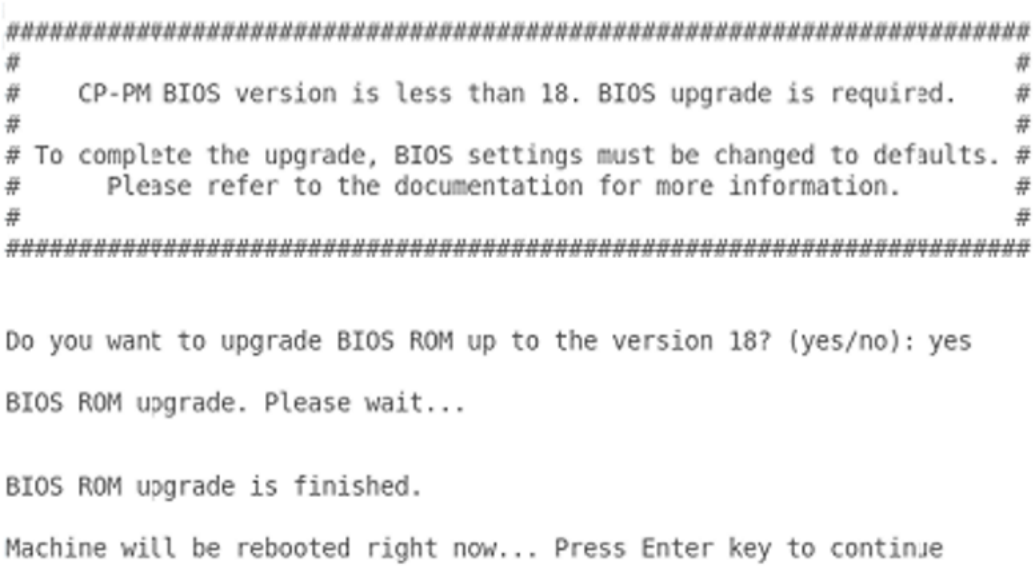


Figure 137: CP PM BIOS upgrade window

6. Type `yes` to proceed with the automatic upgrade.
7. Verify that the BIOS upgrade is finished.
8. Press `F` to restart the server.
9. During the restart memory check, press `Ctrl c` to access the CP PM BIOS setup menu.

   Note:

   If you miss the timing to press Ctrl c you must restart the system and try again. The Linux Base installation software displays a warning if you do not reset the CP PM BIOS to factory defaults.

   The CP PM BIOS setup screen appears, as shown in the following figure.

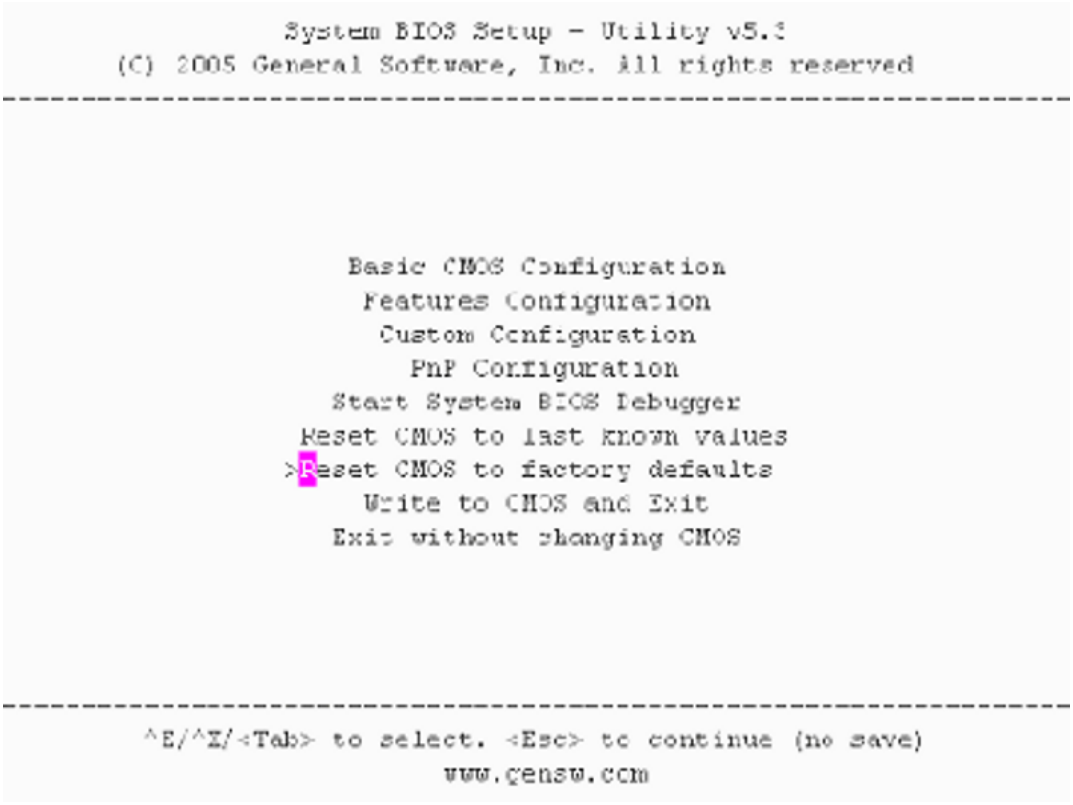


Figure 138: CP PM BIOS setup window

10. Select **Reset CMOS to factory defaults** from the menu.

    The CP PM BIOS reset screen appears, as shown in the following figure.

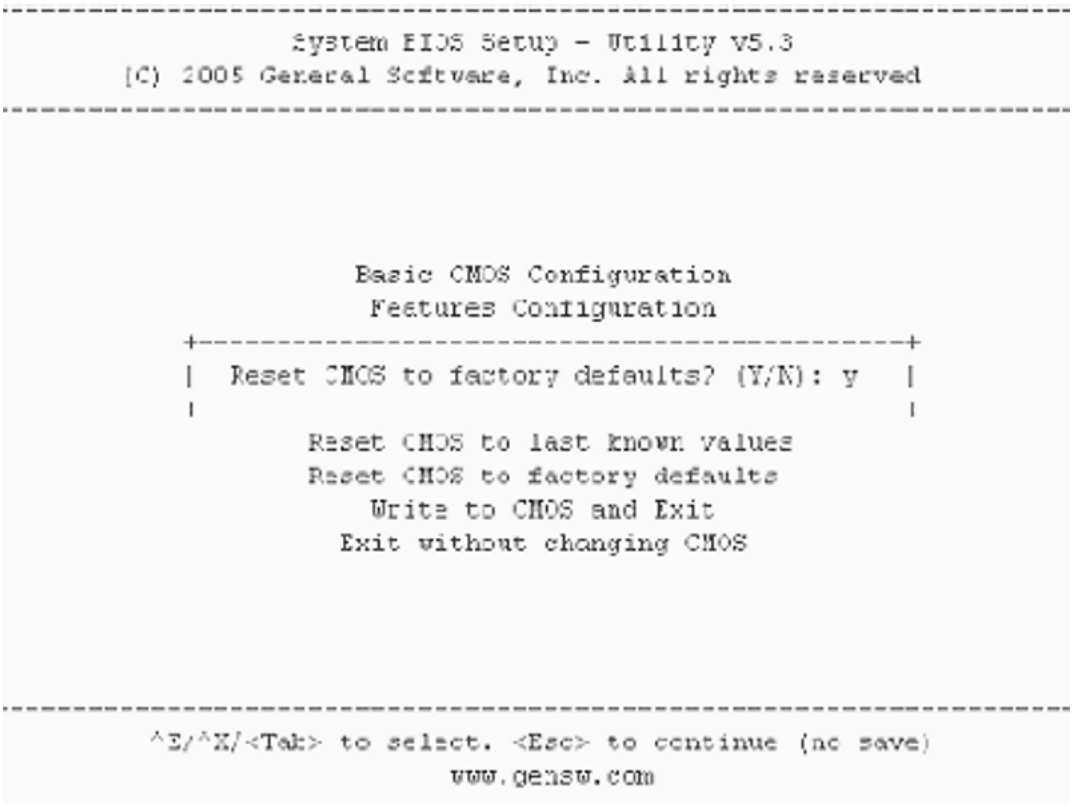


Figure 139: CP PM BIOS reset window

11. Press `y` to reset CMOS to factory defaults.
12. The system restarts. After initial boot, the CP PM initial boot screen appears and the new BIOS version is displayed. Verify the BIOS version is 18. You can now press the F key to boot from the faceplate CF card and proceed with the Linux Base software installation.

CP PM Signaling Server

This section contains instructions to install and connect the NTDW61BAE5 and NTDW66AAE5 models of the CP PM Signaling Server to the ELAN and TLAN subnets of a CS 1000E and CS 1000M system, respectively. The CP PM Signaling Server is a circuit card and therefore is not mounted in a rack. This section also contains instructions to connect a maintenance terminal to the CP PM Signaling Server.

The NTDW61BAE5 model of the CP PM Signaling Server is designed for use in a CS 1000E system. It is inserted into a slot of the Media Gateway (MG 1000E or MG 1000B). The Media Gateway also hosts the Gateway Controller that has Ethernet ports for connecting to the ELAN and TLAN subnets of your CS 1000 system. However, it is common in a CS 1000E system for the Call Server to connect to the Gateway Controller through the ELAN port. If the Call Server does not connect to the Gateway Controller through this port, the NTDW61BAE5 model of the CP PM Signaling Server uses it to connect to the ELAN subnet of the CS 1000E system. If the Call Server uses the Gateway Controller ELAN port, the CP PM Signaling Server connects directly to the ELAN and TLAN Ethernet switches from the faceplate ELAN and TLAN Ethernet ports.

The NTDW66AAE5 model of the CP PM Signaling Server is designed for use in a CS 1000M system. It is inserted into a slot of a Universal Equipment Module (UEM). UEMs do not have built-in ELAN and TLAN Ethernet ports. These Ethernet ports must be installed on the back of the UEM to enable the CP PM Signaling Server to connect to the ELAN and TLAN subnets of your CS 1000 system.

The following figure shows the faceplates of the two models of the CP PM server with labeling for all components (NTDW61BAE5 on the left and NTDW66AAE5 on the right).

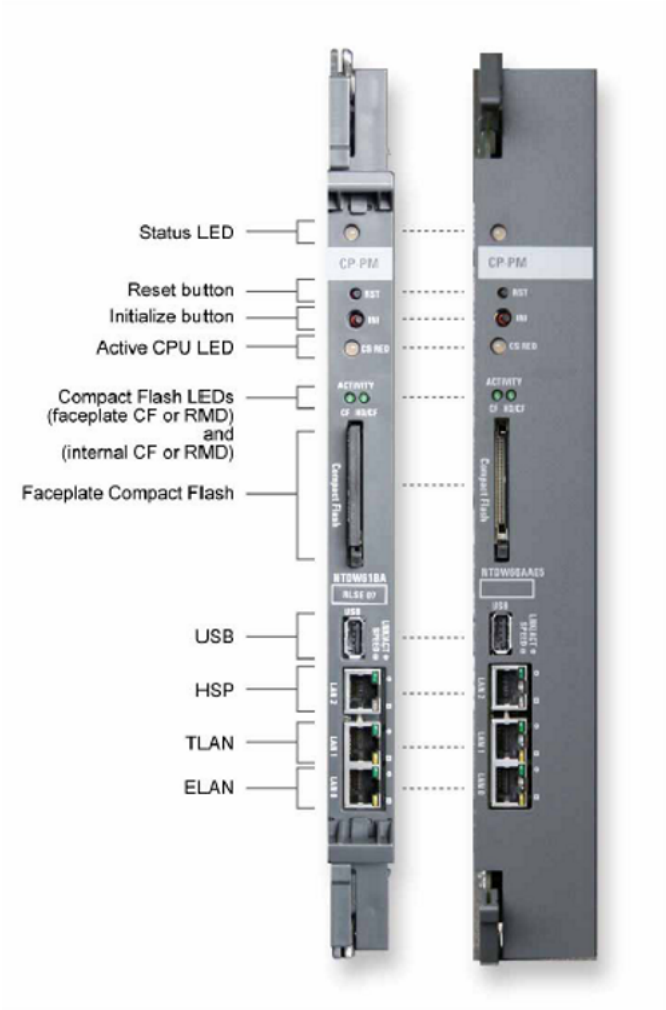


Figure 140: Faceplates of the CP PM server

Refer to the preceding figure when you perform the following procedures.

Connecting a CP PM Signaling Server

Perform the following procedure to connect a CP PM Signaling Server.

1. Establish a maintenance terminal connection at the back of the Media Gateway (CS 1000E) or Universal Equipment Module (CS 1000M) shelf.

The com (SDI) port of the CP PM server is routed through the backplane to the 50-pin MDF connector on the back of the MG or UEM shelf. A special cable (NTAK19EC) ships with the CP PM server that adapts the 50-pin MDF connector to a 25-pin DB connector. You need a 25-pin to 9-pin straight-through serial cable to connect from the 25-pin DB connector to the serial port on the back of your PC.

a. Connect the NTAK19EC cable (shipped with the CP PM server) to the 50-pin MDF connector on the back of the shelf.

b. Connect a 25-pin to 9-pin straight-through serial cable to the 25-pin DB connector at the end of the NTAK19EC cable.

c. Connect the other end of the serial cable to the serial port on the maintenance terminal.

2. Insert the CP PM server into the slot corresponding to the shelf where you connected the NTAK19EC cable.

   The server is hot-pluggable so you can insert it without powering off the system.

   The maintenance terminal is now connected to the server.

3. Connect the CP PM Signaling Server to the ELAN and TLAN subnets of the CS 1000 system.

   - If you have a CS 1000E system, perform Connecting a CP PM Signaling Server to the ELAN and TLAN subnets of a CS 1000E system on page 221.
   - If you have a CS 1000M system, perform Connecting a CP PM Signaling Server to the ELAN and TLAN subnets of a CS 1000M system on page 222.

4. Configure the baud rate for the serial port on the Signaling Server to 9600 bits per second.

   Note:

   The CP PM Signaling Server ships with the serial port configured to 9600 bits per second.

   To verify or change the baud rate on a CP PM Signaling Server, see Changing the baud rate on a CP PM Signaling Server on page 219.

5. Configure the connected maintenance terminal.

Changing the baud rate on a CP PM Signaling Server

Perform this procedure to verify or change the baud rate on a CP PM Signaling Server.

1. Press the **RST** button on the faceplate of the Signaling Server to boot the Signaling Server.
2. Press `Ctrl+C` keys at the same time to invoke the BIOS Setup menu.

   The CP PM System BIOS Menu screen appears.

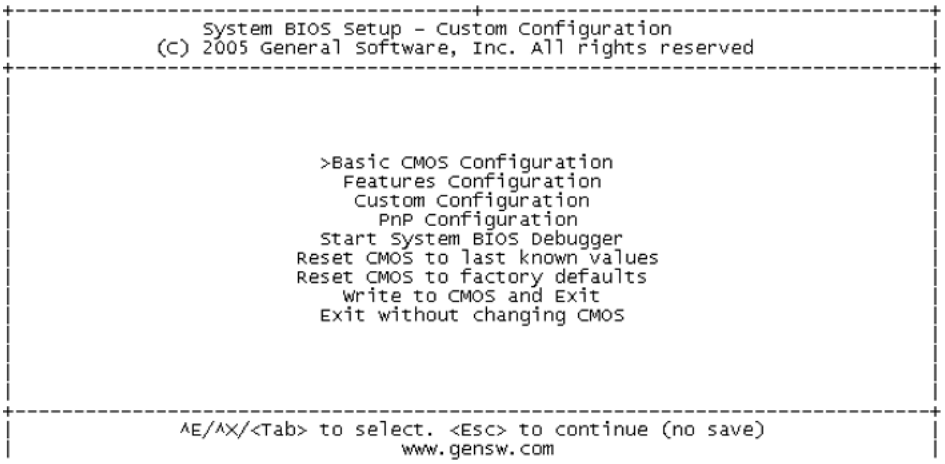


Figure 141: CP PM System BIOS menu

3. Navigate to **Custom Configuration** and select the option.

   The Custom Configuration screen appears.

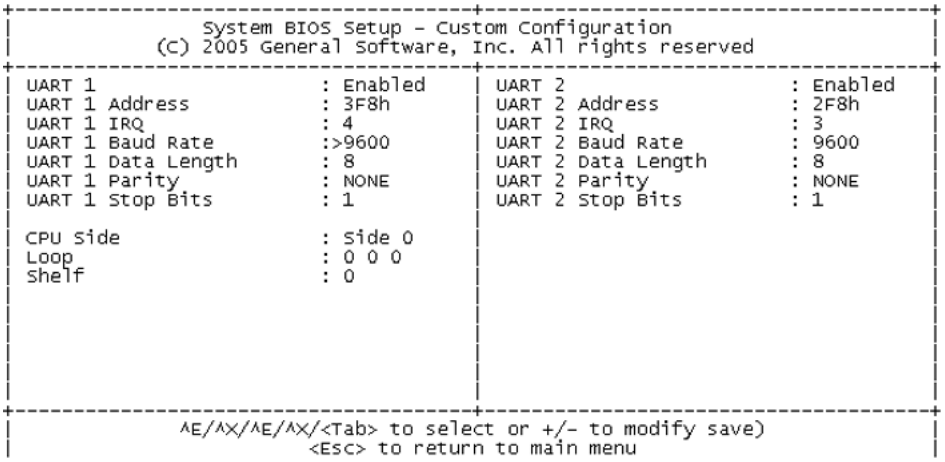


Figure 142: CP PM Customer Configuration

4. Navigate to the **UART 1 Baud Rate** option and change as necessary.
5. Navigate to the **UART 2 Baud Rate** option and change as necessary.

   Note:

   UART 2 connection does not print BIOS messages.

6. Press **Esc** to save the settings and return to the BIOS Menu screen.
7. Select **Write to CMOS and Exit** to exit the CP PM server BIOS menu.

Installation in a CS 1000E system

The NTDW61BAE5 model of the CP PM Signaling Server is designed for use in an Avaya CS 1000E system. The first task that must be performed is to install the hard drive shipped with the server.

You can insert the NTDW61BAE5 model of the CP PM server into any slot of a CS 1000E Media Gateway (MG 1000E or MG 1000B) or 11C cabinet or chassis, except slot 0. Slot 0 is reserved for a Small System Controller (SSC) card or a Gateway Controller. Keying prevents the NTDW61BAE5 model from being inserted into this slot.

Warning:

Do not insert the NTDW61BAE5 model of the CP PM server into any slot of a CS 1000M Universal Equipment Module (UEM). Doing so can cause electrical shorts on adjacent circuit cards.

Connecting a CP PM Signaling Server to the ELAN and TLAN subnets of a CS 1000E system

Perform the following procedure to connect a CP PM Signaling Server (model NTDW61BAE5) to the ELAN and TLAN subnets of a CS 1000E system.

1. Connect the Signaling Server to the ELAN subnet.
   - if the CS 1000 Call Server is not connected to the Gateway Controller.
     - Insert the end of one customer supplied 25-cm RJ-45 CAT5 Ethernet cable into the ELAN network interface port (ELAN port) on the faceplate of the CP PM Signaling Server.
     - Insert the other end of the 25-cm RJ-45 CAT5 Ethernet cable into the Gateway Controller ELAN Ethernet port.
   - if the CS 1000 Call Server is connected to the Gateway Controller
     - Insert the end of a longer RJ-45 CAT5 Ethernet cable (not supplied) into the ELAN network interface port (ELAN port) on the faceplate of the CP PM Signaling Server.
     - Insert the other end of the RJ-45 CAT5 Ethernet cable into an Ethernet port on the ELAN Ethernet switch.
2. Connect the Signaling Server to the TLAN subnet.
   - if the CS 1000 Call Server is not connected to the Gateway Controller
     - Insert the end of one customer supplied 25-cm RJ-45 CAT5 Ethernet cable into the TLAN network interface port (TLAN port) on the faceplate of the CP PM Signaling Server.

- Insert the other end of the 25-cm RJ-45 CAT5 Ethernet cable into the Gateway Controller TLAN Ethernet port.

• if the Call Server is connected to the Gateway Controller

- Insert the end of a longer RJ-45 CAT5 Ethernet cable (not supplied) into the TLAN network interface port (TLAN port) on the faceplate of the CP PM Signaling Server.
- Insert the other end of the RJ-45 CAT5 Ethernet cable into an Ethernet port on the TLAN Ethernet switch.

Note:

If the Call Server is connected to the Media Gateway Controller, you must obtain CAT5 Ethernet cables that are long enough to connect the Signaling Server directly to the ELAN and TLAN Ethernet switches from the faceplate ELAN and TLAN Ethernet ports.

Connecting a CP PM Signaling Server to the ELAN and TLAN subnets of a CS 1000M system

Perform this procedure to connect a CP PM Signaling Server (model NTDW66AAE5) to the ELAN and TLAN subnets of a CS 1000M system.

Important:

IMPORTANT!

Connecting a CP PM Signaling Server to the ELAN and TLAN subnets of a CS 1000M system causes a service disruption.

1. Insert the end of an RJ-45 CAT5 Ethernet cable (not supplied) into the ELAN network interface port (ELAN port) on the back of the CS 1000M UEM.

   You installed this ELAN port at the back of the UEM when you installed the Signaling Server in the UEM.

2. Insert the other end of the RJ-45 CAT5 Ethernet cable into an Ethernet port on the ELAN Ethernet switch.
3. Insert the end of another RJ-45 CAT5 Ethernet cable (not supplied) into the TLAN network interface port (TLAN port) on the back of the CS 1000M UEM.

   You installed this TLAN port at the back of the UEM when you installed the Signaling Server in the UEM.

4. Insert the other end of the RJ-45 CAT5 Ethernet cable into an Ethernet port on the TLAN Ethernet switch.

CP DC card

The Common Processor Dual Core (CP DC) server is a dual core platform supported for all of the Signaling Server applications. It can also be used for Co-Res CS and SS systems for up to approximately 1000 users with a Media Gateway Card.

As of Communication Server 1000 Release 7.6, the CP DC card requires 4 GB of memory, which for some deployments would be a memory upgrade.

For more information about the supported configurations and memory requirements of the CP DC card, see *Communication Server 1000E Planning and Engineering, NN43041–220*.

Determining CP DC memory size

Perform the following procedure to determine the CP DC memory size.

1. Connect to the CP DC server remotely by using SSH or locally by using a serial port.
2. Log on to the CP DC server.
3. Issue the Linux command to read the `/proc/meminfo` file.

   The results (from a 4 GB CP DC) display as shown in the following example:

```
[admin2@cap26
~]$ cat /proc/meminfo
MemTotal:      4117636 kB
MemFree:        111044 kB
Buffers:        483440 kB
...
```

CP MG card

The CP MG card functions as a Server and the Gateway Controller while occupying slot zero in a chassis, cabinet and MG 1010.

- CP MG 32: This hardware is a combination Server and a Gateway Controller with 32 DSPs. It frees up a slot and is used in a Co-Res CS and SS mode for cost effective solution for Branch Offices under 100 users.
- CP MG 128: This hardware is a combination Server and a Gateway Controller with 128 DSPs. It frees up a slot and is the standard solution for Co-Res CS and SS systems for up to approximately 700 users and for Branch Offices.

As of Communication Server 1000 Release 7.6, the CP MG card requires 4 GB of memory, which for some deployments would be a memory upgrade.

For more information about the supported configurations and memory requirements of the CP MG card, see *Communication Server 1000E Planning and Engineering, NN43041–220*.

Determining CP MG memory size

Perform the following procedure to determine the CP MG memory size.

1. Connect to the CP MG server remotely by using SSH or locally by using a serial port.
2. Log on to the CP MG server.
3. Issue the Linux command to read the `/proc/meminfo` file.

   The results (from a 4 GB CP MG) display as shown in the following example:

```
[admin2@cap24
~]$ cat /proc/meminfo
MemTotal:      3049016 kB
MemFree:        217700 kB
Buffers:        578140 kB
```

Dell R300 server

The Dell R300 server provides the following features:

- Intel Xeon (quad-core) processor
- Two 80 GB SATA Hard drives (1 configured)
- Four GB PC2-4200 ECC DDR2 SDRAM (2 GB configured)
- Two 10/100/1000BaseT Ethernet ports
- Three USB ports
- One CD-R/DVD ROM drive
- One serial port
- A reset button

The following figure shows the front view of the Dell R300 server.

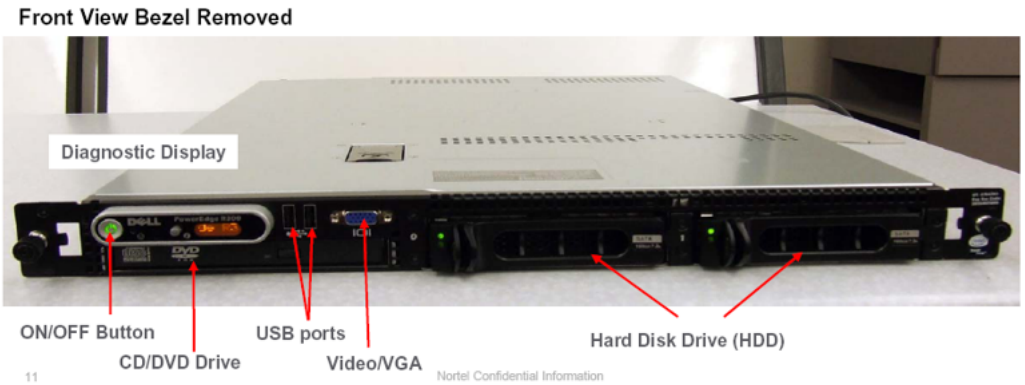


Figure 143: Dell R300 server front view

The following figure shows the rear view of the Dell R300 server.

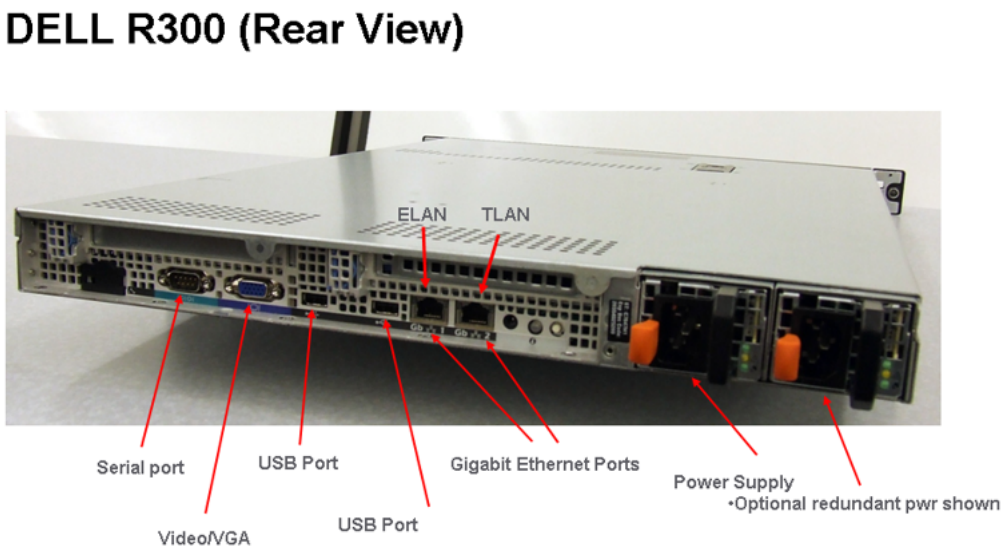


Figure 144: Dell R300 server rear view

Configuring the COM1 serial port on a Dell R300 server

Perform the following procedure to configure the COM1 serial port.

1. Press **F2** to navigate to the BIOS configuration main menu screen using a Keyboard Video Monitor (KVM) terminal.

   OR

   Press **ESC-2** to navigate to the BIOS configuration main menu screen using the console terminal.

   The BIOS configuration main menu screen appears, as shown in Figure 145: BIOS configuration main menu window on page 226.

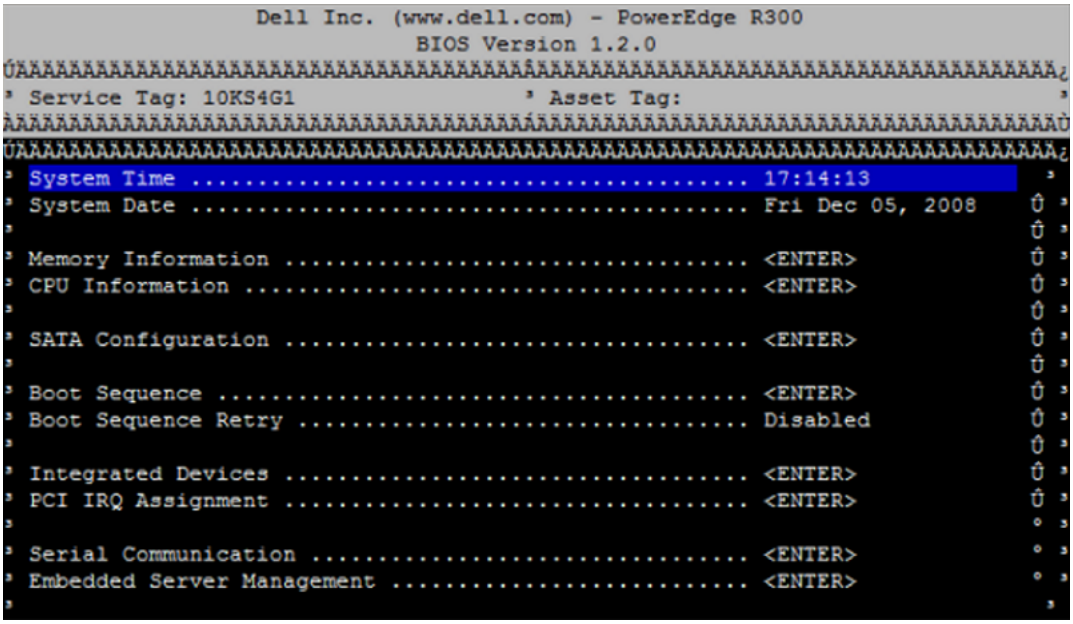


Figure 145: BIOS configuration main menu window

2. In the BIOS configuration main menu screen, select **Serial Communication** and press **Enter** to continue. The Serial Communication screen appears.
3. In the Serial Communication line, type `On with Console Redirection through COM1`.
4. In the External Serial Connector line, type `COM1`.
5. In the Failsafe Baud Rate line, type `9600`.
6. In the Remote Terminal Type line, type `Remote Terminal Type`.
7. In the Redirection After Boot line, type `Enabled`.

   The Serial Communication screen containing the correct values appears in Figure 146: Serial Communication window on page 227.

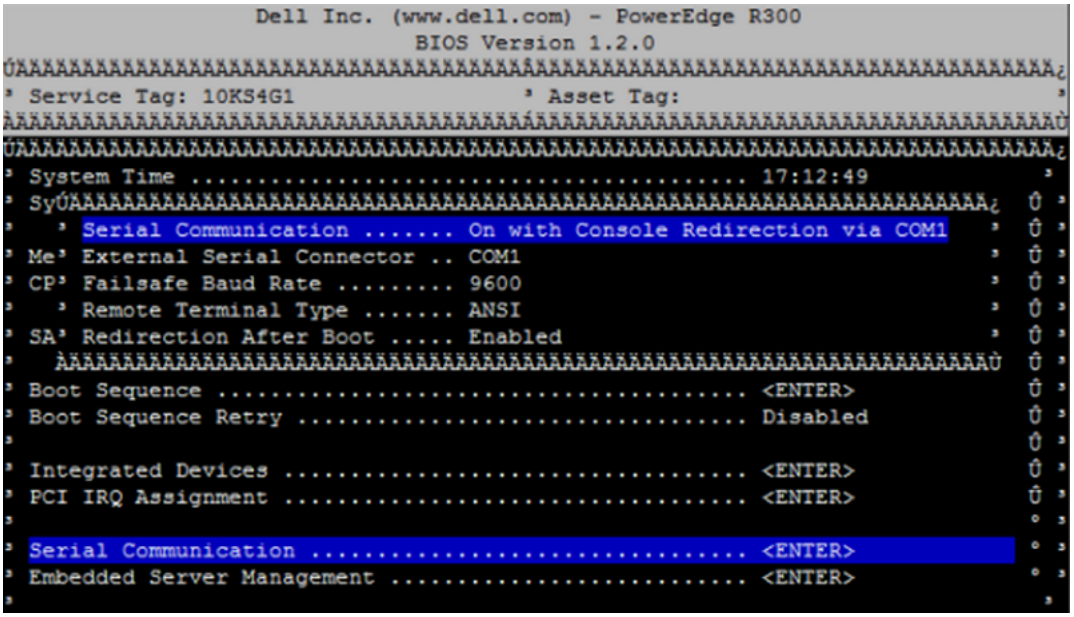


Figure 146: Serial Communication window

8. Press **Esc** to return to the BIOS configuration main menu.

   In the BIOS configuration main menu screen you can perform other changes or you can exit and save the changes you made.

9. If you want to exit and save your changes, press **Esc**.

   A prompt to save changes appears, as shown in Figure 147: Save changes and exit window on page 227.

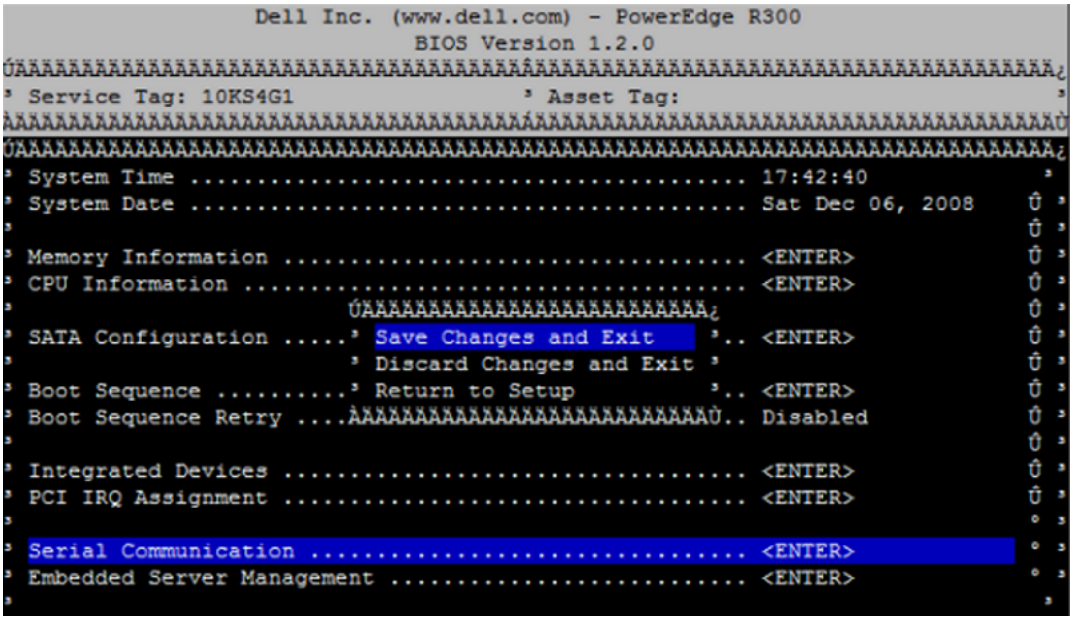


Figure 147: Save changes and exit window

10. Select **Save Changes and Exit**, and then press **Enter**.

Setting the BIOS password for the Dell R300 server

Perform the following procedure to set the BIOS password.

1. Press **F2** to navigate to the BIOS configuration main menu screen using a Keyboard Video Monitor (KVM) terminal.

   OR

   Press **ESC-2** to navigate to the BIOS configuration main menu screen using the console terminal.

   The BIOS configuration main menu screen appears, as shown in Figure 148: BIOS configuration main menu window on page 228.

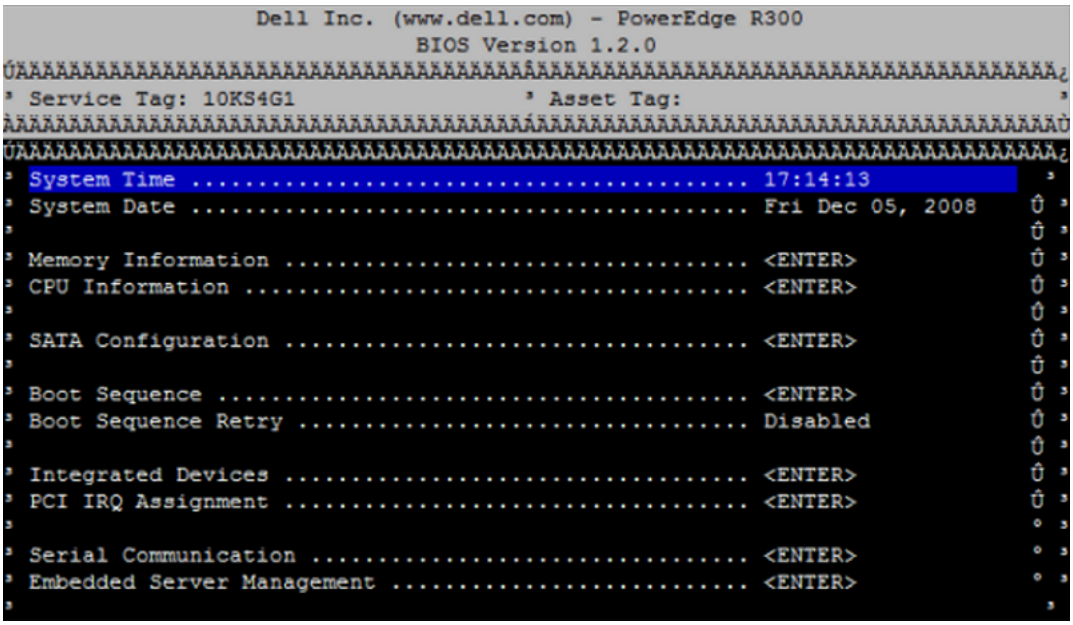


   Figure 148: BIOS configuration main menu window

2. In the main menu screen, select System Security and press Enter.

   The System Security menu appears, as shown in Figure 149: System Security menu on page 229.

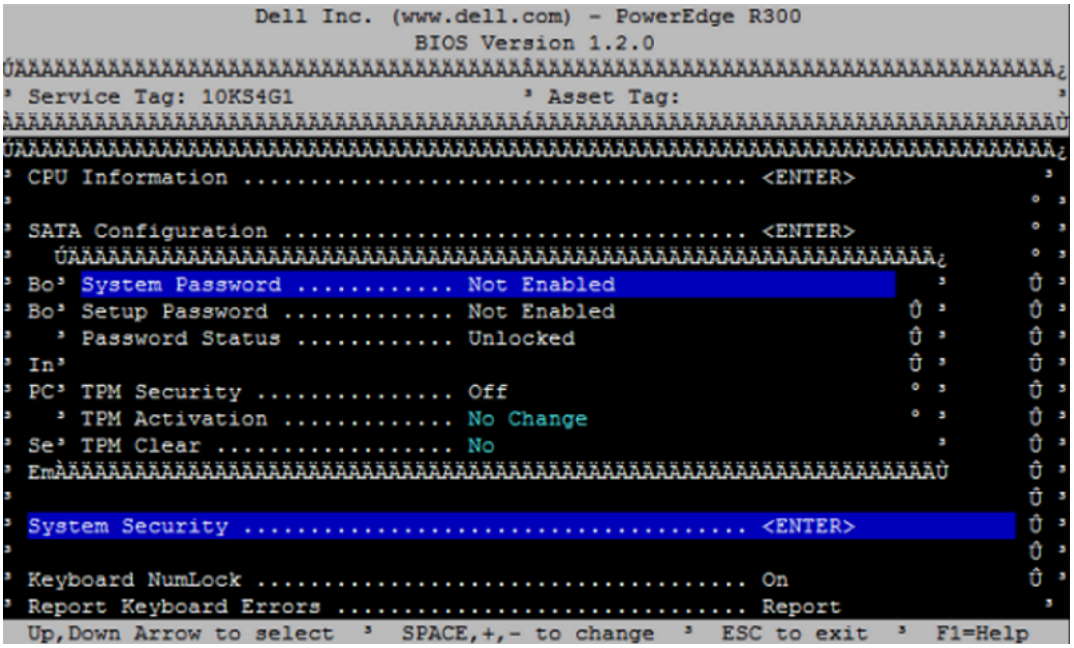


Figure 149: System Security menu

3. In the System Security menu, select **Setup Password** and press **Enter**.

   The password entry screen appears, as shown in Figure 150: Password entry window on page 229.

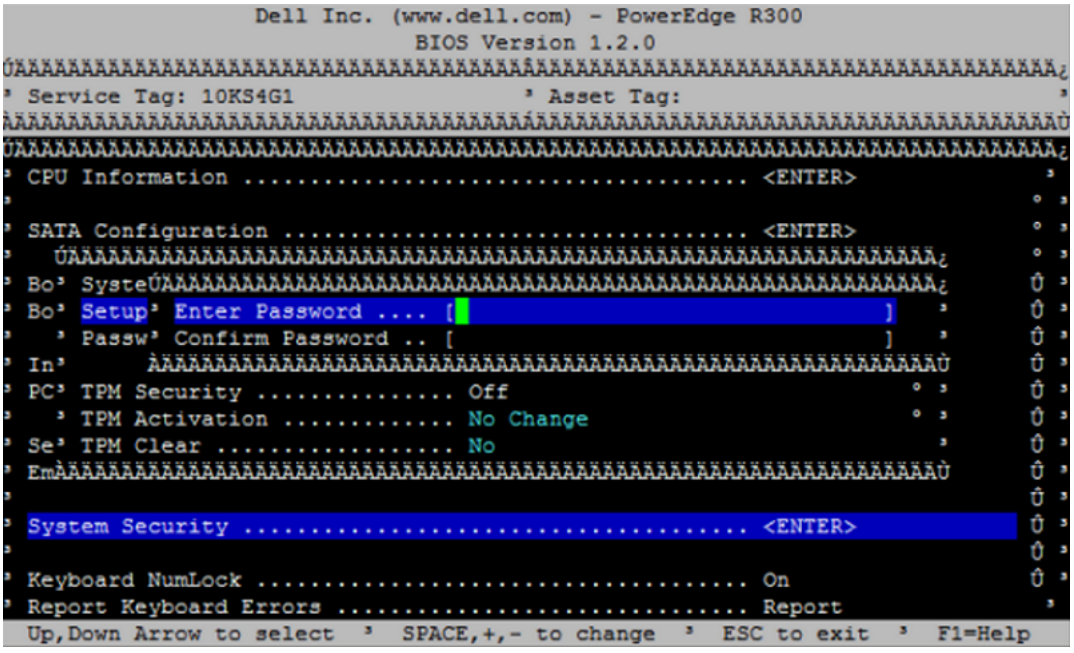


Figure 150: Password entry window

4. Type the new password. Press **Enter** to continue.
5. Type the password again to confirm the values, and then press **Enter**.

The password is now enabled, as shown in Figure 151: Password enabled window on page 230.

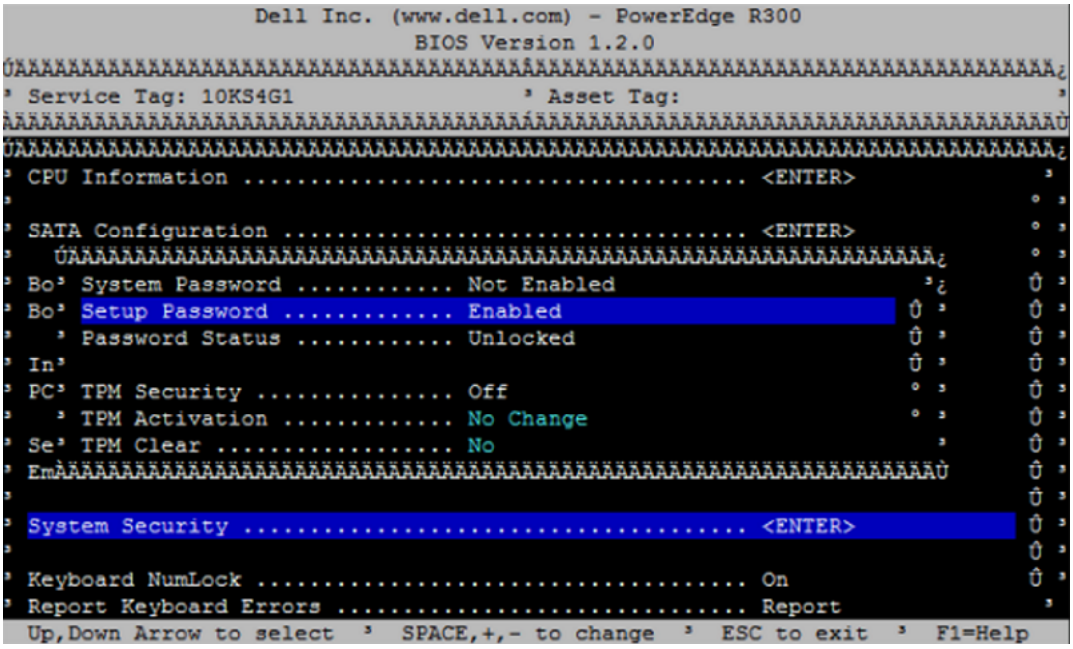


Figure 151: Password enabled window

6. Press **Esc** to return to the BIOS configuration main menu.

   In the BIOS configuration main menu screen you can perform other changes, or your can exit and save the changes you made.

7. If you want to exit and save your changes, press **Esc**.

   A prompt to save changes appears, as shown in Figure 152: Save changes and exit window on page 231.

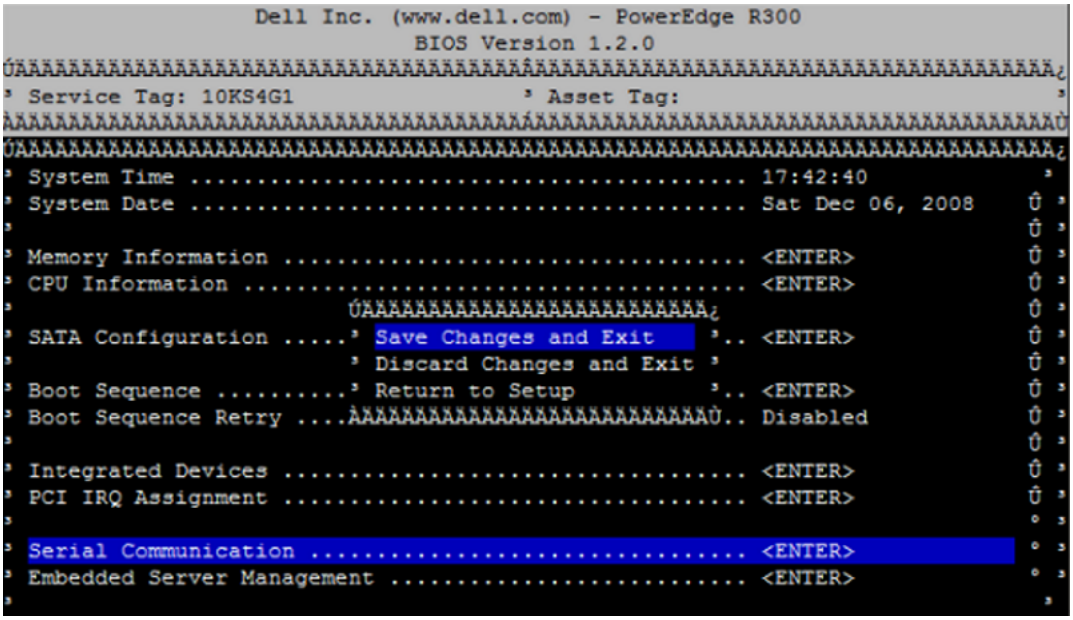


Figure 152: Save changes and exit window

8. Select **Save Changes and Exit**, and then press **Enter**.

Configuring RAID settings

Avaya does not support PER PLM Raid drive configurations.

HP DL320 G4 server

The HP DL320 G4 server provides the following features:

- Intel Pentium 4 processor (3.6 GHz)
- Two 80 GB SATA Hard drives (1 configured)
- Four GB PC2-4200 ECC DDR2 SDRAM (2 GB configured)
- Two 10/100/1000BaseT Ethernet ports
- Three USB ports
- One CD-R/DVD ROM drive
- One serial port
- A reset button

Figure 153: HP DL320 G4 front view on page 232 shows the front view of the HP DL320 G4 server.

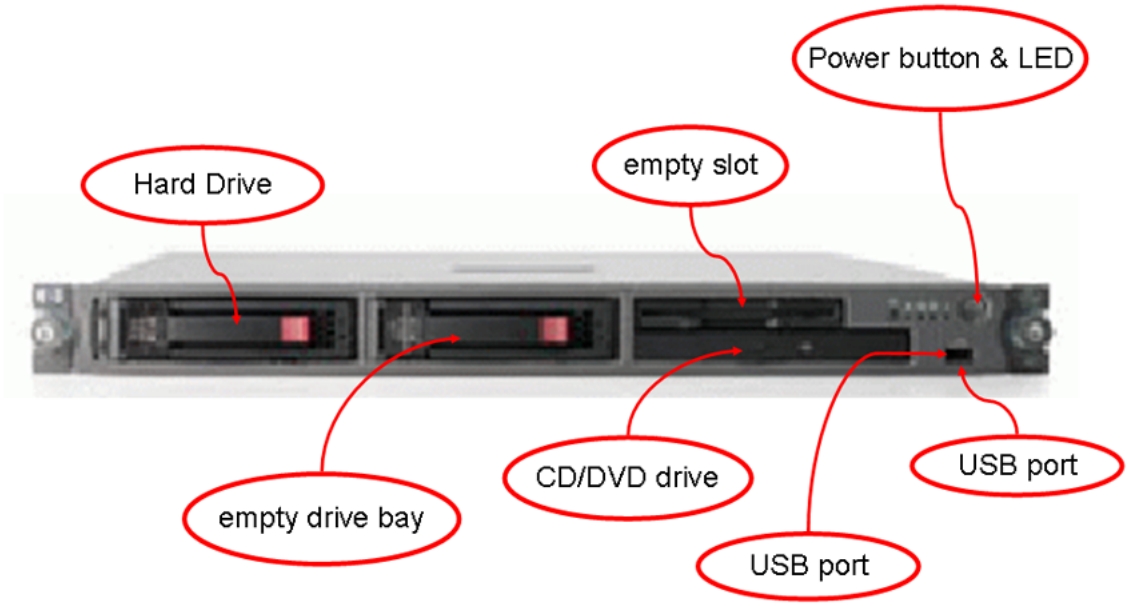


Figure 153: HP DL320 G4 front view

Figure 154: HP DL320 G4 front view: LEDs

Table 8: HP DL320 G4 LED item description and status

Item	Description	Status
1	UID button LED (Unit Identification)	Blue – Identification is activated. Flashing blue – System is remotely managed. Off – Identification is deactivated.
2	Internal health LED	Green –- System health is normal. Amber – System is degraded. To identify the component, check the system board LEDs.

Table continues…

Item	Description	Status
		Red – Critical. To identify the component in a critical state, check the system board LEDs. Off – System health is normal (when in standby mode).
3	NIC 1 link/activity LED	Green – Network link exists. Flashing green – Network link and activity exist. Off – No link to network exists.
4	NIC 2 link/activity LED	Green –Network link exists. Flashing green – Network link and activity exist. Off – No link to network exists.
5	Drive activity LED	Green – Drive activity is normal. Amber – Drive failure occurred. Off – No drive activity.
6	Power button and LED	Green – System is on. Amber – System is shut down, but power is still applied. Off – Power not available.

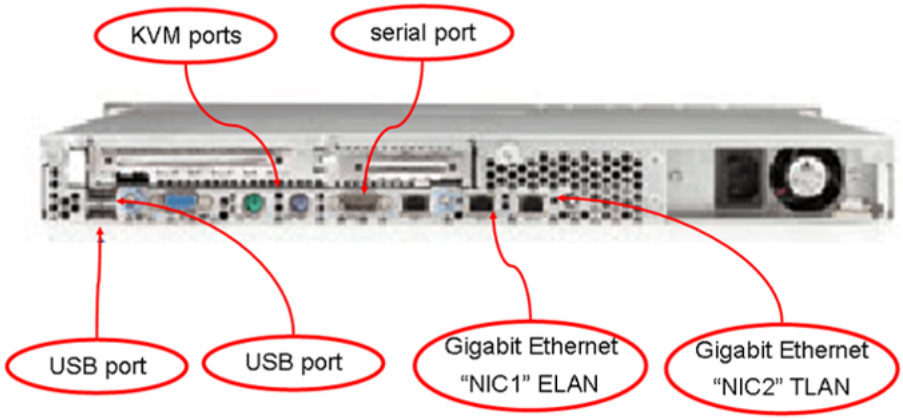


Figure 155: HP DL320 G4 rear view

Important:

The TLAN and ELAN port positions are reversed (L and R, 1 and 2) compared to the IBM x306m server.

HP DL320 G4 BIOS settings

The Basic Input Output System (BIOS) settings on the HP DL320 G4 server shipped through Avaya are correct. The BIOS settings do not require adjustment unless they are reset due to a fault or

through maintenance. If a reset of the BIOS settings occurs, check the serial port option. The HP DL320 G4 BIOS settings can be seen at Table 9: HP DL320 G4 default BIOS settings on page 234. The HP DL320 G4 servers provide a physical COM1 serial port and a virtual (ILO) COM2 serial port. If the setting for the serial console port is Auto, output can be directed to either the COM1 port or COM2 ILO port. Set the serial console port option to COM1 to ensure the console output goes to the physical COM1. See Configuring the COM1 serial port on an HP DL320 G4 server on page 234 for instructions. The HP DL320 G4 server shipped through Avaya has a default baud rate of 9600 bits per second and does not require a reset. If an error occurs and you want to reset the baud rate, or if you want to change to another baud rate, see Changing the baud rate on an HP DL320 G4 Signaling Server on page 235 for instructions.

For information about how to enable or disable the BIOS password on the HP DL320 G4 server see Setting the HP DL320 G4 server BIOS password on page 237.

Table 9: HP DL320 G4 default BIOS settings

BIOS value	Default setting
Devices and I/O port - serial port A	Enabled
Devices and I/O port - baud rate	9600 baud
Devices and I/O port - type of connector	9-pin serial female
Start options - legacy USB support	Disabled

Configuring the COM1 serial port on an HP DL320 G4 server

1. Press Power to boot the server.

   The server boots and the HP DL320 G4 boot screen appears.

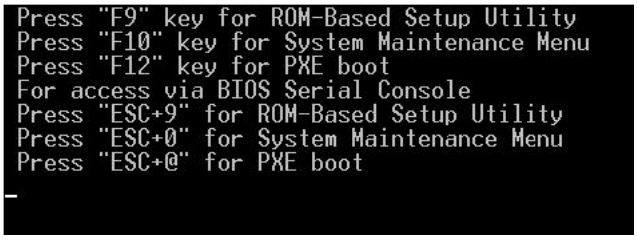


Figure 156: HP DL320 G4 server boot screen

Note:

If the server is already up and running, power the server off and on to restart and receive the HP DL320 G4 boot screen.

2. Press F9 to invoke the ROM-based setup utility (RBSU) menu screen.

   The RBSU menu screen appears.

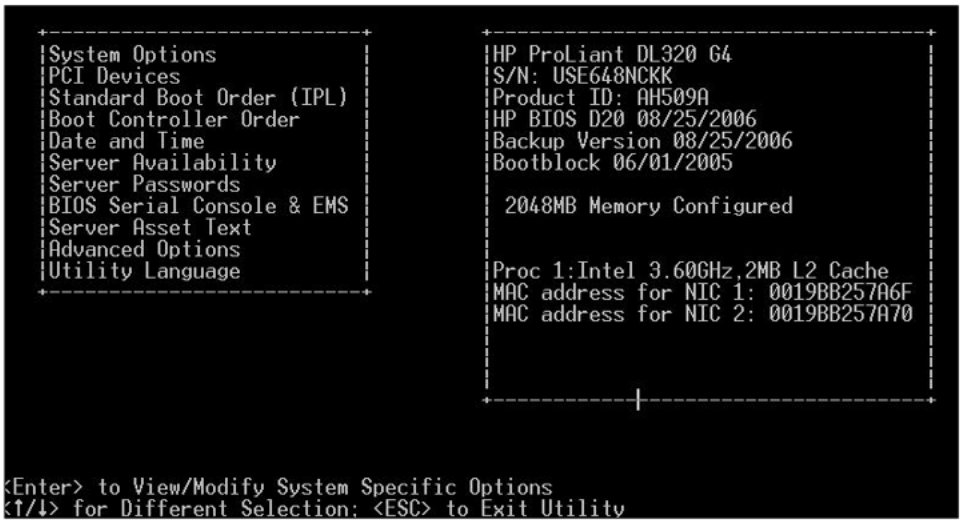


Figure 157: HP DL320 G4 server RBSU menu

3. Navigate to the **BIOS Serial Console & EMS** option and press Enter.

   A BIOS Serial Console & EMS configuration menu screen appears.

4. Navigate to the **BIOS Serial Console Port** option and press **Enter**.

   A BIOS Serial Console Port configuration screen appears. This screen presents you with four options:

   - 1 | Auto
   - 2 | Disabled
   - 3 | COM1
   - 4 | COM 2

5. Navigate to the **COM1** option and press **Enter**.

   This configures the COM1 port as the serial port for communicating with the connected maintenance terminal.

   The BIOS Serial Console & EMS configuration menu screen reappears.

6. Press **ESC** to exit the BIOS Serial Console & EMS configuration menu screen.

   The RBSU menu screen reappears.

7. Press **ESC** to exit the ROM-based Setup Utility.

Changing the baud rate on an HP DL320 G4 Signaling Server

Important:

The HP DL320 G4 server shipped through Avaya has a default Baud rate of 9600 bits per second and does not require a reset. Use this procedure only if you want to use another Baud rate, or to correct the Baud rate after it is reset due to an error.

1. Press Power to boot the server.

   The server boots and the HP DL320 G4 boot screen appears.

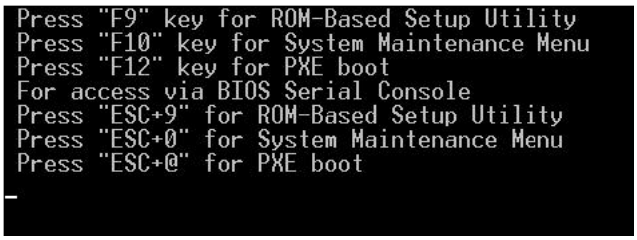


Figure 158: HP DL320 G4 server boot screen

Note:

If the server is already up and running, power the server off and on to restart and receive the HP DL320 G4 boot screen.

2. Press **F9** to invoke the ROM-based Setup Utility (RBSU) menu screen.

   The RBSU menu screen appears.

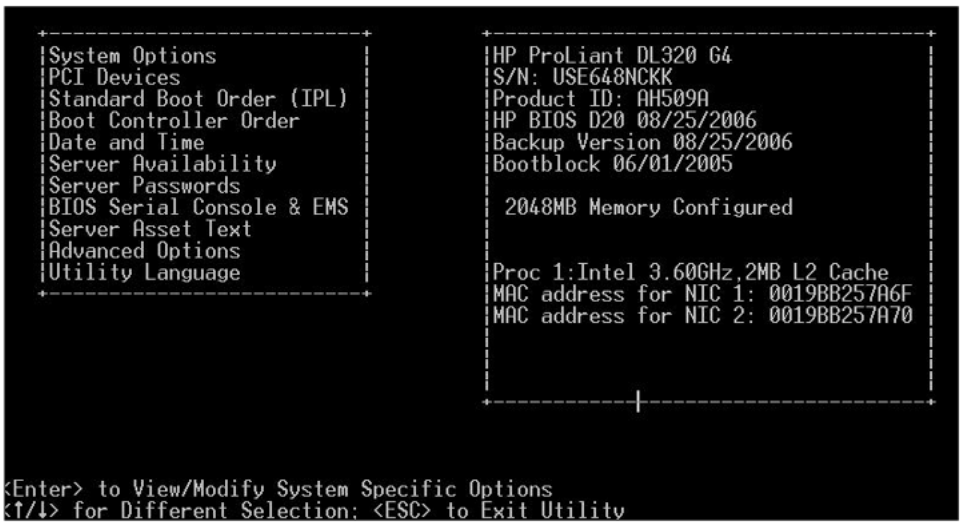


Figure 159: HP DL320 G4 server RBSU menu

3. Navigate to the **BIOS Serial Console & EMS** option and press Enter.

   A BIOS Serial Console & EMS configuration screen appears.

4. Navigate to the **BIOS Serial Console Baud Rate** option and press Enter.

   A BIOS Serial Console Baud Rate configuration window appears. This window presents you with four settings for the serial port speed:

   - 9600
   - 19200
   - 57600
   - 115200

5. Navigate to the **9600** setting and press **Enter**.

   This configures the serial port speed to 9600 bits per second.

The BIOS Serial Console & EMS configuration menu screen reappears.

6. Press ESC to exit the BIOS Serial Console & EMS configuration menu screen.

   The RBSU menu screen reappears.

7. Press ESC to exit the ROM-based Setup Utility.

Setting the HP DL320 G4 server BIOS password

1. Press Power to boot the server.

   The server boots and the HP DL320 G4 boot screen appears.

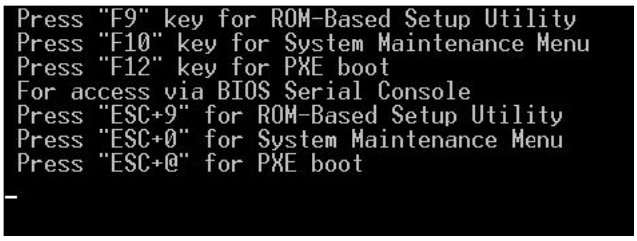


Figure 160: HP DL320 G4 server boot screen

Note:

If the server is already up and running, power the server off and on to restart and receive the HP DL320 G4 boot screen.

2. Press **F9** to invoke the ROM-based setup utility (RBSU) menu screen.

   The RBSU menu screen appears.

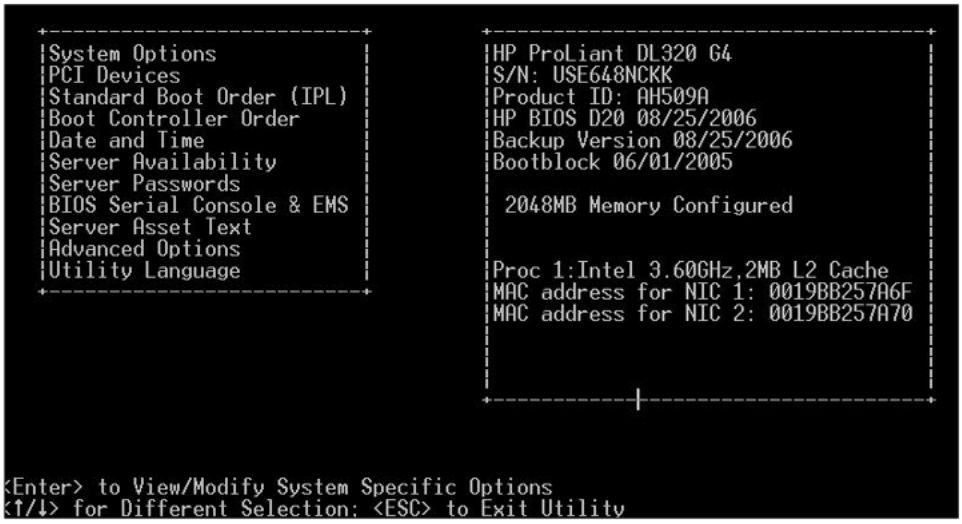


Figure 161: HP DL320 G4 server RBSU menu

3. Select the Server Passwords option and press Enter.
4. Select the Set Admin Password option and press Enter.
5. At this point refer to the manufacturer's manual for specific instructions on how to enable or disable the BIOS password.

For additional operating information see the Server Product Guide on the resource CD-ROM shipped with the HP DL320 G4 server .

Connecting an HP DL320 G4 Signaling Server

In geographic regions that are susceptible to electrical storms, Avaya recommends that you plug the HP DL320-G4 server into an AC surge suppressor.

The following figure depicts the back of an HP DL320 G4 server.

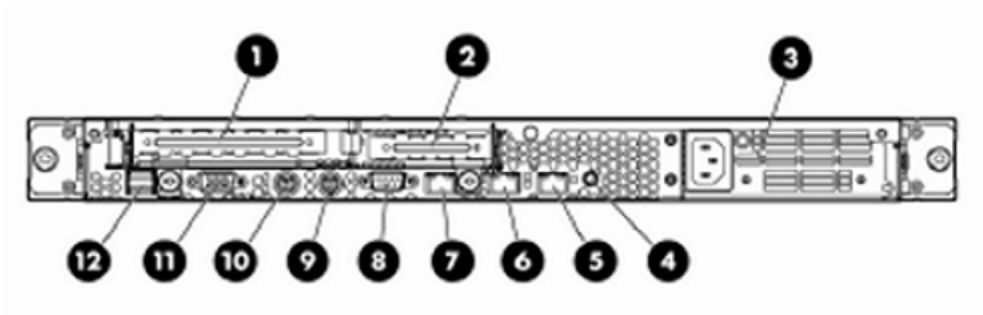


Figure 162: Back of an HP DL320 G4 server

1. Connect the server to the TLAN subnet.

   Insert the RJ-45 CAT5 (or better) cable into the connector labeled with the number 5 (TLAN network interface) on the back of the server.

2. Connect the server to the ELAN subnet.

   Insert the RJ-45 CAT5 (or better) cable into the connector labeled with the number 6 (ELAN network interface) on the back of the server.

3. Connect a DTE–DTE null modem serial cable from the serial port on the back of the server (COM1) to a maintenance terminal.

4. Connect the server power cord.

   a. Check that the power cord is the type required in the region where you are installing the server.

      Do not modify or use the supplied AC power cord if it is not the correct type.

   b. Attach the female end of the power cord to the mating AC power receptacle on the right side of the back panel. Plug the male end of the AC power cord into the AC power source (wall outlet).

5. Configure the COM1 serial port as the communication port for the connected maintenance terminal.

   See Configuring the COM1 serial port on an HP DL320 G4 server on page 234 for instructions.

6. Set the baud rate for the COM1 serial port on the Signaling Server to 9600 bits per second.

See Changing the baud rate on an HP DL320 G4 Signaling Server on page 235 for instructions.

Note:

The HP DL320-G4 Signaling Server ships with the serial port configured to 9600 bits per second.

7. Configure the connected maintenance terminal.

HP DL360 G7 server

The HP DL360 G7 server provides the following features:

- Intel E5620 Quad core processor (2.4 GHz)
- 146 GB Dual port hard drive, SAS 2.5" form factor, 10 000 RPM
- Base configuration:
  - 272 total: RAID 5, 3 x 146 GB drive
- Serial attached SCSI
- Three USB ports
- One optical drive
- One USB port in the front, Two USB ports in the back, and one internal USB
- One serial port
- 4 x 1 GB Network Interface Card (NIC) ports

The Common Server capacity ratings are the same as the COTS2 servers. For more information about the COTS2 ratings, see *Communication Server 1000E Planning and Engineering, NN43041–220*.

HP documentation

To view or download all HP ProLiant DL360 G7 server documentation, go to the HP Web site http://www.hp.com.

Front panel components

The following figure shows the front view of the HP DL360 G7 server.

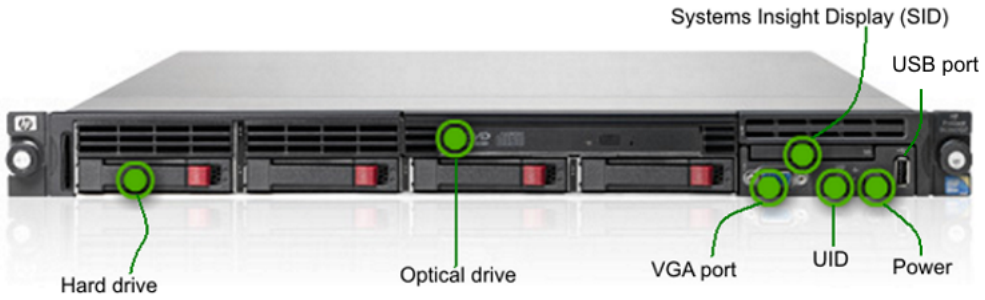


Figure 163: HP DL360 G7 front panel view

Front panel LED lights and buttons:

The following figure shows the LED lights and power button on the front panel of the HP DL360 G7 server. For a description of the LED lights and power button, see Table 10: HP DL360 G7 front panel LED description and status on page 240.

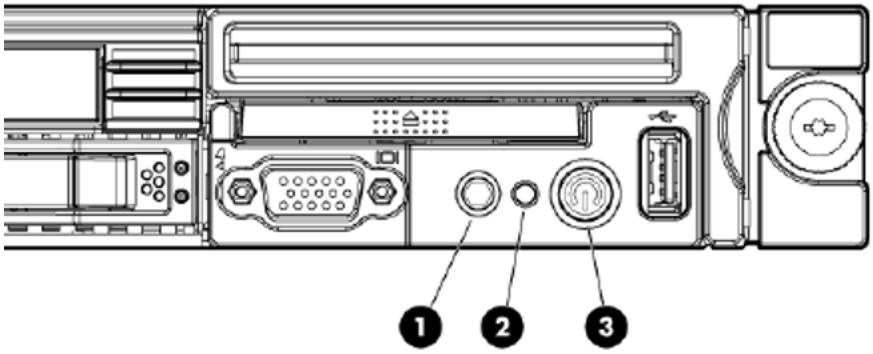


Figure 164: Front panel LED lights and buttons

Table 10: HP DL360 G7 front panel LED description and status

Item	Description	Status
1	UID button LED (Unit Identification)	Blue: Identification is activated. Flashing blue: System is remotely managed. Off: Identification is deactivated.
2	Internal health LED	Green: System health is normal. Amber: System is degraded. To identify the component, check the system board LEDs. Red: Critical. To identify the component in a critical state, check the system board LEDs. Off : System health is normal (when in standby mode).

Table continues…

Item	Description	Status
3	Power On/Standby button and system power LED	Green: System is on. Amber: System is in standby, but power is still applied. Off : Power cord is not attached, power supply failure has occurred, no power supplies are installed, facility power is not available, or the power button cable is disconnected.

Back panel components

The following figure shows the back panel view of the HP DL360 G7 server.

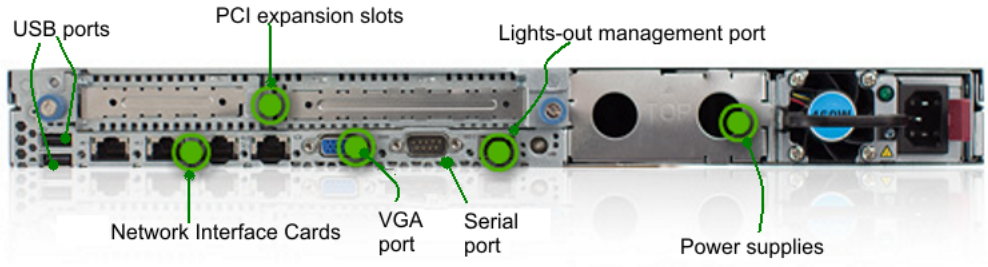


Figure 165: HP DL360 G7 back panel view

Note:

The HP DL360 G7 server is shipped with the Integrated Lights Out (iLO3) as a standard feature. The Avaya installed applications do not depend on iLO for operation. For more information about iLO, see http://www.hp.com/servers/lights-out.

ROM-Based setup utility interface

This section provides procedures for configuring the HP DL360 G7 server from the ROM-Based Setup Utility (RBSU). You can configure a physical COM1 serial port to the BIOS serial console. By default, the BIOS serial console is configured to Auto. You can disable the BIOS serial console in the RBSU. For information about how to configure the BIOS Serial Console port on the HP DL360 G7 server, see Configuring the BIOS serial console on page 241.

For more information about the ROM-Based Setup Utility interface, see *HP ROM-Based Setup Utility User Guide* on the Documentation CD or go to the HP Web site. For details about navigating the HP Web site, see HP documentation on page 239.

Configuring the BIOS serial console

Verify or configure the BIOS serial console.

Note:

The BIOS Serial Console is auto enabled by default.

1. Press the power button to start the server.
2. Press `F9` to access the ROM-Based Setup Utility (RBSU) menu.
3. From the RBSU main menu, navigate to the **BIOS Serial Console & EMS** option, and press `Enter`.
4. Navigate to the **BIOS Serial Console Port** option, and press `Enter` to view or modify.

   A BIOS Serial Console Port configuration screen appears. There are four options:

   - Auto BSC Enabled
   - Disabled
   - COM1
   - COM2
5. Navigate to the **Disabled** option, and press `Enter` to save your selection.

   The BIOS Serial Console & EMS configuration menu screen reappears.
6. Press `ESC` to exit the BIOS Serial Console & EMS menu.

Configuring the baud rate

Verify or configure the baud rate on an HP DL360 G7 Signaling Server.

Note:

The HP DL360 G7 server is configured with a default Baud rate of 9600 bits per second.

1. Press the Power button to start the server.
2. Press `F9` to access the ROM-based setup utility (RBSU) menu.
3. From the RBSU main menu, navigate to **BIOS Serial Console & EMS**, and press `Enter`.
4. Navigate to the **BIOS Serial Console Baud Rate** option, and press `Enter` to view or modify.

   There are four options:

   - 9600
   - 19200
   - 57600
   - 115200
5. Navigate to the **9600** option, and press `Enter` to save your selection.
6. Press `ESC` to exit the BIOS Serial Console & EMS menu.

Configuring VT100 terminal emulation

BIOS Serial Console supports ANSI and VT100 terminal emulation. VT100 is supported by all terminal emulation programs.

1. Press the power button to start the server.
2. Press `F9` to access the ROM-Based Setup Utility (RBSU) menu.
3. From the RBSU main menu, navigate to **BIOS Serial Console & EMS**, and press `Enter`.
4. Navigate to the **Terminal Emulation Mode** option, and press `Enter` to view or modify.

   A BIOS Serial Console Port configuration screen appears. There are two options:

   - VT100
   - ANSI
5. Navigate to the **VT100** option, and press `Enter` to save your selection.

   The BIOS Serial Console & EMS configuration menu screen reappears.
6. Press `ESC` to exit the BIOS Serial Console & EMS menu.

Connecting an HP DL360 G7 Signaling Server

In geographic regions that are susceptible to electrical storms, Avaya recommends that you plug the HP DL360 G7 server into an AC surge suppressor. To view the back panel of an HP DL360 G7 server, see Back panel components on page 241.

1. Connect the server to the TLAN subnet.

   Insert the RJ-45 CAT5 (or better) cable into the Network Interface Card (NIC) 2 slot in the back of the server.
2. Connect the server to the ELAN subnet.

   Insert the RJ-45 CAT5 (or better) cable into the Network Interface Card (NIC) 1 slot in the back of the server.
3. Connect a DTE-DTE null modem serial cable from the serial port on the back of the server (configured as COM1) to a maintenance terminal.
4. Connect the server power cord.

   Warning:

   Check that the power cord is the type required in the region where you are installing the server. Do not modify or use the supplied AC power cord if it is not the correct type.
5. Configure the COM1 serial port as the communication port for the connected maintenance terminal.

   See Configuring the BIOS serial console on page 241 for instructions.

6. Configure the baud rate for the COM1 serial port on the Signaling Server to 9600 bits per second.

   See Configuring the baud rate on page 242 for instructions.

   Note:

   The HP DL360 G7 server ships with the serial port configured to 9600 bits per second.

7. Configure the connected maintenance terminal.

   For VT100 terminal emulation, see Configuring VT100 terminal emulation on page 243.

HP DL360p G8 server

Features

The HP DL360p Gen8 server provides the following features:

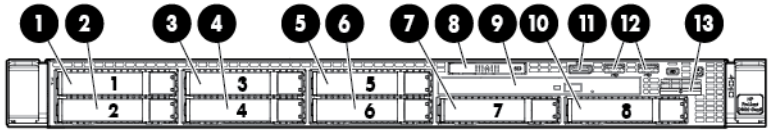
- Intel E5-2630 6-core processor (2.3 GHz)
- 8 GB of RAM PC3-12800E DDR3
- Two 300 GB hard drives
- Serial attached SCSI
- RAID 1, P420 (512M) Raid Controller
- One optical drive DVD+/-RW, SATA, INTERNAL
- Seven USB ports: two USB ports in the front, four USB ports in the back and one internal USB
- One serial port
- 1 GB Quad-Port Network Interface Card (NIC)

The Common Server R2 capacity ratings are the same as the COTS2 and Common servers. For more information about the COTS2 ratings, see Communication Server 1000E Planning and Engineering, NN43041–220.

HP Documentation

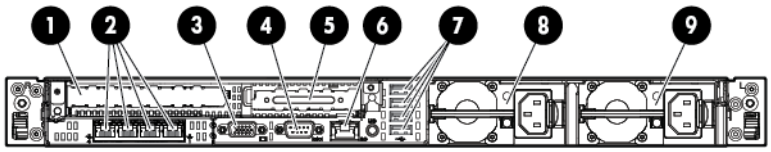
To view or download HP ProLiant DL360p G8 server documentation, go to the Avaya Support Site http://www.support.avaya.com

Front view of HP DL360p G8 Server



No.	Description
1	Hard Drive Bay
2	Hard Drive Bay
3	Hard Drive Bay
4	Hard Drive Bay
5	Hard Drive Bay
6	Hard Drive Bay
7	Hard Drive Bay
8	Slide-out System Insight Display (SID)
9	Optical Disk Drive Bay
10	Hard Drive Bay
11	Video Connector (requires Front Video Adapter Kit)
12	Two (2) USB Connectors
13	Active Health and Network Status LEDs

Rear view of HP DL360p G8 Server



No.	Description
1	PCIe 3.0 Full height/half length x16 expansion slot
2	Flexible LOM ports (Shown: 4 ports 1 Gb each/ Optional: 2 ports 10 Gb each)
3	Video connector
4	Serial connector
5	PCIe 3.0 Low Profile x8 expansion slot
6	iLO Management Engine NIC connector
7	Four (4) USB connectors
8	Power supply bay 2 (Shown populated: Optional Power Supply for Redundant Power)
9	Power supply bay 1 (Primary Power Supply)

Configuring the BIOS serial console

About this task

Use the procedure below to verify or configure the BIOS serial console.

Note:

The BIOS Serial Console is auto enabled by default.

Procedure

1. Press the power button to start the server.
2. Press F9 to access the ROM-Based Setup Utility (RBSU) menu.
3. From the RBSU main menu, navigate to the BIOS Serial Console & EMS option, and press Enter.
4. Navigate to the BIOS Serial Console Port option, and press Enter to view or modify.

A BIOS Serial Console Port configuration screen appears. There are four options:

- Auto BSC Enabled
- Disabled
- COM1
- COM2

5. Navigate to the Disabled option, and press Enter to save your selection.

   The BIOS Serial Console & EMS configuration menu screen reappears.

6. Press ESC to exit the BIOS Serial Console & EMS menu.

Configuring the baud rate

About this task

Use this procedure to verify or configure the baud rate on an HP DL360p G8 signaling server.

Note:

The HP DL360p G8 server is configured with a default Baud rate of 9600 bits per second.

Procedure

1. Press the Power button to start the server.
2. Press F9 to access the ROM-based setup utility (RBSU) menu.
3. From the RBSU main menu, navigate to BIOS Serial Console & EMS, and press Enter.
4. Navigate to the BIOS Serial Console Baud Rate option, and press Enter to view or modify.

   There are four options:

   - 9600
   - 19200
   - 57600
   - 115200

5. Navigate to the 9600 option, and press Enter to save your selection.
6. Press ESC to exit the BIOS Serial Console & EMS menu.

Connecting an HP DL360p G8 signaling server

About this task

In geographic regions that are susceptible to electrical storms, Avaya recommends that you plug the HP DL360p G8 server into an AC surge suppressor. To view the back panel of an HP DL360 G8 server, see Back view of HP DL360p G8 server on page 246.

Procedure

1. Connect the server to the TLAN subnet.

   Insert the RJ-45 CAT5 (or better) cable into the Network Interface Card (NIC) 2 slot in the back of the server.

2. Connect the server to the ELAN subnet.

   Insert the RJ-45 CAT5 (or better) cable into the Network Interface Card (NIC) 1 slot in the back of the server.

3. Connect a DTE-DTE null modem serial cable from the serial port on the back of the server (configured as COM1) to a maintenance terminal.

4. Connect the server power cord.

   Warning:

   Check that the power cord is the type required in the region where you are installing the server. Do not modify or use the supplied AC power cord if it is not the correct type.

5. Configure the COM1 serial port as the communication port for the connected maintenance terminal.

   See Configuring the BIOS serial console on page 246

6. Configure the baud rate for the COM1 serial port on the Signaling Server to 9600 bits per second.

   Configuring the baud rate on page 247

   Note:

   The HP DL360p G8 server ships with the serial port configured to 9600 bits per second.

7. Configure the connected maintenance terminal.

   For VT100 terminal emulation, see Configuring VT100 terminal emulation on page 243

HP DL360 G9 server

Features

The HP DL360 Gen9 server provides the following features:

- Intel E5-2620v3 6-core processor (2.4 GHz)
- 16 GB of RAM PC4-1866 DDR4 (24 DIMM slots, 4 used)
- Two 300 GB simple swap Serial-attached SCSI (SAS) hard drives (8 front bays, 2 used)
- One optical drive DVD+/-RW, SATA, INTERNAL
- USB ports: one USB 2.0 and one USB 3.0 in the front, two USB 3.0 in the back and two internal USB 3.0 ports

- One serial port
- 1 GB Quad-Port Network Interface Card (NIC)

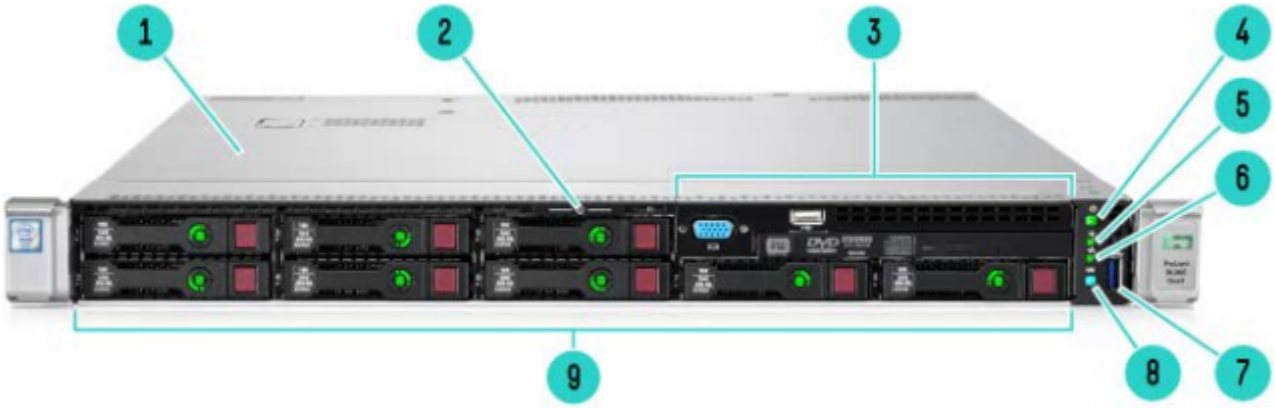
The Common Server R3 capacity ratings are the same as the COTS2 and Common servers. For more information about the COTS2 ratings, see *Communication Server 1000E Planning and Engineering, NN43041–220*.

HP Documentation

To view or download HP ProLiant DL360 G9 server documentation, go to the Avaya Support Site http://www.support.avaya.com

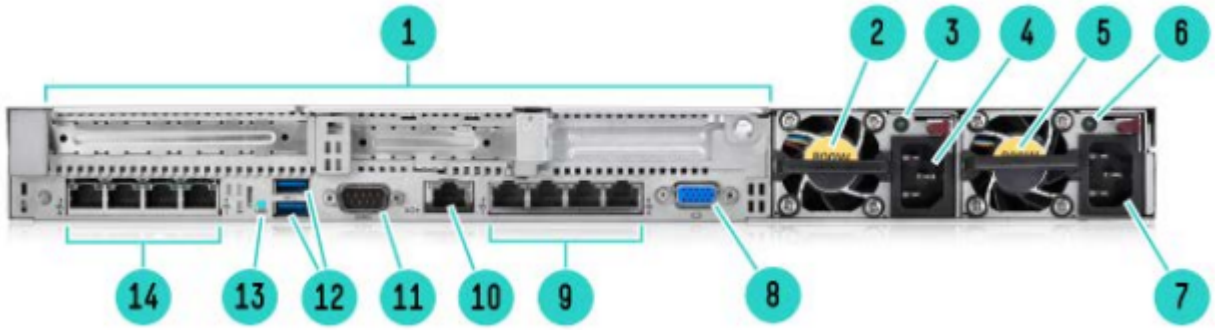
Front view of HP DL360 G9 Server

The following figure shows the front view of the HP DL360 G9 server.



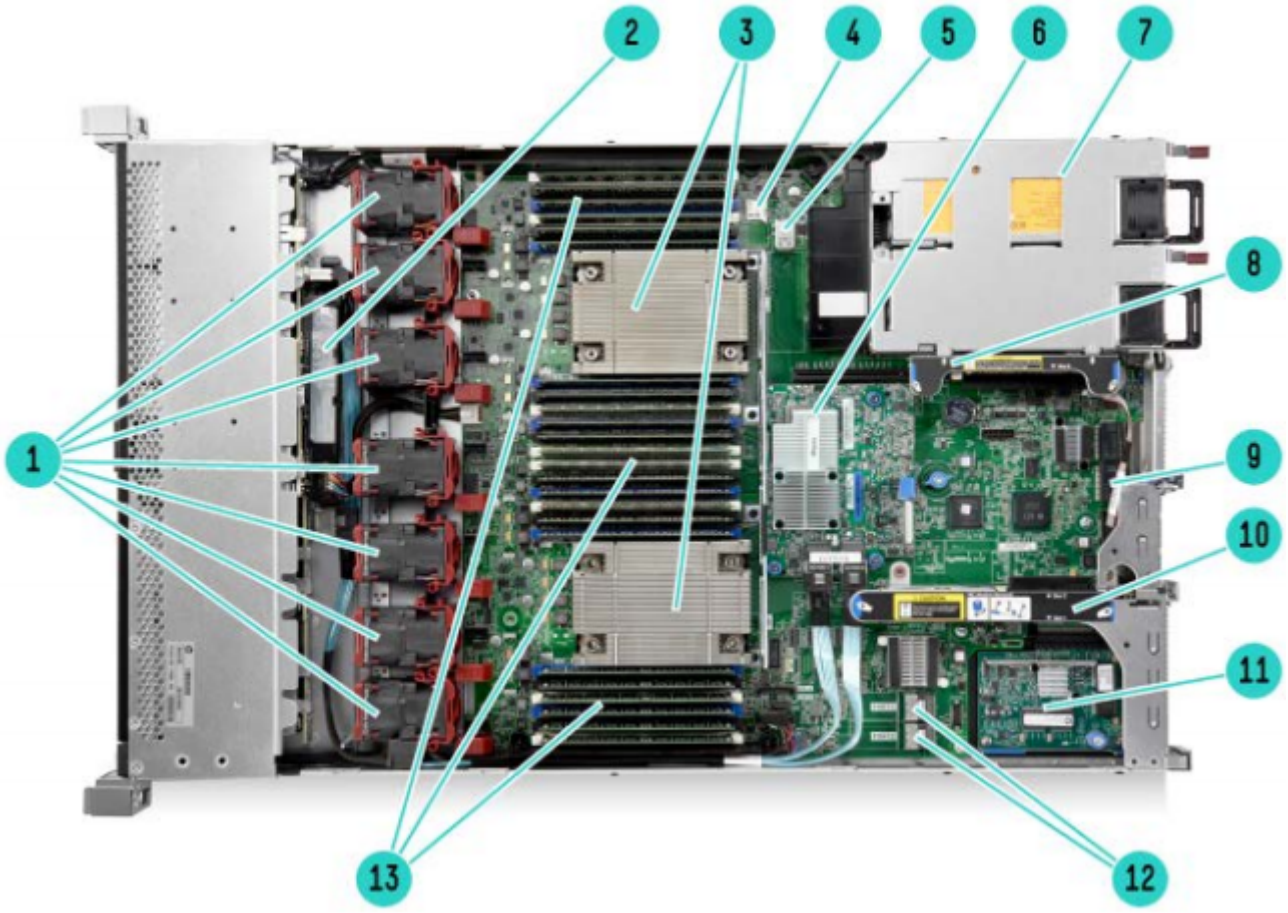
No.	Description
1	Access Panel
2	Serial Label Pull Tab
3	HPE Universal Media Bay or NVMe (VGA, USB 2.0 and DVD-RW)
4	Power On/Standby button and system power LED button
5	Health LED
6	NIC Status LED
7	USB 3.0 Connector
8	Unit Identification Button & LED
9	SAS/SATA/SSD/NVMe Drive Bays

Rear view of HP DL360 G9 Server



NO.	Description
1	PCIe 3.0 Slots 1-3
2	HPE Flexible Slot Power Supply Bay 2
3	Power Supply 2 Status LED
4	Power Supply 2 C13 Connection
5	HPE Flexible Slot Power Supply Bay 1
6	Power Supply 1 Status LED
7	Power Supply 1 C13 Connection
8	Video Connector
9	Embedded 4x1GbE Network Adapter
10	Dedicated iLO 4 connector
11	Serial Port Connector (Optional)
12	USB 3.0 Connectors (2)
13	Unit Identification LED
14	FlexibleLOM bay (Optional)

Internal view of HP DL360 G9 Server



No.	Description
1	5 Standard Fans Ship for 1P and 7 Standard Fans Ship for 2P
2	HPE Smart Storage Battery (Optional)
3	2 Processors with HPE Smart Socket Guide
4	MicroSD card slot
5	Dual Internal USB 3.0 connector
6	HPE Flexible Smart Array or Smart HBA (Optional)
7	2 HPE Flexible Slot Power supplies
8	Secondary PCIe 3.0 riser for PCIe slot 3 (requires CPU 2)
9	Embedded 4x1Gbe NIC
10	Primary PCIe 3.0 riser for PCIe slots 1 & 2

Table continues…

No.	Description
11	FlexibleLOM Bay (Optional)
12	Embedded SATA Controller ports
13	24 DDR4 DIMM slots (12 per processor)

Configuring the BIOS serial console

For information about configuring the BIOS serial console see HP DL360 G8 Configuring BIOS on page 246.

Configuring the baud rate

For information about configuring the baud rate, see HP DL360 G8 Configuring baud rate on page 247.

Connecting an HP DL360 G9 signaling server

Before you begin

In geographic regions that are susceptible to electrical storms, Avaya recommends that you plug the HP DL360 G9 server into an AC surge suppressor. To view the back panel of an HP DL360 G9 server, see Rear view of HP DL360 G9 Server on page 249.

Procedure

1. Connect the server to the TLAN subnet.

   Insert the RJ-45 CAT5 (or better) cable into the Network Interface Card (NIC) 2 slot in the back of the server.

2. Connect a DTE-DTE null modem serial cable from the serial port on the back of the server (configured as COM1) to a maintenance terminal.

3. Connect the server power cord.

   Warning:

   Check that the power cord is the type required in the region where you are installing the server. Do not modify or use the supplied AC power cord if it is not the correct type.

4. Configure the COM1 serial port as the communication port for the connected maintenance terminal. See HP DL360 G8 Configuring BIOS on page 246.

5. Configure the baud rate for the COM1 serial port on the Signaling Server to 9600 bits per second. See HP DL360 G8 Configuring baud rate on page 247.

Note:

The HP DL360 G9 server ships with the serial port configured to 9600 bits per second.

6. Configure the connected maintenance terminal. For VT100 terminal emulation see Configuring VT100 terminal emulation on page 243.

IBM x306m server

The IBM x306m server provides the following features:

- an Intel Pentium 4 processor (3.6 GHz)
- 2 simple swap Serial ATA, 80 GB (1 drive configured)
- 8 GB of RAM PC4200 DDR II by means of 4 DIMM slots (2 GB configured)
- Two Gigabit Ethernet ports
- Four USB ports (two front, two back)
- One DVD-COMBO (DVD/CD-RW) drive
  - You use this to load the Signaling Server software files for the Signaling Server, Voice Gateway Media Cards, and IP Phones
- One serial port (back of Signaling Server)
- A reset button

For complete details and specifications about the IBM x306 server, visit the manufacturer's Web site at http://www.ibm.com.

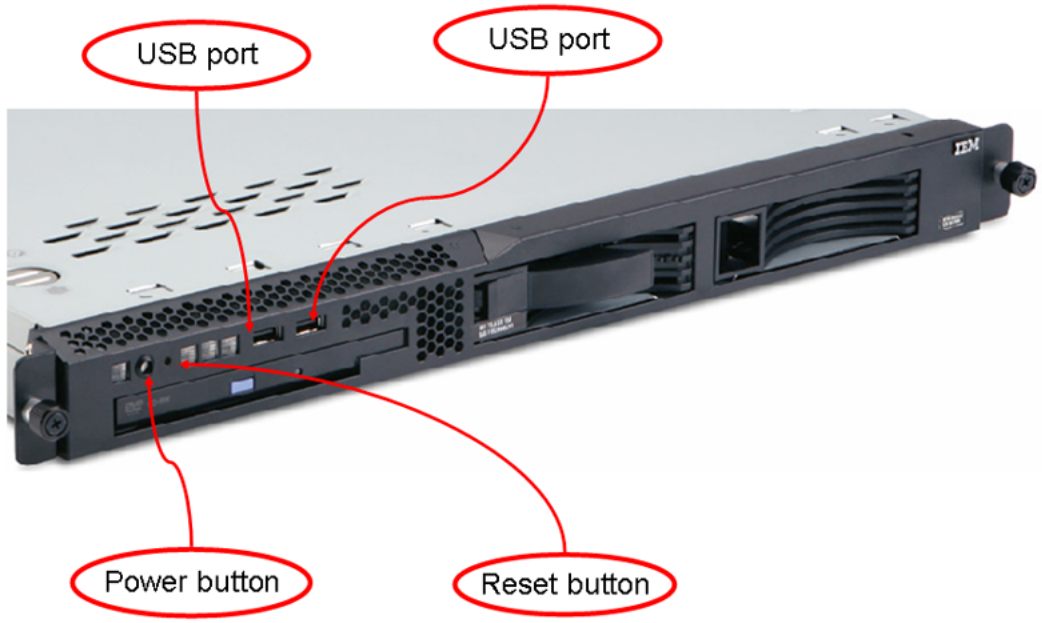


Figure 166: IBM x306m front view

Figure 167: IBM x306m front view: LEDs

Table 11: IBM x306m LED description and status

Description	Status
Power LED	If this LED is lit, it indicates that the server is turned on. If this LED is off, it indicates that AC power is not present, or the power supply or the LED itself failed.

Table continues…

Description	Status
Hard disk LED	If this LED is lit, it indicates that a hard disk drive is in use.
Locator LED	When this LED is lit, it is lit remotely by the system administrator to aid in visually locating the server.
System Error LED	If this LED is lit, it indicates that a system error occurred.

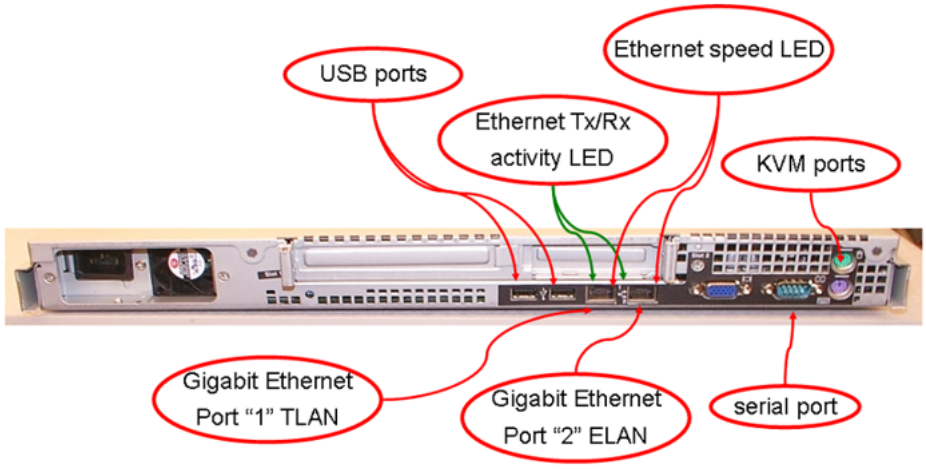


Figure 168: IBM x306m rear view

Important:

The TLAN & ELAN port positions are reversed (L and R, 1 and 2) compared to the HP DL320 server. Ethernet speed LED:

- Lit indicates Ethernet network speed of 1 Gbps.
- Off indicates Ethernet network speed is 10/100 Mbps.

IBM x306m BIOS settings

The following BIOS settings are for the IBM x306m server that are shipped through Avaya.

Table 12: IBM x306m default BIOS settings

BIOS value	Default setting
Devices and I/O port - serial port A	Enabled
Devices and I/O port - baud rate	9600 baud
Devices and I/O port - console type	PC ANSI

Table continues…

BIOS value	Default setting
Devices and I/O port - flow control	Off
Devices and I/O port - continue C.R. after POST	On
Devices and I/O port - type of connector	9-pin serial female
Start options - legacy USB support	Disabled

The IBM x306m server default BIOS settings can be changed by a BIOS reset or other maintenance activity. To return the BIOS settings to the appropriate values, see Changing the baud rate on an IBM X306m Signaling Server on page 259 for instructions.

For information about how to enable or disable the BIOS password about the IBM x306m server, see Setting the IBM x306m server BIOS password on page 258.

Changing the BIOS settings on an IBM x306m server

1. Press the Power switch to boot the server.

   The server boots and the Press F1 for Configuration/Setup message appears on the maintenance terminal.

   Note:

   If the server is already up and running, power the server off and on or press the reset button to restart and receive the Press F1 for Configuration/Setup message.

2. Press F1 to invoke the IBM x306m server Configuration/Setup Utility.

   The Configuration/Setup Utility menu screen appears.

Figure 169: IBM x306m server Configuration/Setup Utility menu

3. Navigate to the **Devices and I/O Ports** option and press Enter.

   The Devices and I/O Ports menu screen appears.

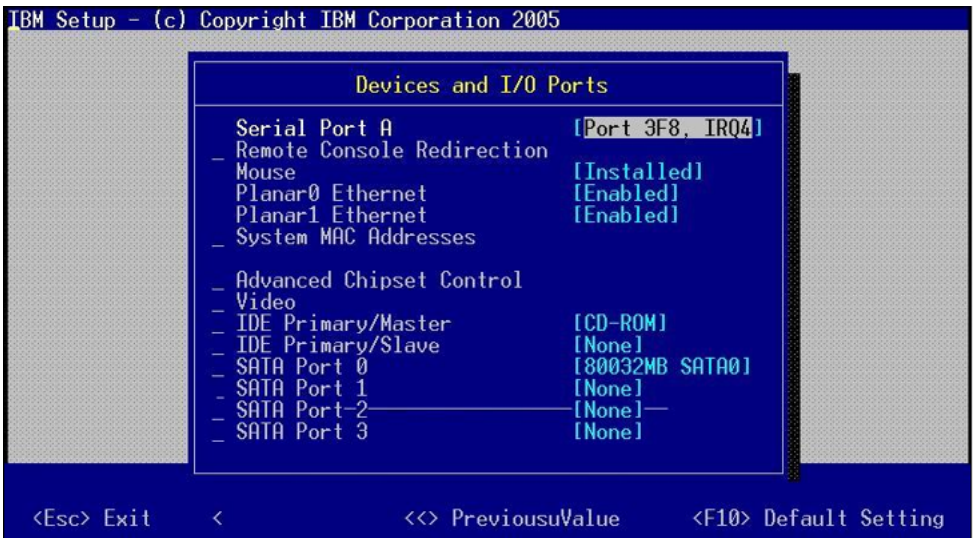


Figure 170: Devices and I/O Ports menu

4. Navigate to the **Remote Console Redirection** option and press Enter.

   The Remote Console Redirection screen appears.

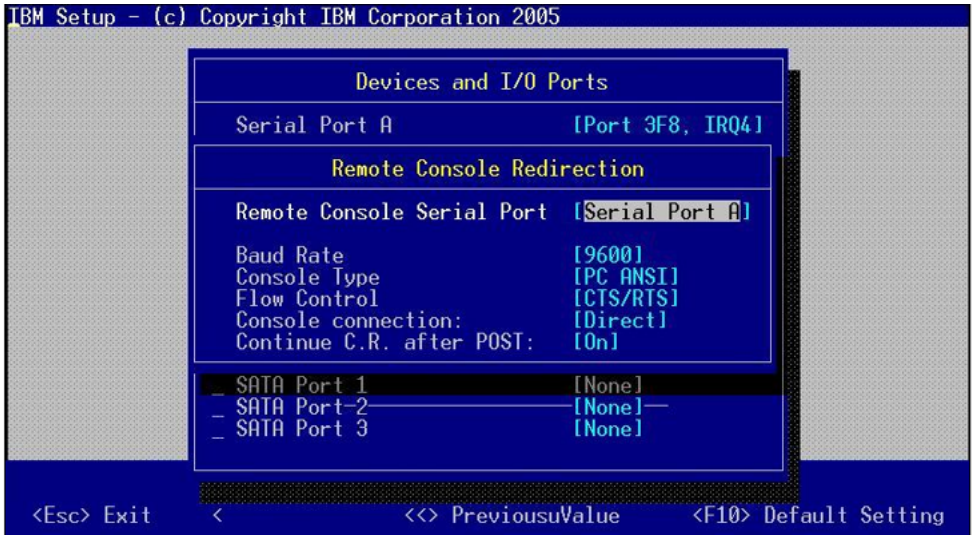


Figure 171: IBM x306m server Remote Console Redirection

5. Navigate to the option you wish to change and enter the appropriate value.
6. Press Enter to change the setting.
7. Press ESC to exit the **Remote Console Redirection** option.

   The Devices and I/O Ports menu screen appears.
8. Press ESC to exit the **Devices and I/O Ports** option.

   The Configuration/Setup Utility menu screen appears.
9. Navigate to the **Save Settings** option and press Enter to save the changed parameters.

10. Navigate to the **Exit Setup** option and press Enter to exit the IBM x306m Configuration/ Setup Utility.

    The server will restart automatically.

Setting the IBM x306m server BIOS password

1. Press the Power switch to boot the server.

   The server boots and the Press F1 for Configuration/Setup message appears on the maintenance terminal.

   Note:

   If the server is already up and running, power the server off and on or press the reset button to restart and receive the Press F1 for Configuration/Setup message.

2. Press F1 to invoke the IBM x306m server Configuration/Setup Utility.

   The Configuration/Setup Utility menu screen appears.

Figure 172: IBM x306m server Configuration/Setup Utility menu

3. Select the System Security option and press Enter.
4. Select the Administrator Password option and press Enter.
5. At this point refer to the manufacturer's manual for specific instructions on how to enable or disable the BIOS password.

For additional operating information see the Server Product Guide on the resource CD-ROM shipped with the IBM x306m server .

Connecting an IBM X306m server

In geographic regions that are susceptible to electrical storms, Avaya recommends that you plug the IBM X306m server into an AC surge suppressor. Use the following procedures to connect an IBM X306m server.

The following figure depicts the back of an IBM X306m server.

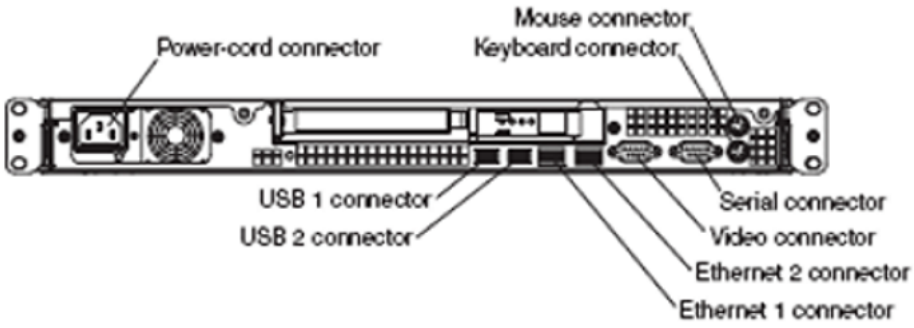


Figure 173: Back of an IBM X306m server

1. Connect the server to the TLAN subnet.

   Insert the RJ-45 CAT5 (or better) cable into the Ethernet 1 connector (TLAN network interface) on the back of the server.

2. Connect the server to the ELAN subnet.

   Insert the RJ-45 CAT5 (or better) cable into the Ethernet 2 connector (ELAN network interface) on the back of the server.

3. Connect a DTE–DTE null modem serial cable from the serial port on the back of the Signaling Server to the serial port on a maintenance terminal.

4. Connect the server power cord.

   a. Check that the power cord is the type required in the region where you use the server.

      Do not modify or use the supplied AC power cord if it is not the correct type.

   b. Attach the female end of the power cord to the mating AC power receptacle on the left side of the server back panel. Plug the male end of the AC power cord into the AC power source (wall outlet).

5. Configure the baud rate for the serial port on the Signaling Server to 9600 bps. See Changing the baud rate on an IBM X306m Signaling Server on page 259 for instructions.

   Note:

   The IBM X306m Signaling Server ships with the serial port configured to 9600 bps.

6. Configure the connected maintenance terminal.

Changing the baud rate on an IBM X306m Signaling Server

Perform the following procedure to verify or change the baud rate on an IBM X306m Signaling Server.

1. Press the Power switch to boot the server.

The server boots and a **Press F1 for Configuration/Setup** message appears on the maintenance terminal.

Note:

If the server is running, press the Reset button on the front of the IBM X306m server to restart and receive the **Press F1 for Configuration/Setup** message.

2. Press **F1** to invoke the IBM X306m server Configuration/Setup Utility.

   The Configuration/Setup Utility menu screen appears.

Figure 174: IBM X306m server Configuration/Setup Utility menu

3. Navigate to the **Devices and I/O Ports** option and press **Enter**.

   The Devices and I/O Ports menu screen appears.

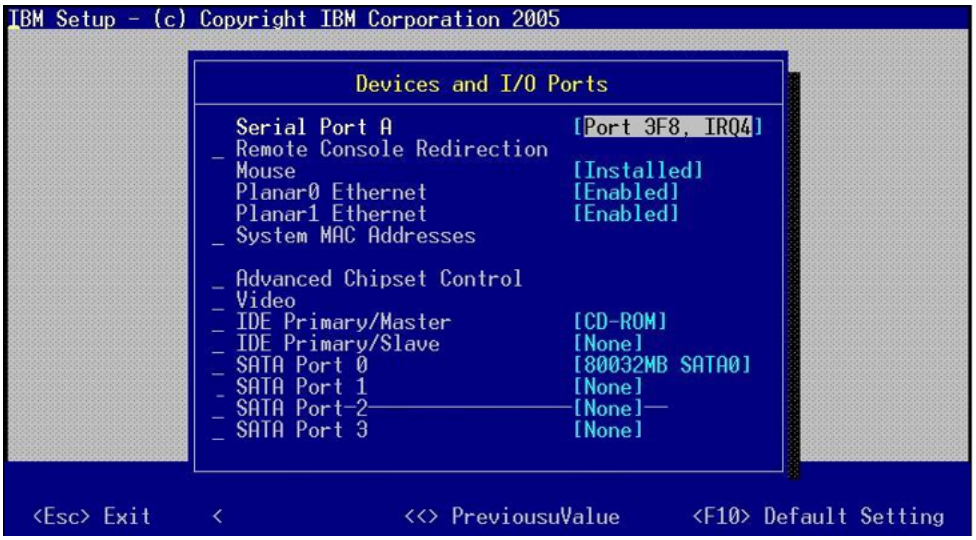


Figure 175: IBM X306m server Devices and I/O Ports menu

4. Navigate to the **Remote Console Redirection** option and press **Enter**.

The Remote Console Redirection screen appears.

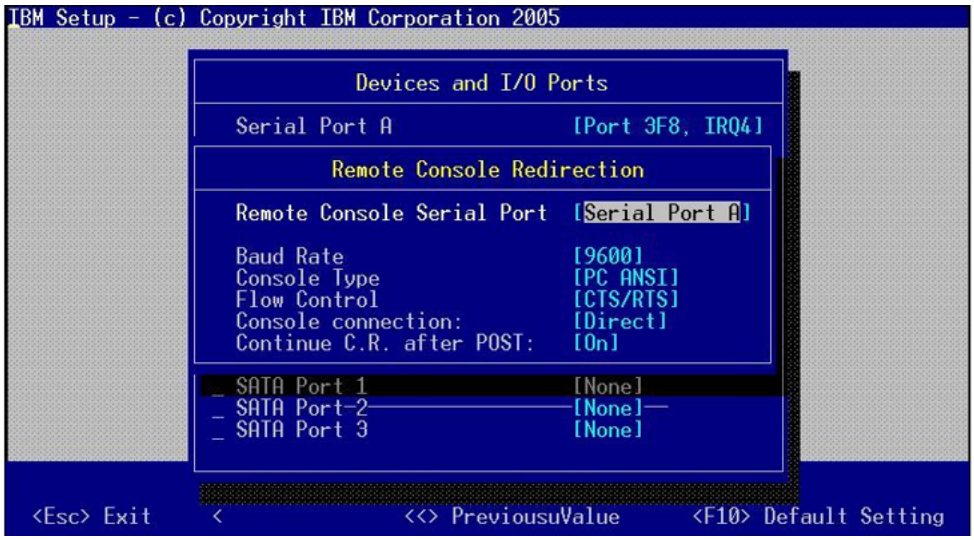


Figure 176: IBM X306m server Remote Console Redirection

5. Navigate to the **Baud Rate** option and enter the value 9600.
6. Press **Enter** to change the serial port speed to 9600 bits per second.
7. Press **ESC** to exit the **Remote Console Redirection** option.

   The Devices and I/O Ports menu screen appears.
8. Press **ESC** to exit the **Devices and I/O Ports** option.

   The Configuration/Setup Utility menu screen appears.
9. Navigate to the **Save Settings** option and press **Enter** to save the changed parameters.
10. Navigate to the **Exit Setup** option and press **Enter** to exit the IBM X306m Configuration/ Setup Utility.

    The server restarts automatically.

Refer to the Server Product Guide on the resource CD-ROM shipped with the IBM X306m server for additional operating information.

IBM x3350 server

The IBM x3350 server provides the following features:

- Intel Core 2 Quad CPU –2.66GHz
- 250 Gbyte RAID 1 array (2x 250 Gbyte hard drives, hot-swappable)
- 4 Gbyte memory
- CD-RW/DVD drive

- Redundant power supply (hot-swappable)
- Dual GigaBit ethernet ports

For complete details and specifications about the IBM x3350 server, visit the manufacturer's Web site at http://www.ibm.com.

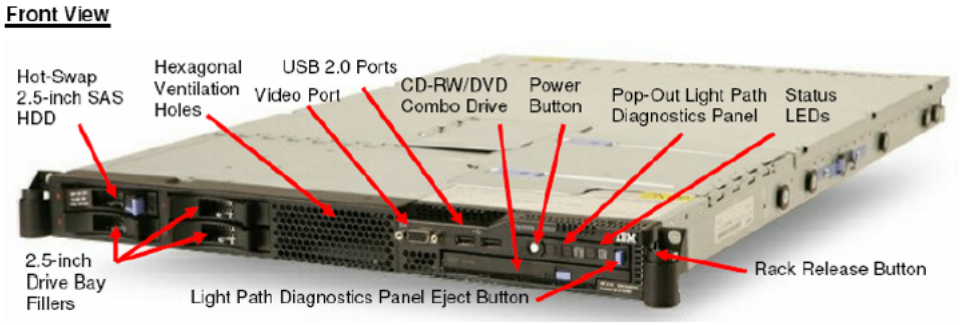


Figure 177: IBM x3350 server front view

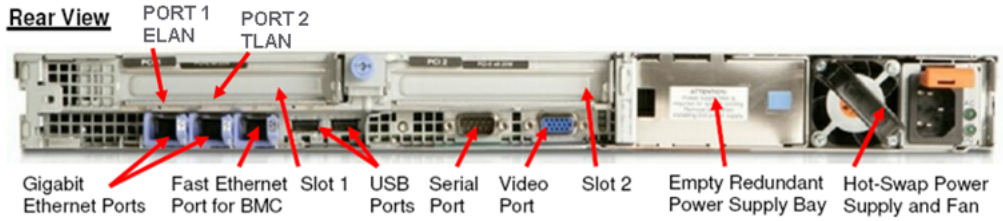


Figure 178: IBM x3350 server rear view

If you connect to the IBM x3350 server with a terminal for setup, the server does not function with the serial cable that was previously shipped with the ISP 1100 or other COTS platforms. The IBM x3350 server requires the new NTRX26NPE6 9 pin female to 9 pin female null modem cable, as shown in the following figure.

Figure 179: NTRX26NPE6 9 pin female to 9 pin female null modem cable

Configuring COM port settings for the IBM x3350 server

Perform the following procedures for configuring the BIOS settings.

1. Press F1 to navigate to the BIOS configuration main menu screen using a Keyboard Video Monitor (KVM) terminal.

   OR

   Press ESC-1 to navigate to the BIOS configuration main menu screen using the console terminal.

   The BIOS Configuration/Setup Utility main menu screen appears, as shown in Figure 180: BIOS Configuration/Setup Utility main menu window on page 264.

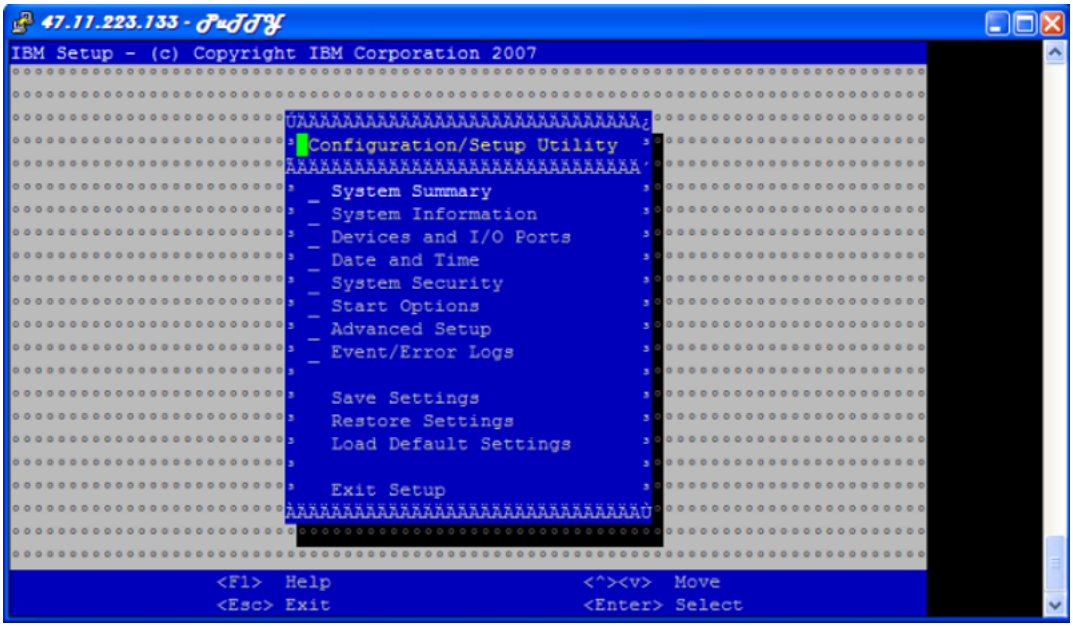


Figure 180: BIOS Configuration/Setup Utility main menu window

2. In the BIOS Configuration/Setup Utility main menu select Devices and I/O Ports and press Enter.

   The Devices and I/O Ports screen appears, as shown in Figure 181: Devices and I/O Ports window on page 264.

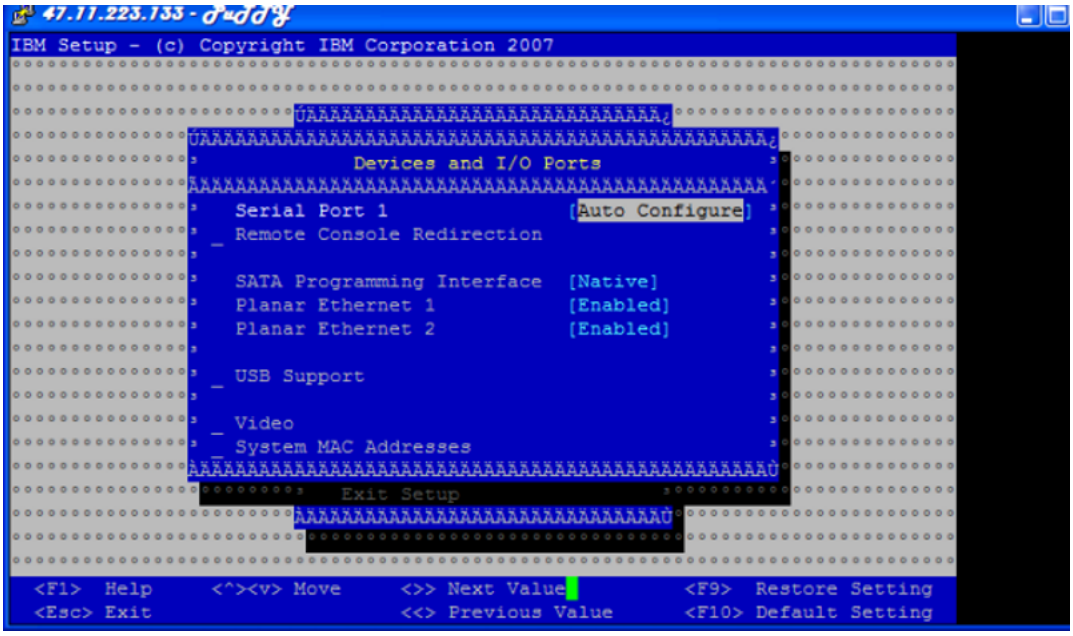


Figure 181: Devices and I/O Ports window

3. In the Devices and I/O Ports screen, select Remote Console Redirection and press Enter. The Remote Console Redirection screen appears, as shown in Figure 182: Remote Console Redirection window on page 265.

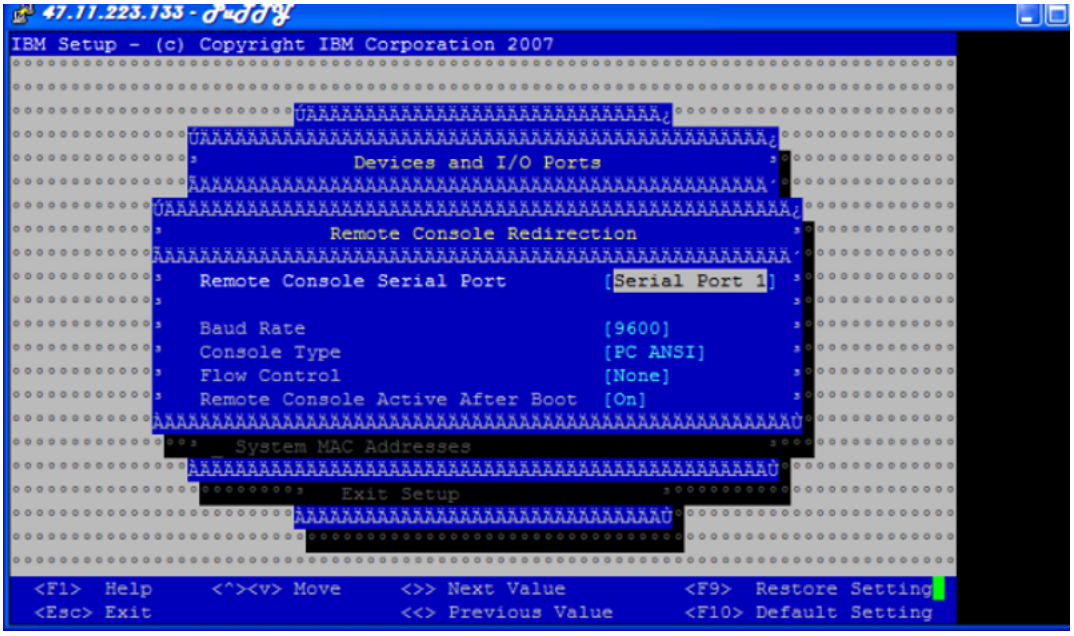


Figure 182: Remote Console Redirection window

4. Navigate to Remote Console Serial Port and type Serial Port 1.
5. Navigate to Baud Rate and type 9600.
6. Navigate to Console Type and type PC ANSI.
7. Navigate to Flow Control and type None.
8. Navigate to Remote Console Active After Boot and type On.
9. Press Esc twice to return to the BIOS Configuration/Setup Utility main menu.
10. In the BIOS Configuration/Setup Utility main menu screen, select Save Settings and press Enter. A confirmation prompt appears, as shown in Figure 183: Save Settings confirmation window on page 266.

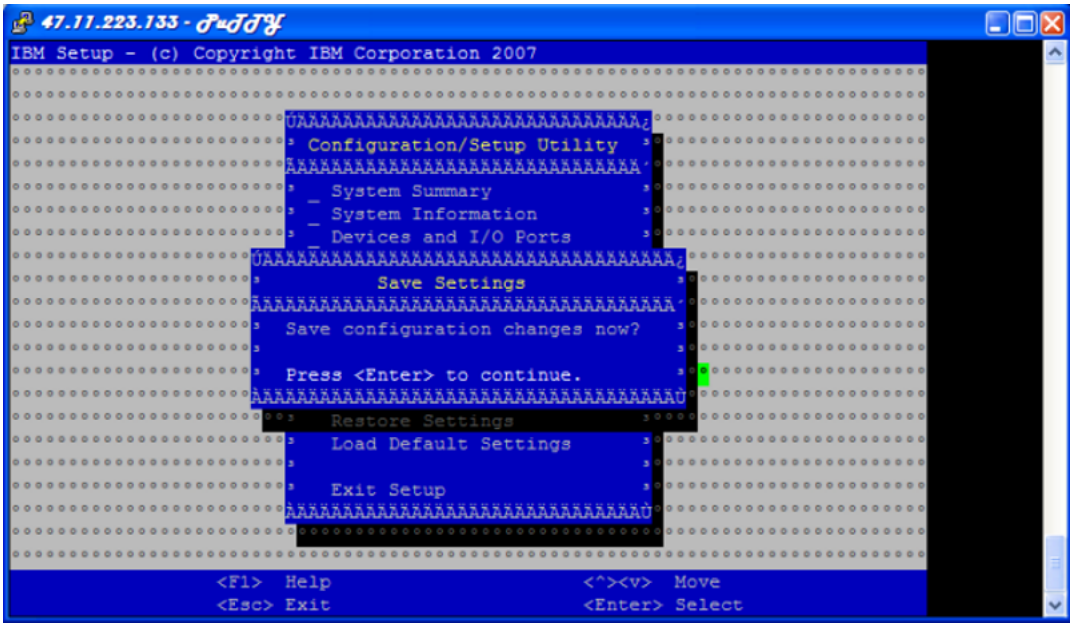


Figure 183: Save Settings confirmation window

11. In the Save Settings confirmation screen press enter to confirm your changes.

    The BIOS Configuration/Setup Utility main menu screen appears.

12. Press Esc to exit the BIOS Configuration/Setup Utility main menu.

    A confirmation screen appears, as shown in Figure 184: BIOS Configuration/Setup Utility main menu exit confirmation window on page 266.

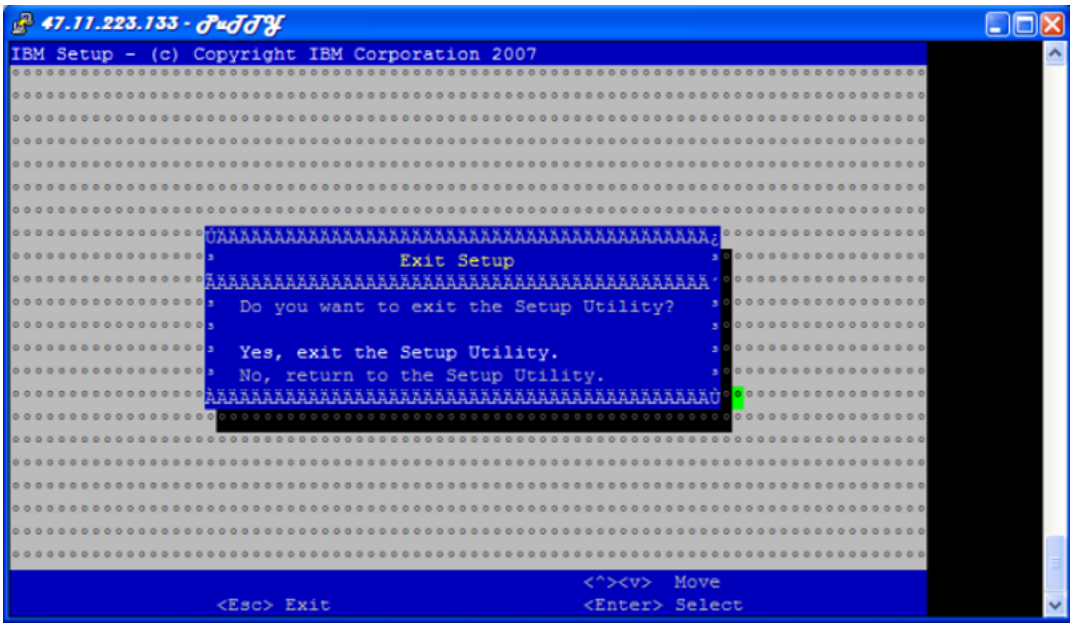


Figure 184: BIOS Configuration/Setup Utility main menu exit confirmation window

13. Navigate to Yes, exit the Setup Utility and press Enter.

Setting the BIOS password for the IBM x3350 server

Perform the following procedure for setting the BIOS password.

1. Press F1 to navigate to the BIOS configuration main menu screen using a Keyboard Video Monitor (KVM) terminal.

   OR

   Press ESC-1 to navigate to the BIOS configuration main menu screen using the console terminal.

   The BIOS Configuration/Setup Utility main menu screen appears, as shown in Figure 185: BIOS Configuration/Setup Utility main menu window on page 267.

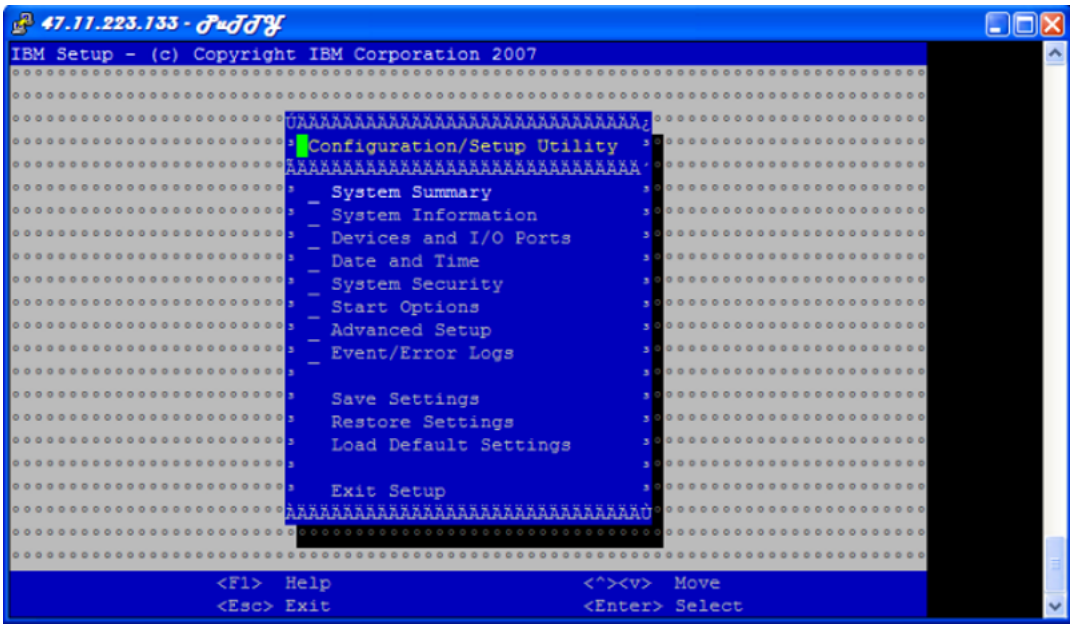


Figure 185: BIOS Configuration/Setup Utility main menu window

2. In the BIOS Configuration/Setup Utility main menu screen, select System Security and press Enter.

   The System Security menu appears, as shown in Figure 186: System Security menu on page 268.

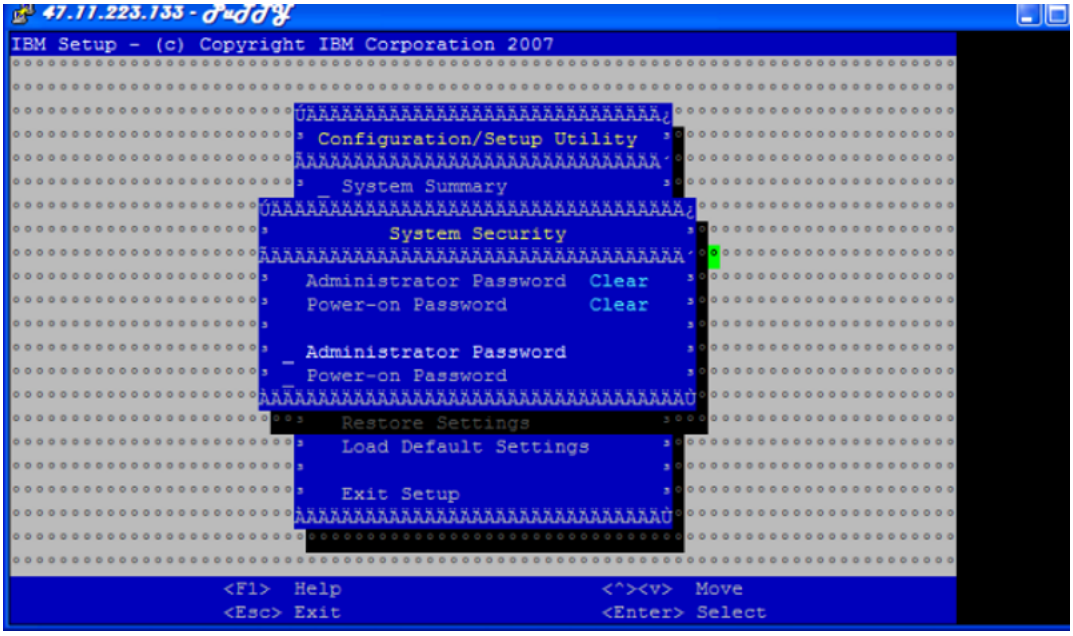


Figure 186: System Security menu

3. In the System Security menu, navigate to Administrator Password and press Enter.

   The Administrator Password menu screen appears, as shown in Figure 187: Administrator Password menu window on page 268.

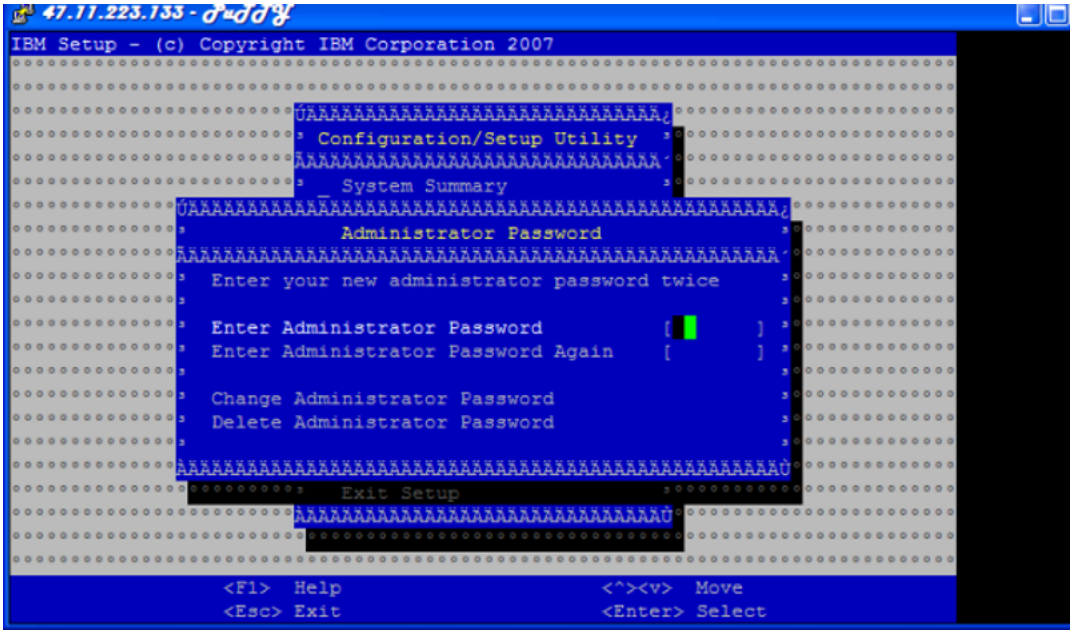


Figure 187: Administrator Password menu window

4. In the Administrator Password menu screen, navigate to Enter Administrator Password and type a password.
5. Navigate to Enter Administrator Password Again an retype the password.

6. Navigate to Change Administrator Password and press Enter.

   The Change Administrator Password confirmation screen appears, as shown in Figure 188: Change Administrator Password confirmation window on page 269.

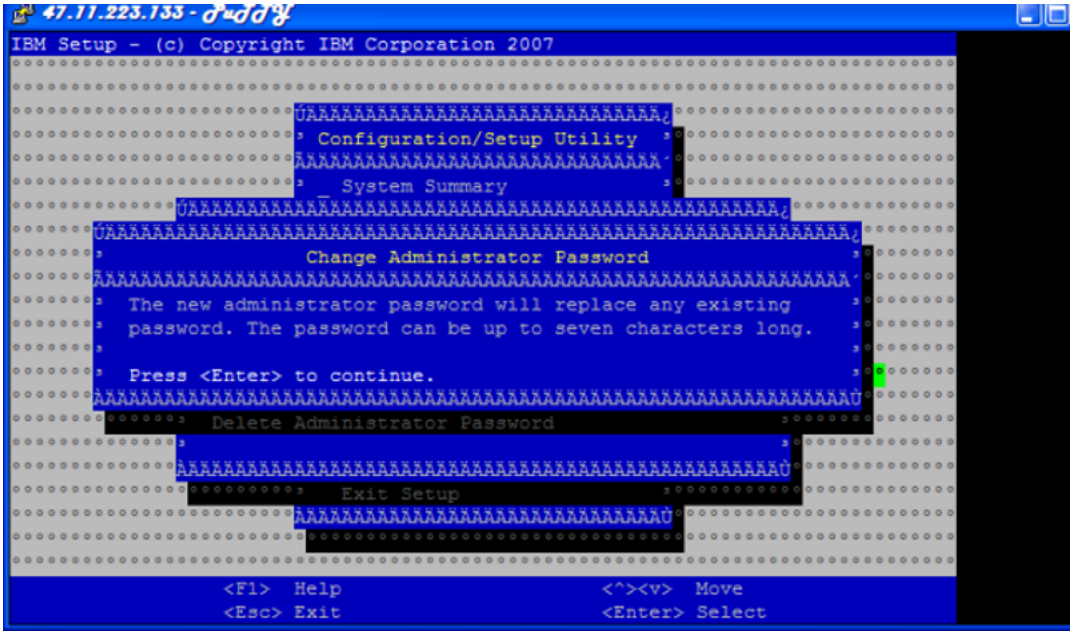


Figure 188: Change Administrator Password confirmation window

Appendix B: Installation times

This section contains the average installation times using a variety of installation methods.

Average installation times by media type

Note:

The numbers in the following table are approximate and actual times can vary according to network characteristics and other factors.

The following table provides the average Linux Base installation times on the supported hardware platforms by media type.

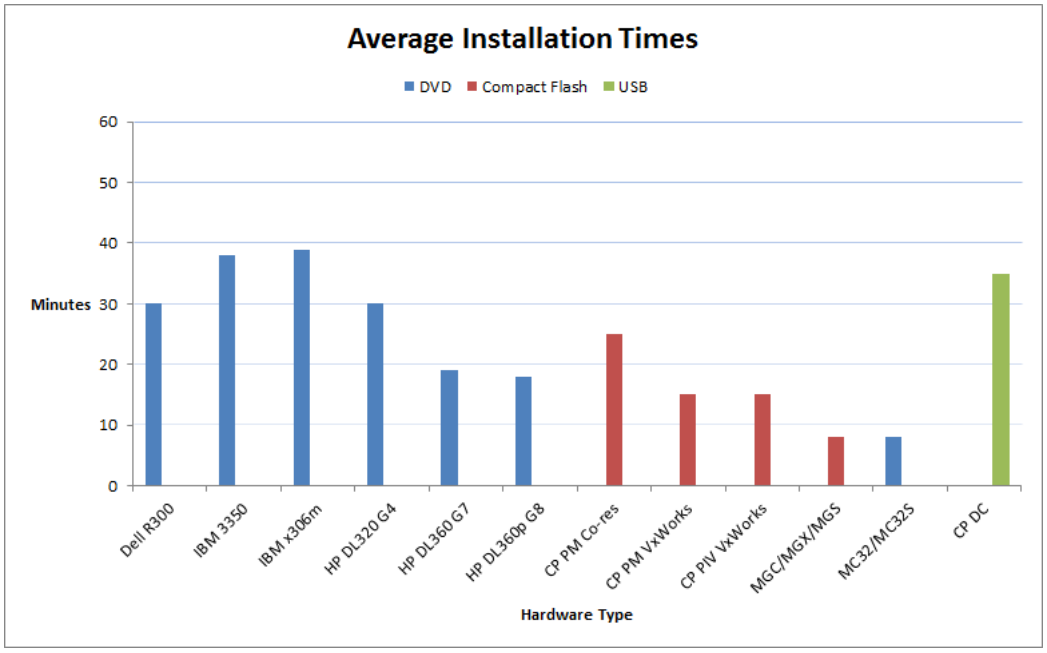


Figure 189: Average installation times by media type

Linux Base and application deployment—average installation time

Note:

The numbers in the following table are approximate and actual times can vary according to network characteristics and other factors.

The following table provides the average installation time using Deployment Manager. Deployment Manager includes a system upgrade of the Linux Base installation and application deployment.

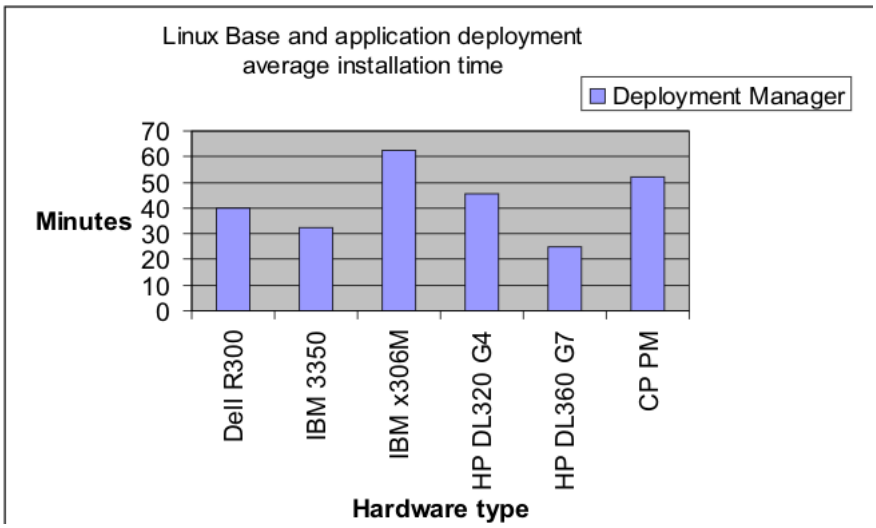


Figure 190: Average installation time using Deployment Manager

Appendix C: Avaya Aura® Media Server

This section is for information related specifically for Avaya Aura® Media Server.

Note:

Avaya Aura® Media Server was formerly known as Media Application Server (MAS).

Checklist for adding a new maintenance release for Avaya Aura® MS

The following checklist describes how to up-issue a new Avaya Aura® MS software load (.nai file). If a new maintenance release of Avaya Aura® MS is available, you can reinstall the Avaya Aura® MS .nai file. You are not required to perform a complete Avaya Communication Server 1000 (Avaya CS 1000) member upgrade.

If you are upgrading an Avaya Aura® MS that belongs to a cluster, you must upgrade each Avaya Aura® MS in the cluster. Upgrade the servers in the following order:

- Primary Avaya Aura® MS
- Secondary Avaya Aura® MS
- Standard Avaya Aura® MS

1. Using Element Manager, backup your Avaya Aura® MS data to an available destination, for example, Local server or remote FTP server. For more information about Avaya Aura® MS data backup using Element Manager, see the Avaya Aura® MS documentation *Implementing and Administering Avaya Aura® Media Server*.
2. Log on to the Primary UCM (Deployment Server) using an account with the NetworkAdministrator role assigned, as described in Logging on to Unified Communications Management on page 77.
3. Delete the Avaya Aura® MS service for the server being up-issued, as described in Deleting a Network Service on page 93.
4. Undeploy the Avaya Aura® MS application, as described in Removing applications on a server on page 106.
5. Restart the Jboss-Quantum application on the Avaya Aura® MS member server.
6. Delete the Avaya Aura® MS .nai file, as described in Deleting a software load on page 80.

7. Load the up-issued Avaya Aura® MS .nai file from the Deployment Manager library, as described in Software loads on page 78.
8. Recreate a new Avaya Aura® MS service to the server where you want to install Avaya Aura® MS, as described in Adding a Avaya Aura MS service on page 90.
9. On the Deployment View page, choose **Servers** from the **View** list, and click **Commit**.
10. Deploy the Avaya Aura® MS application, as described in Deploying applications on a Server on page 104.
11. Restore the Avaya Aura® MS data from the Element Manager Avaya Aura® MS data backup location.

    Note:

    You must restore the data for each Avaya Aura® MS within a cluster.

Checklist for upgrading a stand-alone MAS

The following checklist describes how to upgrade a standalone MAS running version 6.4 software for Communication Server Release 7.0 to MAS version 7.0 for Communication Server Release 7.5 or later. Before beginning this procedure, ensure you have obtained the required Avaya Aura® MS licences.

Note:

Avaya Aura® MS cluster upgrade is not applicable for migration from Communication Server Release 7.0 to Communication Server Release 7.5 or later.

1. Using Element Manager, backup your MAS data. For more information about MAS data backup using Element Manager, refer to the MAS documentation.
2. Using Avaya Unified Communication Management, perform the MAS system upgrade. For more information, see Checklist for adding a new maintenance release for Avaya Aura MS on page 272.
3. Restore the MAS data from the Element Manager MAS data backup location.
4. Restart the Jboss-Quantum application on the server where MAS is deployed.
5. Apply the required licenses.

Quick Fix Engineering Avaya Aura® MS patches

Install a Quick Fix Engineering (QFE) patch (also referred to as a hot fix), to deliver and apply a patch to Avaya Aura® Media Server. QFE can also refer to an individual fix. A QFE patch is a temporary fix you apply to Avaya Aura® MS that has not gone through a product verification cycle.

Apply QFE patches only to systems that require an immediate fix and cannot wait for an official release.

Important:

Only install a QFE patch if advised by Avaya.

You must always install QFE patches sequentially, because QFE patches are dependent on previous patches. For example, you must install QFE-platform-7.0.0.xx-0001 before you install QFE-platform-7.0.0.xx-0002.

In an N+1 cluster configuration, apply a patch to one node at a time while you divert calls to the other nodes.

Prerequisites to Quick Fix Engineering patch installation:

- Back up your system before you install a QFE patch. If a problem occurs during the patch installation, you can use the backup to restore your system to the previous configuration. For more information about Avaya Aura® MS data backup and restoration, refer to the Avaya Aura® MS documentation.
- Install the latest software version for Avaya Aura® MS.
- Install any previous QFE patches for the installed software version.

For information about Avaya Aura® MS patch installation, see *Installing, Upgrading, and Patching Avaya Aura® Media Server*.

Appendix D: Avaya Linux Base CLI commands

Avaya Linux Base CLI commands contains a list of the command line interface (CLI) commands used in Avaya Linux Base. Type **(linuxbase-command) -h | --help | help** at the command prompt to display a brief summary of the CLI command, as shown in Table 13: Linux CLI command help on page 275. Type **man (linuxbase-command)** at the command prompt for a more detailed description, as shown in Table 14: Linux man command example on page 275.

Table 13: Linux CLI command help

```
$ poos --help
Usage:
poos (patch_id)|-app *(app_name)*|--help,-h
Options:
(patch_id)
Deactivate patch with (patch_id) handle.
-app *(app_name)*
Deactivate all patches for the application (app_name).
--help Print this help message and exit.
```

Table 14: Linux man command example

```
$ man poos
POOS(1) User Contributed Avaya Documentation POOS(1)
NAME
poos - Put a patch out of service.
SYNOPSIS
poos (patch_id)| -app (app_name) | --help,-h
DESCRIPTION
Remove a patch from service. The patch is removed from service from all
processes in which it was in service.
```

Table continues…

```
OPTIONS

(patch_id)

Deactivate patch with (patch_id) handle.

-app (app_name)

Deactivate all patches for the application (app_name).

--help Print this help message and exit.
```

EXAMPLE

```
Deactivate patch with 2 handle

$ poos 2

Patch handle: 2

Please ensure that the application solid is stopped before proceeding patch un-
installation. Do you want to continue patch un-installation? (Y/N) [N]? y

Performing the uninstallation:

Performing uninstall RPM patch... Preparing...
########################################### [100%]

1:avaya-cs1000-solid ########################################### [100%]

executing Solid DB post install...

Installation avaya Solid database server completed.

Unstalling the Solid database server package done

Done.

The RPM patch uninstallation is completed.

The patch 2 has been deactivated successfully.

Deactivate all sunAm patches

$ poos -app sunAm

Patch handle: 0

Performing the uninstallation:

The patch 0 has been deactivated successfully.

SEE ALSO pload, pout, pins, pstat, plis

5.50 2007-12-18 POOS(1)
```

Avaya Linux Base uses common (no access restrictions) CLI commands plus 8 categories of CLI commands that correspond to the 8 Avaya Linux Base user groups. The 8 categories of CLI commands are shown in the following list:

- backupadmin
- dbadmin

- logadmin
- maintadmin
- patchadmin
- securityadmin
- systemadmin
- timeadmin

Table 15: Common CLI commands

Command	Description
appVersionShow	Print the application software version for the server.
baseVersionShow	Print the Base software version for the server.
echo	Display a line of text on the terminal screen.
find	Search for files in a directory hierarchy.
ftp	Transfer files to and from a remote network site.
ifconfig	Configure a network interface.
ls - ll	List directory contents.
man	Format and display the online manual pages.
printenv	Print all or part of environment.
scp	Copy files between hosts on a network using ssh.
sftp	Transfer files to and from a remote network site secure file transfer program.
ssh	Run OpenSSH SSH client (remote login program) to provide secure encrypted communications between two untrusted hosts over an insecure network.
su	Run a shell with substitute user and group IDs.
swVersionShow	Print the server's software version.
telnet	Communicate with another host using the TELNET protocol.
whoami	Print the user name associated with the current effective user ID.

Table 16: backupadmin CLI commands

Command	Description
sysbackup	Perform a system backup of installed, configured, and running base and applications.

Table 17: maintadmin CLI commands

Command	Description
consoleShow	Displays console speed.
gnome-system-monitor	GNOME process viewer and system monitor with a nice easy-to-use interface.
netstat	Print network connections, routing tables, interface statistics, masquerade connections, and multicast memberships.
pcapConfig	Configure PCAP for Linux.
pcapCtrlRemove	Stops the PCAP for Linux listener interface.
pcapCtrlStart	Start the PCAP for Linux listener interface.
pcapRestart	Restart PCAP for Linux.
pcapStatus	Displays the current status of PCAP for Linux.
pcapStop	Stop PCAP for Linux.
wireshark	Network protocol analyzer.
pcap	Tools for Linux is a network packet capture utility.
ppp	Initiate a PPP connection.
tcpdump	Command-line packet analyzer.

Table 18: patchadmin CLI commands

Command	Description
freeDiskSpace	Cleans up /var and /admin partitions to allow Service Pack installation.
issp	Generates a list of installed RPMs, SUs and patches.
pins	Put the patch in service.
plis	Show detailed information about the patch.
pload	Load the patch into the system database.
poos	Put the patch out of service.
pout	Unload the patch from the system database.
pstat	Show a list of installed patches.
spins	Put a Service Pack into service.
spload	Load a Service Pack (bundle of patches and SUs) into the system database.
spout	Unload a Service Pack (bundle of patches and SUs) from the system database.
spstat	Show the installed and in service SPs.

Table 19: securityadmin CLI commands

Command	Description
basefirewallconfig	Configure firewall settings.
checkIPsecStatus	Use “Check IP Security Status” command.
disableAllTargets	Disable all IPSec targets and remove all IPSec data.
harden	Command to manage Avaya Communication Server 1000 hardening items.
harden audit status	Displays the status of the Linux Audit Daemon.
harden banners set/file	Modify the banner text. The banner text will be replaced by the content from the file.
harden banners status	Enables or disables the pre-login banners.
harden basic reapply	Apply basic hardening changes. Ensures that the basic hardening items are in secure status.
harden coredumps status	Enables or disables the coredump service.
harden ftp status	Shows that FTP service is turned on or off.
harden help	Displays help information for using the command.
harden nettools status	Enables or /disables the nettools service.
harden nfs help	Displays help information for using the command.
harden nfs on	Enables Network File System (NFS) when deploying the primary security server.
harden nfs off	Disables NFS after deployment is complete.
harden nfs status	Shows that NFS is turned on or off.
harden passwd_days off	Disable previously configured parameters.
harden passwd_days on	Enables previously configured parameters.
harden passwd_days set -max	Configure the value of the PASS_MAX_DAYS parameter. The default value is 90.
harden passwd_days set -min	Configure the value of the PASS_MIN_DAYS parameter. **Note:** This parameter must be set to a value > or = 1. The default value is 1.
harden passwd_days status	Provides the current value of the parameters from hardening storage.
harden rlogin	Apply hardening to remote logons. **Note:** rlogin is only available in Co-res Avaya CS and SS configurations.
harden ssh_filter -allow add –subnet	Add a subnet to the allowed list.

Table continues…

Command	Description
harden ssh_filter -allow del	Delete a host IP 1 from the allowed list.
harden ssh_filter -allow del -IP	Delete a host IP from the corresponding (allow or deny) filtration list.
harden ssh_filter -allow del –subnet	Delete a subnet from the allowed list.
harden ssh_filter -deny add -IP	Add a host to the deny list.
harden ssh_filter -deny del -IP	Delete a host IP from the deny list.
harden ssh_filter -deny del <number>	Delete a host IP from the corresponding filtration list. Each host entity (per line) has logical ordinal number in XML file storage. <number> is this sequence number.
harden ssh_filter status	Shows the list of the names of the hosts which are allowed to connect to Linux Base by SSH.
harden status	Retrieve the status of Linux Base Enhanced Hardening options.
harden telnet status	Shows that telnet service is turned on or off.
harden tftp status	Shows that TFTP service is turned on or off.
isssDecom	Clean up ISSS settings and delete ISSS configuration files.
isssReset	Reset ISSS configuration.
isssShow	Print out ISSS settings.
masterfirewallconfig	Master firewall configuration.
nfsexportsconfig	Network File System Export Configuration.
sshconfig	Configure SSH keys.

Table 20: systemadmin CLI commands

Command	Description
appinstall	Install Avaya applications. **Note:** Do not use the appinstall command unless you are directed to use it by Avaya support.
appstart	Stop, start, or restart Avaya applications.
arp	Manipulate the system ARP cache.
baseparamsconfig	Configure base parameters. **Warning:** Do not change the FQDN of the primary or backup security server when you use the baseparamsconfig command.

Table continues…

Command	Description
defaultSAconfig	Configure signature algorithm (SHA1withRSA or SHA256withRSA) which will be used in the system by default.
datetimeconfig	Configure the date and time.
dnsconfig	Configure DNS values.
ecnconfig	Configure Explicit Congestion Notification settings.
hdStat	Displays the size of the hard disk.
hostconfig	Configure the static lookup table for host names.
memShow	Displays available, free, and used server memory.
memSizeShow	Displays the total server memory.
networkconfig	Configure network settings. **Warning:** Do not change the FQDN of the primary or backup security server when you use the networkconfig command.
ntpconfig	Configure Network Time Protocol settings.
reboot	Restart the entire system.
routeconfig	Configure routing entries. **Note:** When you use routeconfig to add a host route you do not need to provide a netmask. If you do provide a netmask, the format must be 255.255.255.255.
stty	Change and print terminal line settings.
sysbackup	Configure and perform a system backup of installed, configured, and running base and applications.
syslogFacilitySet	Set the facility value.
syslogLevelSet	Set a value for level.
syslogShow	Display syslog processes. **Note:** The help key is not valid for **`syslogShow`**. If you want to retrieve help information, you must use the format **`syslogShow -h`** or **`syslogShow -help`**.
sysrestore	Perform a restore of base and application data (backed up by sysbackup).
timeadj	Specify system clock parameters.

Table continues…

Command	Description
upgrade	Select the backup data source and reinstall Linux Base.

Note:

You might need to add the primary host entry in backup and member servers before you can access them using the **hostconfig** command.

The command syntax is **admin2 user ---> hostconfig add -ip <PRIMARY SERVER IP> -host <PRIMARY SERVER HOST NAME> -domain <PRIMARY SERVER DOMAIN NAME>**.

Table 21: timeadmin CLI commands

Command	Description
datetimeconfig	Configure the date and time.
ntpconfig	Configure Network Time Protocol settings.
timeadj	Specify system clock parameters.

Appendix E: Troubleshooting

This chapter contains information on troubleshooting application deployment errors.

Deployment errors

The following table provides a list of the possible errors that can appear during application deployment with a description of the possible causes and actions to help troubleshoot the error.

Table 22: Deployment errors

Error Message	Description	Action
Applications are already installed.	Possible causes: Case: deploy is called when Avaya Applications are already installed.	From the **Deployment Actions** list, choose **Deploy**.
Applications are not installed.	Deployment manager status may not have been correct initially. Case: deploy is called when Avaya Applications are already installed. This case supports auto-recovery – the server status should reset to correct one automatically.	No action is required, the server status should be reset to correct value.
Error occurred while backup of target.	Possible causes: General error for any backup failure. Any one of the backup scripts failed. Network problem.	Check your network (on TLAN) between the deployment server and the target. Check your network between the target and the SFTP server. Check permissions on the file system. Check whether the SFTP server has enough free disk space to keep the backup archive.
Failed to clear a directory in pre-installation phase.	Possible causes: Generic error. Could be some permission issue.	Check the permissions. Try the operation again.
Failed to create a directory in pre-installation phase.	Possible causes: Generic error. Could be some permission issue.	Check the permissions. Try the operation again.
Input parameter(s) validation failed.	Possible causes: Provided keycode file does not exist (something must	Browse and validate the keycode again.

Table continues…

Error Message	Description	Action
	have gone wrong during the keycode file upload).	
Can't copy installation xml.	Possible causes: Some permission problem which is disallowing the copy of the install.xml file under the /admin partition.	Check file permissions of the /admin partition. Repeat the operation again.
No configure.xml files found.	Corrupted .nai file. Damaged installation.	Upload the software load again. Try the application installation again. Backup the data, and reinstall Linux Base again.
Please login as a user with valid permissions to use Deployment Manager.	Deployment manager is not running as user admin2.	Make sure that Jboss is running as user admin2. Perform “ps –ef | grep jbossd” and check whether the user is admin2
Cannot get preconfig data.	Possible causes: Can be set if preconfig data are found on the target but cannot be extracted from an archive file.	Try again, and if problem persists, get Avaya help.
Failed to prepare or transfer deployment data. Make sure the network connection to your target is in working condition. See Help for more details.	Possible causes: Network connection between the deployment server and the target may have some problem Available disk size and permission problem.	Try the operation again. Check available disk space.
Installation data preparations error.	Possible causes: Couldn’t create the necessary files for this particular target.	Try again, and if problem persists, get Avaya help.
Restore of applications failed.	Possible causes: General error for any restore failure. Any one of the backup scripts failed. Network problem.	Check network connection, permissions and try one more time. Make sure that there is enough space on the server to keep restore archive. Check the linuxbase.log from Base manager.
RPM database is corrupted. Re-installation of Linux Base is required.		
RPM installation failed.	Possible causes: Corrupted .nai file.	Check the appinstall_stderr.log, appinstall_stdout.log and linuxbase.log. Check to see whether there is any dependency problems (which will be indicated in the appinstall_stderr.log). Try the operation again.
RPM uninstallation failed.		

Table continues…

Error Message	Description	Action
Operation is blocked by another process. Please try again.	Possible causes: Applicable for Deploy, Undeploy, Backup, Restore and Upgrade cases. Indicates that semaphore is busy and operation cannot be started to avoid data integrity corruption.	Wait for sometime and try the same operation again.
Remote script failed.	Possible causes: Generic error. Applicable for Deploy, Undeploy, keycode validate and Upgrade cases. Set if for example, remote script cannot be executed, command is not found, not enough permissions and so on.	Check permission of the file system. Check the connection between the deployment server and the target.
Transfer failed.	Possible causes: SCP operation (remote copy command) failed.	Check your network (on TLAN) between the deployment server and the target.
Undeployment error.	Possible causes: There are some patches that cannot be removed.	Check the appinstall_stderr.log , appinstall_stdout.log, and the linuxbase.log. Check the network connection. Try undeployment again.
Undefined parameter.	Possible causes: Some mandatory values are not set in deployment manager properly.	Set all required values, and try the operation again. Seek help from Avaya.
Undefined parameter.	Possible causes: Some mandatory values are not set in deployment manager properly.	Set all required values, and try the operation again. Seek help from avaya.
An unexpected error occurred.		Please try the operation again. If not successful seek help from Avaya.
Error occurred while restoring Could not retrieve the information for the target on the deployment server.	Please try the operation again. If not successful seek help from Avaya.	
Error occurred while saving target.	Possible causes: Problem in writing the target information on the deployment server. Frequency: Very Low Severity: Major	Please try the operation again. Go to the folder /var/opt/avaya/deployment/deployed/<hostname> and check for any permission or disk space issues that could prevent writing to this folder. If not successful seek help from Avaya.
Could not retrieve UCM elements temporarily. Please refresh the page.	Possible causes: There was a problem retrieving the linux Base element(s) from UCM. Refresh the page by clicking on the refresh link.	Refresh the page by clicking on the refresh link.

Table continues…

Error Message	Description	Action
Target in an invalid status for requested action.	Possible causes: Someone else may have started another operation on the target. The information on the deployment server is corrupted.	Refresh the page. Try again later. If not successful seek help from Avaya.
Error occurred while deploying/upgrading/ undeploying target.	Possible causes: Could not make the system call to execute the linux Base commands to perform the deploy/ upgrade/undeploy operation.	Seek help from Avaya.
Failed to generate a pre configuration file.	Possible causes: ElementInternalID is blank for the chosen call server. Could not create the cs1000.properties file. Error while writing to the cs1000.properties file. Could not create the csinst.ini file. Could not create the preconfiguration directory.	Check the file system for disk space and permissions.
Maximum number (3) of simultaneous deployment reached.	There are already 3 deployment operations in progress.	Wait for at least one deployment to complete before starting a new deployment.
Could not validate keycode. Error occurred during validation process.	Could not make the system call to run the keycode validation base command.	Check whether the keycodeValidate API exists on the server. Also check whether executable permissions are set properly.
Keycode file missing on target, or can't read the file.	There has been some problem in the keycode uploading process.	Browse and validate the keycode again. Check whether the keycode is of non-zero size.
Version in keycode does not match software version to be installed.		Make sure that the Release and Issue of the keycode are matching the version of the software to be installed. Obtain a proper keycode or use the proper software version.
System type in keycode does not match the hardware type.		Browse and validate the keycode again. Obtain a proper keycode or use the proper software version.
Keycode file corrupted.		Browse and validate the keycode again. If it does not work, try regenerating the keycode.
Cannot detect dongle, dongle missing, or cannot read the dongle.	Dongle is not installed (or not properly installed) on the system. Dongle is hot-plugged in without restarting the server. Dongle is bad.	Make sure the dongle is properly installed. Restart the server with the dongle installed. Replace the dongle with a good one.
Keycode does not match dongle.	Keycode maybe invalid. Dongle maybe invalid.	Make sure the keycode is right and the dongle is right, and they match.

Table continues…

Error Message	Description	Action
Keycode file contains invalid load build cycle.	The load build cycle on the keycode is not valid. Only valid load build cycle is “MR (market release)”.	Obtain a keycode with a valid load build cycle.
Could not validate keycode. Error occurred during validation process.	Could not execute the keycode validation software.	Make sure that the kcv software is present, and with executable permission.
Could not mount software load: Invalid mount point. Restart the server and try again.		
Could not find a valid software load. File or media may be invalid.	Software load .nai file maybe corrupt.	Try uploading the .nai file again.
Software load could not be copied to the deployment server.		Check whether there is enough disk space on the deployment server to copy the .nai file.
Software Load media is not accessible. Media not present or busy.		Check whether the CD/DVD or Compact Flash is inserted properly in the drive. Check whether the CD/DVD or Compact Flash has the application software or customer database, whichever you are trying to upload.
Could not determine hardware type of this server.	The h/w type is not in the baseOs.properties file.	Check the /admin/avaya-linuxbase-info file for the SYSTEM_HW_PLATFORM field. If it is proper, then do a system restart, otherwise seek help from Avaya.
Failed to get Software Load information - install.xml file does not exist.	Install.xml file is missing in the load (i.e. corrupted software load)	Try uploading the software load .nai file again. Check the directory /var/opt/avaya/deployment/app_loads/<app_load>/ to see whether the install.xml file is present. Check whether the .nai file you got is of expected size.
Failed to get Software Load information - Could not read install.xml.	Could not read install.xml file. Must be corrupted.	Try uploading the software load .nai file again. Check whether the .nai file you got is of expected size.
Failed to access software load data file. Please try again.	Could not access the software load .nai file.	Check whether you can access this file on your PC or the CD/DVD or compact flash that you are trying to upload from. Check whether it has the right permissions.
Software load add is already in progress.	Another user has started a software upload process.	Refresh the page. This should show the same page as the other user is

Table continues…

Error Message	Description	Action
		getting. Wait until the other upload is done before initiating the software add.
Software load already exists. If you would like to replace the existing load, please delete it from the table and add again.	The software load that you are trying to upload already exists on the deployment server.	As suggested, first delete the software load from the table. Then try the add again.
Failed to create the preconfig directory for call server configuration.	Could not create the directory /var/opt/avaya/deployment/deployed/<hostname>/preconfig/cs or /var/opt/avaya/deployment/deployed/<hostname>/preconfig/em. Could be disk space issue or permission issue.	Check the disk space and permissions for the above mentioned directory.
Unable to retrieve target server details. Please cancel and try again.		
Maximum number (3) of software loads reached on this server. Please delete one of the loads before proceeding with an add operation.		
Cannot delete the selected software load(s). Make sure all deployment and upgrade operations are completed before deleting a load.	Some other user maybe performing a deployment or upgrade which uses this load.	Wait till other operations are done (can check on the deployment targets page), and then retry the deletion.
Backup file is null or the file type is invalid.	Possible causes: Backup file is empty, or the extension is not .tar.gz as expected. Severity: Minor	Browse an appropriate backup file.
Backup file not found.		
An I/O error occurred while uploading backup file.		
Unexpected error occurred while uploading backup file.		
Backup file name is invalid.	Backup filename extension is not .tar.gz as expected.	Make sure that proper backup file is being used.
Keycode file is null or the file type is invalid.	Keycode file that was browsed is empty or the extension is not .kcd as expected.	Choose a proper keycode file that ends with .kcd.

Table continues…

Error Message	Description	Action
Keycode file not found.	Keycode file upload had some issues.	Browse and validate the keycode again. Make sure that the keycode is valid.
An I/O error occurred while uploading keycode file.	Keycode file upload had some issues.	Browse and validate the keycode again. Make sure that the keycode is valid.
Unexpected error occurred while uploading keycode file.	Keycode file upload had some issues.	Browse and validate the keycode again. Make sure that the keycode is valid.
An I/O error occurred while uploading customer database file.	Customer database file upload had some issues.	Browse and upload the customer database again. Make sure that the customer database is valid.
Unexpected error occurred while uploading customer database file.	Customer database file upload had some issues.	Browse and upload the customer database again. Make sure that the customer database is valid.
An I/O error occurred while extracting customer database archive file.	Customer database file upload had some issues.	Browse and upload the customer database again. Make sure that the customer database is valid.
Failed to extract customer database from the archive file.	Customer database file upload had some issues.	Browse and upload the customer database again. Make sure that the customer database is valid.
Software version delete failed for one/more selected loads.		
Error occurred while backing up target.	Could not make the system call to execute the base commands appBackup.	Check whether the appBackup script exists on the server, with executable permission.
Error occurred while restoring target.	Could not make the system call to execute the base commands appRestore. System call got interrupted for some reason.	Check whether the appRestore script exists on the server, with executable permission.
Invalid IPv4 format.		
Maximum number of backups reached. Please delete any of the existing backups for the same target using Backups management.	Only three backups are allowed to be stored on the deployment server, per target.	
Failed to delete one/more backups.		Try refreshing the page, and try the delete again.
Maximum number (3) of simultaneous restores reached.	Only three restore operations are allowed simultaneously.	Wait for a short period of time, and then try the restore operation.

Table continues…

Error Message	Description	Action
Maximum number (3) of simultaneous backups reached.	Only three backup operations are allowed simultaneously.	Wait for a short period of time, and then try the backup operation.
Selected file does not match required format(.tar.gz).		
Server path cannot be empty.		
Required fields cannot be empty.		
Server IP address cannot be empty.		
Username cannot be empty.		
Password cannot be empty.		
Not enough disk space available for backup. Please ensure that the /var partition has at least 20% space available, and try the backup again.		
Could not validate size of the disk. Please try again.		
Note - An automatic status update was not available. Click the refresh link (above, right) to verify current status.	Could not retrieve information from UCM regarding the targets. This is a temporary problem due to concurrent access and race conditions.	As suggested, refresh the page again.
Failed to delete elements on this target. Please manually delete the elements from UCM elements table.	After undeployment, DM deletes the associated elements (CS 1000, NRSM, Subscriber Manager depending on what was deployed). For some reason, it couldn't delete these elements.	Go to the UCM elements page and find the corresponding elements, and delete them.
Call server ELAN IP cannot be empty or invalid IPv4 format.		
Call server tape ID cannot be empty.		Check the tape ID on the call server dongle.
Call server tape ID must be alphanumeric		Check the tape ID on the call server dongle. It cannot have any special characters.

Table continues…

Error Message	Description	Action
MAC address format is invalid.		
The target is performing an operation launched from another deployment server. Please try again later.	If you are performing a operation centrally, then it could be that some other user is performing some operation locally on the box and vice versa.	Make sure that no one else is performing any operation on the box from anywhere else.
Cannot find install.xml file.	Corrupted .nai file.	Upload the software load again.
Cannot add node in Element Manager. Signaling Server does not appear in list.	Applications were deployed locally and the target server does not belong to a group.	Avaya recommends using Deployment Manager Preconfiguring process using Deployment View on page 74 to configure target servers. Otherwise, create a CS 1000 group and Commit the locally deployed server.

Linux Base installation errors

The following list contains information to help you troubleshoot errors during the Linux Base installation. For more information about hard drive, memory, and BIOS requirements for the COTS and CP PM platforms, see Hardware platforms on page 204.

Insufficient hard drive capacity

The platform must meet the hard drive and memory requirements; otherwise, the Linux Base installation fails and the server returns to the previous state.

If the hard drive is less than 40 GB, the following screen appears:

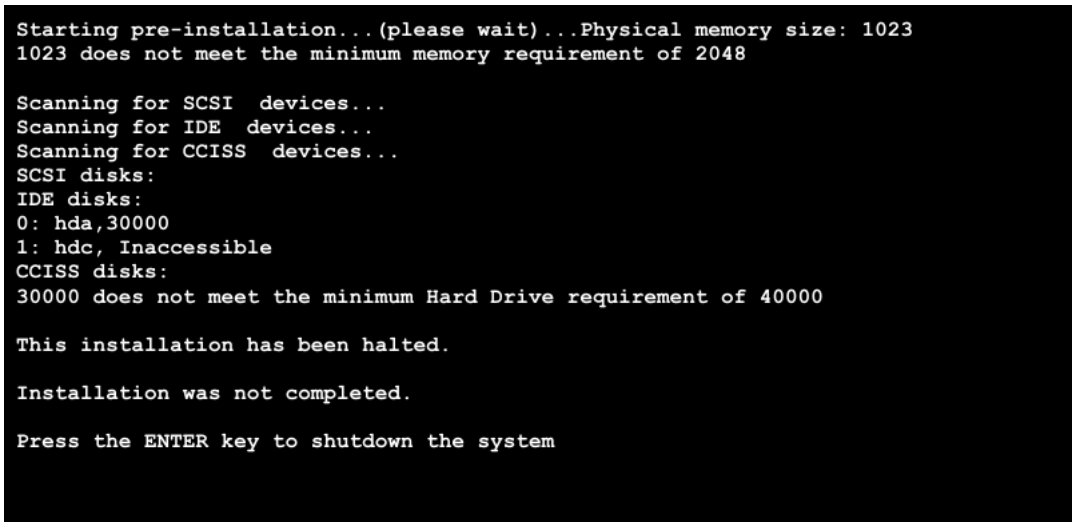


Figure 191: Insufficient hard drive capacity

Insufficient memory size

If there is less than 1 GB of memory available, the following screen appears:

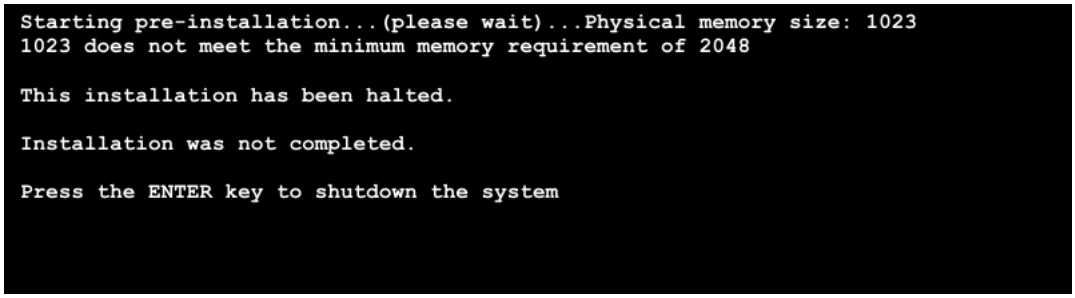


Figure 192: Insufficient memory size

Log file

Description:

The status of the Linux Base version did not change during a new installation and the applications did not deploy.

Action:

Check the `/var/log/avaya/linuxbase.log` file.

If the logs shows that the applications deployed properly but it is not reflected in Deployment Manager, then UCM registration was not successful. You can also use the **`swVersionShow`** command to see if deployment was successful.

Backup security server configuration error

The FQDN of the backup security server is associated with the TLAN IP address of the server. Although the backup security server is also connected to the ELAN, you must always configure it using the TLAN. If you used the ELAN IP address to join the security domain when installing and configuring the backup security server, you can correct this issue by doing the following:

1. Power down the backup security server.
2. From the Primary security server, remove the backup security server from the list of elements.
3. Rebuild the backup security server.
4. Rejoin the backup security server to the security domain.

Appendix F: Network configuration for Secure File Transfer Protocol (SFTP) data backup

Use the guidelines in this appendix to assist in data backup to an SFTP server. The section Network configuration on page 293 provides details on network requirements and the section SFTP logon on page 293 provides SFTP logon details. The section SFTP network configuration requirements on page 294 provides specific Embedded Local Area Network (ELAN) and Telephony Local Area Network (TLAN) requirements for SFTP network configuration.

Network configuration

The network must be configured correctly for data backup to an SFTP server. In order to configure the network you must understand the difference between the ELAN and the TLAN. The ELAN and TLAN are defined as follows:

- ELAN - The ELAN is a secure local area network. The scope of this network is limited to one subnet or node; however the scope of the ELAN network can be expanded to cover multiple nodes with advanced router (data path) configurations.
- TLAN - The TLAN spans the entire enterprise network. Every node on the TLAN has access to every other node.

  The TLAN supports both IPv4 and IPv6 addresses.

Note:

The definitions of ELAN and TLAN are a subset of the definitions provided in the voice media gateway cards section of *Avaya Signaling Server IP Line Applications Fundamentals, NN43001-125*.

SFTP logon

Data backup to an SFTP server requires a user logon, password, and path to access the SFTP server storage. The user logon can contain a maximum of 32 characters comprised of lower and

uppercase letters, numeric digits, and the special characters _ . - and $. You cannot use the character - at the beginning of the logon string and you can use $ only at the end of the logon string.

Avaya Linux Base uses the character / to specify paths in the system. Use the / character when you specify the SFTP directory.

SFTP network configuration requirements

The SFTP option requires an operational ELAN network because the backup and recovery of data must use the ELAN interface. Avaya recommends the destination SFTP server reside on the same ELAN network as the source SFTP server. If the destination SFTP server resides outside the subnet of the source SFTP server, use one of the two options shown in Table 23: SFTP network configuration requirements on page 294.

Note:

Not all Windows based SFTP servers can be used as SFTP backup servers. The following Windows based SFTP servers can be used:

- Sysax Multi Server
- OpenSSH for Windows

The following Windows based SFTP servers are not supported:

- Core FTP mini-sftp-server
- CrushFTP
- freeFTPd
- NullFTP
- TitanFTP
- winSSHD

Table 23: SFTP network configuration requirements

Option	Details
1	The router connecting the two subnets must be configured to allow pings to pass through. This ensures there is a valid data path between the two subnets If the default gateway is set to the TLAN interface gateway, a routing entry is required to ensure that all ELAN data uses only the ELAN NIC. Use the CLI command **`routeconfig`** to add the routing entry. An example of the **`routeconfig`** command is as follows: routeconfig add -net destination_ip -netmask subnet_mask -gw gateway_ip -dev eth0
2	On the source server set the ELAN interface gateway as the default gateway.

Appendix G: Change the FQDN of a Primary or Backup Security Server

This appendix contains the following procedures for changing the FQDN of a Primary or Backup Security Server:

- Changing the FQDN of a Primary Security Server on page 295
- Changing the FQDN of a Backup Security Server on page 296

Related links

Changing the FQDN of a Primary Security Server on page 295
Changing the FQDN of a Backup Security Server on page 296

Changing the FQDN of a Primary Security Server

Use the following procedure to change the FQDN for a Primary Security Server.

1. Perform a Primary Security Server and Backup Security Server database backup, as described in *Linux Platform Base and Applications Installation and Commissioning, NN43001–315*.
2. Create an inventory list of all applications deployed on the Primary Security Server and Backup Security Server.
3. Create a list of all member servers joined to the Primary Security Server.
4. Unregister all VxWorks devices, as described in *Security Management Fundamentals, NN43001–604*.
5. Perform a fresh Linux base install on the Primary Security Server and Backup Security Server, as described in *Linux Platform Base and Applications Installation and Commissioning, NN43001–315*.

   Note:

   If you change the domain name of the Primary Security Server during Linux base installation, you must make the same change to the Primary Security Server domain name during Linux base installation on the Backup Security Server.
6. Configure the Primary Security Server and deploy the necessary applications, as described in *Linux Platform Base and Applications Installation and Commissioning, NN43001–315*. Use the Primary Security Server application inventory list that you created in Step 2 on page 295 to determine which applications to deploy.

7. Apply the latest Service Pack on the Primary Security Server, as described in *Patching Fundamentals, NN43001–407*.
8. Restore application data on the Primary Security Server, as described in *Linux Platform Base and Applications Installation and Commissioning, NN43001–315*.

   Note:

   When you restore application data, ensure that you select the **Restore data for deployed applications only** checkbox.
9. Configure the Backup Security Server, as described in *Unified Communications Management Common Services Fundamentals, NN43001–116*.
10. Deploy the necessary applications on Backup Security Server, as described in *Linux Platform Base and Applications Installation and Commissioning, NN43001–315*. Use the Backup Security Server application inventory list that you created in Step 2 on page 295 to determine which applications to deploy.
11. Restore application data on the Backup Security Server, as described in *Linux Platform Base and Applications Installation and Commissioning, NN43001–315*.

    Note:

    When you restore application data, ensure that you select the **Restore data for deployed applications only** checkbox.
12. If you change the domain name of the Primary Security Server, you must change the Primary Security Server domain name on all member servers. For information about changing the Primary Security Server domain name on member servers, see *Linux Platform Base and Applications Installation and Commissioning, NN43001–315*.
13. Join all member servers to the Primary Security Server, as described in *Unified Communications Management Common Services Fundamentals, NN43001–116*.
14. Join all VxWorks devices to the Primary Security server, as described in *Security Management Fundamentals, NN43001–604*.

Related links

Change the FQDN of a Primary or Backup Security Server on page 295

Changing the FQDN of a Backup Security Server

Use the following procedure to change the FQDN of a Backup Security Server.

1. Perform a Backup Security Server database backup, as described in *Linux Platform Base and Applications Installation and Commissioning, NN43001–315*.
2. Create an inventory list of all applications deployed on the Backup Security Server.
3. Perform a fresh Linux base install on the Backup Security Server, as described in *Linux Platform Base and Applications Installation and Commissioning, NN43001–315*.

Note:

If you change the domain name of the Primary Security Server during Linux base installation, you must make the same change to the Primary Security Server domain name during Linux base installation on the Backup Security Server.

4. Configure the Backup Security Server, as described in *Unified Communications Management Common Services Fundamentals, NN43001–116*.
5. Deploy the necessary applications on Backup Security Server, as described in *Linux Platform Base and Applications Installation and Commissioning, NN43001–315*. Use the Backup Security Server application inventory list that you created in Step 2 on page 296 to determine which applications to deploy.
6. Restore application data on the Backup Security Server, as described in *Linux Platform Base and Applications Installation and Commissioning, NN43001–315*.

Note:

When you perform the application data restoration, ensure that the **Restore data for deployed applications only** checkbox is selected.

Related links

Change the FQDN of a Primary or Backup Security Server on page 295

Appendix H: Passthrough end user license agreement

Index

A

adding
System Manager roles 154
AMS 7.6
changes 133
installation process diagram 135
Linux Base support 133
supported platforms 134
amspatch 148
amsupgrade tool
examples 147
syntax 147
Avaya MS
change IP address and hostname 156
configure default admin password 152
Content Store data replication 155
upgrading and migrating MAS 7.0 data 143
Avaya MS 7.6
accessing EM 149
certificate management 157
Deployment Manager 147
hyperlinks 149
license server 157
media port management 160
patching 148
Avaya MS and MAS 7.0
upgrade and data migration process flow 142
Avaya MS Element Manager
Role Based Access Control 151
using RBAC with System Manager 153
Avaya MS Element Manger
login options 151
Avaya MS EM
RBAC 151
using RBAC with System Manager 153
Avaya MS RBAC
enabling 152
Avaya MS upgrade
navigation 141

C

Changing compatibility view setting 44
compatibility mode 44
configure FQDN
hostconfig 154
Configuring the baud rate 252
Configuring the BIOS serial console 252
Connecting an HP DL360 G9 signaling server 252

D

downloading
System Manager Certificate Authority certificate 157

F

front panel 245
Front view of HP DL360 G9 Server 249

H

hostconfig
using 154
HP DL360 G9 server 248

I

importing
System Manager certificate authority certificate 159
System Manager-signed certificate for Avaya MS Element Manager 159
installing AMS 7.6
prerequisites 134
installing Avaya MS
using preexisting administration partition 138
installing Avaya MS 7.6
formatting existing administration partition 136
Internal view of HP DL360 G9 Server 251
Internet Explorer
compatibility view setting 44

M

MAS 7.0
data migration limitations 140
Migrating Avaya MS 7.0 data
CLI 146

P

prerequisites
Avaya MS 7.6 upgrade 141

R

rear panel 246
Rear view of HP DL360 G9 Server 249

S

server front view 245
server rear view 246
System Manager
    create certificate 158
System Manager Certificate Authority certificate
    download 157
System Manager roles
    add 154

T

turn off compatibility mode 44

U

upgrade
    load sharing clusters of Avaya MS 142
    simplex Avaya MS 142
upgrading Avaya MS 7.6 upgrade
    prerequisites 141