Upgrades Guide
Avaya Communication Server 1000

Release 7.6
NN43001-408
Issue 01.02
May 2013

Notice

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

Documentation disclaimer

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

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked 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 its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

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

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 currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products”. 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 (in the event the applicable Documentation permits installation on non-Avaya equipment) 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, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software that 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”). 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 Documentation or on Avaya’s website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Note to Service Provider

The Product may use Third Party Components that have Third Party Terms that do not allow hosting and may need to be independently licensed for such purpose.

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: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third

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

Avaya is a registered trademark of Avaya Inc.

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

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: New in this release

The following section details what is new in the *Upgrades Guide, NN43001–408* for Avaya Communication Server 1000 Release 7.6.

Features

This document contains information on the new Health Check (HC) Tool and Upgrade application. For information about the new features for this release, see *New in this Release, NN43001–115*. For a complete list of features, see the *Feature Listing Reference, NN43001–111*.

Other changes

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

Revision History

May 2013	Standard 01.02. This document is up-issued to include a link to the Product Compatibility Matrix in the Customer Service chapter.
March 2013	Standard 01.01. This is a new document to support Avaya Communication Server 1000 Release 7.6.

Conventions

Terminology

In this document, the following terms apply:

- On systems where System Manager 6.2 manages CS 1000, the term UCM in the documentation refers to UCM in System Manager. On systems where System Manager does not manage CS 1000, the term UCM in the documentation remains unchanged.
- On systems where System Manager 6.2 manages CS 1000, the term Subscriber Manager in the documentation refers to User Profile Management in System Manager; on systems where System Manager 6.1 manages CS 1000, the term Subscriber Manager refers to Subscriber Manager in System Manager. On systems where System Manager does not manage CS 1000, the term Subscriber Manager in the documentation remains unchanged.
- On systems where Session Manager is available, the term NRS in the documentation refers to Session Manager. On systems where Session Manager is not available, the term NRS in the documentation remains unchanged.

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

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

Product Compatibility Matrix

To review the most up-to-date product compatibility, go to www.avaya.com/support. From this Web site, locate the Product Compatibility Matrix under the **Tools** banner at the bottom of the page.

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 at the bottom of the page.

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: Health Check Tool

Introduction

The Health Check (HC) tool provides status information, including a health rating score, for the different elements of the Communication Server 1000 (CS 1000) system. This information can be used to guide service personnel to the areas of the system that require maintenance or further diagnostics.

Health Check is a PC-based GUI application configured by the user to identify the functionality and network address of the components to be monitored. Once configured, Health Check connects to CS 1000 components including the Call Server, Signaling Server, Media Gateway Controller and Media Cards, through an SSH port through the ELAN connection of each component.

The Health Check application logs into the required shells of the defined components (SL1, pdt, debug, su, bash) with the user IDs and passwords provided by the user during configuration. Upon connection, and based on the functionality of the component, the application issues a set of commands and status requests, and records the results. A pre-defined set of commands is used so that the information gathered is interpreted and handled in a controlled way.

Once the testing of each component is complete, an HTML report providing an executive level summary of the components is generated. The summary report contains links to other HTML report files that present a more comprehensive view of the details down to the component level. In addition, certain CS 1000 log files can be scanned for the existence of specific information, and reported on if found. Another test includes the verification of the presence of certain critical system files.

As the components and files are reviewed by the HC tool, any deviation from what is expected is counted. As each component test suite is completed, an accumulated count or score is assigned to the component. A score of 0 is an indication that nothing unexpected was detected. The higher the score, the more likely that issues exist that require attention. Reviewing the HC report, the craftsperson can assess the details and results of the tests conducted to formulate plans for any corrective measures required.

If any issues occur, check all tool options to gather information prior to contacting Avaya Support.

Installing the Health Check Tool

The Health Check tool must be installed on a Windows XP or Windows 7–based PC with network connectivity to the ELAN of the CS 1000 system components to be monitored. The host PC must also have the latest version of Java Runtime Environment installed. Java Runtime Environment is a free application that can be downloaded from www.java.com.

The Health Check Tool software is available for download from the Avaya Support website: http://support.avaya.com.

Installation Procedures:

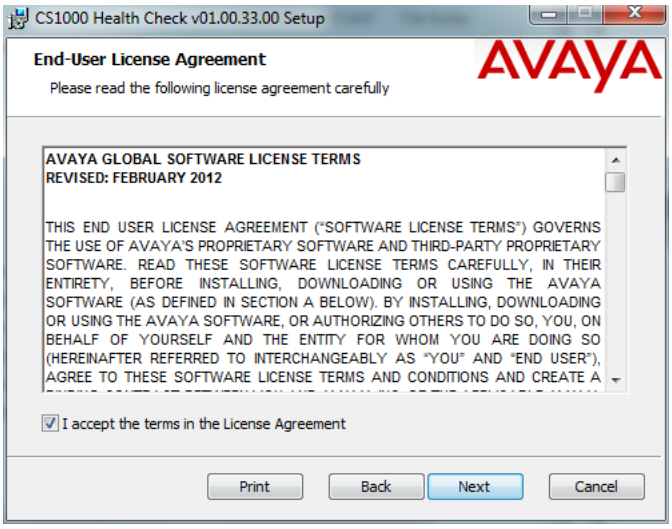
1. Ensure the latest Java Runtime Environment is installed on the host PC. If not, install the latest version.
2. Download the HealthCheck.msi installer to the host PC.

   The Health Check Tool software is available for download from the Avaya Support website: http://support.avaya.com.
3. Double-click the HealthCheck.msi file from the download location on the host PC.

   The **Health Check Setup Wizard** is launched, as shown.

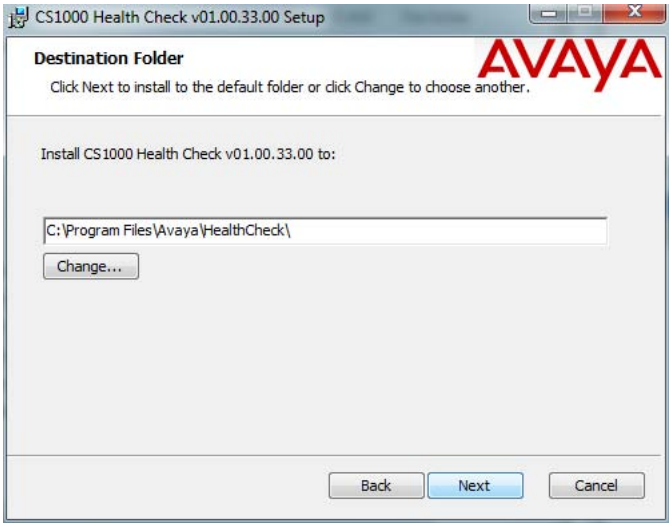
4. Click the **Next** button to continue with the installation.

   The **End-User License Agreement** screen appears.



5. Place a check in the box to accept the terms of the License Agreement and click the **Next** button to continue with the installation.

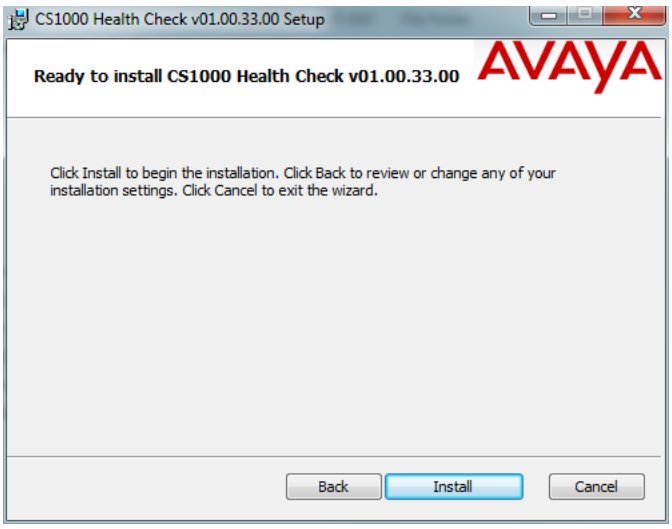
   The **Destination Folder** screen appears, as shown.



6. Click **Next** to accept the default folder location.

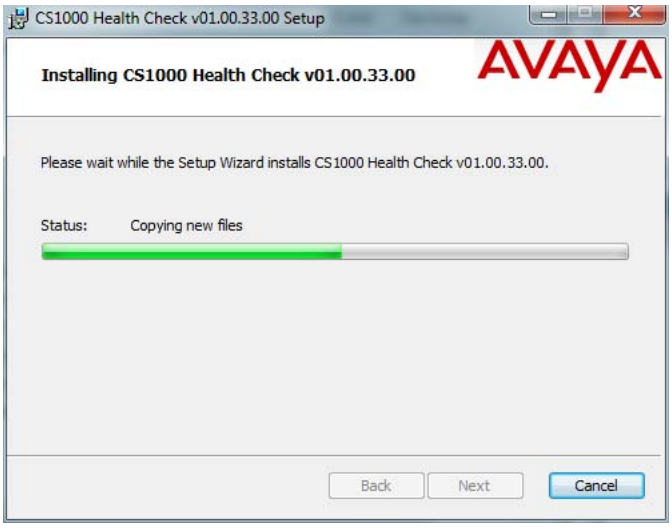
   Note:
   Avaya recommends that you do not change the default folder location.

   The **Ready to install** screen appears, as shown.

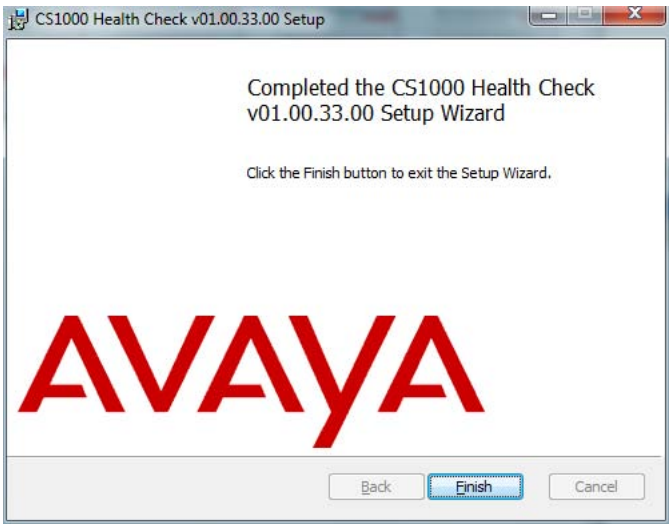


7. Click **Install** to begin the software installation.

   The **Installation Status** screen appears, as shown.



   The **Setup Completed** screen appears, as shown.



8. Click the **Finish** button to exit the Setup Wizard.

When the installation is completed, the Avaya Health Check tool icon appears on the host PC desktop. Now that the Health Check Tool is installed, it must be configured with the basic information that allows the application to contact the various system elements to retrieve data. Basic configuration information includes the component IP address and login credentials (user IDs and passwords).

Using the Health Check Tool

Accessing the Health Check Tool:

Once, installed, the Health Check Tool can either be accessed directly from the user's PC or through a Remote Desktop session using **LogMeIn**

Device Access:

The Health Check Tool is capable of communicating with one device, with several devices within a CS 1000 system, or with a set of multiple CS 1000 systems. It communicates directly from the host PC to each device that can be reached directly through the network. Each individual device is configured to be connected directly or through a proxy device to the host PC.

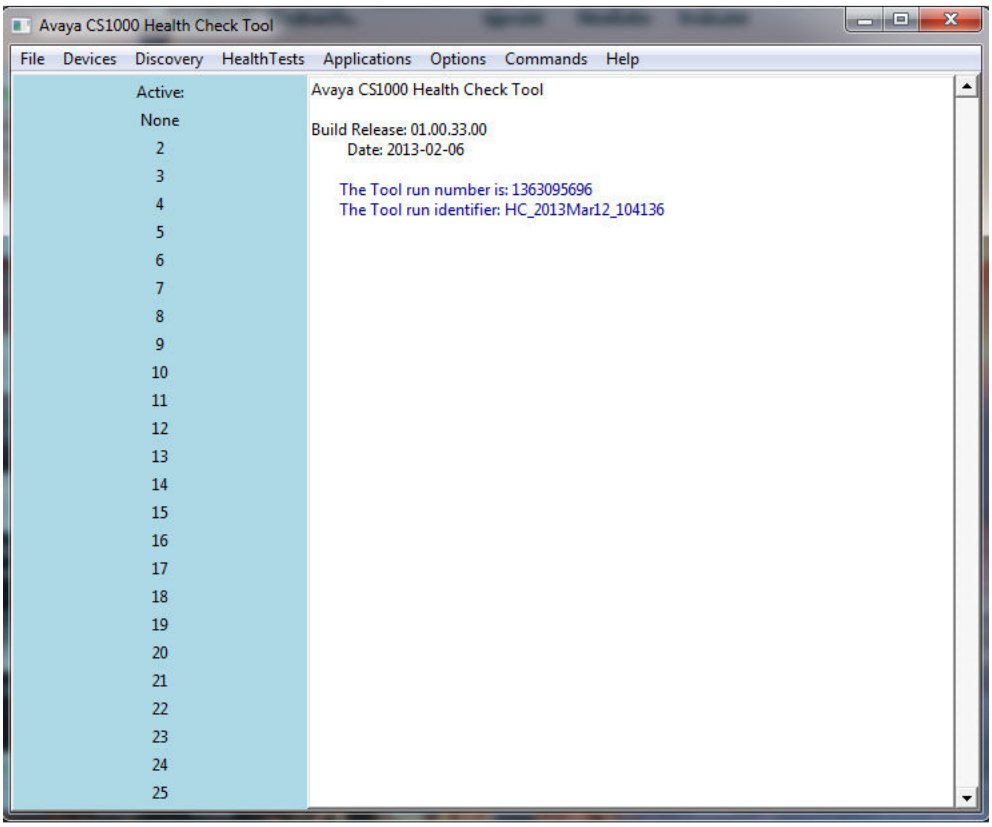
If the Health Check fails to obtain a valid and sustained SSH connection to a device, or fails to log in with the credentials provided, it indicates that errors to proceed were encountered. All such issues must be resolved in order to continue using the Health Check Tool.

Note:

Networks with unstable or slow connections (such as long ping delays) can cause errors with the Health Check Tool.

GUI Interface:

The GUI is used to configure, select, and execute Health Check testing . When Health Check is launched, the GUI opens to the main screen, as shown.



- The **Build Release** is the version number of the Health Check Tool and the date the version was issued.
- The **Tool run number** is a timestamp that is used to uniquely identify all of the files that are about to be generated by the Health Check Tool.
- The **Tool run identifier** is a unique name assigned to the generated files making them easy to find in the log files.

Menu Bar:

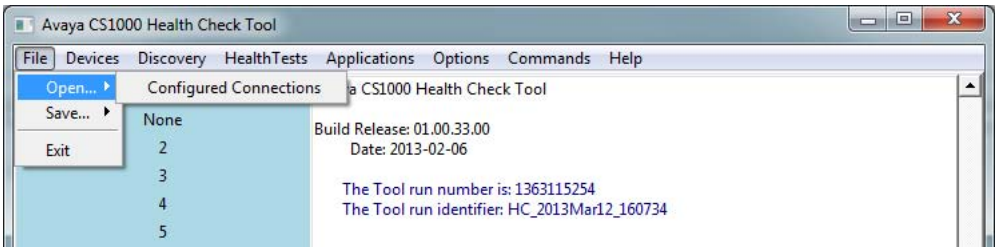
The Health Check GUI menu bar includes the following selections:

- File
- Devices
- Discovery
- HealthTests
- Applications
- Options

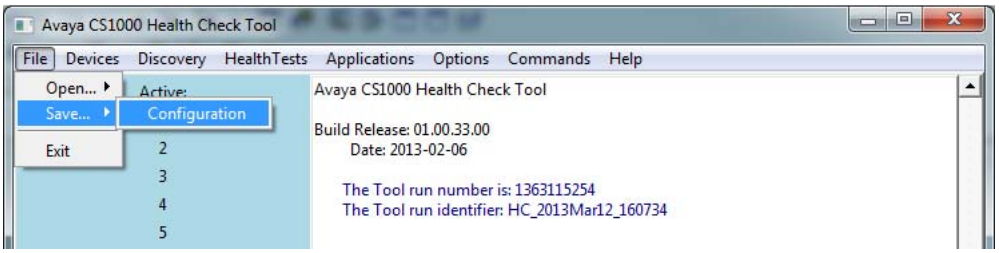
- Commands
- Help

The **File** menu includes:

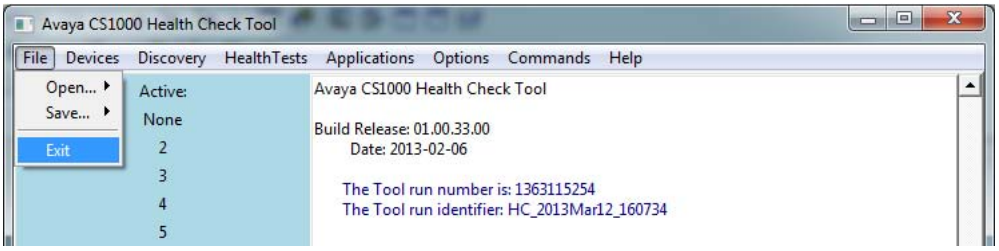
- **Open** — used to open Configured Connections.



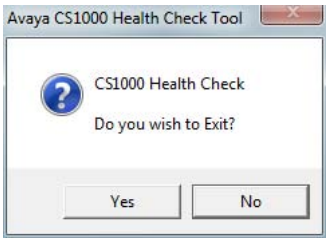
- **Save** — used to save the Configuration file that is currently open.



- **Exit** — used to properly close the Health Check Tool.

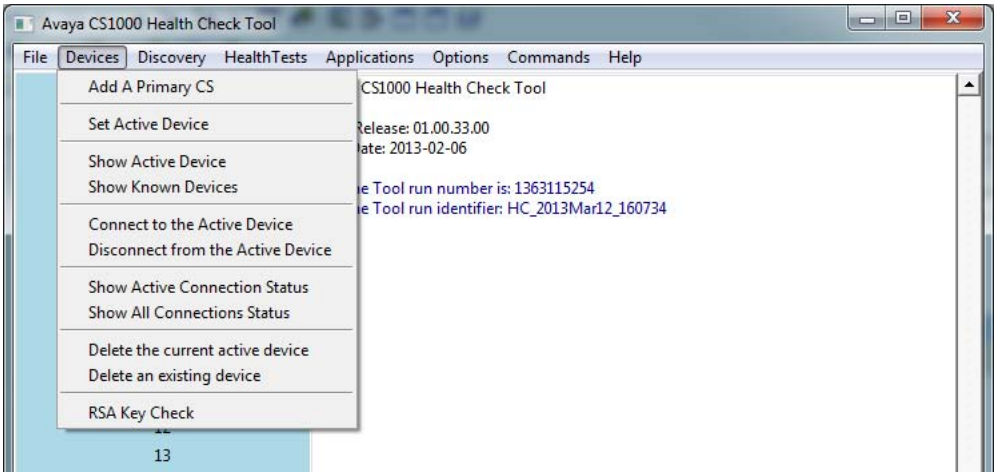


- Click **YES** to confirm that you want to exit the Health Check Tool.



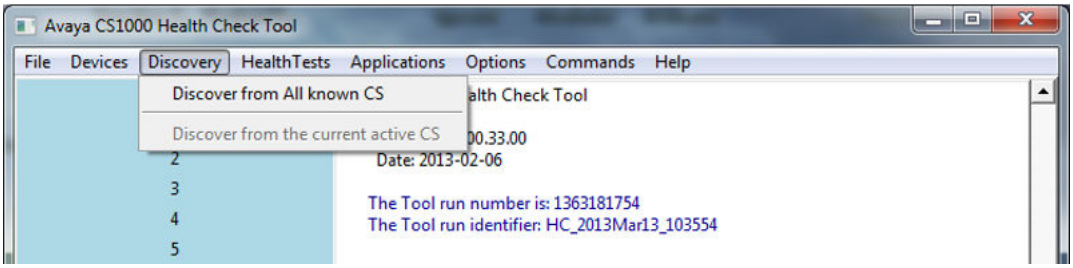
The **Devices** menu includes:

- **Add A Primary CS** — used to configure the Primary Call Servers (CS) to be monitored by the Health Check Tool.
- **Set Active Device** — used to select the device you want to designate as active to the Health Check Tool.
- **Show Active Devices** — used to display the list of devices that are currently active.
- **Show Known Devices** — used to display the list of devices that are known by the Health Check Tool.
- **Connect to the Active Device** — used to instruct the Health Check Tool to make a connection to the active device.
- **Disconnect from the Active Device** — used to instruct the Health Check Tool to disconnect from the active device.
- **Show Active Connection Status** — used to display the connection status of the active device.
- **Show All Connections Status** — used to display the connection status of devices that are known by the Health Check Tool.
- **Delete the current active device** — used to delete a currently active device that no longer needs to be monitored by the Health Check Tool.
- **Delete an existing device** — used to delete an existing device that no longer needs to be monitored by the Health Check Tool.
- **RSA Key Check** — used to check if the RSA key of a device is cached to the Host PC.



The **Discovery** menu includes:

- **Discover from All known CS** – instructs the Health Check Tool to query all known Call Servers for the purpose of determining what components are known by those Call Servers.
- **Discover from the current active CS** – instructs the Health Check Tool to query the current active Call Server for the purpose of identifying the components connected to the active Call Server.



Note:

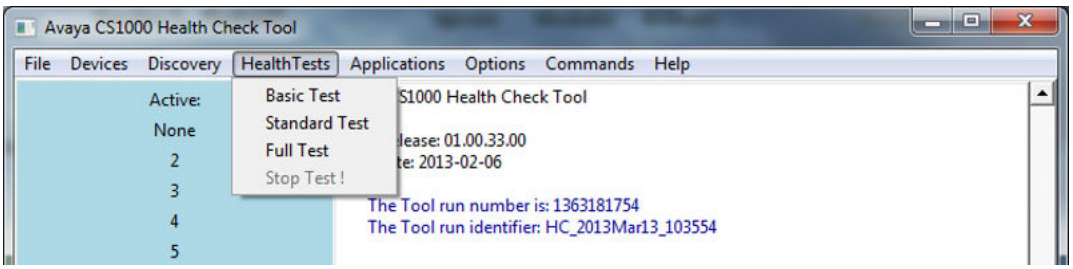
Call Servers must be configured before automatic discovery can occur.

Components identified during automatic discovery can include:

- Call Servers
- Signaling Servers
- Media Gateway Controllers (MGC, MGX and MGS)
- Media Cards (MC32, MC32S)

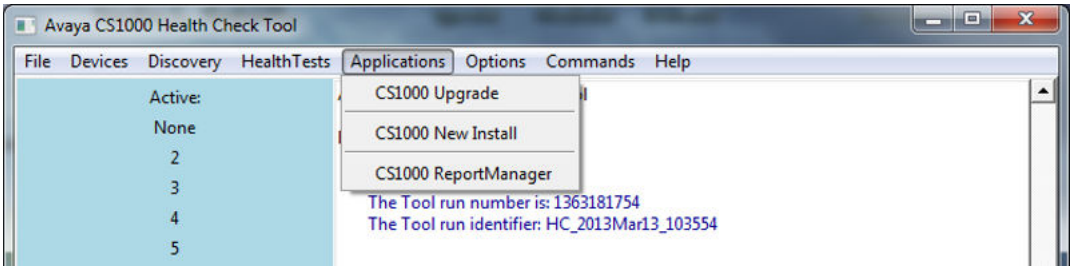
The **HealthTests** menu includes:

- **Basic Test** — used to instruct the Health Check Tool to run the Basic test, which executes the smallest set of commands to determine a health count for the currently active devices.
- **Standard Test** — used to instruct the Health Check Tool to run the Standard test, which executes all of the commands from the Basic Test, plus additional commands to determine a health count for the currently active devices.
- **Full Test** — used to instruct the Health Check Tool to run the Full test, which executes the full suite of commands (all from Basic and Standard, plus additional commands) to determine a health count for the currently active devices.
- **Stop Test !** — used to instruct the Health Check Tool to stop the test that is currently running.



The Applications menu includes:

- **CS1000 Upgrade** — facilitates the upgrade process.
- **CS1000 New Install** — facilitates the new installation process.
- **CS1000 ReportManager** — pulls the complete set of test results together into a single consistent HTML report and stores it on the host PC. You can view the stored reports through your PC browser.

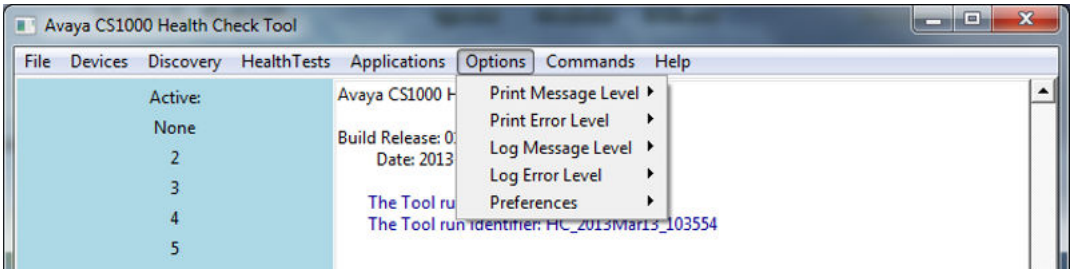


Note:

For more information on the Upgrade and New Install applications, refer to the Upgrade application Introduction on page 37.

The **Options** menu includes:

- **Print Message Level** — used to set the detail level for the informational messages that are shown in the user command window. The range is from 0 – 9, with 9 providing the highest level of detail and 0 providing the lowest level of detail.
- **Print Error Level** — used to set the detail level for the error messages that are shown in the user command window. The range is from 0 – 5, with 5 providing the highest level of detail and 0 providing the lowest level of detail.
- **Log Message Level** — used to set the detail level provided for the informational messages that are logged. The range is from 0 – 5, with 5 providing the highest level of detail and 0 providing the lowest level of detail.
- **Log Error Level** — used to set the detail level provided for the error messages that are logged. The range is from 0 – 5, with 5 providing the highest level of detail and 0 providing the lowest level of detail.
- **Preferences** — used to change or view the file path roots for files created by the Health Check Tool.

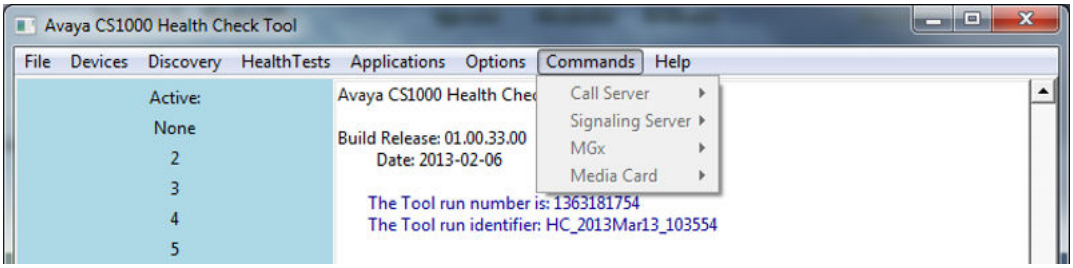


Note:

Avaya recommends that all of the file types generated by the Health Check Tool be stored in the default base directory created by the tool during installation: *C:/myReports*. If the File Path Root location is changed, be sure to store all types of files in the same directory.

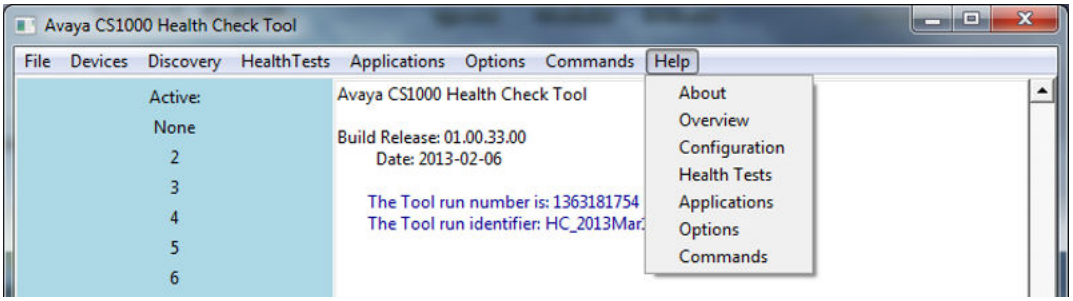
The **Commands** menu is used to issue commands to the following types of devices:

- Call Server
- Signaling Server
- MGx
- Media Card



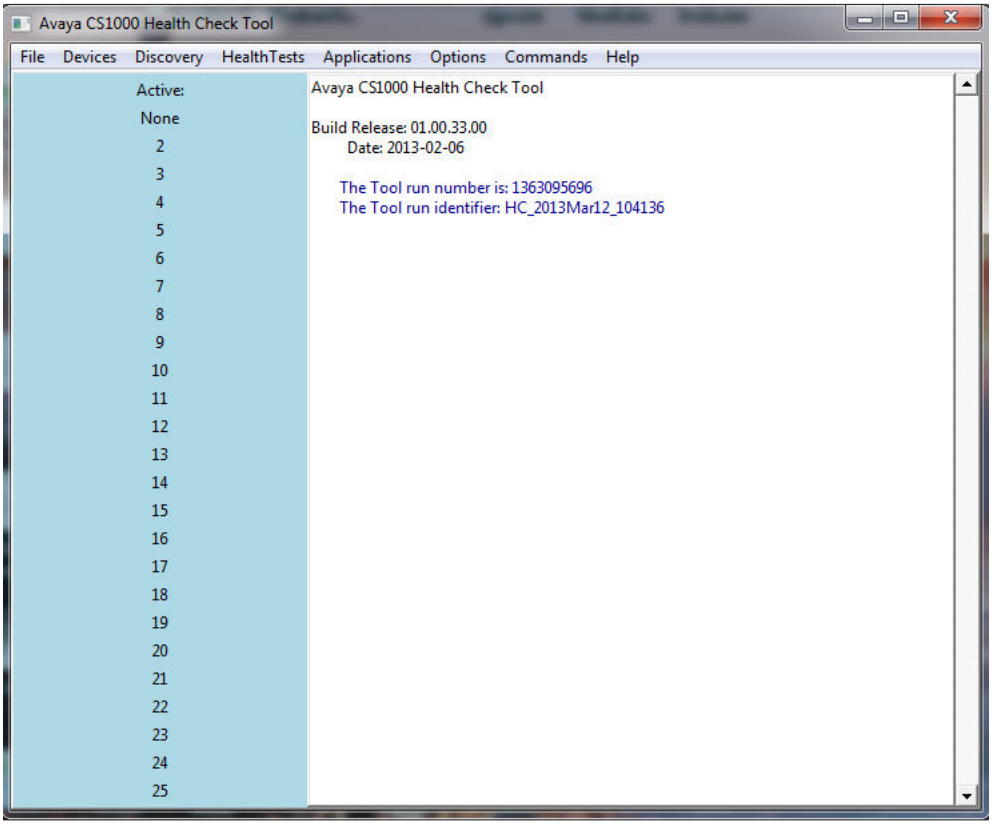
The **Help** menu includes:

- **About** — displays the build level and date of the Health Check Tool application.
- **Overview** — displays general help information.
- **Configuration** — displays configuration help information.
- **Health Tests** — displays health test help information.
- **Applications** — displays applications help information.
- **Options** — displays options help information.
- **Commands** — displays commands help information.



Configuring the Health Check Tool

When you launch Health Check tool, the main screen appears:



To get started, you must configure the information the Health Check tool needs in order to connect to your system and retrieve system health information. This information is either held in a configuration file or must be created.

Note:

In High Availability mode, the Health Check Tool only communicates with the active IP of the Call Server. To add a primary Call Server, add the IP address of the active Call Server and then discover the other Call Server as an associated device. In split mode, the Health Check Tool can communicate with both Call Server IPs. You can add a primary Call Server using the active Call Server IP, then discover Call Servers for associated devices, and add the primary Call Server using the inactive Call Server IP without needing to discover Call Servers.

Loading an existing configuration

If you have used Health Check previously, you may have saved a configuration file to disk. The configuration file is in text (.txt) or XML (.xml) format.

To open an existing configuration file, select: **File > Open > Configured Connections**.

The **Choose file** dialog box opens to the last location where you saved a file or the default recommended file location if the previous file location is no longer available (such as a flash drive that is no longer disconnected). After you have selected and opened a saved configuration file, the devices within the file are loaded into the application.

Creating a new configuration

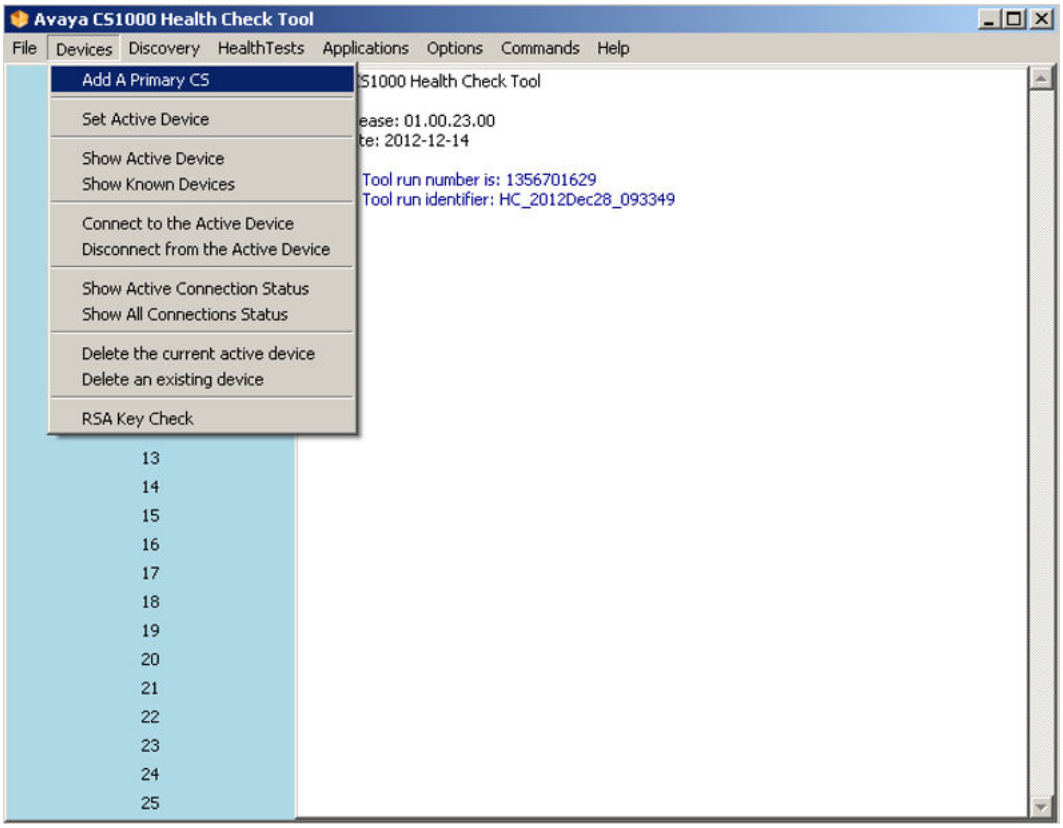
To configure a new Health Check tool configuration, complete the following steps:

- Adding a new primary Call Server.
- Requesting Health Check to discover other devices known to this Call Server.
- Saving the configuration to an XML file.

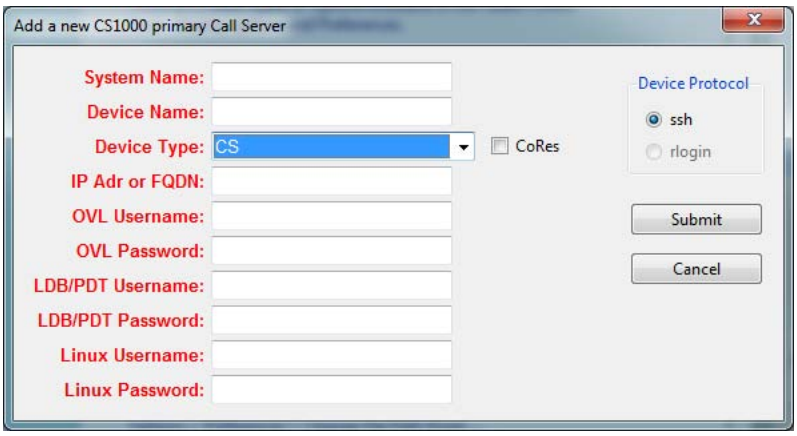
The following sections describe these steps in more detail.

Adding a new primary Call Server:

- From the **Devices** menu, select **Add a Primary CS**, as shown.



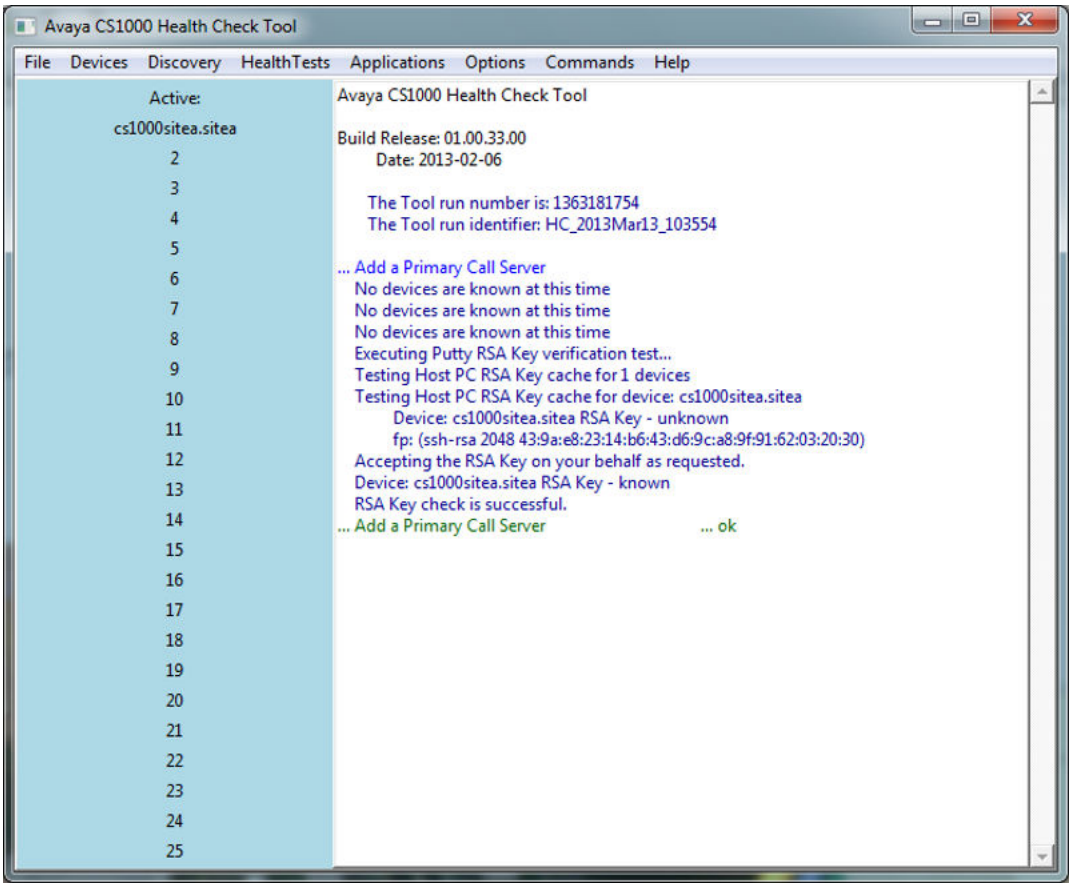
The **Add a new CS1000 primary Call Server** screen appears, as shown.



Enter the required information into the fields. If the system is a Co-Resident Call Server and Signaling Server, place a check in the CoRes box.

- **Linux Username** - enter the second level username (admin2).
- **Linux Password** – enter the second level password associated with the CS 1000 Linux Base Username (admin2).

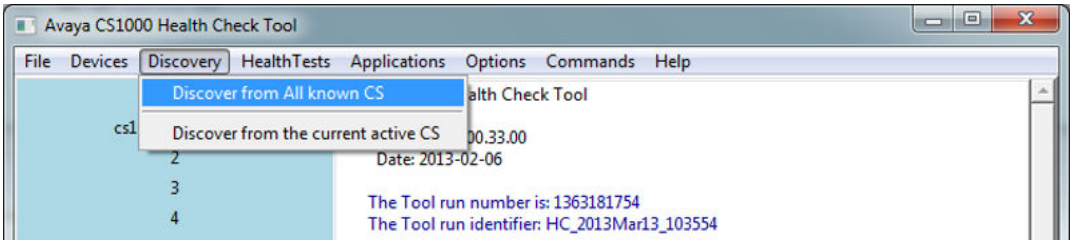
Once you have submitted the primary call server configuration, the main window should update indicating that the primary Call Server has been added and is now the active device, as shown.



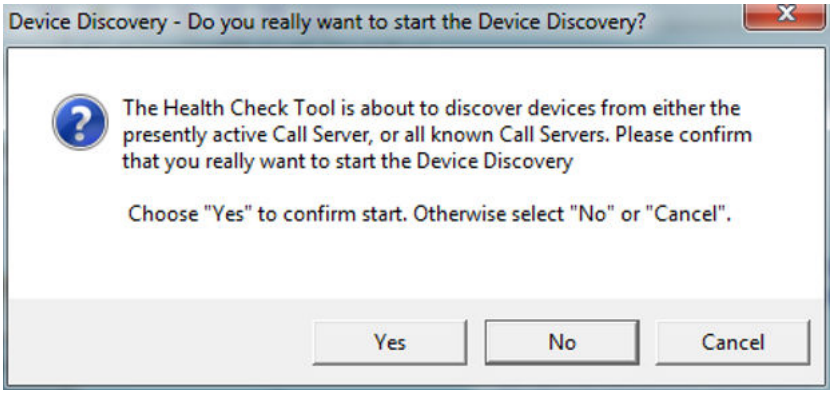
Requesting Health Check to discover known devices:

If the primary Call Server was added successfully, and the device is designated as the active device, you can begin the automatic **Discovery** process.

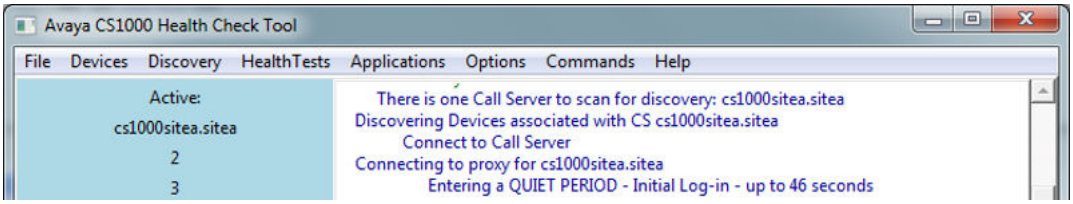
- From the **Discovery** menu, select **Discover from all known CS**, as shown.



- When prompted, click **Yes** to allow the Health Check Tool to discover devices from the Call Server, as shown.



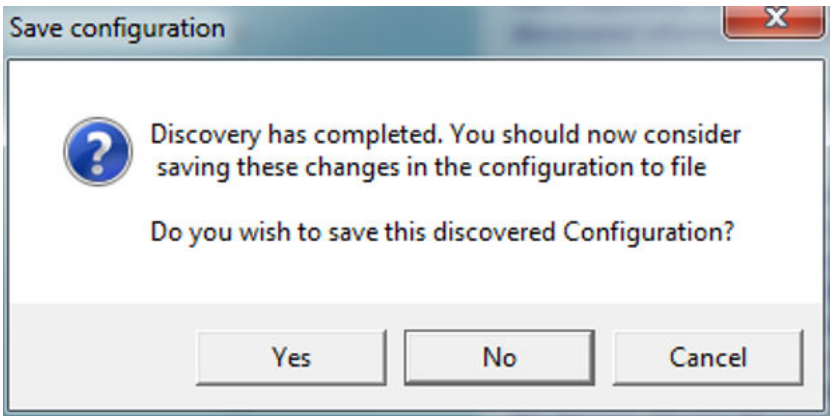
The main window updates indicating that it is discovering devices associated with the primary Call Server, as shown.



During the discovery process, the Health Check tool assigns names to each of the devices starting with the System Name.

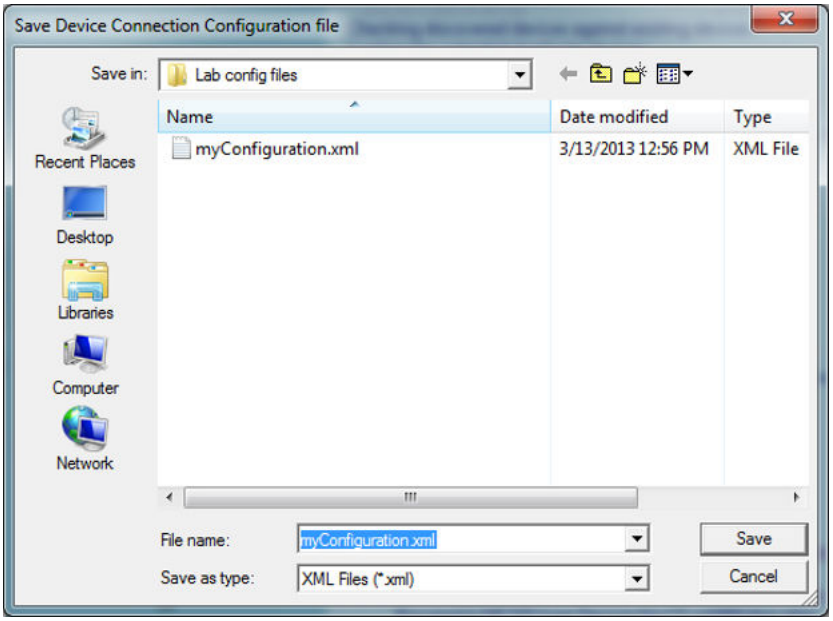
Saving the configuration file:

When automatic Discovery is complete, a dialog box appears asking you to save the discovered Configuration. This saves the configuration file that includes the primary Call Server and all of the discovered devices.



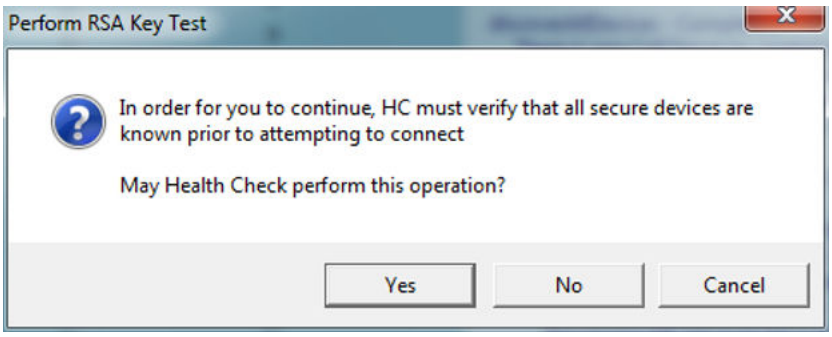
- Click **Yes** to save the configuration file containing the primary Call Server and the discovered devices.

The **Save Device Connection Configuration file** dialog box appears, as shown.



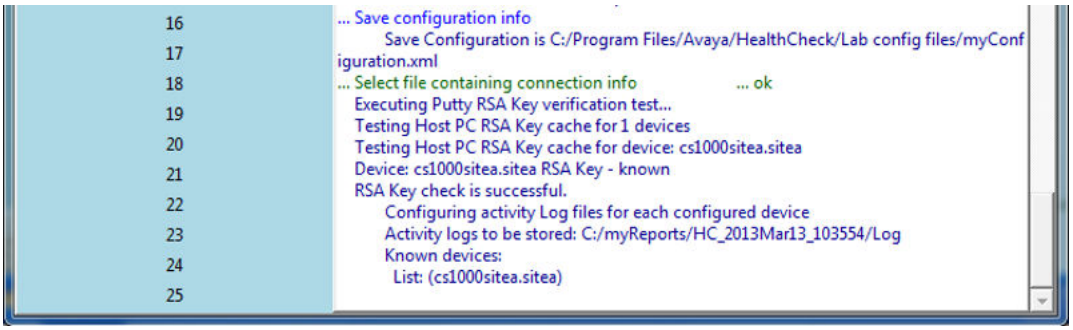
- Enter a descriptive name for the configuration file and click **Save**.

The **Perform RSA Key Test** dialog box appears, as shown. This check is performed to verify that the RSA key for this device is cached to the Host PC.

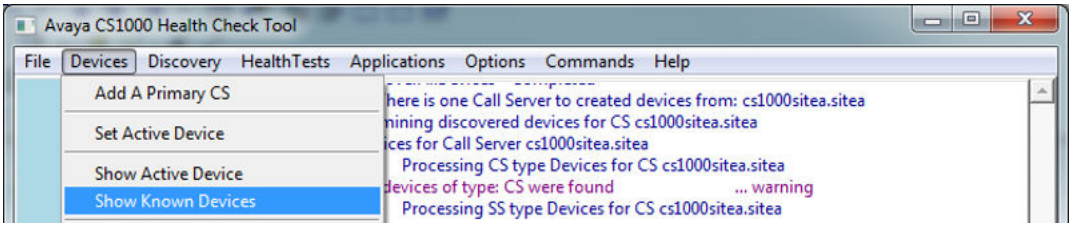


- Click **Yes** to permit the Health Check Tool to verify all devices are known before attempting to connect.

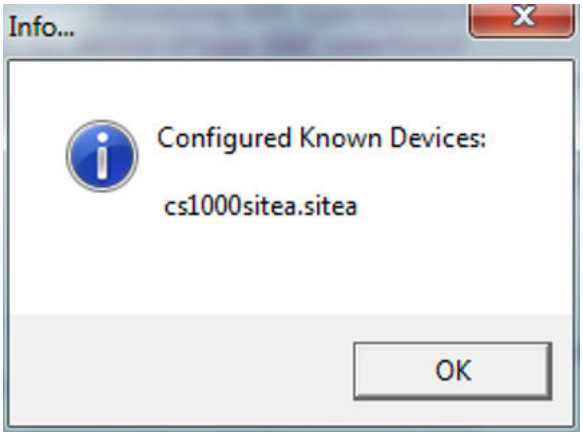
The main window updates, indicating that the RSA check was successful, as shown.



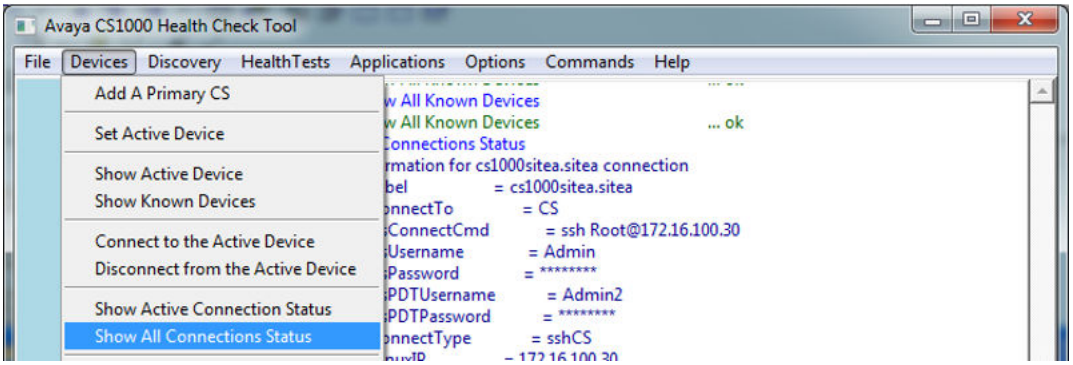
From the **Devices** menu, select **Show Known Devices**, as shown.



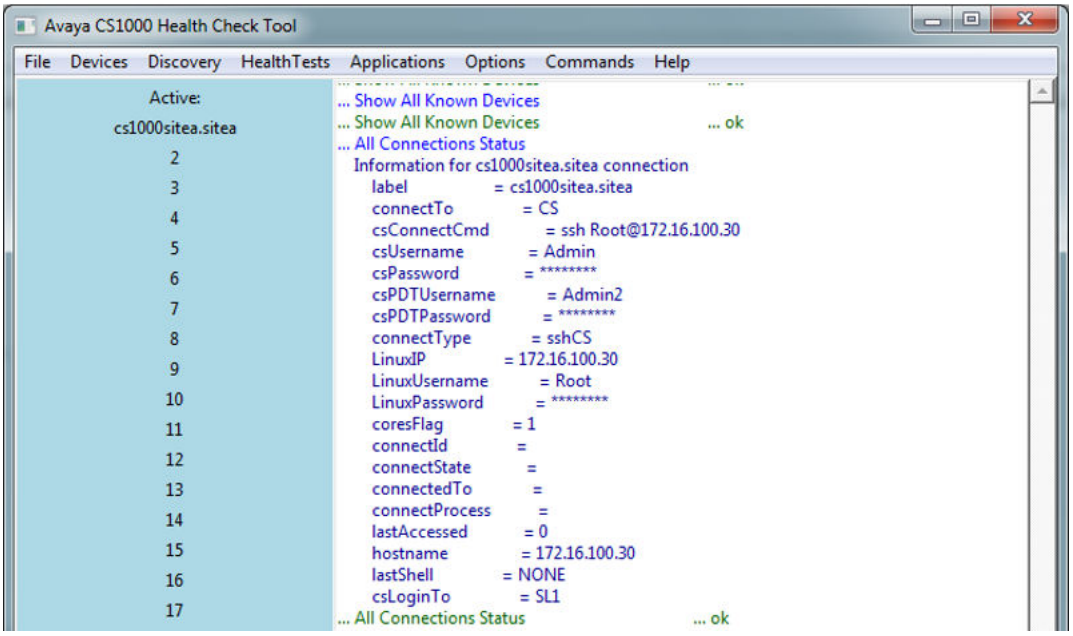
Verify that the system components appear as configured known devices, as shown.



From the **Devices** menu, select **Show All Connections Status**, as shown.



Verify that the connection status of all of the known devices is **ok**,as shown.



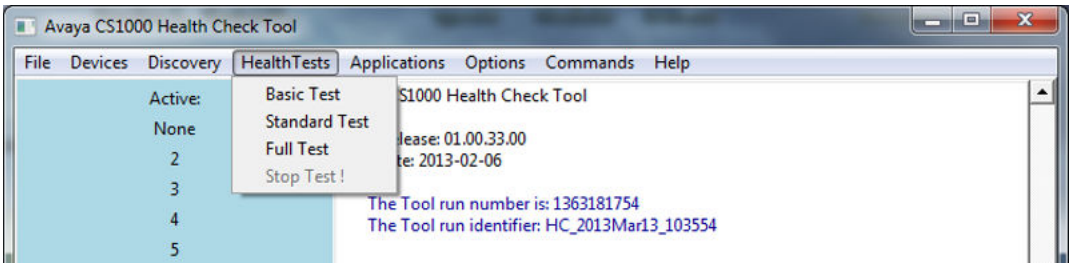
The Health Check tool is now configured and ready to use to check the health of the system.

Running a Health Check

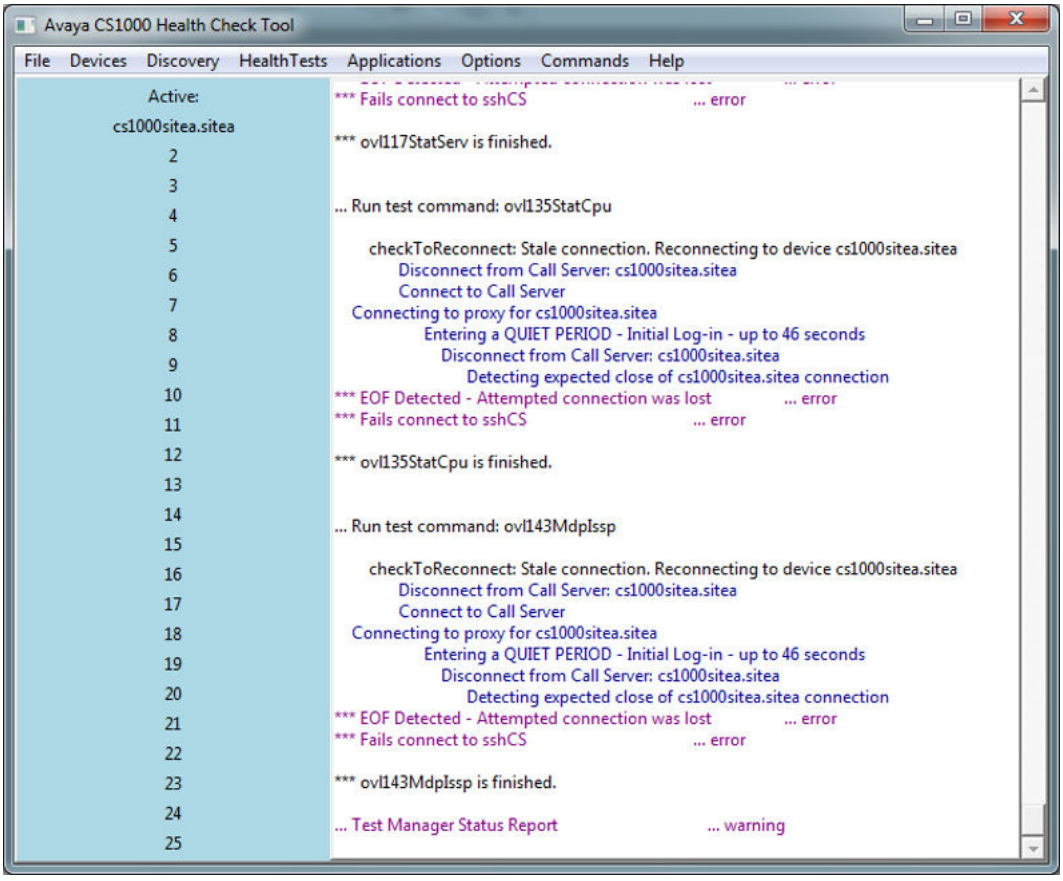
The Test Manager component of the Health Check tool keeps track of the pre-defined testing selected through the GUI for each of the supported devices. It issues the commands to each device and allows the collection of the information from each device that is stored in a results file. It provides header information containing test run statistics such as time, date, and run sequence, for each test on each device. This information collected is used by the Report Manager to generate results reports.

The **Test Manager** is accessed from the **HealthTests** menu, as shown. There are three types of tests you can run:

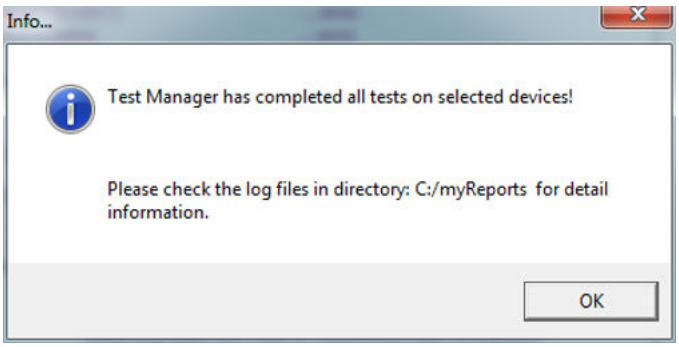
- Basic Test — executes the smallest set of commands to determine a health count for the currently active devices.
- Standard Test — executes all the commands from the Basic Test, plus additional commands to determine a health count for the currently active devices.
- Full Test—executes the full suite of commands (all from Basic and Standard, plus additional commands) to determine a health count for the currently active devices.



The Health Check main window shows the progress of the Test.



When the test is complete, a dialog box opens indicating that Test Manager has completed all the tests on the selected devices, as shown.



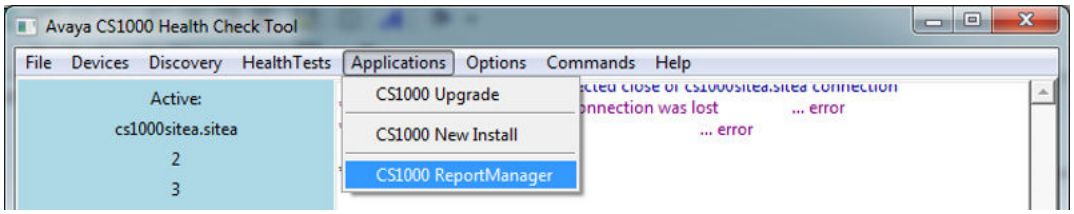
- Click **OK** to close the dialog box.

Now that the testing is complete, you can use the Report application to view the test results.

Health Check Report Manager

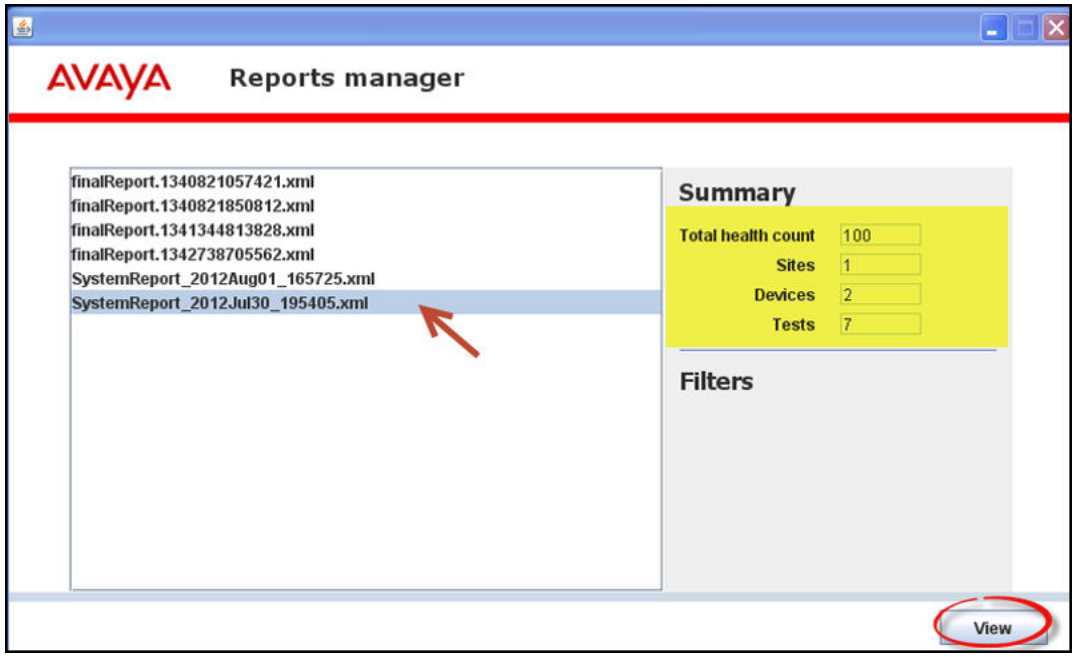
The Health Check Report Manager compiles the completed set of test results, collected by the Test Manager, together into a single consistent HTML report and stores it on the host PC. You can view the stored reports through the PC browser using the Report Manager application.

- From the **Applications** menu, select **CS1000 ReportManager**, as shown.

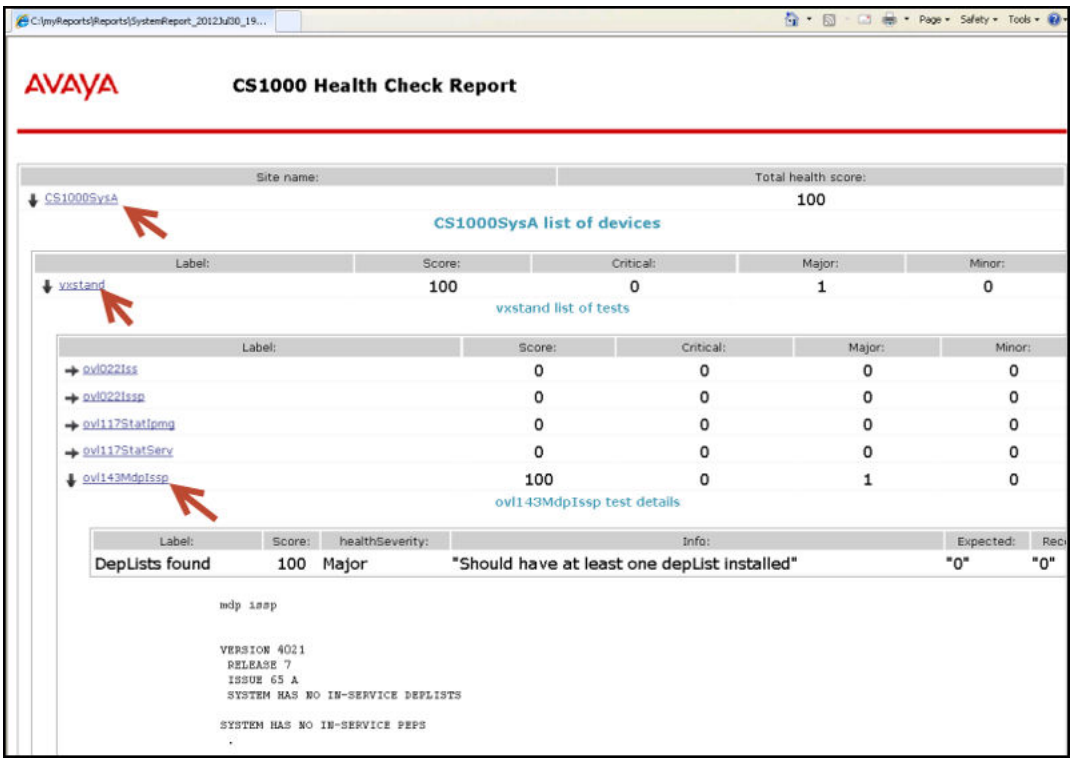


The **CS 1000 Report Manager** screen appears, as shown.

- Select the report to be viewed from the available list, as shown and click **View**.



The report is displayed in a browser window, as shown.



- Click the hyperlink for the system to expand the report to show the Call Server.
- Click the hyperlink for the Call Server to expand the report to show individual components.
- Click the hyperlink for each component to show test results to the component level.

Health Check component summary

The following table provides a brief description of each component supporting the Health Check Tool.

Table 1: Health Check components

Component	Description
Test Manager	The Test Manager keeps track of the pre-defined testing for each of the supported devices that you selected through the GUI . It issues the commands to each device and allows the collection of the information from each device that is stored in a results file. It provides header information containing test run statistics such as time, date, and run sequence, for each test on each device. This information is used by the Report Manager to generate results reports.

Component	Description
File Manager	The File Manager ensures that all devices have a file open to record the test results from each device. It also verifies that the file is in the correct state (open when active and flushed to file when not active). Other mechanisms are also in place to ensure the files are properly controlled.
Execution Manager	The Execution Manager fundamentally ties all of the managers together so that Health Check functions run smoothly.
Report Generation Manager	The Report Manager pulls the complete set of test results together into a single consistent HTML report and stores it on the host PC. You can view the stored reports through the PC browser.
Log Manager	The Log Manager keeps track of the log file destination locations on the Host PC. It is used when log files from the devices are transferred over to the Host PC.
Configuration Manager	The Configuration Manager keeps track of the incoming configuration data for each device in which Health Check makes a connection. It verifies that all necessary data for each connection is present in the device configuration file. Once loaded, the Connection Manager keeps track of each configured device so the other components within Health Check can readily obtain required information such as device type or IP address.
Connection Manager	The Connection Manager keeps track of the configured devices (from Configuration Manager) and which of the configured devices is the **Active** device. When Health Check reads a configuration file from a device, it designates the device as **Active**. You can also set the status of a device to Active by issuing the command **setDevicedevicename**. The device referenced can be any properly-configured device available when the command is issued. The command can only be issued to devices successfully configured through the Configuration Manager. To display the list of all known devices, enter the command **showDevices**. The first device in the displayed list is the Active device. Commands issued without referencing a device are issued against the Active device. The Connection Manager determines if a connection to a device is established and initiates the connection if it is not already established.
Connection Control	Connection Control ensures that the correct parameters are collected and distributed to the connecting applications used by Health Check in order to provide connectivity to the configured devices. Connection control uses the publicly-available PLINK.EXE application to provide session connections from Health Check to the various devices. This application supports the SSH protocol used by the Health Check tool. Health Check also uses the publicly-available PuTTY application PSCP.EXE for SFTP. Both PLINK.EXE and PSCP.EXE are included in the self-extracting Health Check application.

Supported CS 1000 Components

The following list of core components, if supported by CS 1000 Release 7.6, are also supported by the Health Check tool:

- All Call Servers types
- All Signaling Servers types
- MGC
- MGX
- MC32, MC32S
- UCM
- Linux Base Operating System

Call Server Commands:

The CS 1000 Call server OVL and PDT shells are used to extract the information required by the Health Check tool. Some commands are used to obtain a summary of the system configuration, while others are used to collect the information used to formulate the health rating.

Chapter 4: New Installation and Upgrade Applications

Introduction

The New Installation and Upgrade applications, components of the Health Check Tool, are introduced to provide guidance through the major steps of the new installation and upgrade processes. The Health Check tool is a PC-based GUI application available for download from the Avaya Support portal as a self-extracting file. The application does not change the installation or upgrade programs of the various system elements. It simply guides you through the process by identifying required tasks and recommending best practices, such as capturing critical pre-upgrade information.

The actual installation/upgrade tasks are performed manually under the direction of the New Installation and Upgrade applications. The flow followed by the tool matches the best practices already contained in the Installation and Upgrades documentation. The application divides required tasks into sections that provide an estimated time for completion and references to proper documentation and/or a best practices checklist. The tool also automates a number of the pre-upgrade/installation steps, which decreases the time spent to complete the tasks.

The New Installation and Upgrade applications are launched through the Health Check Tool and they use the tools functionality to establish communications with the CS 1000 components.

New Installation Application procedure

The Avaya Health Check Tool must be installed on a Windows-based PC in order to access the New Installation Application.

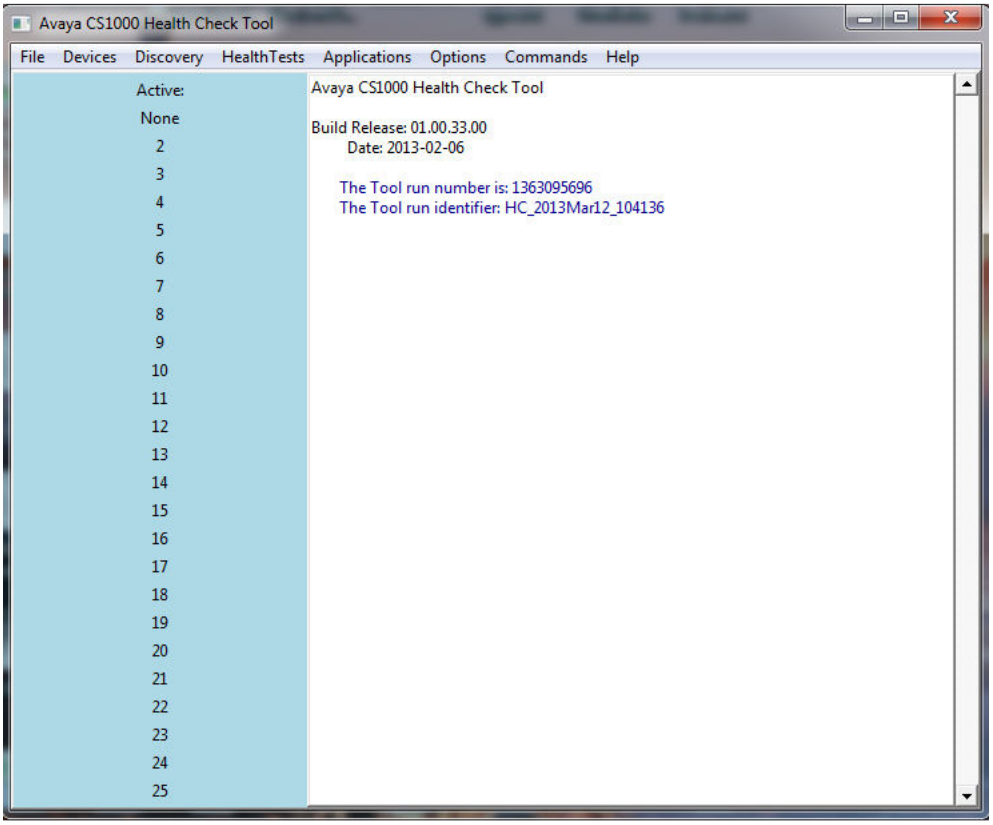
Note:

For detailed information on installing the Health Check Tool, see Installing the Health Check Tool on page 12

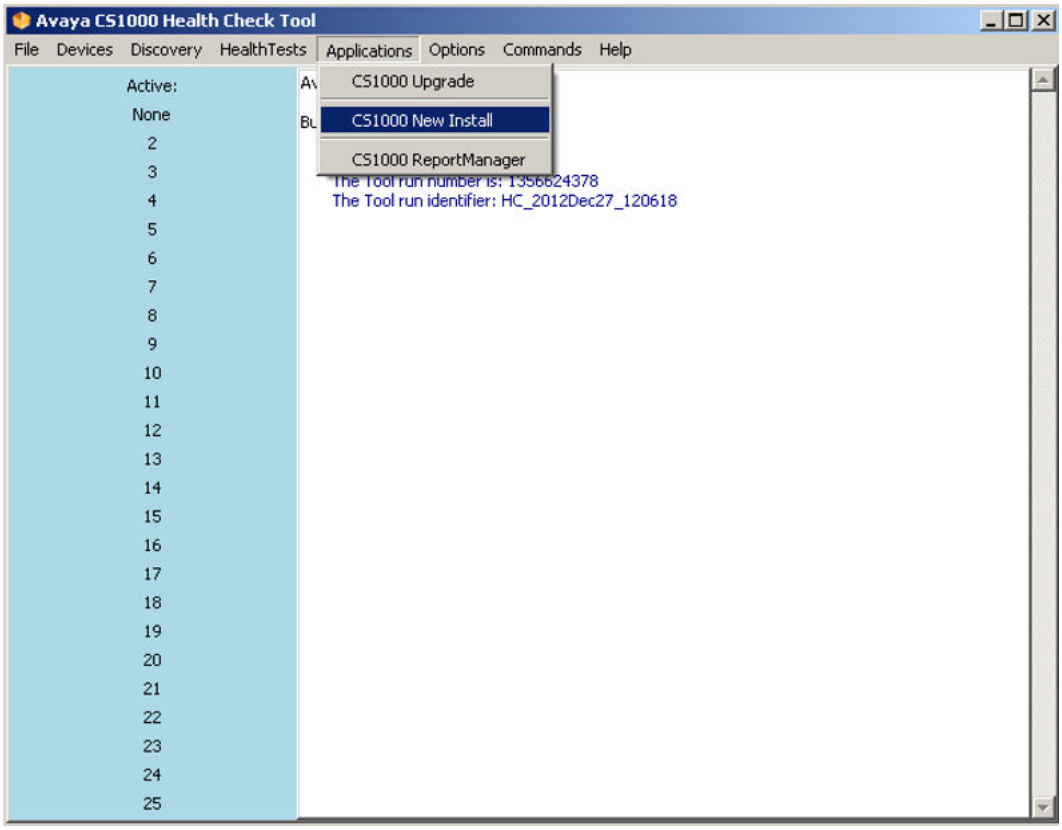
Running the New Installation Application:

For a new installation, perform the following steps.

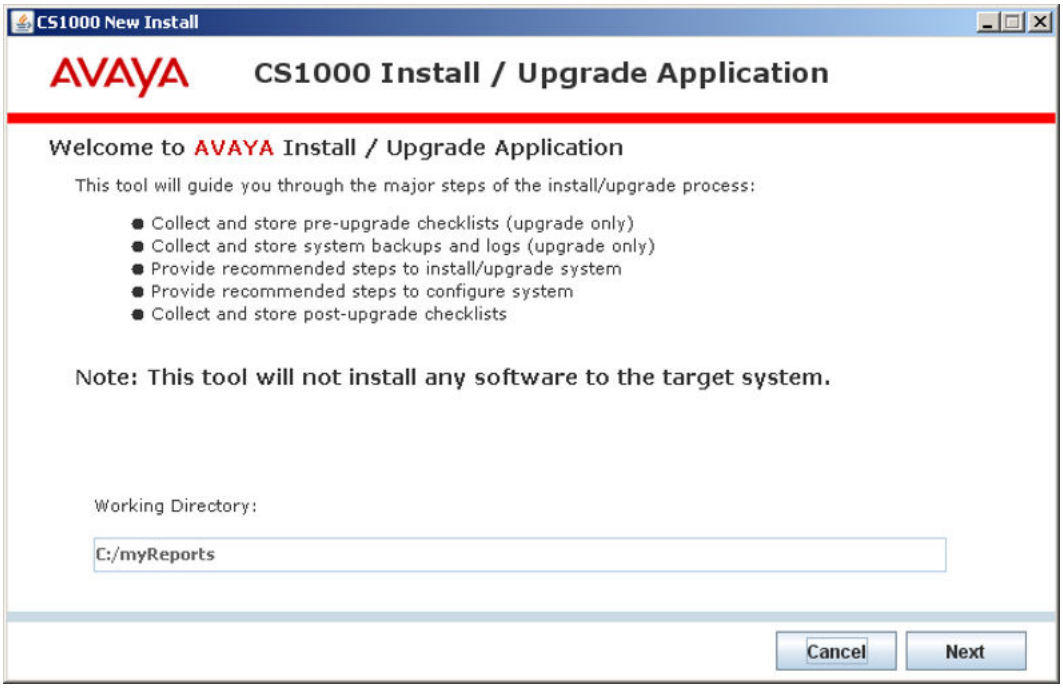
1. Launch the Health Check Tool. The Health Check Application screen appears, as shown.



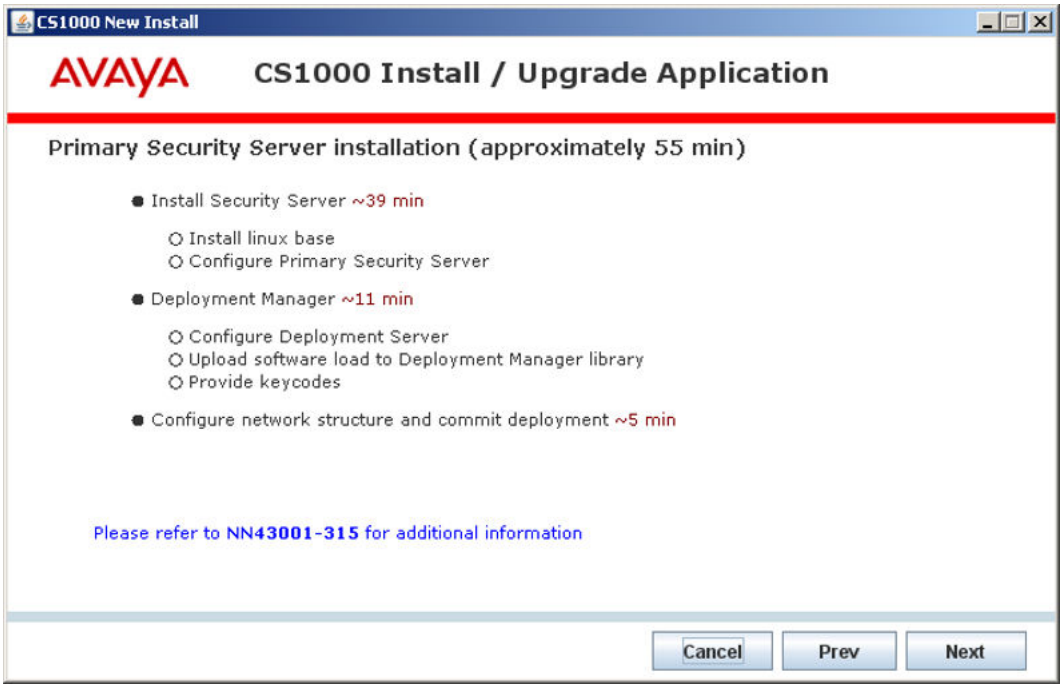
2. From the **Applications** menu, select **CS1000 New Install**, as shown.



3. The **Avaya CS 1000 Install/Upgrade Application Welcome** screen appears, as shown. Click **Next** to proceed.



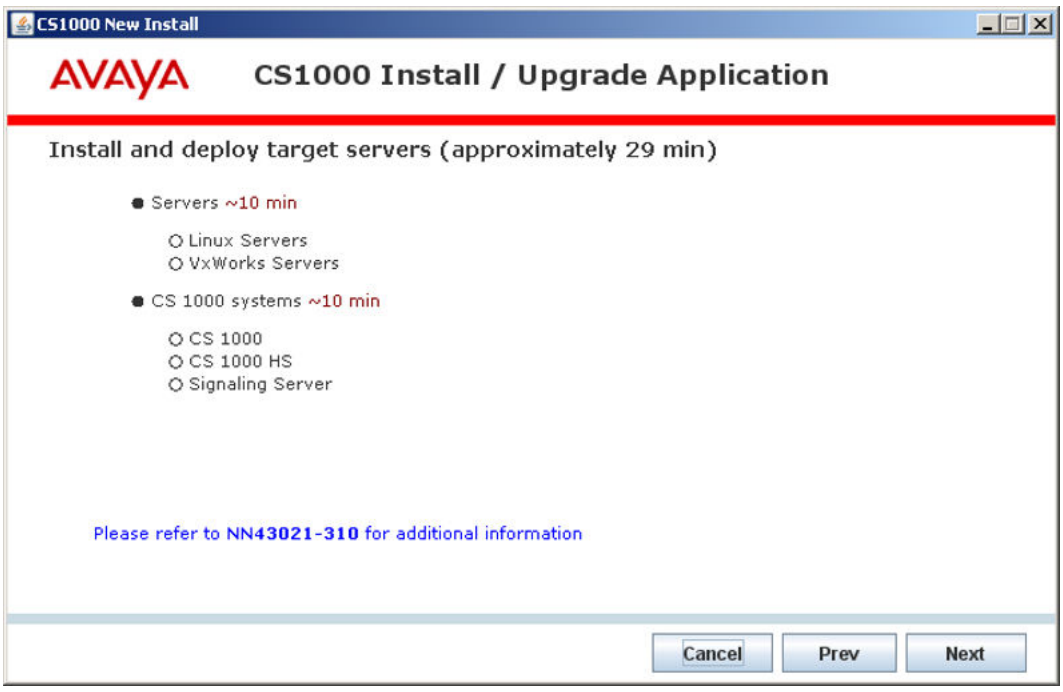
4. The **Primary Security Server** installation screen appears, as shown.
   - Complete the required tasks.
   - Click **Next** to proceed.



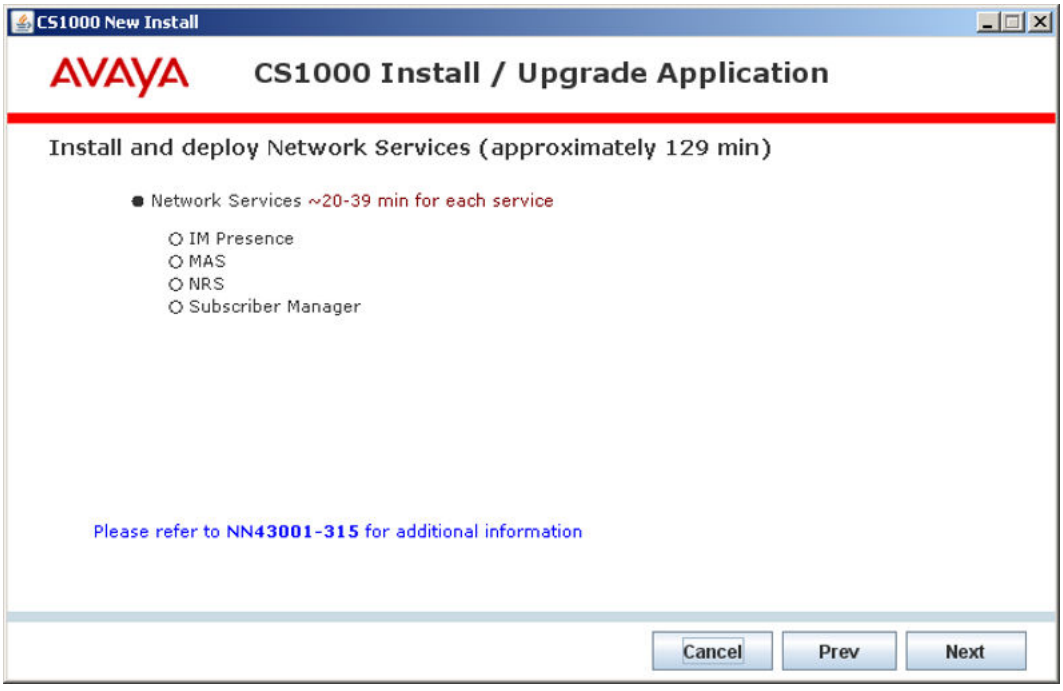
Note:

References to required documentation as well as the approximate time required to complete each task are provided when appropriate.

5. The **Install and deploy target servers** screen appears, as shown.
   - Complete the required tasks.
   - Click **Next** to proceed.

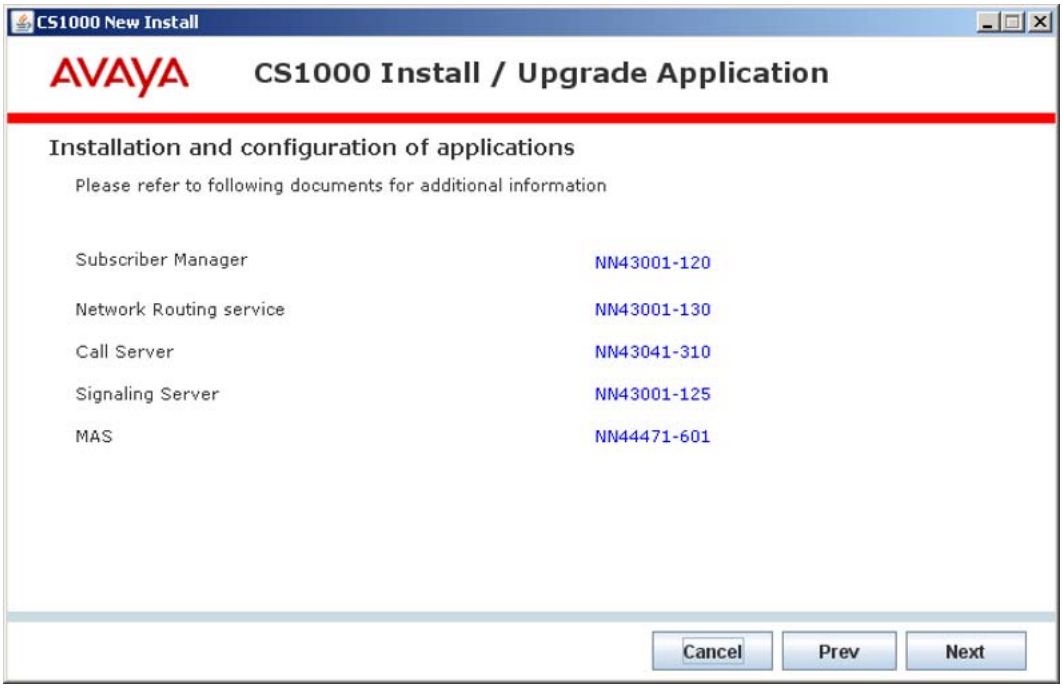


6. The **Install and deploy Network Services** screen appears, as shown.
   - Complete the required tasks.
   - Click **Next** to proceed.



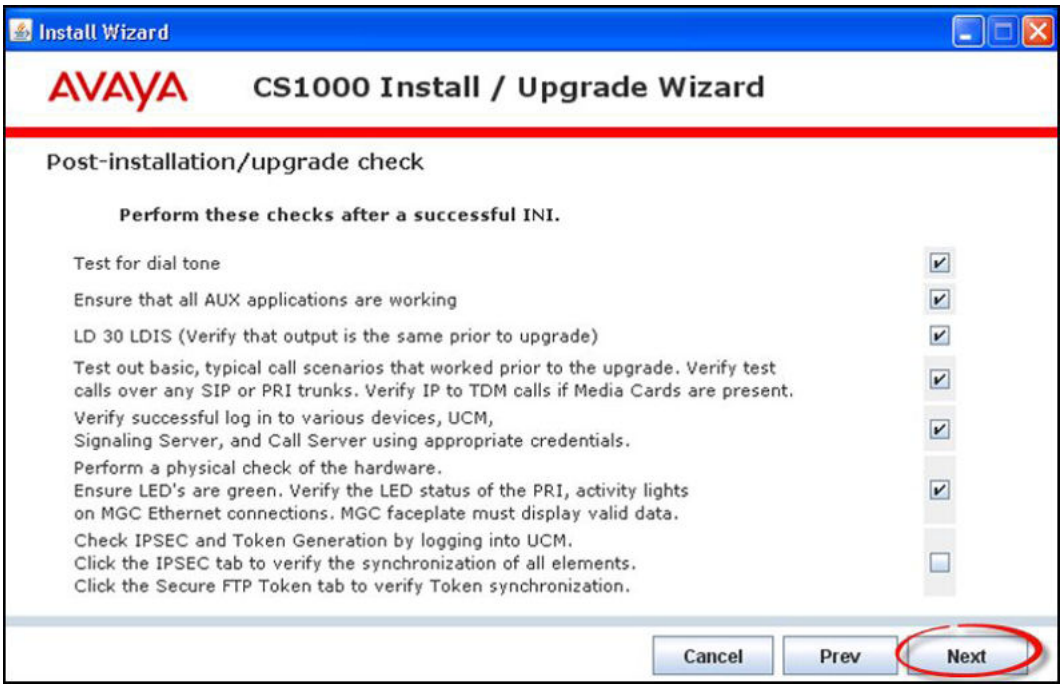
7. The **Installation and configuration of applications** screen appears containing a list of documentation, as shown.

- Refer to the documentation as required .
- Click **Next** to proceed.

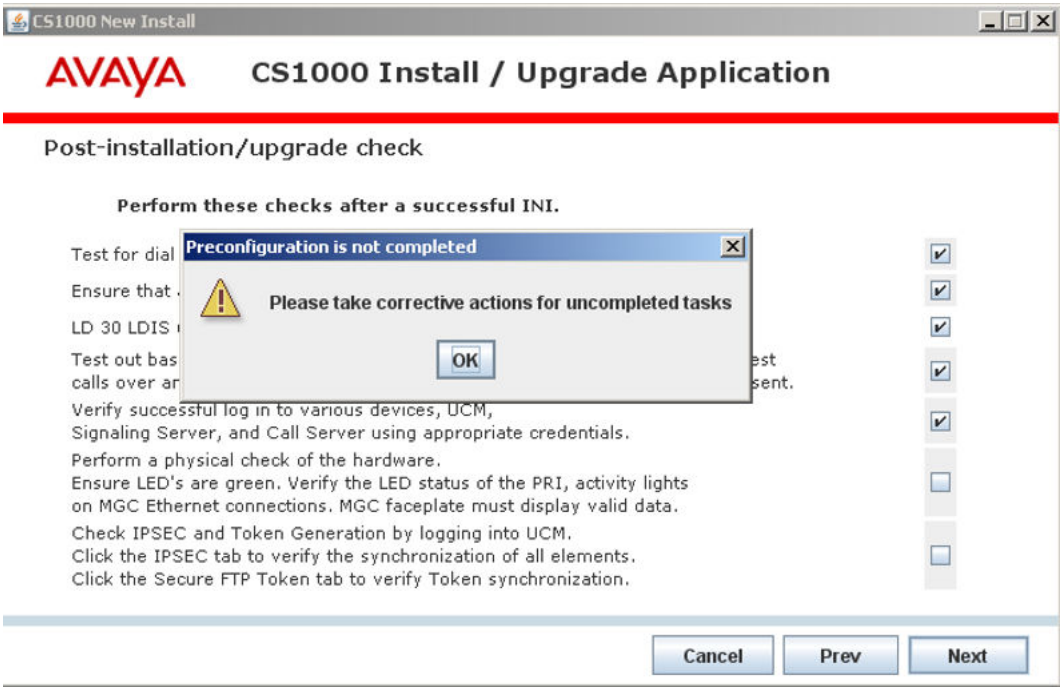


8. The **Management Security Parameters** screen appears, as shown.
   - Complete the required tasks
   - Click **Next** to proceed.

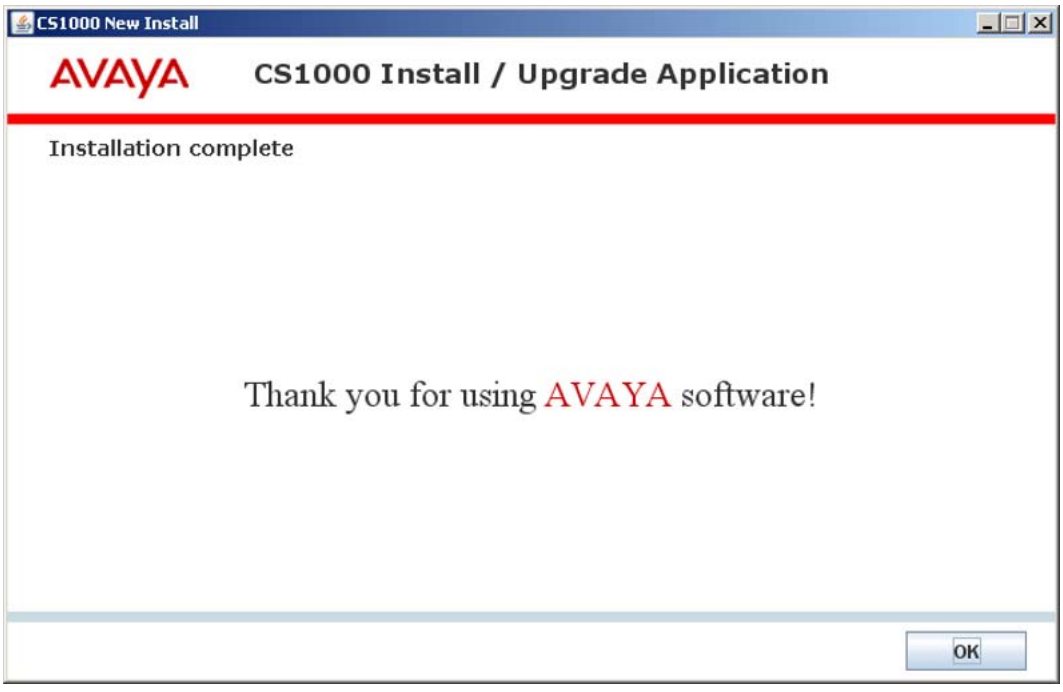
9. The **Post-Installation/upgrade** screen appears, as shown.
   - Perform the post installation tasks listed, after a successful INI.
   - Place a check in each box.
   - Click **Next** to proceed.



10. If all boxes are not checked, you are reminded to take corrective actions for uncompleted tasks, as shown.
    - Click **OK** to proceed.



11. The **Installation complete** screen appears, as shown.
    - Click **OK** to exit the New Installation Application.



Upgrade Application procedure

The Avaya Health Check Tool must be installed on a Windows-based PC with network connectivity to the CS 1000 system to be upgraded. Before you can run the Upgrade Application to upgrade an existing system, you must also configure the Call Server in the Health Check Tool. This configuration is required so the Upgrade Application can connect to the Call Server and retrieve the information required to perform the upgrade.

Note:

For detailed information on installing the Health Check Tool, see Installing the Health Check Tool on page 12.

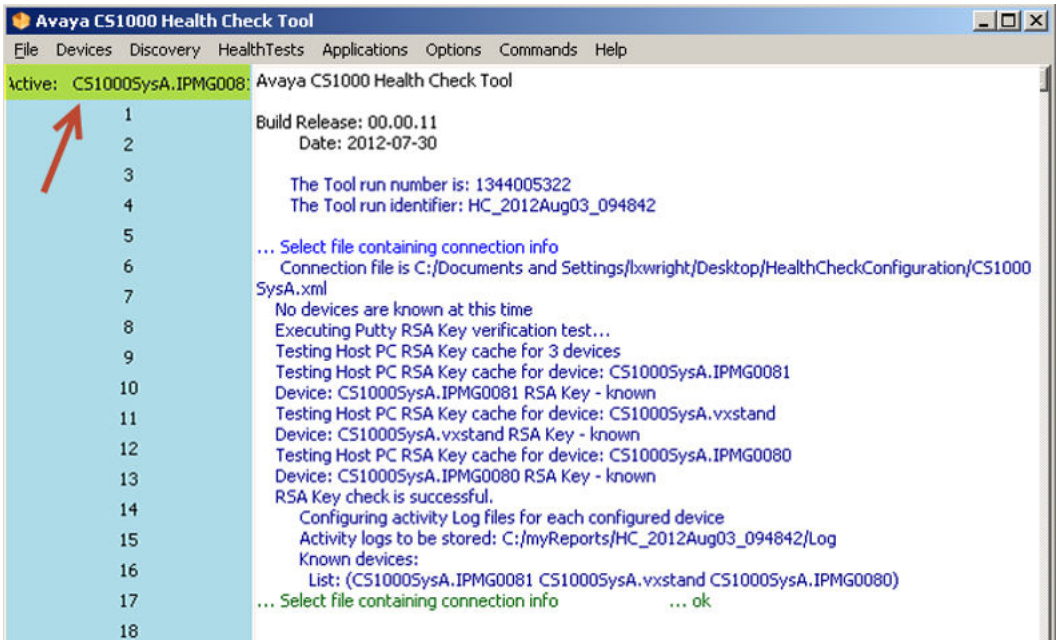
Note:

For detailed information on configuring the Health Check Tool, see Configuring the Health Check Tool on page 22

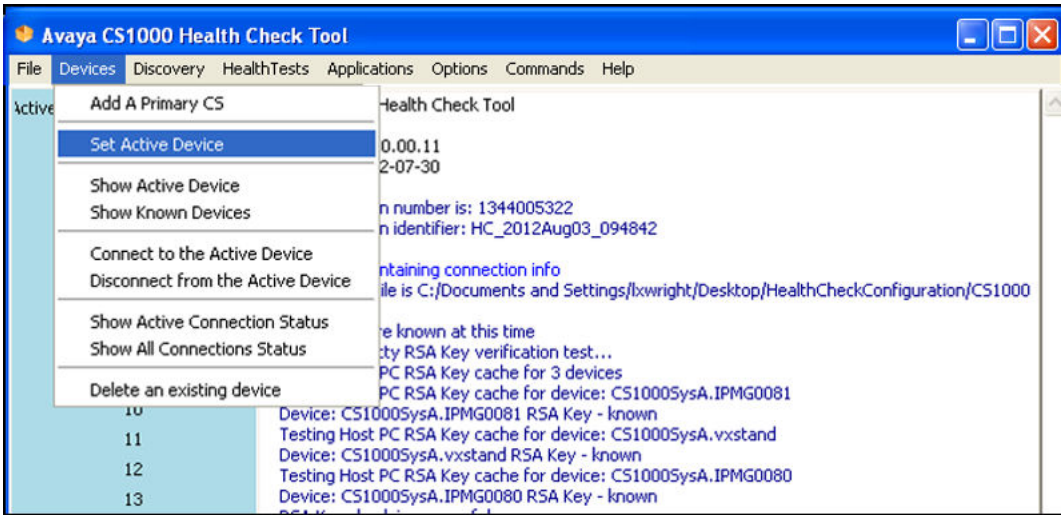
Running the Upgrade Application:

Once the Health Check Tool has been installed and configured to support the CS 1000 system to be upgraded, you can launch the tool and run the Upgrade Application.

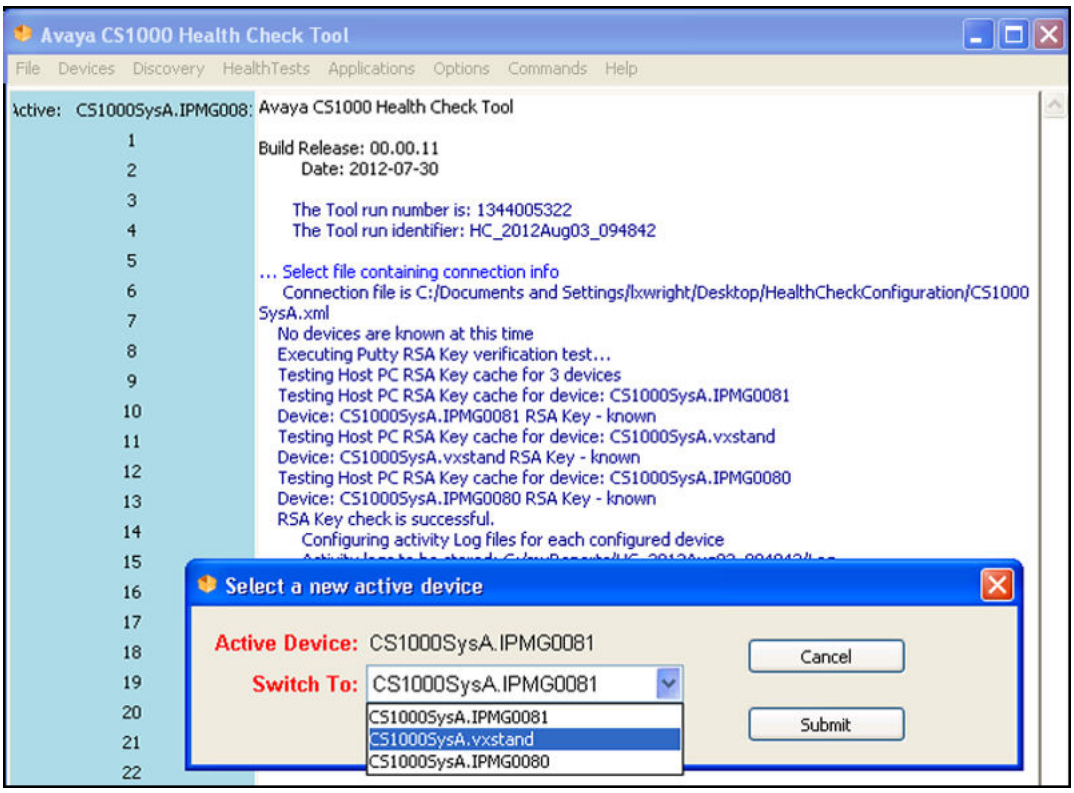
1. Launch the Health Check Tool.
2. From the **File** menu, select **Open** > **Configured Connections** to locate the configuration file for the system to be upgraded.
3. Select the file for the system to be upgraded and click **Open**.
4. Verify that the Call Server is set as the active device. In the example that follows, the IPMG is the active device.



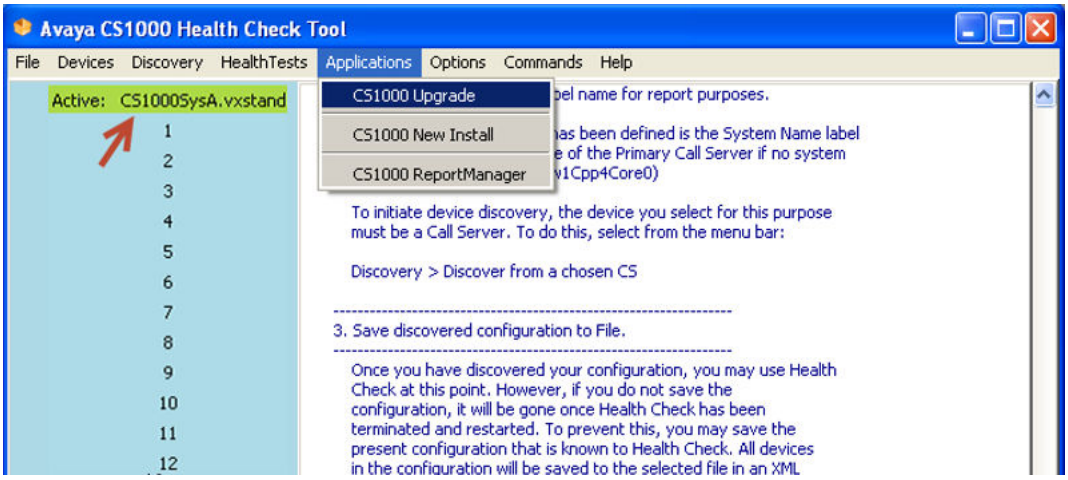
5. To set the Call Server as the active device, from the **Devices** menu, choose **Set Active Device**.



6. Choose the Call Server from the **Select a new active device** pull-down menu and click **Submit**.



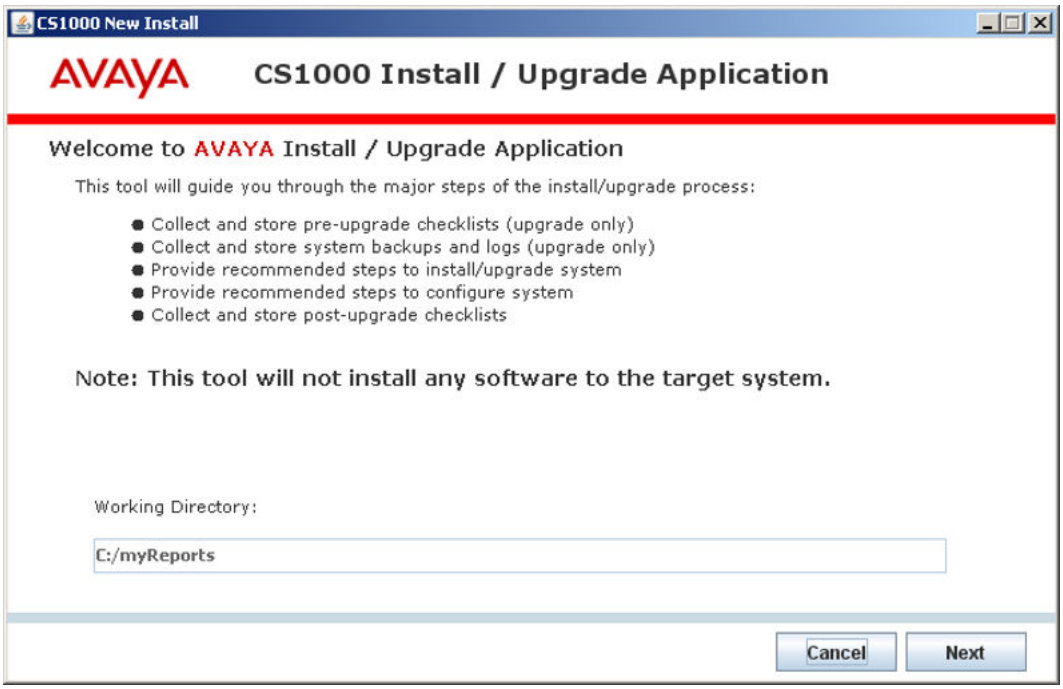
7. With the Call Server set as the active device, from the **Applications** menu, select **CS1000 Upgrade Application**.



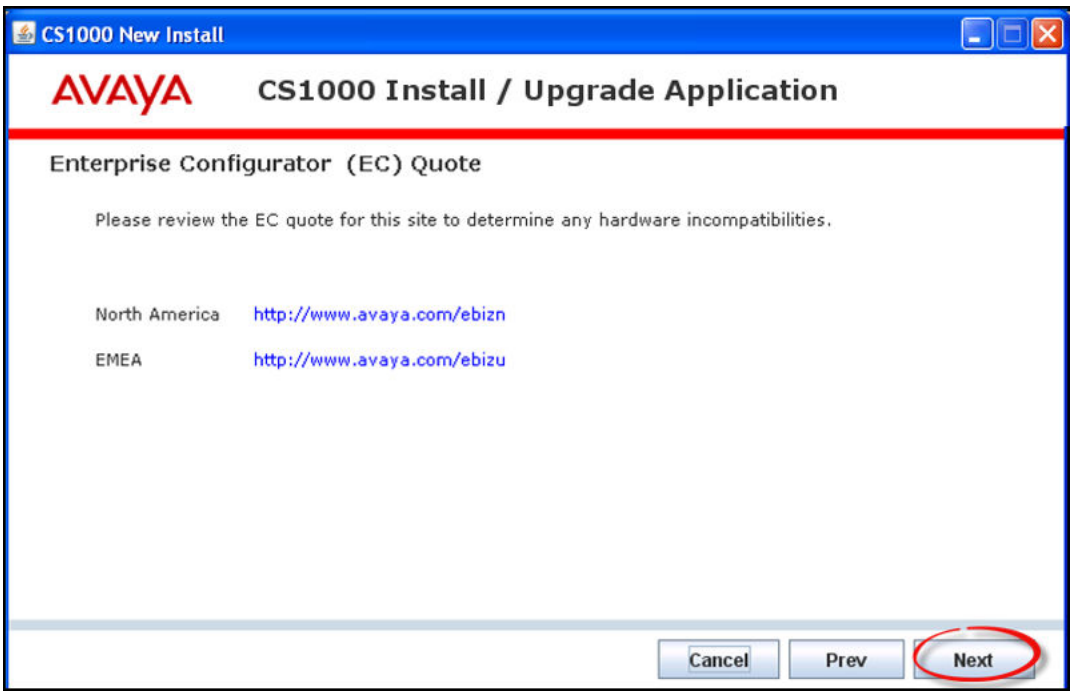
Note:

The Health Check Tool now attempts a connection to the active device, based on the Call Server information previously entered. This is done to confirm the information provided is valid, prior to launching the Upgrade Application. If it fails to connect to the Call Server, appropriate messages are shown in the main console window.

8. If the Health Check Tool connects successfully, the **CS 1000 Upgrade Application Welcome** screen appears, as shown. Click **Next** to proceed.



9. The **Enterprise Configurator (EC) Quote** screen appears, as shown, reminding you to review the EQ quote for this site to determine if there are any hardware incompatibilities.
   - Select the link for the appropriate EC tool.
   - Enter the Quote number. Review the quote displayed by the EC tool for any hardware incompatibilities.
   - Click **Next** to proceed.

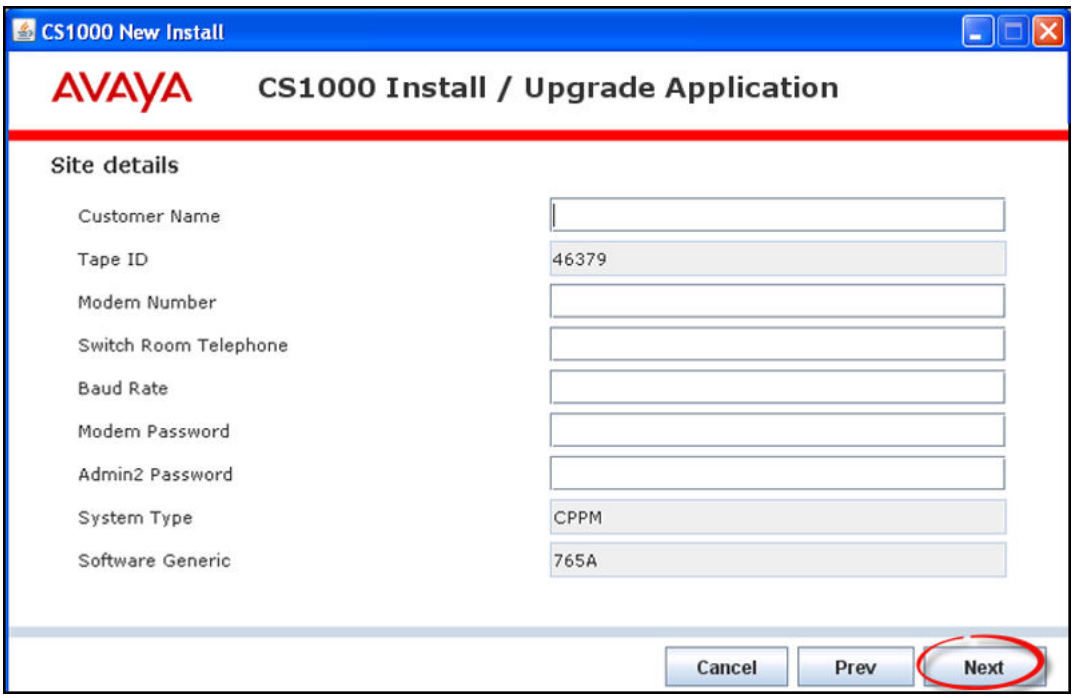


Note:

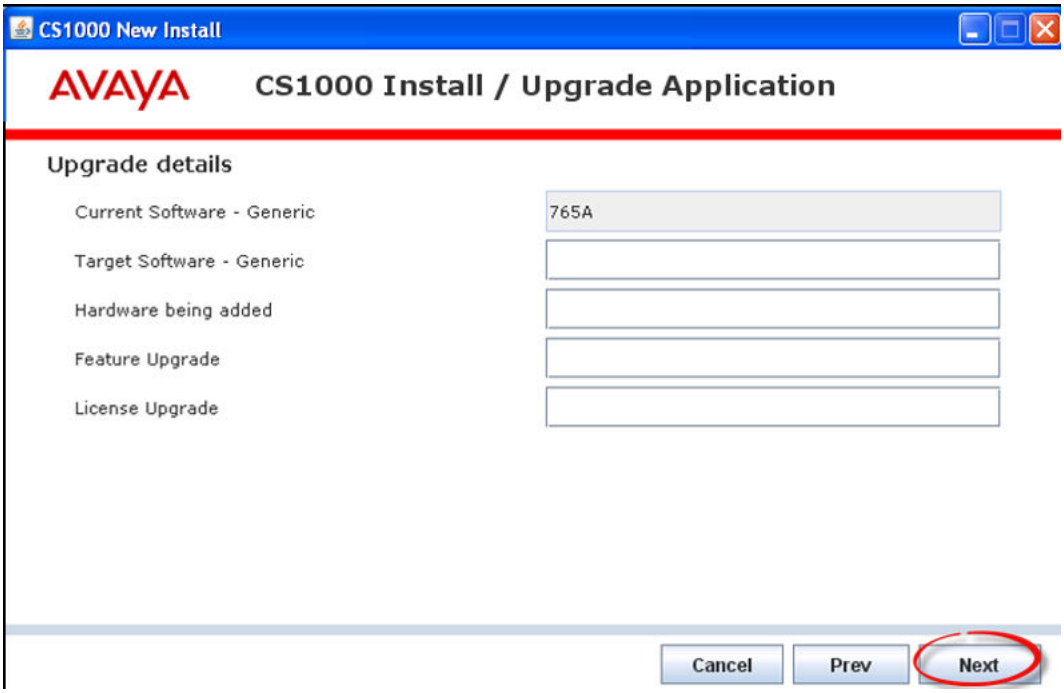
It is critical to identify and plan for any incompatibilities that exist between current installed hardware and the target software version before starting the upgrade.

10. The **Site details** screen appears, pre-populated with information from the system, as shown.

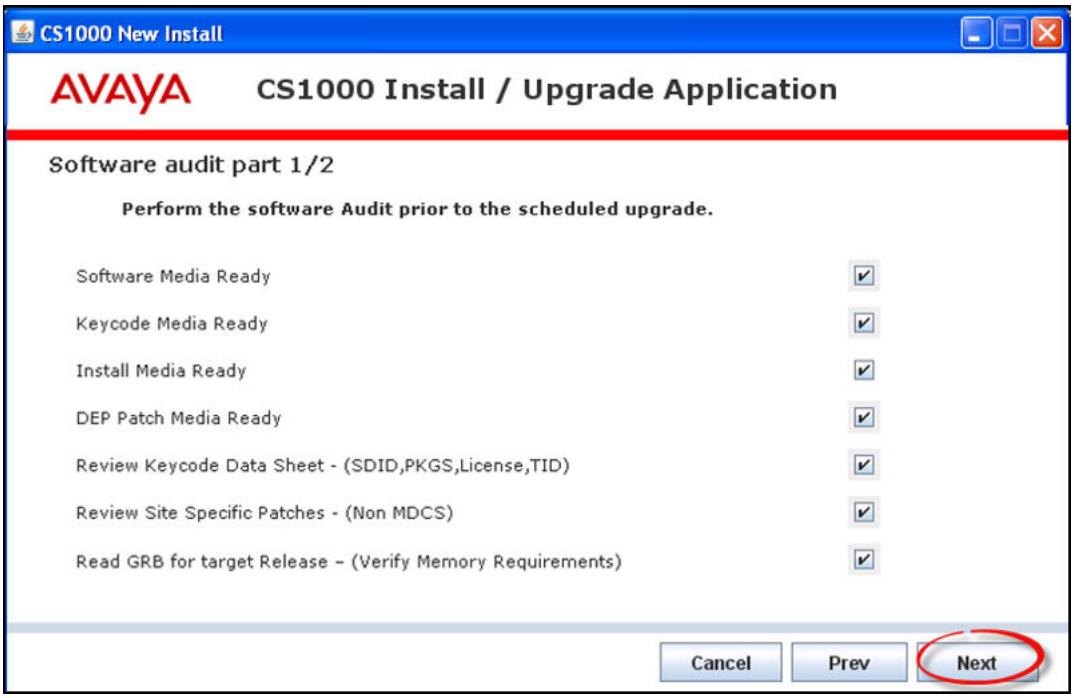
    - Enter the remaining site details.
    - Click **Next** to proceed.



11. The **Upgrade details** screen appears, pre-populated with the current software version, as shown.
    - Enter the required information.
    - Click **Next** to proceed.



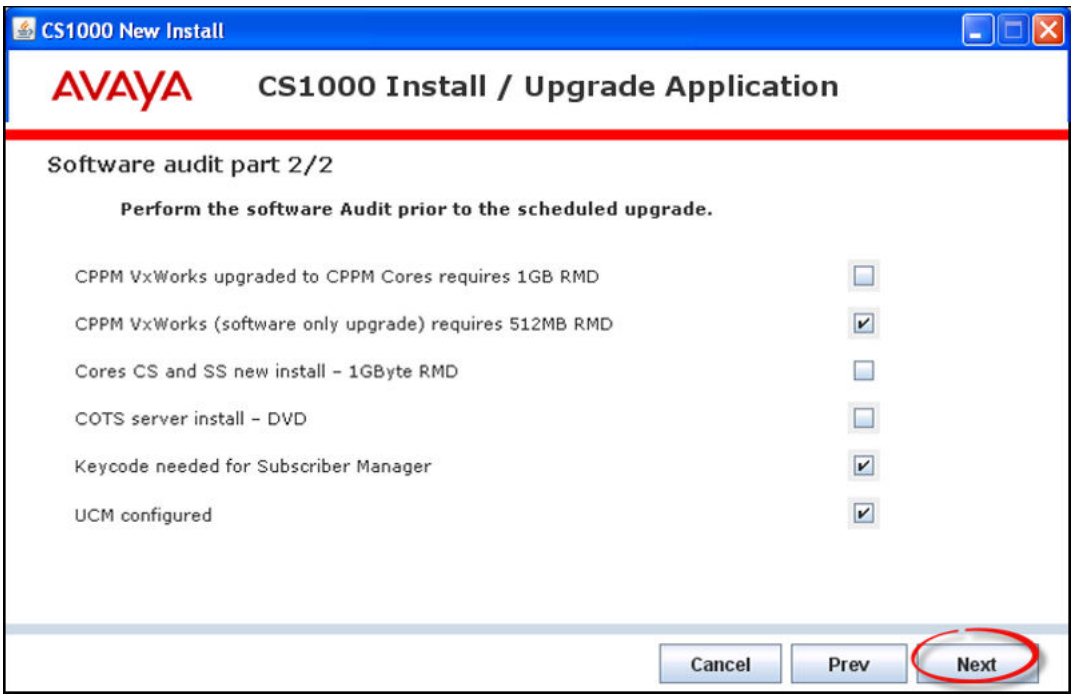
12. The **Software Audit part 1/2** screen appears, advising you to perform a software audit , as shown.
    - Perform the software audit before starting the upgrade.
    - Place a check in each box.
    - Click **Next** to proceed.



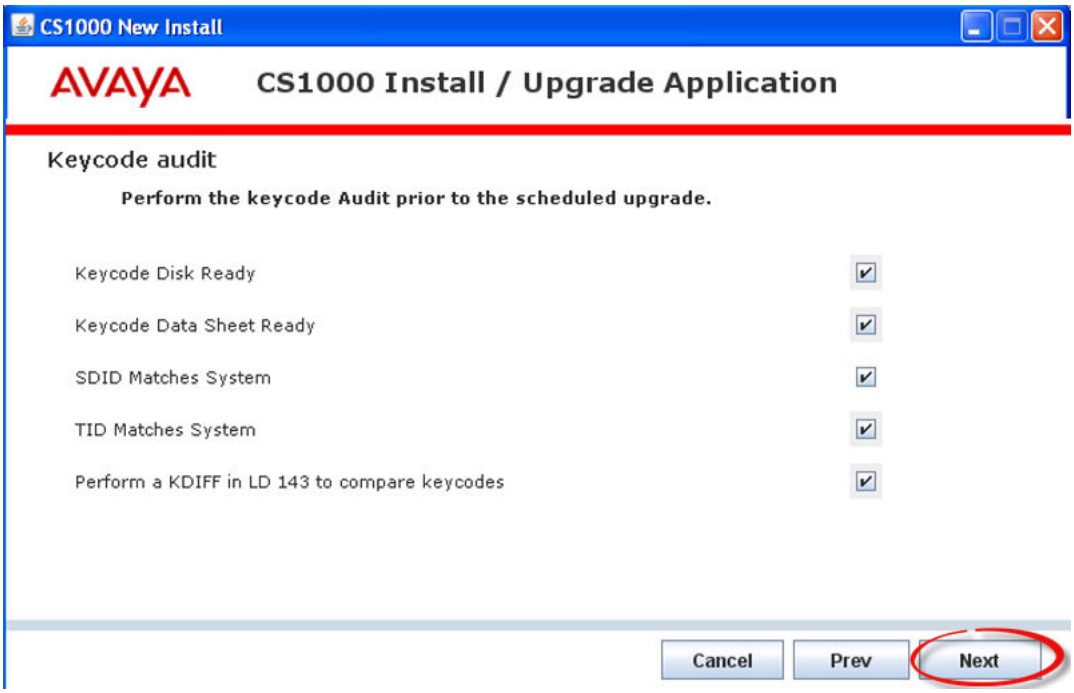
Note:

If all boxes are not checked, you are reminded to take corrective actions for uncompleted tasks.

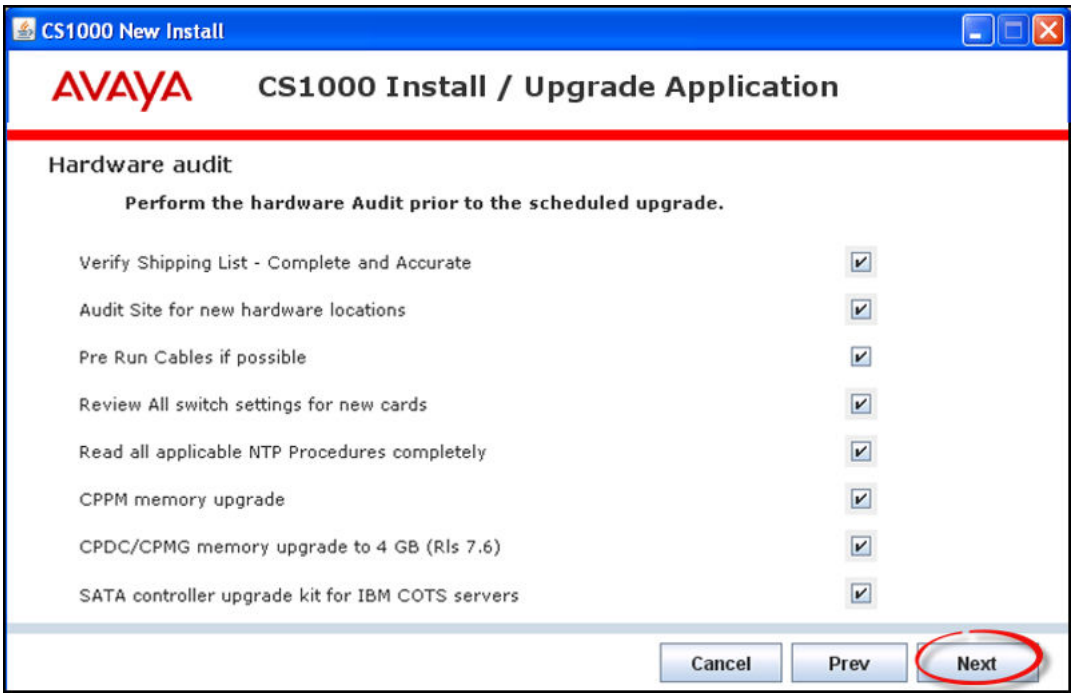
13. The **Software Audit part 2/2** screen appears, as shown.
    - Complete the remaining software audit tasks.
    - Place a check in each box.
    - Click **Next** to proceed.



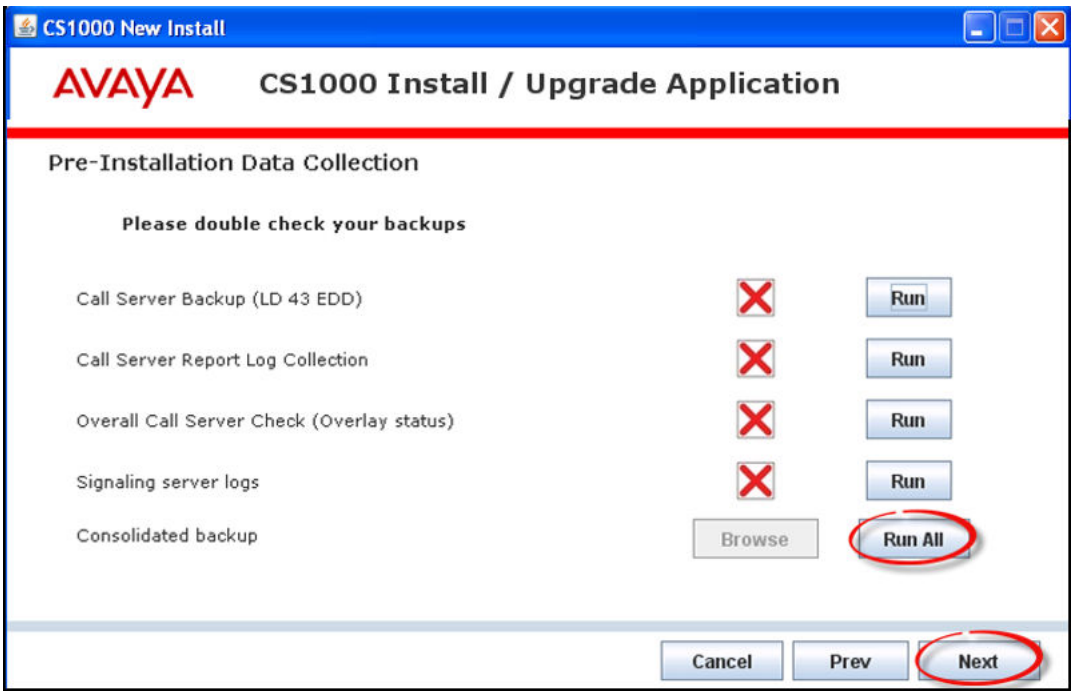
14. The **Keycode audit** screen appears, as shown.
    - Perform the Keycode Audit before the scheduled upgrade.
    - Place a check in each box.
    - Click **Next** to proceed.



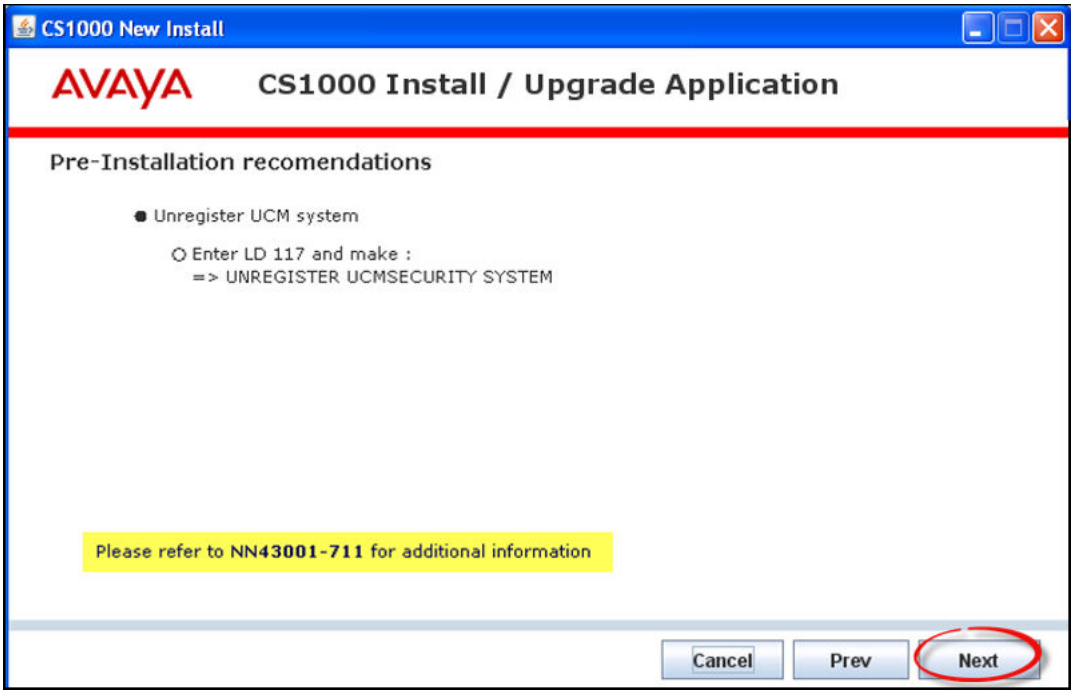
15. The **Hardware audit** screen appears, as shown.
    - Perform the required hardware audit tasks.
    - Place a check in each box.
    - Click **Next** to proceed.



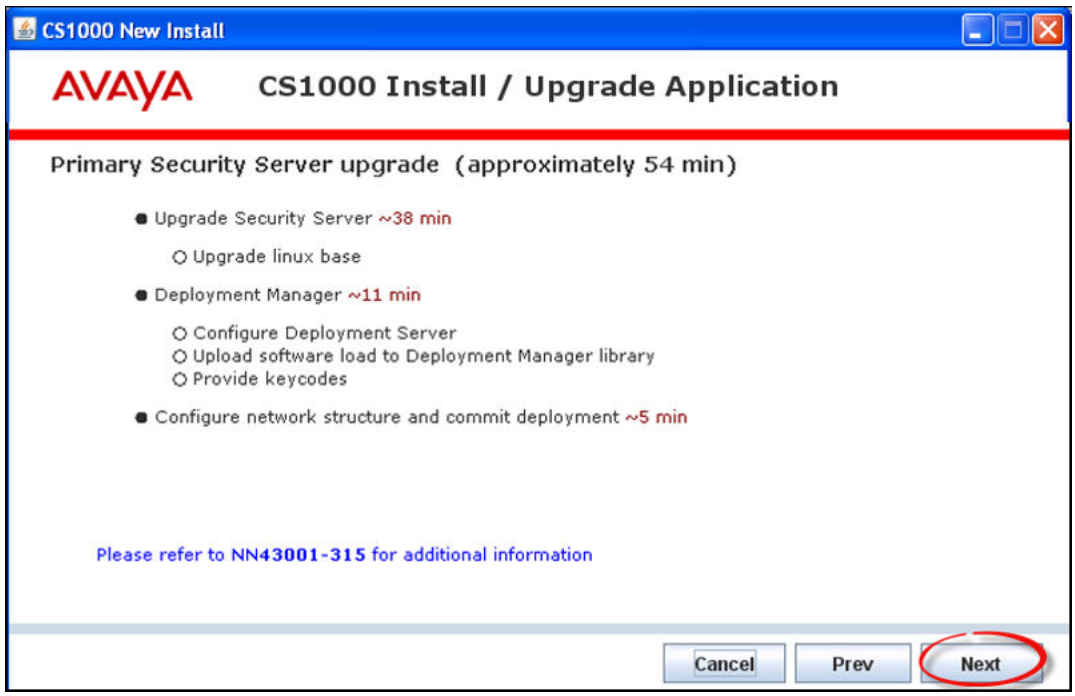
16. The **Pre-Installation Data Collection** screen appears, as shown.
    - Click the **Run** button for each individual item.
    - Or click the **Run All** button to run all of the data collection tasks.
    - Click **Next** to proceed when data collection tasks are completed.



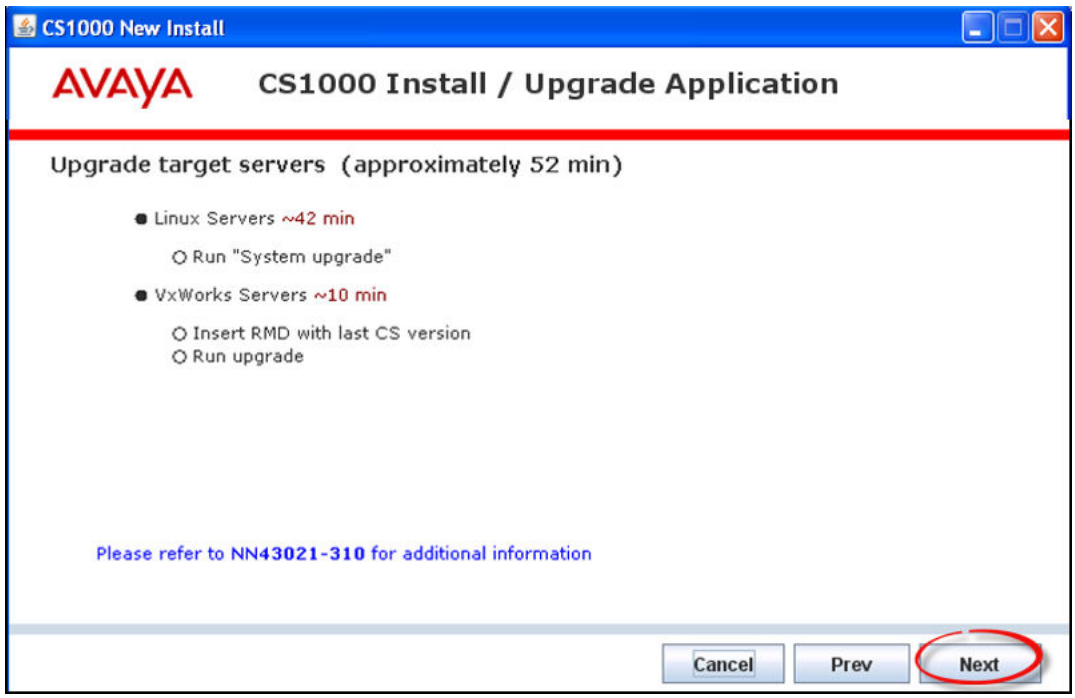
17. The **Pre-Installation recommendations** screen appears, as shown. Perform the suggested tasks and click **Next** to proceed.



18. The **Primary Security Server upgrade** screen appears, as shown.
    - Complete the required tasks.
    - Click **Next** to proceed.

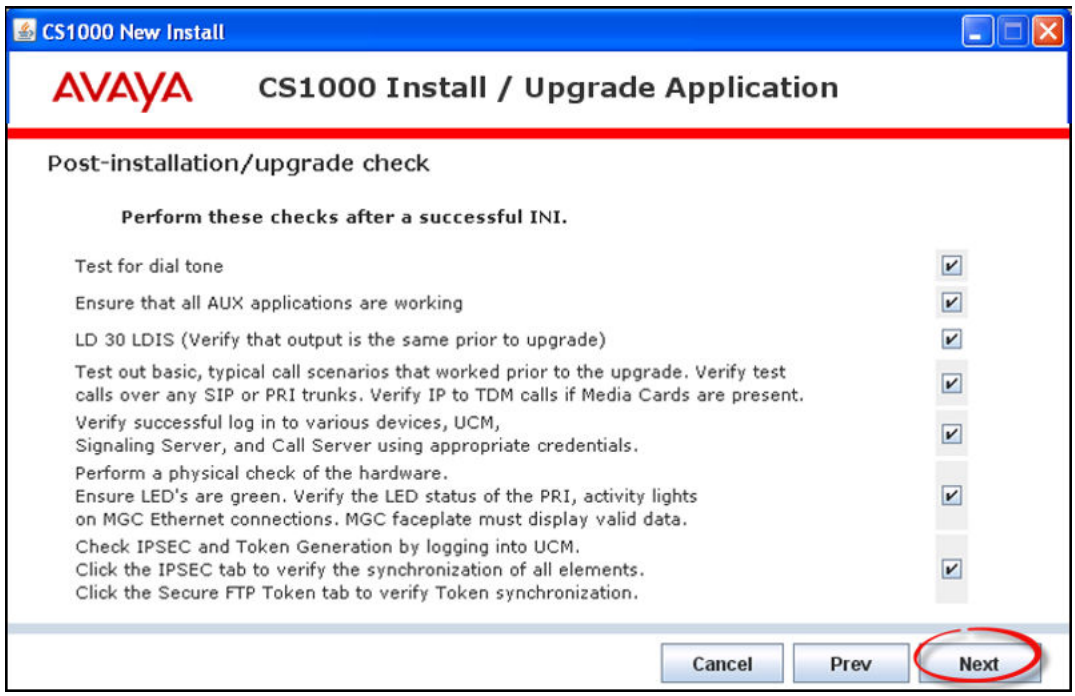


19. The **Upgrade Target Servers** screen appears, as shown.
    - Complete the required tasks.
    - Click **Next** to proceed.



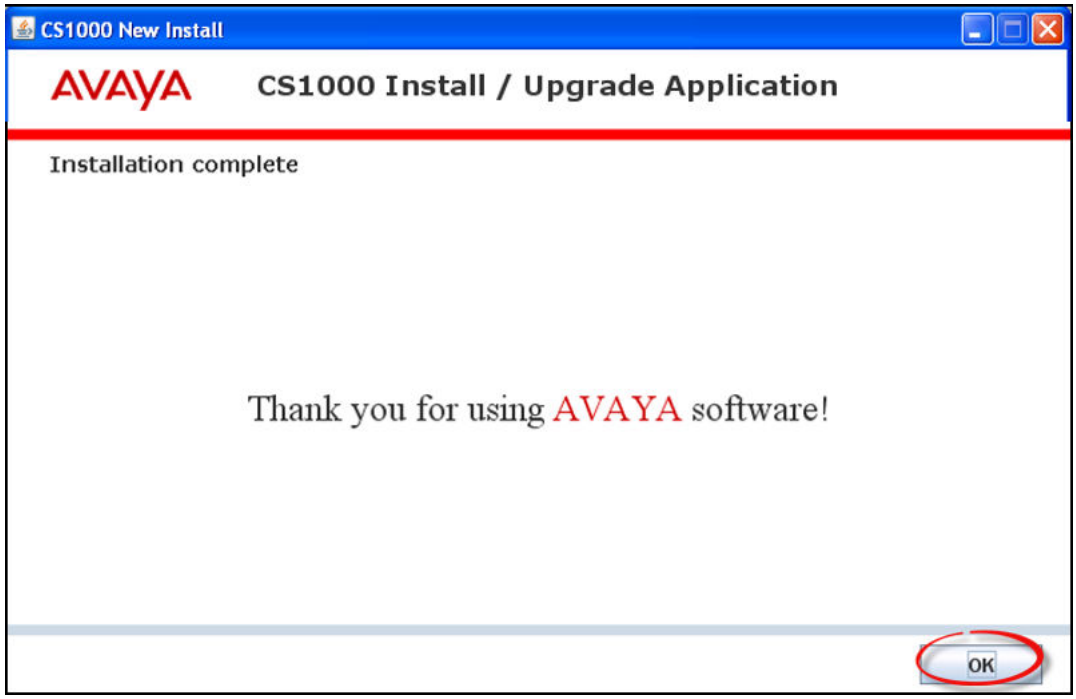
20. The **Management Security Parameters** screen appears, as shown.
    - Complete the required security configuration tasks.
    - Click **Next** to proceed.

21. The **Post-Installation/upgrade** screen appears, as shown
    - Perform the post-installation tasks listed, after a successful INI.
    - Place a check in each box.
    - Click **Next** to proceed.



22. The **Installation complete** screen appears, as shown.

    • Click **OK** to exit the Upgrade Application.



Note:

The log files created during the upgrade process should be reviewed upon completion

Appendix A: CS1000 installation and upgrade checklists

Use these Avaya Communications Server 1000 Installation and Upgrade Checklists as an aid to assist during installations or upgrades of CS 1000 systems.

While all possible attempts are made to ensure the accuracy of the information contained in this section, it is not intended to be the definitive source regarding such topics. The definitive source for installation and upgrade information is the Product Specific Documentation, Product Bulletins, and General Release Bulletins.

In the event of any discrepancies, the Product Specific Documentation, Product Bulletins, or General Release Bulletins are deemed to be correct.

Navigation

This section contains the following topics:

Contact information and signatures

Make a copy of the checklists in this document and return the originals to the RACS Engineer assigned.

Review all reference material and documentation for Communications Server 1000 Release 6.0/7.X prior to installation.

Reference documentation for Communications Server 1000 6.0 and 7.X can be found at:

http://support.avaya.com

Note:

Some of the preparation steps in this document require that you have access to system passwords. Take appropriate steps to guarantee the security of your passwords.

Contact information

Project # / Contract #:		Requested install date:	
Site Address:		Date of pre-site:	
Project Manager/ Leader:		Purchase Order #:	
Completed by home office			
Site ID:			
Clarify ticket (if applicable):			
Installer:		Phone:	
Installation coordinator:		Phone:	
Customer			
Name:			
Contact:			
Email address:			
Customer address:			
Address line 2:			
City:			
State:		Phone:	
Zip:		Fax:	
LAN Administrator			
Name:			
Email address:			
Phone:			
Fax:			
Switch Technician			
Name:			
Email address:			

Phone:	
Fax:	
Distributor	
Name:	
Contact:	
Email address:	
Phone:	
Fax:	

Signatures (as required)

Dist./Sales contact:		Date:	
Customer contact:		Date:	

Pre-installation checklists

Related topics:

CS 1000 prerequisites on page 61
System and site requirements on page 68
Power and grounding on page 71
Cabinet installation on page 83
Cabling installation on page 84
System operation on page 86
System software on page 89
VoIP networking parameters on page 90
Product Bulletins for vintage and release updates on page 92

CS 1000 prerequisites

Complete this checklist to ensure that you meet the prerequisite switch requirements for Communications Server 1000. Check the items in the checklist to confirm that they have been completed. Provide additional information where requested.

This checklist is to be completed and verified during coordination conference calls. The Installation Coordinator is responsible for forwarding copies of this document to parties involved with installation.

The responsibilities for completing this checklist are as follows:

Checklist section	To be completed by Distributor (Switch Technician)	To be completed by customer
Communications Server 1000 readiness		
Contact Center readiness		
CallPilot readiness		
Telephony Manager readiness		

CS 1000 readiness (one week prior to work window)

Important:

The Communications Server 1000 and related systems (such as CallPilot and Contact Center) should be locked down. No MAC work should be done until the upgrade has been completed. Any emergency changes should be entered into a sequential log. The end customer should be made to understand that undocumented changes may be lost in the event backup databases are required during the work window.

What is the configuration of the voice switch (PBX) being used? • Option 11C Cabinet • Option 11C Chassis • Communication Server 1000M Chassis/ Cabinet • Communication Server 1000S • Communication Server 1000M Single Group/ Multi Group • Communication 1000E • Option 61C, 81C **Note:** Indicate the Call Server power type and Model, including Geographic Redundancy.	System type: | Software release: | SN: |

Note: Download the latest software, patches, and loadware at http://www.avaya.com	

	Yes	No	Date
Audit the Software upgrade package: 1. Verify that media containing the current software is available. 2. KDIF keycode check: SLT Levels and Package audit. 3. Verify the correct hardware components (such as RAM or Dongles) are present. 4. Verify minimum vintages for existing hardware are in place. 5. Download software deployment packages from support.avaya.com 6. PEP and Loadware Library (ESPL) 7. Download current Linux Base Patches, Deplists, Loadware and Site Specific PEPs.			
Obtain current NTPs from AVAYA: • Reference documentation for Communications Server 1000 6.0, 7.0 and 7.5 can be found at: http://support.avaya.com			
Important: Create an IP Address Spreadsheet. Document the following for each element/device: • ELAN / TLAN / CLAN IP Addresses • MAC Address • Host Name / Alias Name • Subnet Mask / Gateway • FQDN for the security Server • Node IP **Note:** Ensure the planned network subnet configuration will support any additional IP Addresses required for the upgrade and to allow for future expansion.			

	Yes	No	Date
Ensure that sufficient and the appropriate type of removable media is available 1. The 128MB RMD is used to backup the call server database 2. The Software Delivery Card (SDC) contains the following: a. Avaya CS 1000E Release software b. keycode files c. CS 1000E Release Dependency List (PEPs) for Large and Small d. default database (if initiated during the installation) 3. The 1GB FMD is the hard drive for the CP PM Call Server. **Note:** The 1GB CF FMD is required for a SA or HA CP PM configuration. **Note:** For CP PM Linux , it is required that 2GB CF cards are used.			
Install new hardware if possible 1. Rack and power up any new hardware that can be, without impacting the system. 2. Upgrade memory on any Elements that are below minimum requirements. Each element will need to be removed from service to complete this work. The maintenance window(s) should be scheduled to occur prior to the work window.			
Have DNS Servers been identified for use with the Communications Server 1000 system?			
Has the DNS Database been created/updated with the TLAN information?			
Has the FQDN to be used with the Communications Server 1000 system been identified? **Note:** If no DNS server is available, the DNS information must be added in Linux Base. The host names are			

<table>
<tr><th></th><th>Yes</th><th>No</th><th>Date</th></tr>
<tr><td>always related to the TLAN IPs only. Never add ELAN IPs to the host file or any DNS server unless performing a managed services LAN configuration. The host table on the managing PC should also be modified with the FQDN information.</td><td></td><td></td><td></td></tr>
<tr><td>Does the system currently have PI or Site Specific patches installed?
If yes, cross reference the ESPL to ensure Release 6.0 versions (if applicable) are obtained prior to the work window at https://espl.avaya.com/espl/.
If a patch rewrite is required, contact Avaya to determine the lead time before scheduling the installation or upgrade.</td><td></td><td></td><td></td></tr>
<tr><td>Have you attached a printout of all patches applied (MDP ISSP from all elements)?</td><td></td><td></td><td></td></tr>
<tr><td>Have phones and personnel been identified for post-work testing purposes?
<table><tr><th colspan="2">Phone 1</th></tr><tr><td>DN</td><td></td></tr><tr><td>TN</td><td></td></tr><tr><td>Tester:</td><td></td></tr></table><table><tr><th colspan="2">Phone 2</th></tr><tr><td>DN</td><td></td></tr><tr><td>TN</td><td></td></tr><tr><td>Tester:</td><td></td></tr></table></td><td></td><td></td><td></td></tr>
</table>

CS 1000 (48 to 24 hours prior to work window)

Note:

This is your restore point in the event back out procedures are required.

<table>
<tr><th></th><th>Yes</th><th>No</th><th>Date</th></tr>
<tr><td>Important:
It is imperative that ALL system components that have the ability to export/backup their DB are touched at this time.</td><td></td><td></td><td></td></tr>
<tr><td>Test the DNS server database</td><td></td><td></td><td></td></tr>
</table>

	Yes	No	Date
1. Ping all FQDNs. Entries for elements not yet installed or upgraded will not respond; however, the name will resolve to the correct IP Address. 2. If any of the FQDNs do not resolve, correct the DNS DB prior to the upgrade window.			
Perform backups on all elements and applications using removable media. Keep these backups in a secure location. 1. LD 43 EDD for all Call servers. Retain backup of database in secure location 2. If the upgrade is from a Linux server(available from 5.X and up), perform a sysbackup –b on all Linux Elements AFTER the EDDs have been completed. 3. Backup the NRS database 4. Backup PD database - note Release 6.0 and above require a SPTP server **Note:** Do not rely on TM backups, ensure true EDDs are taken.			
Test CLI access (local and remote) to ALL CallServer cores and elements			
Ensure a bridge number or some other coordinated call has been arranged			

Contact Center readiness

	Yes	No	Date
Is Contact Center currently installed?			
Will a new version of Contact Center be installed as part of this work? **Note:** The minimum version of Contact Center supported is 6.0 **Note:** Ensure the Patching levels are current for Contact Center. Some patches may be required for proper interoperability with the new release.			

CallPilot readiness

	Yes	No	Date
Is CallPilot currently installed?			
Will a new version of CallPilot be installed as part of this work? **Note:** The minimum version of Callpilot supported is 4.07. **Note:** Ensure the Patching levels are current for CallPilot. Some patches may be required for proper interoperability with the new release.			

Telephony Manager readiness (not supported on 7.x)

	Yes	No	Date
Is Telephony Manager currently installed?			
Will a new version of Telephony Manager be installed as part of this work? **Note:** The minimum version of Telephony Manager supported is 4.0 **Note:** Ensure the Patching levels are current for Telephony Manager. Some patches may be required for proper interoperability with Communications Server 1000 Release 6.0. (Not supported with Communications Server 1000 Release 7.x.)			

Network

	Yes	No	Date
Is the network using Access Control Lists (ACL's)? If yes, you will need to contact your Network Administrator and have the MAC addresses of the new equipment added to the ACLs.			

System and site requirements

For additional information about system and site requirements, see:

Avaya Communication Server 1000E: Planning and Engineering (NN43041-220)

Avaya Communication Server 1000E: Installation and Configuration (NN43041-310)

Equipment Room Environment	Meets Specifications	
	Yes	No
Temperature is maintained between 15° and 30°C (59° and 86°F) • Absolute temperature: Temperature does not go below 10°C (50°F) or above 45°C (113°F). • Equipment is never exposed to absolute temperature limits for more than 72 hours. [Major]		
Environment temperature for telephones is 0° to 50°C (32° to 122°F).		
Heat sources (such as floor heaters) are not placed near the equipment.		
Temperature does not deviate any more than 10°C (18°F) within any hour. • The temperature differential in the equipment room does not exceed ±3.0°C (±5°F). • A temperature of 22°C (72°F) is recommended. • Temperature: _____° (Indicate C or F) [Major]		
Humidity level for equipment: RH 20% to 55%, noncondensing • Absolute humidity level: Humidity level must not go below RH 20% or above 80%, noncondensing Humidity _____% [Major, Critical if more than 95% or less than 5%]		
Environment does not show any visible signs of moisture. [Critical]		
Ventilating openings on equipment are free of obstructions. [Major]		
The room is clean, relatively dust-free, and well ventilated. [Minor, Major if concrete dust]		
Equipment location is not subject to constant vibration. [Major]		

Equipment Room Environment	Meets Specifications	
	Yes	No
Equipment is located at least 12 ft (3660 mm) away from sources of electrostatic, electromagnetic, or radio frequency interference. [FCC CFR 47 Part 15 for		
Equipment is not located under liquid-carrying pipes. [Major]		
Equipment room is not conducive to generating electrostatic discharge (ESD) [Major]		
Antistatic wrist straps, sprays, mats, or a combination of these is in evidence on-site. [Recommendation]		
Switch room door has a lock installed. [Minor]		
Electric locks, such as push button access code or card reader locks are not in use unless a battery backup or a key override is provided.		
No tripping or safety hazards exist in the equipment room. [Major]		
Installation is not located close to sources of EMI or RFI, such as high-voltage power lines, radar, broadcast stations, mobile communications, power tools, appliances (such as vacuum cleaners), and office business machines (such as copiers), industrial machines and ultrasonic cleaners, vehicle ignition, arc welders, dielectric heaters, and dimmer switches. [Major]		
Lighting illumination is 50 to 75-ft candles measuring 76 cm (30 in.) above the equipment room floor. [Recommendation]		
Equipment room is protected from receiving direct sunlight. Direct sunlight is prevented from shining on electronic hardware, especially disk units. [Major]		
Adequate floor space has been made available to install equipment racks, patch panels, power systems (UPS), and so on. [Major]		
Flooring is sealed concrete, vinyl, or mastic tile.		
RS-232 terminal and communications devices must not exceed the 50-ft cable length limit unless line drivers are utilized. [Major]		
The storage room for spare parts is secure. [Recommendation]		
If it is not possible that the site maintain the environment of the storage area exactly the same as the environment of the operating equipment, stored materials are allowed time to adjust to the equipment room environment before using them. [Major]		

Equipment Room Environment	Meets Specifications	
	Yes	No
The storage area is dust-free and away from high humidity and machinery such as electric motors of transformers. [Major]		
Circuit cards that are not in use are stored in a protective antistatic bag. [Major]		
Media Gateway, Call Server covers, UEM/IPE Shelf and Cabinet covers are installed. [Major]		
Equipment rear and front clearance must be 36" and side clearance must be 12". [Major]		

Reserve power equipment room	Meets Specifications	
	Yes	No
If the reserve power equipment is located in a separate room, then that room is: • well-ventilated and operating at optimum temperature; specific gravity readings are based on 25° C (77° F) • equipped with protective equipment (such as goggles, face shields, acid-resistant gloves, protective aprons, water for rinsing eyes/skin, and bicarbonate of soda) • well-secured • accessible (the doorway must not be blocked) • in compliance with all floor loading requirements and the noise levels required by OSHA standards 1910.5 (or local standards)		

Maintenance and technician area environment	Meets Specifications	
	Yes	No
A locking cabinet or storage area is in place for backup disks. [Recommendation]		
The area contains a table or desk terminal, printer, or equivalent device. [Recommendation]		
Maintenance workstation is equipped with a: [Major] • dial-up modem or connection to the network; • terminal emulator application such as Telnet or rlogin; • Web browser; • operational maintenance telephone		

Observations or comments:

Power and grounding

Complete this checklist to ensure that electrical power and grounding standards for Communications Server 1000 are met.

Check the items in the checklist to confirm that they have been completed. Provide additional information where requested. This checklist is to be completed and verified during coordination conference calls. The Installation Coordinator is responsible for forwarding copies of this document to parties involved with installation.

Note:

According to *Avaya Communication Server 1000E: Planning and Engineering (NN43041-220)*, Avaya recommends using an isolated ground topology as the preferred method of grounds for use as the CS 1000E single-point ground source. In the absence of such facilities, a portable or hardwired UPS system can be used. It is preferable that UPS systems contain load isolation transformers in their design. Isolated Ground topology is not accepted in Canada according to code.

For additional information about power and grounding, see:

Avaya Communication Server 1000E: Planning and Engineering (NN43041-220)

Avaya Communication Server 1000E: Installation and Configuration (NN43041-310)

Checklist section	To be completed by Distributor (Switch Tech)	To be completed by Customer
CS 1000 System AC service panel		
AC Power and Ground worksheet		
System power and ground connections		

CS 1000E System AC service panel

Item	Meets Specifications	
	Yes	No
The AC supply conductors are dedicated and uninterrupted from the building primary source or transformer to the PBX main AC service panel. (This does not apply to subpanels). [Major]		
Verify that an Isolated Ground (IG) or ACEG conductor is installed from MGN/ X0 to an IG or ACEG bus in the AC panel serving the PBX		

Item	Meets Specifications	
	Yes	No
equipment room. This point becomes the single-point ground reference for the PBX. **Note:** In some cases an AC panel is not a requirement. Various UPS systems establish the same intent and purpose as the panel IG/ACEG bus. The engineer performing the evaluation must research the application and determine its intent. [Critical]		
The IG/ACEG conductor is sized per code. (NEC 250). **Note:** It is recommended that the ACEG conductor be the same size as the largest phase conductor. [Major]		
The IG/ACEG conductor runs in the same raceway (conduit) as the phase and neutral conductors (NEC 250). [Major]		
The IG/ACEG conductor is insulated, permanent, and continuous (no splices). (NEC 250) [Major]		
A dedicated AC panel is installed in the PBX room for the CS 1000E and associated equipment only. Circuits being served for purposes such as lighting, air conditioning, heating, generators, copiers, or motors from the CS 1000E service panel are not recommended. Panel ID: [Major]		
Circuit breakers are identified and labeled at the AC service panel. (NEC 110-22) [Minor]		
Ensure that all voltage and current levels recorded are within the defined limits. **Note:** A licensed Electrician must obtain these results. See the AC Power and Ground worksheet [Critical]		
The workspace clearance around the AC service panel is 3-ft. (NEC 110-26) [Major]		
All RS-232 ancillary devices connected to the system I/O circuit cards must be wired from the same AC panel as the PBX power supplies, with individual hot, neutral, and isolated ACEG ground wires.		
The following current, power, and cooling requirements are met for Communications Server 1000 components:		

Item	Meets Specifications	
	Yes	No
The following power and cooling requirements for Media gateway packs are met:		

Component	Current @ 120/240 V AC (A)		Required UPS power (W)		Thermal dissipation (Btu)	
	Max	Typical	Max	Typical	Max	Typical
NTDU62 Call Server	2.50/ 1.25	1.00/ 0.50	300.00	120.00	1023.90	409.56
NTDU27 Signaling Server	2.00/ 0.90	0.50/ 0.25	200.00	60.00	682.60	204.78
NTDU97 Signaling Server	TBD	TBD	580.00	660.00	1990.00	TBD
NTDU99 Signaling Server	TBD	TBD	350.00	550.00	1024.00	TBD
NTDU14 Media Gateway	1.40/ 0.70	1.17/ 0.58	300.00	190.00	1023.60	648.30
NTDU15 Media Gateway Expander	1.15/ 0.58	1.17/ 0.58	300.00	145.00	1023.60	494.70
MG 1010	TBD	TBD	TBD	TBD	TBD	TBD
MRV Terminal Server	1.60/ 0.80	0.40/ 0.20	192.00	48.00	655.30	163.83
BayStack 470	1.50/ 0.75	0.60/ 0.30	90.00	72.00	324.00	245.74
BayStack 460 (Power over LAN	4.70/2.4 0	0.60/0 .30	295.00	72.00	335.00	245.74
BayStack 460 (Power over LAN for 24 IP Phones	4.70/ 2.40	1.20/ 0.60	364.12	141.12	335.00	245.74
Note: The typical values in the table are intended as a rough guide. Maximum AC input for the BayStack 460 includes maximum power of the Power over LAN. The typical rating has been adjusted to reflect configuring for IP Phones (60 mA at 48 V DC).						
Maximum voltage limits:						
North America	90 and 132 V, single phase		Europe and UK	180 and 250 V, single phase		
Frequency:						
North America	60 Hz		Europe and UK	50 Hz		
Fuse:						
Germany	16 A					

<table>
<tr><th rowspan="2">Item</th><th colspan="2">Meets Specifications</th></tr>
<tr><th>Yes</th><th>No</th></tr>
<tr><td>
<table>
<tr><th rowspan="2">Media gateway pack</th><th rowspan="2">Active off-hook (%)</th><th rowspan="2">Power consumption (W)</th><th rowspan="2">UPS power (W)</th><th colspan="2">Thermal dissipation</th></tr>
<tr><th>W</th><th>Btu</th></tr>
<tr><td>NTDW60 Media Gateway Controller Card</td><td>N/A</td><td>30</td><td>TBD</td><td>TBD</td><td>TBD</td></tr>
<tr><td>NTDW62 MGC DSP daughterboard (32 port)</td><td>N/A</td><td>4</td><td>TBC</td><td>TBD</td><td>TBD</td></tr>
<tr><td>NTDW64 MGC DSP daughterboard (64 port)</td><td>N/A</td><td>4</td><td>TBD</td><td>TBD</td><td>TBD</td></tr>
<tr><td>NTDK20 Small System Controller card</td><td>N/A</td><td>16</td><td>24.0</td><td>24.0</td><td>81.9</td></tr>
<tr><td>NTDK83 100BaseT daughterboard (dual-port)</td><td>N/A</td><td>6</td><td>9.0</td><td>9.0</td><td>30.7</td></tr>
<tr><td>NTDK99 100BaseT daughterboard (single-port)</td><td>N/A</td><td>4</td><td>6.0</td><td>6.0</td><td>20.5</td></tr>
<tr><td>NT5K02 Flexible Analog Line card</td><td>50</td><td>26</td><td>39.0</td><td>6.6</td><td>22.5</td></tr>
<tr><td>NT8D02 Digital Line card</td><td>100</td><td>26</td><td>39.0</td><td>13.0</td><td>44.4</td></tr>
<tr><td>NT8D03 Analog Line Card</td><td>50</td><td>26</td><td>39.0</td><td>6.6</td><td>22.5</td></tr>
<tr><td>NT8D09 Analog Message Waiting Line card</td><td>50</td><td>26</td><td>39.0</td><td>6.6</td><td>22.5</td></tr>
<tr><td>NT8D14 Universal Trunk card</td><td>DID-enabled</td><td>28</td><td>42.0</td><td>42.0</td><td>143.3</td></tr>
<tr><td>NT8D15 E&M Trunk card</td><td>N/A</td><td>29</td><td>43.5</td><td>43.5</td><td>148.4</td></tr>
<tr><td>NTAK09 1.5MByte DTI/PRI card</td><td>N/A</td><td>10</td><td>15.0</td><td>15.0</td><td>51.2</td></tr>
<tr><td>NTAK10 2.0 MByte DTI card</td><td>N/A</td><td>12</td><td>18.0</td><td>18.0</td><td>61.4</td></tr>
<tr><td>NTAK79 2.0 MByte PRI card</td><td>N/A</td><td>12</td><td>18.0</td><td>18.0</td><td>61.4</td></tr>
<tr><td>NTAK50 2.0 MByte PRI card</td><td>N/A</td><td>12</td><td>18.0</td><td>18.0</td><td>61.4</td></tr>
<tr><td>NTRB21 TMDI (1.5 Mbyte DTI/PRIi) card</td><td>N/A</td><td>12</td><td>18.0</td><td>18.0</td><td>61.4</td></tr>
<tr><td>NTVQ01 Media Card (32 port)</td><td>N/A</td><td>18</td><td>27.0</td><td>27.0</td><td>92.1</td></tr>
<tr><td>NTDW65 MC32S Media Card (32 port)</td><td>N/A</td><td>9</td><td>TBD</td><td>TBD</td><td>TBD</td></tr>
</table>
Note:
The UPS power requirement is the cards power consumption divided by the efficiency factor for the Media Gateway power supply plus peak in rush. For Media Gateways, use 1.5 times the wattage to give the UPS wattage, or volt amps (VA).
</td><td></td><td></td></tr>
<tr><td>Power from each outlet meets the input requirements of at least one CS 1000E power supply listed in the following tables (continued):</td><td></td><td></td></tr>
</table>

<table>
<tr><th>Item</th><th colspan="2">Meets Specifications</th></tr>
<tr><th></th><th>Yes</th><th>No</th></tr>
<tr><td>
<table>
<tr><th>AC input requirements for each MG 1000E or MG 1000E Expander</th><th>Y/N</th></tr>
<tr><td colspan="2">(North America)</td></tr>
<tr><td>Voltage</td><td>Recommended: 100-120 Volts
Maximum limits: 90 and 132 Volts, single phase</td></tr>
<tr><td>Frequency</td><td>50-60 Hz</td></tr>
<tr><td>Power (I/P max)</td><td>300 VA maximum</td></tr>
<tr><td>Outlet Type</td><td>120 Volts, 15 Amp supply</td></tr>
<tr><td colspan="2">(Europe and UK)</td></tr>
<tr><td>Voltage</td><td>Recommended: 208/220 Volts
Maximum limits: 180 and 250 Volts, single phase</td></tr>
<tr><td>Frequency</td><td>50-60 Hz</td></tr>
<tr><td>Power (I/P max)</td><td>300 VA maximum</td></tr>
<tr><td>Outlet Type</td><td>208/240 Volts, 15 Amp supply</td></tr>
<tr><td colspan="2">Carried out in accordance with local power specifications.</td></tr>
<tr><td colspan="2">The supplied power is single-phase 240 or three-phase 208 Y and has a system ground conductor</td></tr>
<tr><td colspan="2">(Germany)</td></tr>
<tr><td>Voltage</td><td>Recommended: 230 Volts
Maximum limits: 180 and 250 Volts, single phase</td></tr>
<tr><td>Frequency</td><td>50 Hz</td></tr>
<tr><td>Power (I/P max)</td><td>300 VA maximum</td></tr>
<tr><td>Fuse</td><td>16 A</td></tr>
<tr><td>Outlet Type</td><td>Receptacles by DIN regulation</td></tr>
</table>
</td><td></td><td></td></tr>
<tr><td>Power from each outlet meets the input requirements of at least one CS 1000E power supply listed in the following tables (continued):</td><td></td><td></td></tr>
</table>

<table>
<tr><th>Item</th><th colspan="2">Meets Specifications</th></tr>
<tr><th></th><th>Yes</th><th>No</th></tr>
<tr><td>
<table>
<tr><th>AC input requirements for each MG 1000E or MG 1000E Expander</th><th>Y/N</th></tr>
<tr><td colspan="2">(North America)</td></tr>
<tr><td>Voltage</td><td>Recommended: 100-120 Volts
Maximum limits: 90 and 132 Volts, single phase</td></tr>
<tr><td>Frequency</td><td>50-60 Hz</td></tr>
<tr><td>Power (I/P max)</td><td>300 VA maximum</td></tr>
<tr><td>Outlet Type</td><td>120 Volts, 15 Amp supply</td></tr>
<tr><td colspan="2">(Europe and UK)</td></tr>
<tr><td>Voltage</td><td>Recommended: 208/220 Volts
Maximum limits: 180 and 250 Volts, single phase</td></tr>
<tr><td>Frequency</td><td>50-60 Hz</td></tr>
<tr><td>Power (I/P max)</td><td>300 VA maximum</td></tr>
<tr><td>Outlet Type</td><td>208/240 Volts, 15 Amp supply</td></tr>
<tr><td colspan="2">Carried out in accordance with local power specifications.</td></tr>
<tr><td colspan="2">The supplied power is single-phase 240 or three-phase 208 Y and has a system ground conductor</td></tr>
<tr><td colspan="2">(Germany)</td></tr>
<tr><td>Voltage</td><td>Recommended: 230 Volts
Maximum limits: 180 and 250 Volts, single phase</td></tr>
<tr><td>Frequency</td><td>50 Hz</td></tr>
<tr><td>Power (I/P max)</td><td>300 VA maximum</td></tr>
<tr><td>Fuse</td><td>16 A</td></tr>
<tr><td>Outlet Type</td><td>Receptacles by DIN regulation</td></tr>
</table>
</td><td></td><td></td></tr>
<tr><td>Location of power outlets.

Note:
The maximum distance between a power outlet and the system equipment is met, in relation to the length of the power cord.
• in North America, the power cord is 9 ft, 10 in. (3000 mm).
• outside North America, the power cord is 8 ft, 2 in. (2490 mm).</td><td></td><td></td></tr>
</table>

Observations or comments:

AC Power and Ground worksheet

AC Service Panel Measurements

Note:

If a portable UPS system is used, measurements are only taken on the input/output voltage and the neutral ground voltage. Percent of load must also be notated.

Voltage measurements:	AC		MIN -MAX	
Between neutral and phase A	_____	volts	105v	125v
Between neutral and phase B	_____	volts	105v	125v
Between neutral and phase C	_____	volts	105v	125v
Between ground and phase A	_____	volts	105v	125v
Between ground and phase B	_____	volts	105v	125v
Between ground and phase C	_____	volts	105v	125v
Between phase A and phase B	_____	volts	180v	250v
Between phase A and phase C	_____	volts	180v	250v
Between phase B and phase C	_____	volts	180v	250v
Between neutral and ground (ACEG)	_____	Vrms	0.0v	0.5Vrms
UPS percent of load:				
UPS input voltage:				
UPS output voltage:				
Current Measurements:	AC		MAX	
Neutral conductor amps	_____	amps	See Note 1	
Ground conductor amps (IG or ACEG)	_____	amps	0.5 amps	
Phase A amps	_____	amps		
Phase B amps	_____	amps		
Phase C amps	_____	amps		

Note:

The neutral current must never exceed the current in any single-phase leg. A licensed electrician must take AC service panel measurements. Voltage and current values must comply with technical documentation.

Voltage between neutral and ground can signify poor or loose connections or noncontinuous grounding. Current flow in the grounding conductor can indicate that the neutral has been used for equipment grounding.

If currents are balanced in a three-phase system and there is significant neutral current, then harmonics are present.Harmonics can deteriorate transformers over time by overheating their internal wiring.

Solution: Use transformers specifically designed for harmonic loading (k-factor-rated).

System power and ground connections

Item	Meets Specifications	
	Yes	No
The Signaling Server power cord is plugged into the AC outlet of the rack and the AC outlet of the rack is grounded to its dedicated electrical panel. [Major]		
In a system with more than one MG 1000E powered by multiple service Panels, a #6 AWG (#40 Metric Wire Gauge) ground wire from the rear panel grounding lug of each MG 1000E is connected to an NTBK80 Ground Bar. The ground bar is connected to the Single Point Ground reference. [Major]		

Item	Meets Specifications	
	Yes	No
The Communications Server 1000E systems have ground lugs on the chassis, cabinet and MG 1010 and must be grounded using a #6 stranded conductor.		
The media gateways must be grounded using the following guide:		
** Screw connections to the 19" rack should never be used to provide a ground connection for Avaya equipment. ** Ground conductors should never be daisy chained expect in the specific scenario above where the NTDU14/15 pairs are used.		
** If a UPS is being used, the SPG ground bus needs to source from the same electrical service panel as the UPS.		
If multiple pieces of equipment are installed in a rack, a separate connection is run from the grounding lug on each piece of equipment to the NTBK80 Ground Bar. [Major]		
In an installation where a dedicated panel cannot provide optimal conditions, a load isolation transformer or load isolation transformer-based UPS/Line conditioner with the following characteristics is used: [Major] • 120/208/240 V AC input, over-current protected at primary • 120/208/240 V AC available at secondary outputs, each circuit breaker protected • primary and secondary windings are completely isolated from one another • the load isolation transformer or load isolation transformer-based UPS/Line conditioner is approved for use locally as a stand-alone user product (CSA, UL, or other locally recognized clear markings) • the load isolation transformer or load isolation transformer-based UPS/Line conditioner is capable of providing power to all CS 1000E components operating at the same time at full load • equipment unrelated to the CS 1000E is not powered from a transformer that provides service to the CS 1000E system • the load isolation transformer or load isolation transformer-based UPS/Line conditioner is electrostatically shielded to minimize ELF fields		
Ground conductors are at least #6 AWG (16 mm2) at any point.		
Ground conductors do not carry current under normal operating conditions.		
Spliced conductors are not be used. (Continuous conductors have lower impedance and are more reliable.)		

<table>
<tr><th rowspan="2">Item</th><th colspan="2">Meets Specifications</th></tr>
<tr><th>Yes</th><th>No</th></tr>
<tr><td>All conductors terminate in a permanent way. All terminations are easily visible and available for maintenance purposes.</td><td></td><td></td></tr>
<tr><td>Ground connections are tagged with a clear message such as “Critical Connection: Do Not Remove or Disconnect”.</td><td></td><td></td></tr>
<tr><td>The installation meets the specific grounding requirements for the area: [Major]

<table><tr><td>Germany</td><td>#8 AWG (10 mm) green/yellow wire</td></tr><tr><td>North America, other areas of Europe</td><td>Not smaller than #6 AWG (16 mm) at any point.</td></tr><tr><td>UK</td><td>Two green/yellow wires no thinner than two 10 mm²</td></tr></table></td><td></td><td></td></tr>
<tr><td>A 120VAC non-switched receptacle is provided within 9 ft of the CS 1000E cabinets.Avaya strongly recommends that each Media Gateway and Media Gateway Expansion pair for 1000E systems are powered from one dedicated 120VAC, 15/20 amp branch circuit with individual hot, neutral, and AC equipment ground or isolated ground wires. Installation does not exceed 80% of the maximum branch circuit or UPS load rating. [Major]</td><td></td><td></td></tr>
<tr><td>Media Gateway</td><td></td><td></td></tr>
<tr><td>The NTBK80 ground bar is capable of grounding up to six Media Gateways (either with or without companion Media Gateway Expanders) back to the SPG. If there are more than six Media Gateways (either with or without companion Media Gateway Expanders), the NTDU6201 ground bar is used.</td><td></td><td></td></tr>
<tr><td>The NTDU6201 can be adjusted for various mounting configurations. It accepts 35 #6 AWG(16 mm2) wire connections. The ground bar terminates at the service panel ground.</td><td></td><td></td></tr>
<tr><td>All equipment located in a series of equipment racks that are physically bonded together are grounded to and powered by the same service panel.</td><td></td><td></td></tr>
<tr><td>If additional service panels are required, they are collocated beside the original service panel.</td><td></td><td></td></tr>
<tr><td>If racks are not bonded together, then the equipment located in the racks can be grounded and powered by separate service panels.</td><td></td><td></td></tr>
<tr><td>A #6 AWG (16 mm2) ground wire is connected from the rear panel grounding lug of each Media Gateway to the ground bar.</td><td></td><td></td></tr>
</table>

Item	Meets Specifications	
	Yes	No
The ground bar is connected to a ground source in the dedicated service panel. **Note:** In the UK, the ground wire is connected from the equipment to a ground bar or through a Krone Test Jack Frame.		
The Media Gateway and Media Gateway Expander are considered as the same ground. To ground the Media Gateway Expander, the ground wire is jumpered from it to the grounded Media Gateway.		
Multiple pieces of equipment installed in a rack are grounded with a separate connection from the grounding lug on each piece of equipment to the ground bar.		
If a piece of equipment in a rack does not have a grounding lug, the rack is grounded to the ground bar.		
For all CS 1000E system ground paths, route the correct size of insulated copper conductors is routed inside conduit.		
Each Media Gateway and Media Gateway Expander pair is powered from the same service panel.		
A dedicated electrical panel that is connected to the facility's electrical system is used to power the system and this panel provides power only to the CS 1000E system components and related telecommunications hardware such as TTYs and printers. [Recommended].		
A system ground conductor, sized at a minimum of a #6 AWG stranded, insulated wire is installed from the cabinet ground bus to the ACEG bus in the AC panel. Where UPS systems are employed, a #6 AWG wire can be installed from the cabinet ground bus to the grounded metallic case of the UPS using a ground lug. [Critical if missing; Major if undersized].		
A #6 AWG insulated, stranded conductor is installed between each CS 1000E cabinet ground lug and the cabinet ground bus. [Major]		
All grounding conductors are clearly identified and labeled. [Minor]		
No telecommunications ground bus of the CS 1000E is connected to untested horizontal structural steel, water pipes, or other unreliable ground paths. [Major]		
The cabinet ground bus is mounted near the CS 1000E cabinets. [Major]		
UPS requirements		

Item	Meets Specifications	
	Yes	No
Cabinets are grounded to the same AC service panel or UPS that provides input power to the PBX system. [Major]		
All UPS systems must have a ground lug (to accommodate a minimum of #6AWG wire) or ground bus installed and bonded to the UPS metallic enclosure to allow connections to the PBX system ground bus and the AC panel ACEG bus. **Note:** If the UPS system is equipped with an isolation transformer, the ground lug or bus must be wired from the center tap (X0) of the transformer (The ground lug or bus allows a parallel connection to the CS 1000E single-point ground source in case the UPS power cord is unplugged). [Major]		
#6 AWG grounding conductors are installed from the UPS ground bus or lug to the CS 1000E cabinet ground bus and the ACEG bus in the AC service panel. See items #3 and #10 above. [Major]		
CSUs (Channel Service Units) are connected to reserve power (UPS) or are span powered. [Major]		
Equipment unrelated to the CS 1000E system in any way is not powered from the same 120 VAC receptacles or UPS system as the PBX. [Major]		
In isolated ground environments, other equipment, equipment racks, or metallic conduit do not come in contact with the CS 1000E equipment rack. [Major]		
The earth source, which the CS 1000E system connects to through the AC service panel, has a resistance of 5 ohms or less. [Major]		
Ground conductors are insulated, permanent, and continuous (not spliced). [Major]		
All terminations are easily visible and accessible for maintenance purposes. [Major]		
The dedicated service panel feeds only the CS 1000E and is located as close to the system as possible.		
Each vertical power bar on the 19-inch rack has its own power feed.		
The system ground conductor is insulated, and the same size as the largest conductor and runs between the Main Service Panel (MSP) and the CS 1000E panel.		
Ground conductors are not smaller than #6 AWG.		

<table>
<tr><th rowspan="2">Item</th><th colspan="2">Meets Specifications</th></tr>
<tr><th>Yes</th><th>No</th></tr>
<tr><td>Electrical layout is reflective of a typical ANSI/EIA/TIA607 installation with TMGB and TGB ground blocks.</td><td></td><td></td></tr>
<tr><td>If installation is not at a ANSI/EIA/TIA607 site then a wire is connected from system ground bar to AC Ground at the Service panel.</td><td></td><td></td></tr>
<tr><td>Ground and Neutral bonding occur at either the transformer or at the first disconnect (Main Service Panel).</td><td></td><td></td></tr>
<tr><td>The resistance between the ground post of any equipment and the single-point ground to which it connects is less than 0.25 ohms for an installed Call Server, MG 1000E, MG 1000E Expander, or Signaling Server. [Major]</td><td></td><td></td></tr>
<tr><td>The installation uses one of the following bus bars as a system SPG: [Major]
• building principal ground, normally in a building with one floor
• dedicated TMGB/TGB bonded to the building grounding system
• ACEG bus located inside the PBX service panel</td><td></td><td></td></tr>
<tr><td>Other items</td><td></td><td></td></tr>
<tr><td>QUA6 Power Failure Transfer Units (PFTU) are available to transfer trunk lines during a power or system failure. [Recommendation]
The appropriate AC power cord kit is used for the installation as listed in the following table. (These cords connect a CS 1000E system to a commercial AC power source.)
<table>
<tr><th>Country/ Region</th><th>AC Power Cord</th><th>Voltage Rating</th><th>Current Rating</th><th>Plug Type</th></tr>
<tr><td>North America</td><td>A0379412</td><td>250 V</td><td>10 A</td><td>NEMA 6–15P</td></tr>
<tr><td>Argentina</td><td>A0814961</td><td>250 V</td><td>10 A</td><td>IRAM 2073</td></tr>
<tr><td>North America</td><td>NTTK14</td><td>125 V</td><td>13 A</td><td>NEMA 5–15P</td></tr>
<tr><td>Australia/ New Zealand</td><td>NTTK115</td><td>250 V</td><td>10 A</td><td>AS3112</td></tr>
<tr><td>Europe</td><td>NTTK16</td><td>250 V</td><td>10 A</td><td>CEE(7)VII</td></tr>
<tr><td>Switzerland</td><td>NTTK17</td><td>250 V</td><td>10 A</td><td>SEV 1011</td></tr>
</table>
</td><td></td><td></td></tr>
</table>

Item	Meets Specifications	
	Yes	No
<table><tr><th>Country/ Region</th><th>AC Power Cord</th><th>Voltage Rating</th><th>Current Rating</th><th>Plug Type</th></tr><tr><td>UK/ Ireland</td><td>NTTK18</td><td>250 V</td><td>10 A</td><td>BS1363</td></tr><tr><td>Denmark</td><td>NTTK22</td><td>250 V</td><td>10 A</td><td>AFSNIT</td></tr></table>		

Cabinet installation

For additional information, refer to *Avaya Communication Server 1000E: Installation and Configuration, NN43041-310*.

Item	Meets Specifications	
	Yes	No
Circuit cards are of allowable vintage (no outstanding Product Advisories or Bulletins). [Major]		
Circuit cards are locked into place. [Minor]		
All MDF/IDF blocks are clearly labeled. [Major]		
PBX cabling is not strapped to the exterior of any conduit or raceway as a means of support. [Major]		
MICB cards, where installed, use cards slots 1, 2, 3 in Media Gateways and slots 7, 8, 9 in Media Gateway Expanders only. [Major]		
M2250 consoles utilize 5 consecutive TN units and are properly cross-wired with three power TNs. The AUX cable can be utilized to take the place of two power TNs only. See console cable wh/sl, rd/or, & rd/grn pairs. The M2250 consoles do not require a static discharge ground connection, the connection should be installed to protect any earlier vintage attendant consoles that may be used as replacements. [Major]		
Application tapes and messaging system tape cartridges		
Media is not subject to rapid changes in temperature or humidity. [Major]		
Media is kept away from strong magnetic fields. [Major]		

Item	Meets Specifications	
	Yes	No
Database backups are routinely performed and are readily available. [Major]		
System installation CDs, PC cards are available for the PBX and Applications products in the event of severe system hardware malfunction or data corruption. [Critical]		

Observations or comments:

Cabling installation

For additional information, refer to *Avaya Communication Server 1000E: Installation and Configuration, NN43041-310*.

Outside plant cabling and protectors

Item	Meets Specifications	
	Yes	No
Entrance cable sheath is grounded as close as possible at the point of entry to an approved ground source. [Major] (NEC 800-33; 40)		
Splice cases are properly grounded. [Major]		
Approved protection devices are used for Telco network and campus cables. (Carbon, Gas tube type for network cables; fast-acting, low let-through type on campus cables). (NEC 800) [Major]. For further details, see Product Bulletin 97040 (April) revision 1 relating to protection.		
Protection devices are installed at both ends of a cable in a campus environment. (Silicon Avalanche type. see Oneac 5SDP; 5SAP) [Major] ANSI/UL 497-1995 Specs -10V for digital telephones; 48VDC for analog telephones. For further details, see Product Bulletin 97040 (April) revision 1.		
All protection device grounding conductors are grounded to an approved source with an appropriately sized wire. The grounding conductors must be kept as short and straight as possible. (No sharp bends- 8 radius) (NEC 800-40) [Major]		

Cabinet cabling

Item	Meets Specifications	
	Yes	No
Cabling must be installed in a neat and orderly fashion. [Major]		
MDF cables are seated and secured in place using factory velcro straps. [Major]		
All cables for cabinets, Call Servers, Media Gateways/Expanders, Signaling Servers (SDI, AUX, VGMC ELAN/TLAN, CE-MUX, DS-30X, and 10/100BaseT cables) and adapters are properly fastened. [Major]		
Power wiring must not be installed in a parallel fashion with CAT5 cabling. Installing power wires perpendicular to CAT5 cables is preferred and minimizes effects from EMI or ELF fields. [Major]		
EMI mitigating ferrite rings (NTVQ83AA) are installed on Voice Gateway Media Card TLAN/ELAN patch cables. [Major]		
NTCW84JA assemblies are used for each VGMC connector. [Major]		
CAT5 patch cables are not installed near fluorescent lighting fixtures. [Major]		
ELAN/TLAN patch cables for VGMC and Signaling Server hardware are factory made and kept at 20 cable feet or less. [Recommendation]		
All patch cables are labeled and correlate to a network infrastructure diagram or schematic. [Minor]		
The NTDK95 CE Mux cables, between the Media Gateway and Media Expansion Cabinets, must be installed in the correct direction during Chassis Expansion Cabling installation. If installed in reverse, can result in product malfunction including: low audio; garbled transmission from IP to TDM phones; dropped calls; and invalid card responses. Attach the Expansion Cabinet connecter to the NTDU15 unit. If no labels are present, the Expansion Cabinet contains a ferrite bead on a single wire. For more information, please see Bulletin 2008008579.		

Cross-connect terminal requirements

Item	Meets Specifications	
	Yes	No
To allow for future expansion and equipment changes at the cross-connect terminal, the cross-connect terminal has enough space for		

Item	Meets Specifications	
	Yes	No
connecting blocks to terminate four 25-pair cables from each Media Gateway and for each Media Gateway Expander. [Recommendation]		
When Ethernet connections are used instead of traditional cabling, the Media Card Input/Output adapter is used: • for the 1.5 Mbit DTI/PRI circuit card NTRB21, NTBK04 cable is used • for the 2.0 Mbit DTI circuit card NTAK10, 2.0 Mbit PRI circuit card NTAK79, and 2.0 Mbit PRI circuit card NTBK50, NTBK05 cable is used • each IPE card slot equipped with a Line or Trunk card uses a 25-pair cable from the host Media Gateway or Media Gateway Expander • four conductors for the AUX cable run from the Media Gateway • one 25-pair cable runs from each Power Fail Transfer Unit (PFTU) QUA6 • wiring is in place from telephones and trunks		
In the UK: If the Krone Test Jack Frame is used, only authorized personnel are allowed access the Krone Test Jack Frame and it is installed in a locked room or in an environment that prevents free access to the equipment. For additional information about the cross-connect terminals, see *Avaya Communication Server 1000E: Installation and Configuration (NN43041-310)*.		

Observations or comments:

System operation

For additional information refer to:

X11 Software General Release Bulletin (shipped with new software)

System diagnostics

Item	Meets Specifications	
	Yes	No
LD 30 Network and Signaling Diagnostic (NWS). [Minor]		
LD 34 Tone and Digit Switch and Digitone Receiver (TDS). Check results from the midnight routines. [Major]		
LD 37 Input/Output Diagnostic (IOD). Use STAT command for TTYs. [Major]		
LD 38 Conference Circuit Diagnostic (CNF). Check results from the midnight routines. [Major]		
LD 43 Data Dump (EDD). Check for successful completion of a manual data dump. [Critical]		
LD 44 Software Audit (AUD). Must be configured in BKGD of Ld-17. Check for normal AUD000 messages. [Major]		
LD 48 Status of ELAN and Mail/ESDI Links. Make sure all AMLs that are in use are Active Empty. [Major]		
LD 60 Digital Trunk Diagnostic (DTI/PRI). Use the SSCK command to check system clocks. Locked on to IP daughterboard #1. Also check midnight routines for frame slips, CRC errors. [Major]		
LD 117 STAT HOST		
LD 137 ELNK STAT ELNK command		
GTR, documentation, and Backup logs are located in switch room. **Note:** Ensure appropriate level and system type of technical documents are available. [Minor]		
The PBX maintenance modem and terminal server performs as expected. [Major]		
A terminal server or SEB modem is configured as to allow Telnet access to the system. [Recommendation]		
The system is equipped with a working maintenance terminal and printer. [Major]		
A PC is available on location in order to access Element Manager and NRS [Major]		
Minimum level PEPs are installed in the system. This includes DepList PEPs for the Call Servers, required PEPs for Signaling Servers, and Voice Gateway Media Card PEPs. [Recommendation]		

Item	Meets Specifications	
	Yes	No
IP telephones are on the latest recommended firmware. [Recommendation]		
Signaling Servers are load sharing (equal number of registered IP phones) [Recommendation]		
Printouts of Signaling Server config.ini and bootp.tab files are readily available. pdt> cd /u/config, copy config.ini, copy bootp.tab [Minor]		

Memory size

<table>
<tr><th colspan="4" rowspan="2">Item</th><th>Meets Specifications</th><th></th></tr>
<tr><th>Yes</th><th>No</th></tr>
<tr><td colspan="4">The installation meets the minimum memory requirements:

<table>
<tr><th>Processor</th><th>Flash memory required</th><th>DRAM memory required</th><th>Total memory</th></tr>
<tr><td>Call Server (CP PII)</td><td>N/A</td><td>256 MByte</td><td>256 MByte</td></tr>
<tr><td>Call Server (CP PIV)</td><td>N/A</td><td>512 MByte</td><td>512 MByte</td></tr>
<tr><td>Call Server (CP PM)</td><td>N/A</td><td>1 GByte</td><td>1 GByte</td></tr>
<tr><td>MG 1000E (MGC)</td><td>4 MB</td><td>144 (128 MB of CSP SDRAM + 16 MB of MSP SDRAM)</td><td></td></tr>
<tr><td>MG 1000E (SSC)</td><td>64 MB</td><td>32 MByte</td><td>96 MByte</td></tr>
<tr><td colspan="4">CP PII and CP PIV can be upgraded to a maximum of 2 GB DRAM memory.</td></tr>
</table></td><td></td><td></td></tr>
<tr><td colspan="4">The installation does not exceed the recommended maximum call register count:</td><td></td><td></td></tr>
</table>

Item	Meets Specifications	
	Yes	No
<table><tr><th>System</th><th>Recommended call register count</th><th>Memory required (SL–1 words)</th><th>Memory required (MByte)</th></tr><tr><td>CS 1000E (CP PII)</td><td>25 000</td><td>6 057 000</td><td>23.174</td></tr><tr><td>CS 1000E (CP PIV and CP PM)</td><td>35 000</td><td>8 505 000</td><td>32.444</td></tr><tr><td colspan="4">Note: Call registers are 243 SL-1 words long. One SL-1 word is 4 bytes.</td></tr></table>		

Observations or comments:

System software

Overlay 15/21 Customer Data Block

Item	Meets Specifications	
	Yes	No
SRCD (Auto Set Relocation Code) has a value programmed. [Major if SPRE is 1, Minor if other]		

Overlay 17/22 Configuration Record

Item	Meets Specifications	
	Yes	No
Daily Routine defined as LD 34, 38, 60,137. [Major]		
LD 44 in background routine. [Major]		

Item	Meets Specifications	
	Yes	No
The number of call registers (NCR) within the maximum value required by GRB documentation regarding port size and features used. 1000M- 800 call registers [Major]		
1000M LPIB and HPIB values equal 450. [Recommendation]		
History file is defined as MTC, BUG and is set at minimum length of 60 000 characters. [Major]		
ERRM is configured as ERR, BUG, AUD. [Major]		
RLS IDs are configured for each D-Channel where appropriate. [Major]		

Overlay 11/12/13 digital telephones, attendant consoles, and digitone receivers

Item	Meets Specifications	
	Yes	No
Switchroom phone requires MTA for class of service. [Major]		
Consoles powered through unused TNs are correctly programmed PWR. [Major]		
Consoles are cross-wired properly and must utilize consecutive units. [Major]		
The PBX maintenance modem and terminal server performs as expected. [Major]		

Observations and comments:

VoIP networking parameters

If Avaya Aura System Manager is to be deployed, the server should be located on the CLAN subnet. The TLAN and ELAN subnets should be made routable through a Layer 3 routing device. This configuration will allow System Manager access to the TLAN and ELAN elements without exposing the core system structure to CLAN traffic (including Broadcast, Multicast and DHCP). It is further recommended that a security policy such as an Access Control List (ACL) or equivalent be put in place to prevent unauthorized users or devices from entering the ELAN or TLAN subnets.

Item	Meets Specifications	
	Yes	No
A LAN or WAN assessment has been performed on the customer network. [Critical]		
The layer 2 switch ports are in place for the CS 1000E ELAN/TLAN are configured for auto, autonegotiate. [Major]		
The layer 3 switch ports are in place. [Major]		
The ELAN subnet contains only Communications Server 1000 equipment. Do not expose the ELAN subnet to any non-Avaya broadcasts, multicasts, or DHCP packets. The TLAN subnet is an isolated VOIP network that contains only the Communications Server 1000 elements, peripherals, and user endpoints. Configure peripherals and user endpoints, such as IP Phones, and soft phones in an additional isolated network subnet or in the CLAN. The CLAN is any customer subnet outside of the ELAN and TLAN subnets. The CLAN subnets are part of the customer's pre-existing network configuration. The ELAN, TLAN and CLAN subnets must be separated by layer 3 routing.		
The ELAN subnet and the TLAN subnet are on separate subnets. [Major]		
All applications on the ELAN subnet are on the same subnet. [Major]		
VGMC circuit cards in the same node are on the same TLAN subnet. [Major]		
Minimum of one DSP resource for every TDM port (T-1 trunks, digital phones, analog phones, analog trunks, Avaya CallPilot channels). For non-blocking requirements one DSP per TDM port is a best practice. [Recommendation]		
Layer 2 switches derive UPS power from different branch circuit sources, if possible, in order to minimize single-points of failure. [Recommendation]		
Layer 3 switches derive UPS power from different branch circuit sources, if possible, to minimize single-points of failure. [Recommendation]		

Observations and comments:

Product Bulletins for vintage and release updates

Product Bulletin	Affected Product	Part Description	Defective Part #	Replacement Part #	Reason for Change

Installation checklists

Related topics:

Remote access and Remote Access Service on page 92
Example timelines on page 94
Gotchas on page 97
Vintage requirements on page 103
Release 6.0 upgrade procedure on page 107
Release 7.0 upgrade procedure on page 109
Release 7.5 upgrade procedure on page 111
Release 7.6 upgrade procedure on page 114
UCM security issues on page 117
High scalability on page 118
Geographic redundancy on page 118
FAX issues with VoIP — MGCs on page 120

Remote access and Remote Access Service

Complete this checklist to ensure proper configuration of remote access to Communications Server elements and applications. If using Remote Access Service (RAS), two IP addresses must be provided to set up RAS for dial-in support. These IP addresses should be in sequence, and on the Nortel server subnet.

Check the items in the checklist to confirm that they have been completed. Provide additional information where requested. This checklist is to be completed and verified during coordination

conference calls. The Installation Coordinator is responsible for forwarding copies of this document to parties involved with installation.

The responsibilities for completing this checklist are as follows:

Checklist section	To be completed by Distributor	To be completed by Customer
LogMeIn Support		
Direct modem access		
RAS		
Other remote access support		

LogMeIn Support

Item	Meets Specifications		
	Yes	No	Date of availability
Internet Access to http://www.logmein123.com - confirm site access			
Validate LogMeIn Support is viable **Note:** This will require the site to establish a session with NRIUS support prior to the date of the work window.			

Direct modem access

	Date of availability
	_____

Note:

If you are using a modem, ensure the modem is connecting directly to the server being accessed.

What Communications Server 1000 elements will NRIUS have access to?

- _____
- _____
- _____
- _____
- _____

	Date of availability
• _____ • _____	

Note:

If modem assess is available to the CLI of the Primary Security Server, support will be able to SSH to any registered device.

RAS

	Date of availability
What network subnet range(s) will be accessible via RAS? • _____ • _____ • _____ • _____ • _____ • _____ • _____	_____

Note:

Two local IP addresses will be required to setup RAS for dial-in support. IP address assigned to RAS user (NRIUS) must be part of the Avaya subnet being worked on. These IP Addresses should be sequential.

Other remote access support

	Date
Please detail any alternative modes of remote access that can be provided:	_____

Example timelines

The order of operations described below are examples only. This document in no way defines a mandatory methodology for an upgrade. The order of operation and overlap will depend on the number of personnel and state/type of system to be upgraded.

The times and tasks included in the two examples below do not include additional tasks and timeframes required to prep and test applications such as CallPilot, Contact Center and other third party applications.

Single Communications Server 1000 system installed at a single site

The below estimated timeline assumes a Communications Server 1000 system at a single site with the following components running RLS 5.xx and one technician performing the work with no multitasking:

- 1 CP PM HA Call Server
- 2 TPS CP PM Signaling Servers
- 4 MC 32S VGW elements

1:30	Install UCM Server (Primary Security Server) (Linux Base, BIOS, Application/Database and Patching)
1:15	Upgrade CallServer Core1 (Inactive Core) (Linux Base, BIOS, Application/Database and Patching)
1:15	Upgrade Follower Signaling Server (Linux Base, BIOS, Application/Database and Patching)
1:15	Upgrade Leader Signaling Server (Linux Base, BIOS, Application/Database and Patching)
0:30	Upgrade MC32S cards (5 card simultaneous with 10 cards total)
0:30	Perform middle of the road acceptance testing. (Point of no return – back out here if test results require)
1:00	Upgrade CallServer Core0 (Linux Base, BIOS, Application/Database and patching)
0:30	Acceptance Testing

7.5 hours total estimate, with no lunch break.

Single Communications Server 1000 system installed at multiple sites

The below timeline assumes a Communications Server 1000 system at multiple locations with the following components running RLS 4.xx and three technicians performing the work with multitasking. Both NRS are Co-Res, one at the Main Site and the other at Site #1.

- Primary CPPM HA Callserver at main site
- Alternate CPPM N-Way CallServer #1 at site #1
- Alternate CPPM N-Way CallServer #2 at site #2
- Secondary CPPM N-Way CallServer #1 at site #3
- 2 TPS CPPM Signaling Servers at main site (one is Co-Res NRS)
- 1 TPS CPPM Signaling Server at each Alternate and Secondary site.

- 4 MC32S VGW Elements at main site
- 2 MC32S VGW Elements at each Alternate and Secondary site.

1:45	Tech #1: Install UCM Server (Primary Security Server) (Linux Base, BIOS, Application/Database and patching)
	Tech #2: Upgrade CallServer Core1 (Inactive Core) (Linux Base, BIOS, Application/Database and patching)
	Tech #3: Upgrade Follower Signaling Server (Linux Base, BIOS, Application/Database and patching)
1:00	Tech #2: Upgrade Leader Signaling Server (CO-Res TPS/NRS) (Linux Base, BIOS, Application/Database and patching)
0:15	Tech #3: Upgrade MC32S cards (simultaneous)
0:30	Tech #1: Perform middle of the road acceptance testing. (Point of no return – back out here if test results require)
1:15	Tech #1: Upgrade CallServer Core0 (Linux Base, BIOS, Application/Database and patching)
0:30	Tech #2: Travel time to remote site #1
	Tech #3: Travel time to remote site #2
2:00	Tech #2 and Tech #3 work simultaneously on remote 1 and remote 2
	Tech #2: Remote Site #1
	Tech #2: Upgrade Alternate CallServer #1
	Tech #2: Upgrade Signaling Server (CO-Res TPS/NRS)
	Tech #2: Acceptance Testing
	Tech #3: Remote Site #2
	Tech #3: Upgrade Alternate CallServer #2
	Tech #3: Upgrade Signaling Server
	Tech #3: Acceptance Testing
1:45	Tech #2: Remote Site #3
	Tech #2: Upgrade Secondary CallServer #1
	Tech #2: Upgrade Signaling Server
	Tech #2: Acceptance Testing
0:30	Travel time for Tech #2 and Tech #3 to return to Main Site
1:00	Acceptance Testing

8.5 Hours total estimate, with no lunch break.

Gotchas

Common Issues to be aware of

This tab contains a list of items that if properly prepared for will make the upgrade go smoothly. This is not an all inclusive list, and is also not intended to be used as a keystroke MOP for the solutions provided.

Core

Customer Database	If an attendant console exists on the current install of the Communications Server 1000 system, DO NOT choose Customer Database when upgrading to 6.0. You must choose Default Database and complete the install (including the Deplist Refresh) prior to converting the existing Database. PEP MPLR28682 MUST be present and active in the system prior to importing a customer database that has an attendant console configured. **Warning:** Failure to do so, will corrupt the customer database. If upgrading from a Pre- Release 4.5 to a system post 4.5 and the customer is using Symposium, they may need to turn on CMB in ld 23 for any CDN that goes into the Symposium. **Note:** LD23 prompt under the CDN section: Default is (NO) and from what the site is seeing, this should be set to (YES). For each CDN that they want the correct redirection taking place CMB (NO) YES Deny or Allow redirection to Control DN Mailbox. Symptom: Call goes via CDN to an Agent to a Voice mail, the Voice mail box response id is for the Agent and not for the CDN. If the customer desires it to go to the CDN VM then they will need to turn on CMB. Symptom: Upgrading from Release 25.40 to 6.00 can cause Dial Tone and Ring Back to sound like European (A-Law) and not North American (Mu-Law). Solution: Change the INTN (International Companding Law) from Yes to No and INIing the PBX.
Credentials	Do not use an exclamation point as part of the admin2 password. The ! character will abort the registration process. Do not use admin1, admin2, pdt1, or pdt2 as UserIDs in the UCM administrative users database. Do not use admin or any other UCM UserIDs in the Communications Server 1000 native PWD database. Do not use VxWorks UserIDs in the UCM database. UserID conflicts causes security permission issues which may cause the system to deny access during critical maintenance procedures.

Note:

If admin2 UserID is even present and disabled in UCM prevents admin2 from logging into a VxWorks CallServer.

FIJI	When single slot FIJI cards are deployed, the Loadware (version 29) must be manually downloaded and deployed to allow the cards to complete the FDL process. When seating the new single slot cards, use the following rules: • Core/Net: Slot 9 (leaving slot 8 empty) • Network: Slot 2 (leaving slot 3 empty) **Warning:** Do not use slot 3 or slot 8 for ANYTHING. These slots must be left empty at all times. **Warning:** All double slot FIJI cards MUST be updated to Loadware version 21 PRIOR to installing any single slot FIJI cards. If this process is not done properly, the double slot FIJIs will not function correctly. MPLR26629 can then be loaded. (note that MPLR26629 has been superseded by MPLR28213). **Note:** If upgrading from IGS to FNF ensure the jumper RN27 at location E35 on all 3PE cards are set to the "A" position.
CPSI ports	Also known as Core TTYs. Prior to upgrading, ensure that at least one CPSI port is defined in the ADAN database. In an HA CallServer configuration, the upgrade will proceed as expected until the offline core boots into the new release. At this time the installer will only have access to PDT (no overlay loader prompt will be seen). This is due to no CPSI ports being configured in the upgraded customer database. To resolve this, the installer creating the CPSI port must restore the old release of software. Or, if the system had a PTY configured, they could access the upgraded core using PTY and then build the CORE TTY(s).
3PEs	The RN27 jumper needs to be on the A position (toward the faceplate) on ALL 3PEs
Sys Util Card	With older Card Cages and CP IV you may encounter issues unless you have Sys Util Card. You may get a Dongle error.
Signaling Server	Associate the Signaling Server with the UCM Domain: 1. Logout of the existing local-login session. 2. Enter the servers network login address in the format https://<server address>/network-login. 3. Login using admin credentials, not admin2.

A list of UCM Elements appears.

4. Under CS1000 Services on the left-hand menu, select Software Deployment.
5. When prompted, enter the admin credentials.
6. CS 1000 elements to join the domain. Enter the admin credentials. The Deployment View appears.
7. Make changes on the Deployment View screen.
   a. On the right-hand side, change the view from Servers to CS 1000 systems.
   b. Click Add.
   c. Enter the host name for the CS 1000 System.
   d. Enter an optional description if desired.
   e. Click Next.
   f. Validate the Keycodes.
   g. Select the languages.
   h. Select the database.
   i. Add the Signaling Server.
      Select this server from the drop down list of Signaling Servers.
   j. Click Finish.
   k. The Deployment View displays a CS 1000 tree of elements.
   l. Change the view from CS 1000 systems to Servers.
   m. Click Commit.

Pre-loaded Hard Drive

BIOS

Any CPPM card used for Release 6.0 must be running version 18 BIOS. A fresh install of 6.0 will automatically check the card and upgrade the BIOS for you, however if a pre-loaded hard drive is to be used, care must be taken to ensure the BIOS is upgraded.
When using a pre-loaded HDD, take the following steps to ensure the BIOS is upgraded:

1. Boot the CPPM card, noting the BIOS version displayed during POST (BIOS version number is located in the bottom right corner of the POST banner).
2. If a Linux Base SDC is not available on Site, Using a 2GB Compact Flash Card, create an SDC using the current version of CardPro

(obtain the SDC software and the current version of CardPro from avaya.com).

3. Boot the CPPM into the install program, enter the tools menu and select the BIOS upgrade option.

Date/Time	When installing a pre-loaded HD into a CPPM or other compatible element, The initial password change may fail with a message indicating the password is too new. This issue may occur when the element being used cannot find a valid Time Server on the network. To resolve this, manually change the Linux Date and then update the password.

MC32 (VGMC)

Firmware	MC32 cards (either the NTVQ01BA or BB vintage) should be updated to the most current version of firmware. Note that the BA vintage card has a different current version of firmware than the BB vintage card. When performing the upgrade process as documented in NTP (553-3001-204 or NN43100-500) and version 2.2 of the firmware upgrade bulletin, it should be noted that the PDT login and password must be used instead of the admin level 1 indicated. To prevent overwriting previous release files, MPLR24008 must be loaded onto the MC32 cards before upgrading from release 4.5 to 6.0+. MC32 cards cannot be changed from leader to follower after upgrade. Confirm the Leader flag is not set before upgrade, the 'itgCardShow' command should be executed in IPL shell on SMC card or OAM shell on MC32s card. If an output contains "Role : Leader" string, the Leader flag is set. (Avaya Bulletin: PSN003377u)

FQDN

Domain	If the Primary Security Server Domain is entered incorrectly, the element must be reinstalled from scratch.
Hostname	If the host name is entered incorrectly, it can be changed via the networkconfig command accessed while in Linux CLI.

UCM

Patching	The Linux Base SU and SP patches MUST be loaded after completing the appinstall process but prior to performing the UCM Security Configuration. Failure to do so may cause database corruption. Release 6 does not support Internet Explorer 7.0 and above. Release 7 supports Internet Explorer 6.0, 7.0 and 8.0. Other browser types and versions are not supported.
Date/Time	If the date is not changed to the current date when installing a Linux server the certificates may fail.

Security config	A few sites have experienced the following behaviour: After completing the global security configuration process (when the new browser is opened and the UCM screen appears) the Gobal Security configuration appears to have not yet been completed. This is due to an error in the HOST or FQDN entry used. To resolve this check the HOST and FQDN configuration in Linux to ensure it is correct.
Certificate creation	Certain characters (listed below) cannot be used in the certificate descriptive fields (such as the organization field). Avaya recommends that only alpha/numeric characters be used. Do not use a space or # sign as the first character Do not use a space as the last character Do not use a comma, plus sign, quote symbol, backslash, less than, greater than, or semi-colon in any part of these fields.
Logging in	When installing, upgrading or working with UCM framework (to get access to the UCM element list), you must use the FQDN of the UCM server to log in. If the browser being used is connected to the LAN via a non-routed ELAN subnet, the login attempts will fail, and the session may be directed to the base manager. Once Base Manager has been installed, it is best practice to use the TLAN subnet to configure and administer the UCM elements. ** To maintain a supported configuration, the TLAN subnet is routable to the CLAN subnet or at minimum to a subnet where the IP Phones will reside. If the deployment is to be in an isolated network where the only devices on the CLAN are the IP Phones, a DNS server must be deployed and configured as part of the CS1K installation and located on the TLAN subnet.

System Manager

You must use FQDN to access EM via System Manager. IP is acceptable for System Manager and UCM, but not EM.

Meridian Mail

Not supported	Meridian Mail is physically not supported under Release 5.x+ If the site to be upgraded currently has a Meridian Mail installed, it must be migrated or upgraded to a CallPilot or other supported voice mail system prior to deploying the new Call Server software. All hardware and software configurations relating to Meridian Mail must be removed from the Call Server prior to upgrade. Once the upgrade has been completed, the ENET card configuration cannot be removed. In the event the Meridian Mail is scheduled to be upgraded or migrated during the same timeframe as the Call Server, then an EDDY should be completed prior to removing the Meridian Mail configuration for blackout purposes. An additional EDDY must be completed without the Meridian Mail configurations to be used during the Call Server upgrade.

Network

Layer 2	ACLs (Access Control Lists) require MAC Addresses of new hardware (CP-PM, COTS) to be added or else you can experience one-way speech issues.

FAX

Fax between MGC/X cabinets is a VOIP call. Special concideration is required for Fax over VOIP. See TAB on FAX for details.

MGxPEC

Gold Image on MGxPEC will fail loading FPGA. Install CSP LW first. (Release 7.X)

6.00.18

In December 2009 the Linux Base Software for CS 1000 Release 6.0 systems was upgraded from 6.00.18 to 6.00.18.62 to accommodate the deployment of IM and Presence functionality. At that time, all previous patches for 6.00.18.00 had been integrated into the 6.00.18.62 base.

At this time, patch support for Linux Base Software 6.0.18.00 is being discontinued. For any future patching requirements, the base software will need to be upgraded to 6.00.18.62 at a minimum.

Systems not requiring patch support at this time can remain on 6.00.18.00.

Systems requiring patch support will need to be upgraded to Linux Base Software version 6.00.18.62 prior to being patched. Upgrade to 6.00.18.62 before logging any cases against older software releases.

Misc

The IBM 3350 COTS server requires a null cable, not the cable that came with the ISP-1100.

Option 11C — Automatic conversion is supported directly from an Option 11C. The conversion will require an upgrade to a CP PM, CP DC processor and MGC, or CP MG, not a CP PIV.

Option 61/81 and CS 1000M SG & MG to CS 1000E Database Conversions

An Option 61/81, CS 1000M SG/MG database being migrated to a new CS 1000E database requires modifications to the data to create a new CS 1000E database. However there is no supported software tool, or “in-house conversion” (IHC) codes, to provide the database conversion from an Option 61/81, CS 1000M SG&MG to CS 1000E .

When considering an Option 61/81, CS 1000M SG/MG to CS 1000E migration quote or order, Avaya recommends including an item to cover the cost of the CS 1000E database conversion. This line item on the quote or order will cover the time needed to manually create the new CS 1000E database from the Option 61/81 or CS 1000M SG/MG data.

Do not use a DCH that starts with a 1 on a 1000E Co-res

3900 sets upgrade prior to upgrade window

It is mandatory for all Communications Server 1000 customers upgrading to rls 6.0 to have their M3900 sets upgraded to the latest firmware version prior to the core upgrade, failing to do so will cause problems with M3900 sets during Transfer call scenarios.

A fix for CR (Q01805423-01: 390x during a transfer call have no "Conf" softkey) was introduced. This fix contains changes in both core and Taurus firmware, if Communications Server 1000 system is upgraded to Release 6.0 without upgrading M3900 sets then during the transfer scenario, after the second leg of the call is answered the connect key will not appear.

Vintage requirements

Release 5.5 and 6.0 have minimum vintage requirements for a number of cards and applications. This section contains a list of items that if present in the system must either be removed or updated to a minimum vintage as specified.

Note:

This list may not represent an all inclusive list of cards and vintages. Be sure to reference the GRB document for the release about to be installed to verify all requirements are met.

The General Release Bulletin (GRB) for the version of software to be installed should be read through to ensure all requirements are met. In addition, the document *NN43001-140 Product Compatibility Matrix* should be used to verify minimum vintages and application interoperability levels.

Release 5.5

Minimum Releases: Cards or applications with vintages not listed below must be replaced prior to or part of upgrade procedures.

PEC	Description	Minimum vintage	Notes
NTRB53	Clock Controller	AA and later	
NTRB53	Dual port DTI/PRI	AC, AD, AG and AH	
NTRB53	Line Side T1	AE Release 3	
NTRB53	DTI/PRI2	AB and AD	
NTRB53	FIJI Double Slot	AF (with version 21 Loadware)	
NTRB53	FIJI Single Slot	BB (with version 29 Loadware)	
NTRB53	3 Port Ext (3PE)	F	

PEC	Description	Minimum vintage	Notes
NTRB53	PerSig	R	Bulletin 2007007688, Rev 2
NTRB53	DC Power Supp	CA	
NTRB53	AC Power Supp	BA Rls 1	Possible issues with Rls 3&4
NTRB53	CNI	AC	
NTRB53	Utility Card	BA	
NTRB53	Core/Net Shelf	AA or AB	
NTRB53	Core/Net Module	AB AC DB DC	
NTRB53	CP-PIV CPU	AA or AAE6	
NTRB53	4 Port SDI Paddle	BB	
NTRB53	MSDL	AB or AC	
NTRB53	Clock Controller	Allowed only on 61C	
NTRB53	SSC CPU Contact Center Telephony Manager	HA JA Release 4.2 Release 3.1 SU2	

No Longer Supported: The below cards and applications MUST be removed from the system prior to or part of upgrade procedures.

PEC	Description	Replacement PEC	Description	Notes
QPC139	2 port SDI	NT8D41BB	4 Port Paddleboard	
QPC444	Conference	NT8D17	Conf/TDS	
QPC471	Clock Controller	NTRB53	Global Clock Ctrlr	QPC471 Supported for Opt 61
QPC775	Clock Controller	NTRB53	Global Clock Ctrlr	QPC775 Supported for Opt 61
QPC412	IGS	Contact your Avaya Sales Engineer		Fiber Network Required
NT5D30	DIGS	Contact your Avaya Sales Engineer		Fiber Network Required

PEC	Description	Replacement PEC	Description	Notes
QPC417	Junctor Board IGM	Contact your Avaya Sales Engineer		Fiber Network Required
NT6D65	CNI	NT4N65C	cPCI CNI	
NTRB34	CNI-3	NT4N65C	cPCI CNI	
NT5D21	Core/Net Module	NT4N41	Core/Net Module	
NT5D61	IODUC	Contact your Avaya Sales Engineer		
CNI Cables	CNI Cables	NT4N29AA	cCNI to 3PE Cable	
NT5D03	CPU CP3	NT4N39	CP PIV	
NT5D10	CPU CP4	NT4N39	CP PIV	
QPC472	DTI	NT5D12	Dual Port PRI	
QPC536	DTI 2MB	NT5D97	Dual Port PRI	
QPC720	PRI/DTI	NT5D12	Dual Port PRI	
QPC473	DTI	NT5D97	Dual Port PRI	
QPC786	Digital Trunk and DB	Contact your Avaya Sales Engineer		
NT8D72	PRI interface	Contact your Avaya Sales Engineer		
NTCK43	PRI2	NT5D97	Dual Port PRI	
QPC757	DCHI	NTBK57	DCHI DB	
NT8D74	Clock to IGM Cable	Contact your Avaya Sales Engineer		Fiber Network Required
NT8D76	IGS to IGM Cable	Contact your Avaya Sales Engineer		Fiber Network Required
n/a	Companion Cards	Contact your Avaya Sales Engineer		WLAN Required

PEC	Description	Replacement PEC	Description	Notes
n/a	IGM Terminators	Contact your Avaya Sales Engineer		Fiber Network Required
n/a	Meridian Max	n/a	Contact Center 4.2	
n/a	Meridian Mail	n/a	CallPilot 5.0	
n/a	OTM	n/a	Telephony Manager 4.0	

Release 6.0, 7.x

Minimum Releases: Items listed above apply to Release 6.0 as well as the additional items list below.

Note:

Items listed under 6.0 override any status under 5.x.

PEC	Description	Minimum Vintage	Notes
	Contact Center	Release 6.0	
	CallPilot	Release 5.0	
	Telephony Manager	Release 4.0	

No Longer Supported: The below cards and applications MUST be removed from the system prior to or part of upgrade procedures.

PEC	Description	Replacement PEC
A0810496	CP PII CPU	Contact your Avaya Sales Engineer
NT4N43	cPCI MMDU	Contact your Avaya Sales Engineer
NT4N46	cPCI Card Cage	Contact your Avaya Sales Engineer
NT4N48	cPCI Sys Util	Contact your Avaya Sales Engineer
NTDK19	SSC Upgrade Kit	Contact your Avaya Sales Engineer
NTDK20	SSC CPU	Contact your Avaya Sales Engineer
NTDK50	Main/Expansion Cabinet	Contact your Avaya Sales Engineer
NTDU22	Branch Office	Contact your Avaya Sales Engineer
NTDU23	Media Gateway Expansion	Contact your Avaya Sales Engineer
NTDU24	Media Gateway Trunks	Contact your Avaya Sales Engineer

PEC	Description	Replacement PEC
NTDU25	Media Gateway Cable Kit	Contact your Avaya Sales Engineer
NTDU27	ISP1100 SS	Contact your Avaya Sales Engineer

Release 6.0 upgrade procedure

If upgrading from any release and adding COTS servers or new CP PMs, these devices can have Linux base installation , Linux base patches, and UCM security configuration performed ahead of time.

Before performing an upgrade, back up the database, then disable IPSEC/centralized authenthication (leave security domain). Otherwise, this may cause issues such as elements not being able to join the UCM domain.

Installation steps

Perform the following for each CP PM or COTS server to be installed.

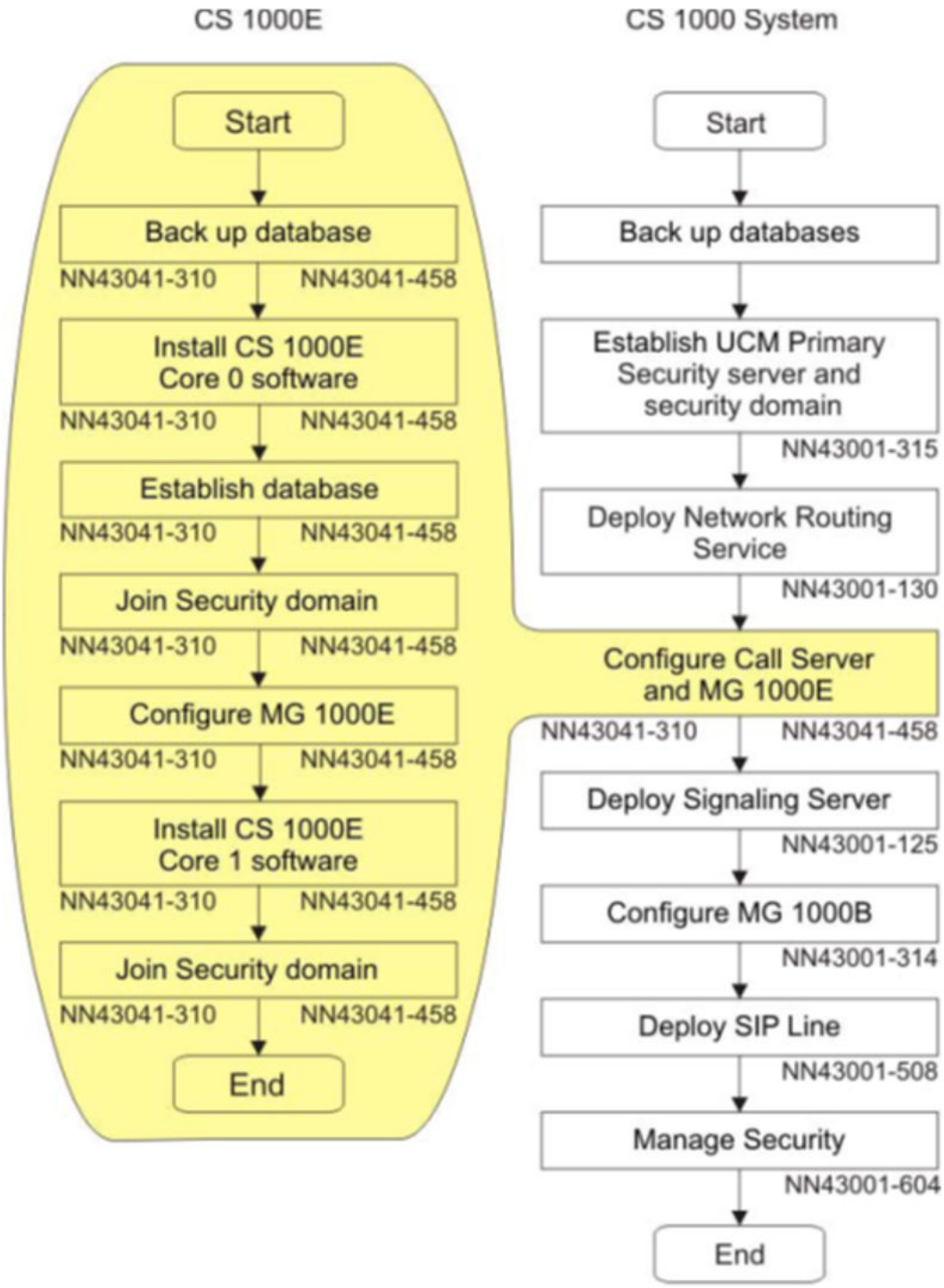
1. Linux base installation:
    a. Install Linux base on a CP PM or COTS server (see *NN43001-315, Linux Platform Fundamentals*)
    b. Install Linux base patches (see product Bulletin from ESPL)
    c. Configure Security with UCM (see *NN43001-116, UCM Fundamentals*)
    d. Upload the nai file in order to deploy the applications.
    e. Deploy Applications with Deployment Manager (SS, NRS, EM) (see *NN43001-315, Linux Platform Fundamentals*)
    f. Apply Service Pack (see https://espl.avaya.com/espl/)

    Note:
    The SP is currently being posted as a zip file but must be renamed from .zip to .ntl once saved to your desktop.
2. Restore old database to new platform:
    a. Convert old database with Database Utility Conversion Tool
    b. Put RMD (CF/USB) in CP PM or CP PIV or COTS
    c. Restore Database
    d. Reboot Call Server to active database.
3. Install new NRS Database:
    a. Save NRS database from ISP1100 to desktop NRSbackup.tar
    b. Log into Primary Security Server

c. Select Elements > Primary NRS

d. Log in and configure the new NRS database

For other flow charts, see *NN43001-100, Library Reference*.



Release 7.0 upgrade procedure

If upgrading from any release and adding COTS servers or new CP PMs, these devices can have Linux base installation , Linux base patches, and UCM security configuration performed ahead of time.

Before performing an upgrade, back up the database, then disable IPSEC/centralized authenthication (leave security domain). Otherwise, this may cause issues such as elements not being able to join the UCM domain.

When upgrading Release 6.0 and 7.0 the upgrade can be pushed from the Deployment Server.

Installation steps

Perform the following for each CP PM or COTS server to be installed.

1. Linux base installation (Primary UCM server):
    a. Install Linux base on a CP PM or CP MG or CP DC or COTS server (see *NN43001-315, Linux Platform Fundamentals*)
    b. Install Linux base patches (see product Bulletin from ESPL)
    c. Configure Security with UCM (see *NN43001-116, UCM Fundamentals*)
    d. Upload the nai file in order to deploy the applications (see *NN43001-315, Linux Platform Fundamentals*).
    e. Create the Deployment view (see *NN43001-315, Linux Platform Fundamentals*).
    f. Deploy Applications with Deployment Manager (SS, NRS, EM) (see *NN43001-315, Linux Platform Fundamentals*)
    g. Apply Service Pack (see https://espl.avaya.com/espl/)

    Note:

    The SP is currently being posted as a zip file but must be renamed from .zip to .ntl once saved to your desktop.
2. Linux base installation (Member UCM server):
    a. Install Linux base on a CP PM or COTS server (see *NN43001-315, Linux Platform Fundamentals*)
    b. Install Linux base patches (see product Bulletin from ESPL)
    c. Configure Security with UCM (see *NN43001-116, UCM Fundamentals*)
    d. Create the Deployment view on the Primary UCM server (see *NN43001-315, Linux Platform Fundamentals*).
    e. Deploy Applications with Deployment Manager (SS, NRS, EM) (see *NN43001-315, Linux Platform Fundamentals*)

3. Restore old database to new platform:
    a. Convert old database with Database Utility Conversion Tool - this is to convert floppies to CF.
    b. Put RMD (CF/USB) into CP PM, CP PIV, CP MG, CP DC or COTS.
    c. Restore Database.
    d. Reboot Call Server to active database.
4. Install new NRS Database:
    a. Save NRS database from ISP1100 to desktop NRSbackup.tar
    b. Log into Primary Security Server
    c. Select Elements, Primary NRS
    d. Log in and configure the new NRS database

Linux SP installation for new system installations

Note:

This information is subject to change. Refer to the Product bulletin in ESPL.

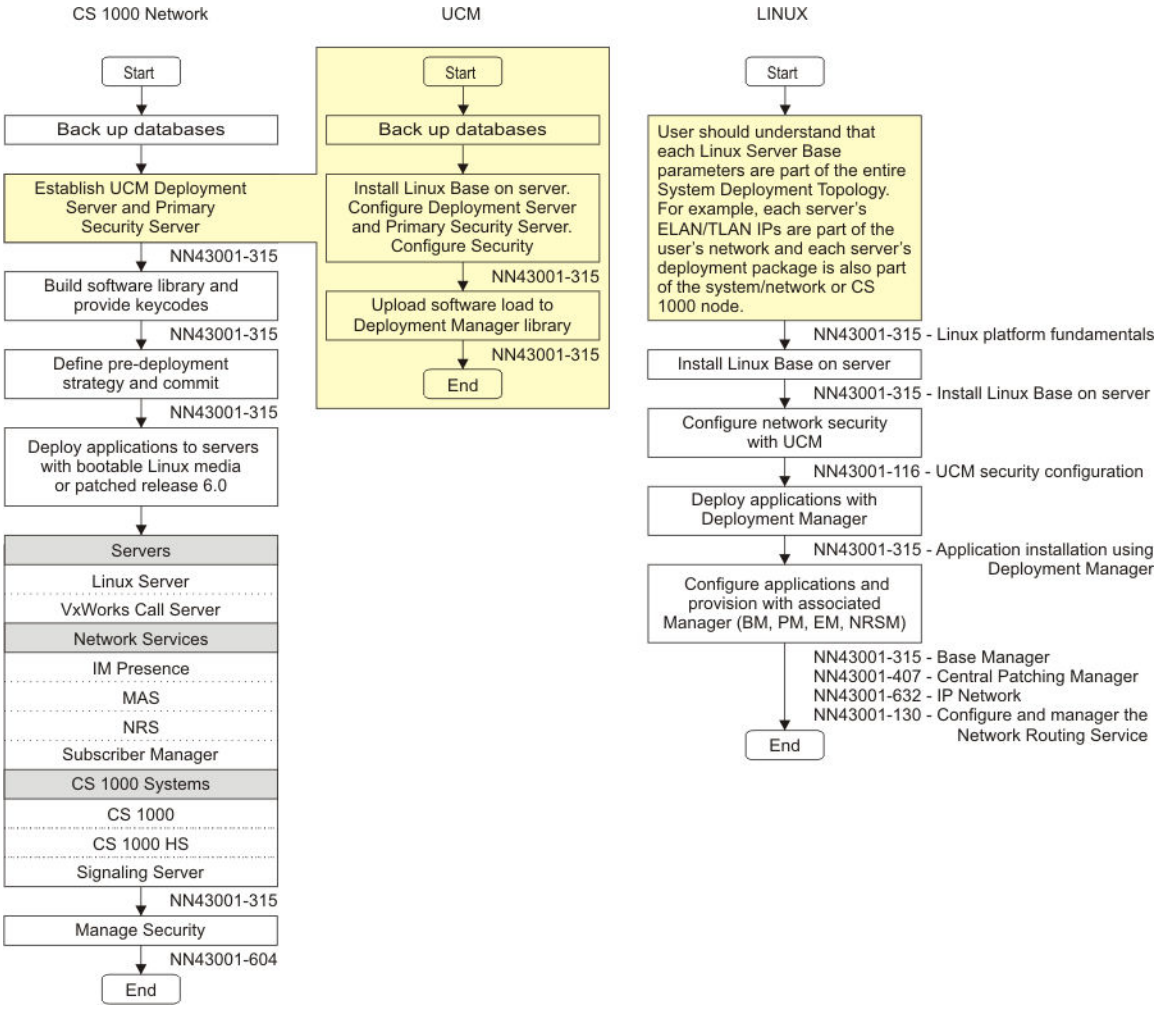
1. Upgrade the UCM primary security server to Release 7.0 software
2. Next, install the latest ‘Linuxbase’ SU on the UCM Primary Security using CLI
    a. upload nortel-cs1000-linuxbase-7.00.20.10-02.i386.000.ntl to /var/opt/nortel/patch.
    b. pload nortel-cs1000-linuxbase-7.00.20.10-02.i386.000.ntl
    c. c. pins <patch handle #>
3. Install the Baseweb SU on the UCM Primary Security Server using CLI method.
    a. upload nortel- cs1000-baseWeb-7.00.20.10-00.i386.000.ntl to /var/opt/nortel/patch directory
    b. pload nortel-cs1000-baseWeb-7.00.20.10-00.i386.000.ntl
    c. pins <patch handle #>
4. Install the Patchweb SU on the UCM Primary Security Server using CLI method.
    a. upload nortel-cs1000-patchWeb-7.00.20.10-01.i386.000.ntl to /var/opt/nortel/patch directory
    b. pload nortel-cs1000-patchWeb-7.00.20.10-01.i386.000.ntl
    c. pins <patch handle #>
5. Upload and install the SP on the UCM Primary Security (UCM Patch Manager can be used).

    Note:

    SU’s/patches will only be applied if the Linux Applications are present. Applications should be deployed first. If the Linux Base has been deployed only

at installation or upgrade, then it will be required to reapply the SP after new applications are added.

6. Upgrade the member servers to Release 7.0 software using the Deployment Manager .
7. Install the Linuxbase SU to the Backup/Member Servers using UCM Patch Manager or CLI.
8. Install the Baseweb and Patchweb SUs to the Backup/Member Servers using UCM Patch Manager.
9. Install the Service Pack to the Backup/Member Servers using UCM Patch Manager (Base Manager or CLI can also be used).



Release 7.5 upgrade procedure

7.50Q/7.50.17

If upgrading from any release and adding COTS servers or new CP PMs, these devices can have Linux base installation , Linux base patches, and UCM security configuration performed ahead of time.

Before performing an upgrade, back up the database, then disable IPSEC/centralized authenthication (leave security domain). Otherwise, this may cause issues such as elements not being able to join the UCM domain.

When upgrading Release 6.0 and 7.0 the upgrade can be pushed from the Deployment Server.

Installation steps

Perform the following for each CP PM or COTS server to be installed.

1. Linux base installation (Primary UCM server):
    a. Install Linux base on a CP PM or CP MG or CP DC or COTS server (see *NN43001-315, Linux Platform Fundamentals*)
    b. Install Linux base patches (see product Bulletin from ESPL)
    c. Configure Security with UCM (see *NN43001-116, UCM Fundamentals*)
    d. Upload the nai file in order to deploy the applications (see *NN43001-315, Linux Platform Fundamentals*).
    e. Create the Deployment view (see *NN43001-315, Linux Platform Fundamentals*).
    f. Deploy Applications with Deployment Manager (SS, NRS, EM) (see *NN43001-315, Linux Platform Fundamentals*)
    g. Apply Service Pack (see https://espl.avaya.com/espl/)

    Note:

    The SP is currently being posted as a zip file but must be renamed from .zip to .ntl once saved to your desktop.
2. Linux base installation (Member UCM server):
    a. Install Linux base on a CP PM or COTS server (see *NN43001-315, Linux Platform Fundamentals*)
    b. Install Linux base patches (see product Bulletin from ESPL)
    c. Configure Security with UCM (see *NN43001-116, UCM Fundamentals*)
    d. Create the Deployment view on the Primary UCM server (see *NN43001-315, Linux Platform Fundamentals*).
    e. Deploy Applications with Deployment Manager (SS, NRS, EM) (see *NN43001-315, Linux Platform Fundamentals*)
3. Restore old database to new platform:
    a. Convert old database with Database Utility Conversion Tool
    b. Put RMD (CF/USB) into CP PM, CP PIV, CP MG, CP DC or COTS.

c. Restore Database

d. Reboot Call Server to active database.

4. Install new NRS Database:

a. Save NRS database from ISP1100 to desktop NRSbackup.tar

b. Log into Primary Security Server

c. Select Elements, Primary NRS

d. Log in and configure the new NRS database

Linux SP installation for new system installations

Note:

This information is subject to change. Refer to the Product bulletin in ESPL.

1. Upgrade the UCM primary security server to Release 7.5 software
2. Next, install the latest ‘Linuxbase’ SU on the UCM Primary Security using CLI

a. upload cs1000-linuxbase-7.50.17.xx-xx.i386.000.ntl to /var/opt/nortel/patch

b. pload cs1000-linuxbase-7.50.17.xx-xx.i386.000.ntl

c. pins <patch handle #>

3. Install the Baseweb SU on the UCM Primary Security Server using CLI method.

a. upload cs1000-baseWeb-7.50.17.xx-xx.i386.000.ntl to /var/opt/nortel/patch directory

b. pload cs1000-baseWeb-7.50.17.xx-xx.i386.000.ntl

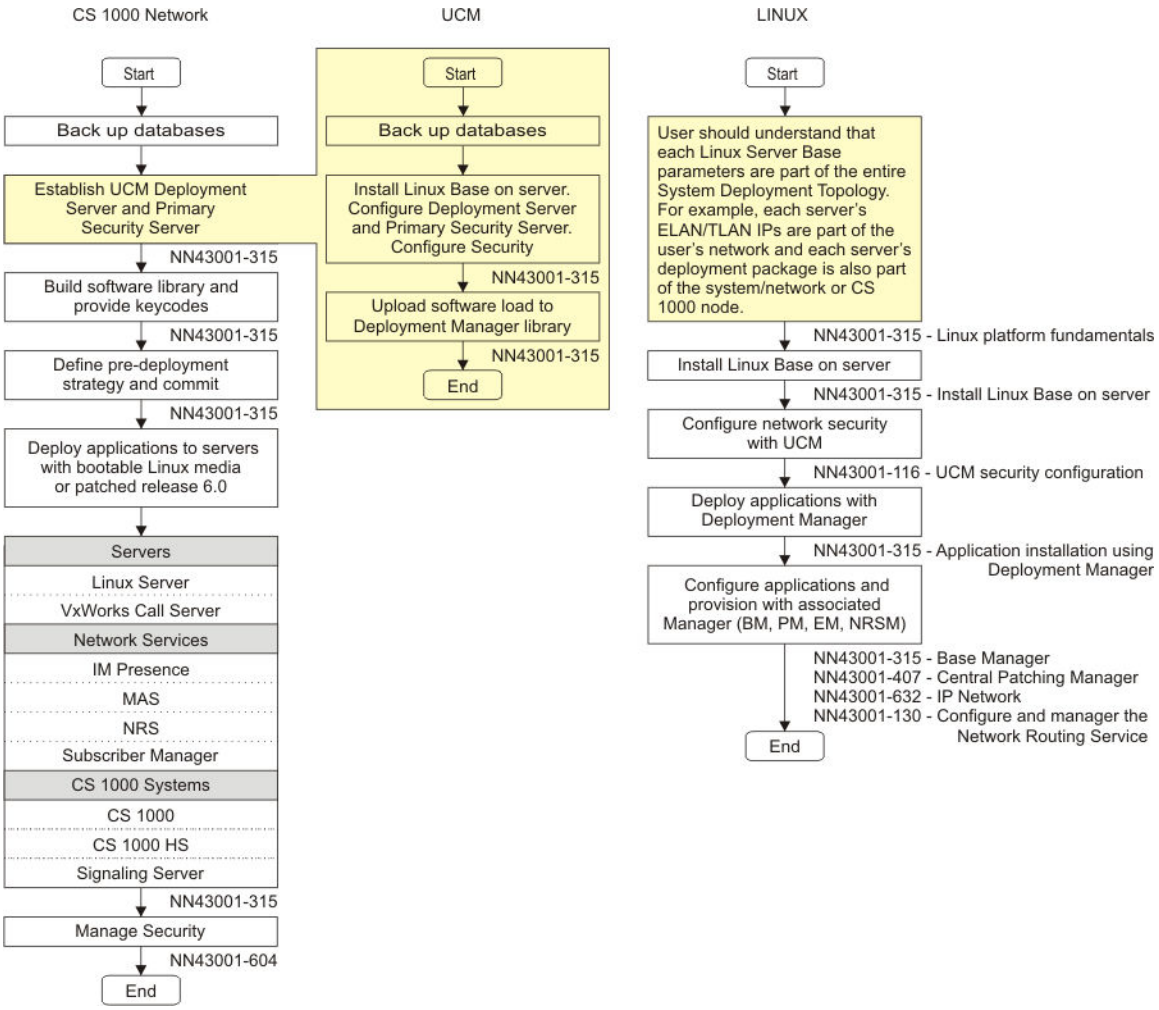
c. pins <patch handle #>

4. Upload and install the SP on the UCM Primary Security (UCM Patch Manager can be used).

Note:

SU’s/patches will only be applied if the Linux Applications are present. Applications should be deployed first. If the Linux Base has been deployed only at installation or upgrade, then it will be required to reapply the SP after new applications are added.

5. Upgrade the member servers to Release 7.5 software using the Deployment Manager .
6. Install the Linuxbase SU to the Backup/Member Servers using UCM Patch Manager or CLI.
7. Install the Baseweb and Patchweb SUs to the Backup/Member Servers using UCM Patch Manager.
8. Install the Service Pack to the Backup/Member Servers using UCM Patch Manager (Base Manager or CLI can also be used).



Release 7.6 upgrade procedure

If upgrading from any release and adding COTS servers or new CP PMs, these devices can have Linux base installation , Linux base patches, and UCM security configuration performed ahead of time.

Before performing an upgrade, back up the database, then disable IPSEC/centralized authenthication (leave security domain). Otherwise, this may cause issues such as elements not being able to join the UCM domain.

When upgrading Release 6.0 and 7.0 the upgrade can be pushed from the Deployment Server.

Installation steps

Perform the following for each CP PM or COTS server to be installed.

1. Linux base installation (Primary UCM server):
    a. Install Linux base on a CP PM or CP MG or CP DC or COTS server (see *NN43001-315, Linux Platform Fundamentals*)
    b. Install Linux base patches (see product Bulletin from ESPL)
    c. Configure Security with UCM (see *NN43001-116, UCM Fundamentals*)
    d. Upload the nai file in order to deploy the applications (see *NN43001-315, Linux Platform Fundamentals*).
    e. Create the Deployment view (see *NN43001-315, Linux Platform Fundamentals*).
    f. Deploy Applications with Deployment Manager (SS, NRS, EM) (see *NN43001-315, Linux Platform Fundamentals*)
    g. Apply Service Pack (see https://espl.avaya.com/espl/)

    Note:
    The SP is currently being posted as a zip file but must be renamed from .zip to .ntl once saved to your desktop.
2. Linux base installation (Member UCM server):
    a. Install Linux base on a CP PM or COTS server (see *NN43001-315, Linux Platform Fundamentals*)
    b. Install Linux base patches (see product Bulletin from ESPL)
    c. Configure Security with UCM (see *NN43001-116, UCM Fundamentals*)
    d. Create the Deployment view on the Primary UCM server (see *NN43001-315, Linux Platform Fundamentals*).
    e. Deploy Applications with Deployment Manager (SS, NRS, EM) (see *NN43001-315, Linux Platform Fundamentals*)
3. Restore old database to new platform:
    a. Convert old database with Database Utility Conversion Tool
    b. Put RMD (CF/USB) into CP PM, CP PIV, CP MG, CP DC or COTS.
    c. Restore Database
    d. Reboot Call Server to active database.
4. Install new NRS Database:
    a. Save NRS database from ISP1100 to desktop NRSbackup.tar
    b. Log into Primary Security Server
    c. Select Elements, Primary NRS
    d. Log in and configure the new NRS database

Linux SP installation for new system installations

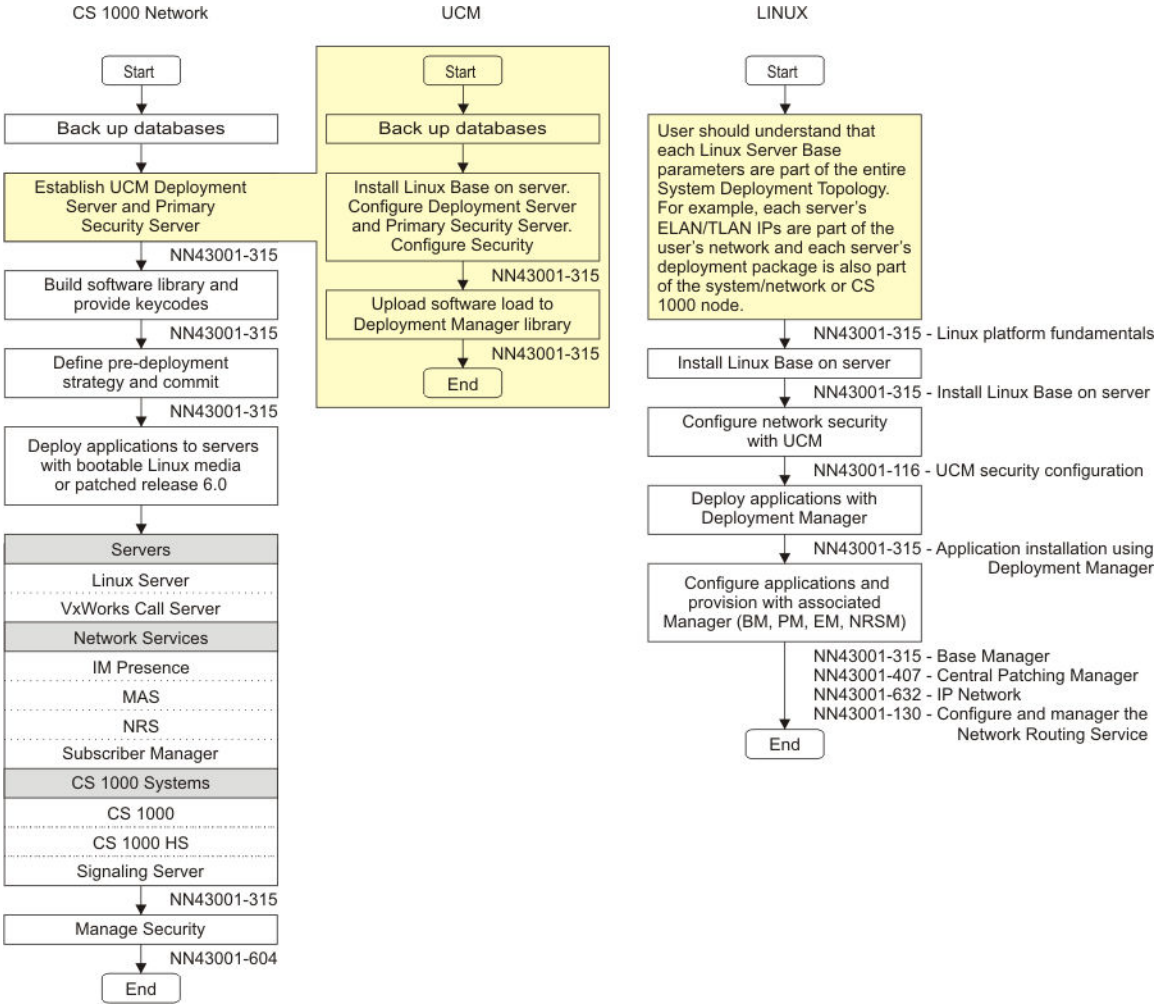
Note:

This information is subject to change. Refer to the Product bulletin in ESPL.

1. Upgrade the UCM primary security server to Release 7.6 software
2. Next, install the latest ‘Linuxbase’ SU on the UCM Primary Security using CLI
    a. upload cs1000-linuxbase-7.60.17.xx-xx.i386.000.ntl to /var/opt/nortel/patch
    b. pload cs1000-linuxbase-7.60.17.xx-xx.i386.000.ntl
    c. pins <patch handle #>
3. Install the Baseweb SU on the UCM Primary Security Server using CLI method.
    a. upload cs1000-baseWeb-7.60.17.xx-xx.i386.000.ntl to /var/opt/nortel/patch directory
    b. pload cs1000-baseWeb-7.60.17.xx-xx.i386.000.ntl
    c. pins <patch handle #>
4. Upload and install the SP on the UCM Primary Security (UCM Patch Manager can be used).

    Note:

    SU’s/patches will only be applied if the Linux Applications are present. Applications should be deployed first. If the Linux Base has been deployed only at installation or upgrade, then it will be required to reapply the SP after new applications are added.
5. Upgrade the member servers to Release 7.6 software using the Deployment Manager .
6. Install the Linuxbase SU to the Backup/Member Servers using UCM Patch Manager or CLI.
7. Install the Baseweb and Patchweb SUs to the Backup/Member Servers using UCM Patch Manager.
8. Install the Service Pack to the Backup/Member Servers using UCM Patch Manager (Base Manager or CLI can also be used).



UCM security issues

VxWorks Element request to join UCM

End User must confirm the confirm the fingerprint of the public key given to it from UCM

The VxWorks Element sends the password to UCM to authenticate

The VxWorks Element stores the UCM SSH key in /e/keys/xxx.xxx.xxx.xxx.properties

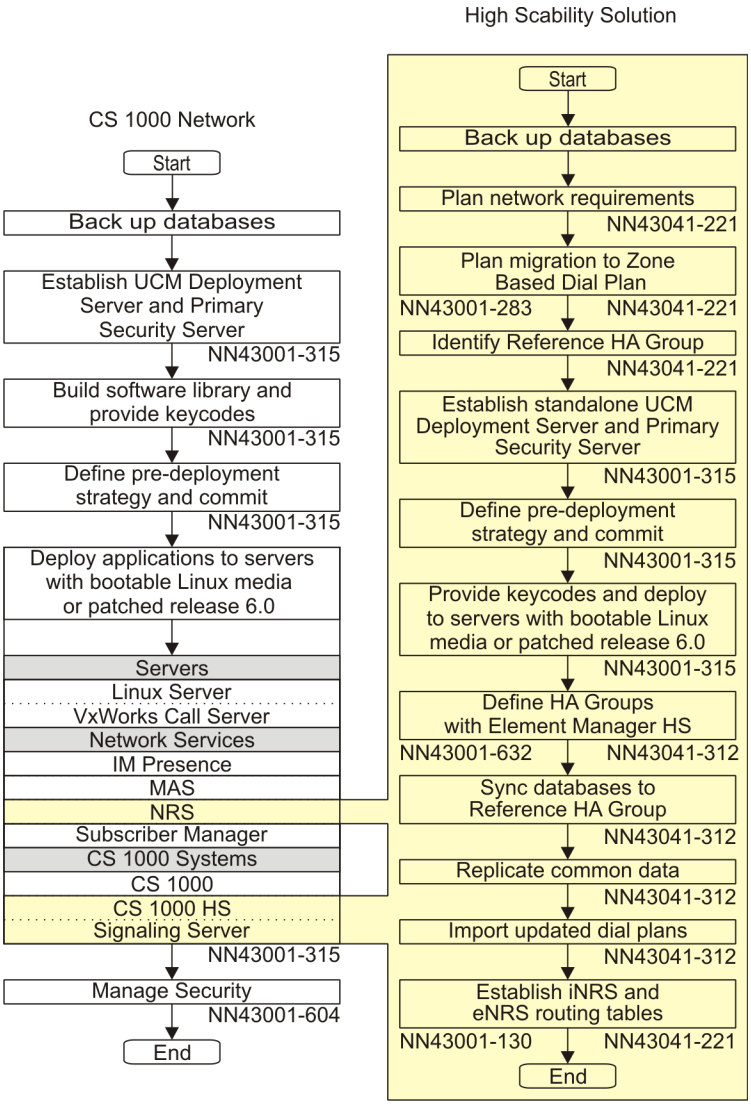
NFC API to sftp properties file to the UCM under directory: /var/opt/nortel/Jboss-Quantum/conf/elementRegistry/element/deployed

To view the content the files: cat <filename>

The registration process on UCM can be viewd in the server.log file /var/opt/nortel/Jboss-Quantum/log/server.log

High scalability

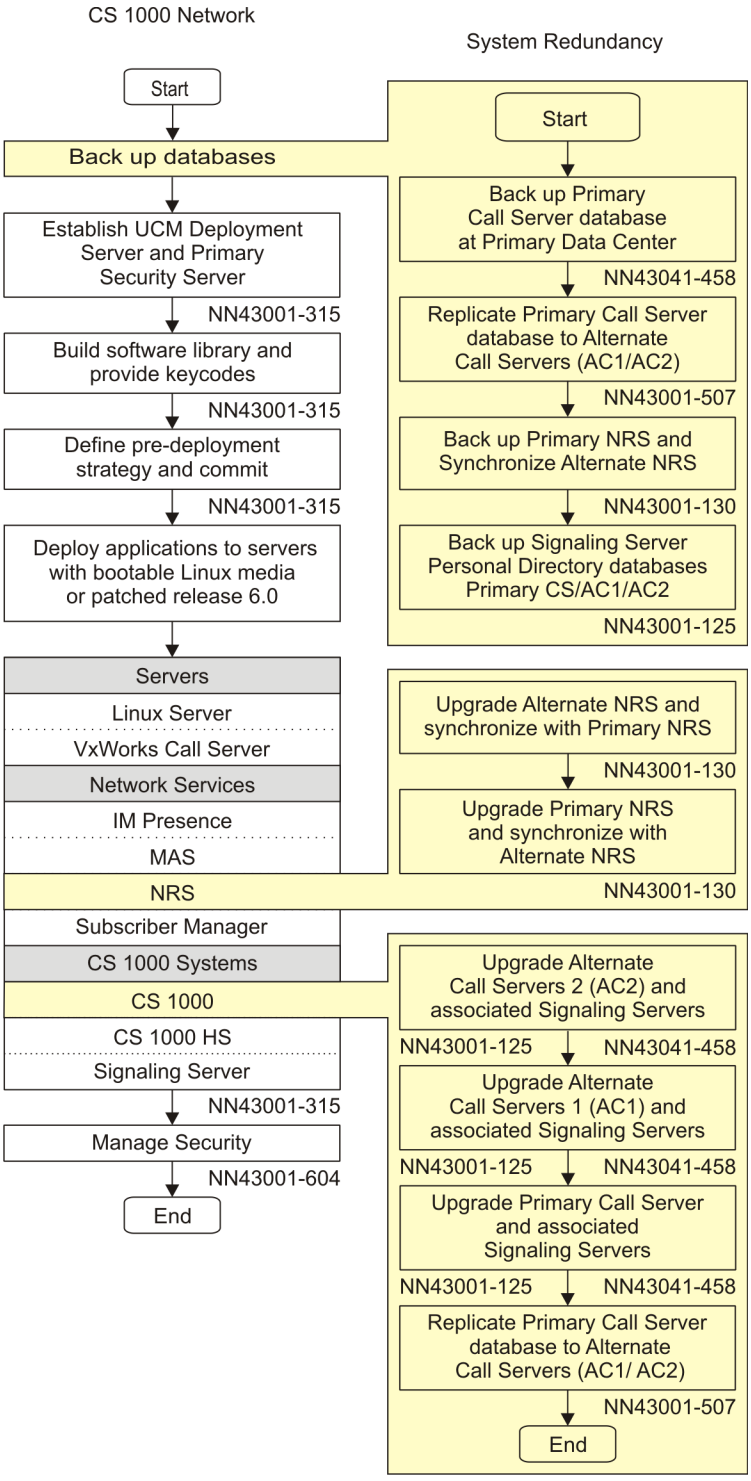
For details, see *NN43041-312, Communication Server 1000E High Scalability Installation and Commissioning*



Geographic redundancy

All components must belong to the same UCM domain.

Cores Call Servers must have routes built to any ELAN device outside of their subnet.


CS 1000 Network
System Redundancy
Start
Back up databases
Establish UCM Deployment Server and Primary Security Server
NN43001-315
Build software library and provide keycodes
NN43001-315
Define pre-deployment strategy and commit
NN43001-315
Deploy applications to servers with bootable Linux media or patched release 6.0
Servers
Linux Server
VxWorks Call Server
Network Services
IM Presence
MAS
NRS
Subscriber Manager
CS 1000 Systems
CS 1000
CS 1000 HS
Signaling Server
NN43001-315
Manage Security
NN43001-604
End
Start
Back up Primary Call Server database at Primary Data Center
NN43041-458
Replicate Primary Call Server database to Alternate Call Servers (AC1/AC2)
NN43001-507
Back up Primary NRS and Synchronize Alternate NRS
NN43001-130
Back up Signaling Server Personal Directory databases Primary CS/AC1/AC2
NN43001-125
Upgrade Alternate NRS and synchronize with Primary NRS
NN43001-130
Upgrade Primary NRS and synchronize with Alternate NRS
NN43001-130
Upgrade Alternate Call Servers 2 (AC2) and associated Signaling Servers
NN43001-125
NN43041-458
Upgrade Alternate Call Servers 1 (AC1) and associated Signaling Servers
NN43001-125
NN43041-458
Upgrade Primary Call Server and associated Signaling Servers
NN43001-125
NN43041-458
Replicate Primary Call Server database to Alternate Call Servers (AC1/ AC2)
NN43001-507
End

FAX issues with VoIP — MGCs

FAX Configuration Recommendations in the Call Server 1000

Fax settings and performance over VoIP solutions vary depending on the network configuration. In order to achieve a successful faxing environment the VoIP solution has to be engineered properly. Following are configuration and network design aspects that need to be taken into consideration when implementing faxing in VoIP solutions:

- **CODECs**
  - T.38: Older fax machines use V.21
  - For lower speeds (V.21) protocol T.38 should be used in the VoIP segments of the call.
  - Modem Pass Through (G.711)

    Newer fax machines use Modem Protocols to achieve higher speeds (V.34)

  The Modem pass through feature is intended for modems and high speed faxes employing V.34, it uses clear channel G.711 over the VoIP segments of the call. The Modem Pass Through will detect the phase reversal tone negotiation used for higher speeds and will tell the DSPs involved in the call to disable echo-cancellation and all other non linear components. MPTD class of service for analog fax lines allows the change of the DSPs between T.38 for lower speeds and G711 for higher speeds.

Important:

MPTD must be used on ALC (Analog Line Cards) units connected to Fax machines when there are trunk cards present in same and other IPMGs that connect to PSTN. This is required to support T.38 and V.34 faxes that could originate or terminate from/to the PSTN.

In order for MPTD to work a system bandwidth strategy of BQ (Best Quality) must be used. The CLS MPTA should be used only for Modems, it will force all calls to use G711.

When going to the PSTN we have no control over the far end, however if the far end supports T.38 and Modem Pass Through, speeds of 33.6 should be achievable.

Note:

Fax performance at higher speeds (33.6) requires that all network elements are properly engineered to support it. When high speed faxes cannot be achieved with a consistent success rate it is recommended to set the fax units at a lower speed (14.4).

Scenarios:

Typical scenarios for Faxing in a CS1KE solution:

- Two faxes connected to analog lines in the same MGC (TDM call, no DSPs)
- Two faxes connected to analog lines in different MGCs of the same CS1K (DSPs are used)
- One fax connected to analog line in an MGC to IP Trunk to a remote system with a fax
- One fax connected to analog line in an MGC to Analog trunk in same MGC to PSTN (Local or LD) fax (No DSPs are involved)
- One fax connected to analog line in an MGC to Digital trunk in same MGC to PSTN (Local or LD) fax (No DSPs are involved)
- One fax connected to analog line in an MGC to Digital trunk in different MGC of the same CS1KE to PSTN (Local and LD) fax (DSPs are used)

Note:

The following scenario is not fully supported for faxing: One fax connected to analog line in an MGC to Analog trunk in different MGC of the same CS1KE to PSTN (Local or LD) fax.

Data Network

Depending on the fax scenarios fax calls can traverse the IP network, either internally (ex: MGC to MGC) or externally (ex: IP Trunks). It is important to engineer the data network to support the following:

- Media card configuration
  - G.711/T.38 codecs 20 ms packet size
  - Round trip delay must be less than 50 ms
  - Packet loss must be less than 0.5% V.34 rate (33.6 kbit/s) as long as far end supports Modem Pass Through feature
  - Mean Jitter is less than 5 ms

Important:

Performance degrades significantly with packet loss (must be less than 0.5%) and when the delay (round trip) is greater than 50 msec and mean jitter is greater than 5msec.

Important:

Avaya has conducted extensive but not exhaustive tests of fax calls in different scenarios. While all tests have been successful, Avaya cannot guarantee that all fax brands will operate properly over all G.711 Voice over IP (VoIP) networks. Before you deploy faxes, test the fax within the network to verify reliable operation. Contact your system supplier or your Avaya representative for more information.

Call Server

Typical recommended configuration for analog lines cards connected to faxes:

- MGCs
  - Enable modem/fax pass through mode: should be enabled in element manager
  - Enable V.21 FAX tone detection: should be enabled in element manager VGW trunks should be in a zone with Best Quality (BQ) setting.
- Analog Lines
  - Class of service: FAXA, this will set the proper trunk capability for fax calls.
  - Class of service: MPTD, this setting will allow lower speed faxes (up to 14.4) to use T.38 and higher speed faxes to use G711 clear channel (no echo cancelation, no nonlinear DSP features).

Post-installation checklist

Item	Meets Specifications	
	Yes	No
All cores are in service and redundant (use switchovers to verify).		
All NRS are redundant.		
All Signaling Servers, MGCs, IPMGs, VGMCs, NRS, and so on are in service.		
Patching, Loadware, and firmware levels for all nodes and cards (such as Cores, Signaling Servers, NRS, and so on) are up to date. If the latest Deplist/SUs are not applied, highlight and document the reason.		
All elements are upgraded to the latest software release.		
Review the alarms for the following: • Both Cores • Lead and one Follower Signaling Server • 2 MC32 cards (if present) • 2 MC32S cards (if present) • 2 IPMGs (if present) (*Any unexpected restarts need to be documented.) • Primary NRS		

Item	Meets Specifications	
	Yes	No
Note: Document any BERR0705 or unexpected restarts in an SR for follow-up investigation.		
All trunk groups that were in service before the upgrade need to be verified to be in service after the upgrade.		
All phones are registered.		
Load balancing is in place and working on the Signaling Servers.		
Validate all registered elements: • Select UCM Secure FTP token link and regenerate the tokens. Elements with issues will fail to receive the token.		
All FIJI cards and rings verified to be in service (customer to verify and report back).		
All fax machines can receive and send calls/faxes (customer to verify and report back).		
All critical call models have been verified to completed (customer to verify and report back).		
All fax machines are SIP compliant.		