Avaya Aura™ Contact Center

Troubleshooting

NN44400-712

Document status: Standard
Document issue: 02.05
Document date: 12 November 2010
Product release: Release 6.0/6.1
Job function: Troubleshooting
Type: Technical Publication
Language type: English

Notices
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
Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer
Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) 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 this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support
Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

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

Copyright
Except where expressly stated otherwise, no use should be made of the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) 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. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

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

Trademarks
The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) 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(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party. Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Downloading documents
For the most current versions of documentation, see the Avaya Support. Web site: http://www.avaya.com/support

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

Contents

New in this release

The following sections describe what is new in *Avaya Aura™ Contact Center Troubleshooting* (NN44400-712) for Release 6.0/6.1.

Navigation

Features

See the following sections for information about feature changes:

High Availability

Avaya Aura™ Contact Center supports High Availability (HA) hot standby resiliency for Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT), Contact Center Multimedia (CCMM) and Contact Center Manager Administration (CCMA).

One set of Contact Center applications (a CCMS, a CCT, a CCMA, and an optional CCMM) actively processes scripts and contacts. This set of applications is called the active set. Another set of Contact Center applications in the same contact center system, is running in hot standby mode. This standby set of Contact Center applications monitors and shadows the active applications in the system and does not process calls.

- The standby CCMS monitors the active CCMS.
- The standby CCT monitors the active CCT.
- The standby CCMM monitors the active CCMM.

Each active and standby pair of applications forms a resilient or replication pair. If any of the active applications fail, the standby applications recognize the failure and start processing contacts. The standby applications must be configured exactly as the active applications. Configuration changes made to the active system during normal operation are automatically copied to the standby applications and the standby applications are configured to take over processing from the active system. Statistical data is also automatically copied to the standby applications.

Use the High Availability utility in Database Utilities to configure High Availability for CCMS, CCT and CCMM. Configure High Availability for CCMA when you install CCMA.

Operating system support

All Contact Center Release 6.0/6.1 server applications are supported on the following operating systems.

- Windows Server 2008 Release 2 64-bit Standard Edition
- Windows Server 2008 Release 2 64-bit Enterprise Edition

Windows 7 support

Information for installing client software on Windows 7 is included in the documentation.

Server virtualization

Contact Center Release 6.0/6.1 introduces support for VMWare and Microsoft Hyper-V. Virtualization. VMWare enables you to share the resources of a single computer across multiple environments. You can host multiple operating systems and multiple applications locally and in remote locations, removing the constraints of physical and geographical limitations. Each server application is supported stand-alone in its own single virtual machine.

Multimedia administration

The Contact Center Multimedia Administration utility is accessed through the Contact Center Manager Administration application. The procedures to perform the Contact Center Multimedia procedures have changed, for more information see Contact Center Multimedia troubleshooting (page 51).

Multimedia only installation

The Contact Center DVD supports installing a non-voice or multimedia only set of Contact Center applications.

Other changes

There are no other changes in this document.

Introduction

The *Avaya Aura™ Contact Center Troubleshooting* (NN44400-712) guide contains the fundamental concepts and procedures required to troubleshoot the server software.

The troubleshooting procedures in this guide are intended for individuals who are familiar with contact centers and who are trained to handle software errors. Users must be aware of the planning and engineering, installation, and configuration involved for the features licensed for your contact center. To handle software errors not covered in this guide, Avaya recommends that you contact Avaya support.

All hardware diagnostics are the responsibility of the platform manufacturer. No hardware procedures are documented in this guide.

No scripting procedures are documented in this guide. For information on how to handle scripting errors, see the *Avaya Aura™ Contact Center Configuration – Service Creation Environment Application Development* (NN44400-510) guide.

No procedures for troubleshooting Predictive Outbound errors are documented in this guide. For information on how to handle Predictive Outbound errors, see the *Avaya Aura™ Contact Center Predictive Outbound Fundamentals* (NN44400-106) guide.

Prerequisites

- Read the *Avaya Aura™ Contact Center Installation* (NN44400-311) guide.
- Read the *Avaya Aura™ Contact Center Fundamentals* (NN44400-110) guide.
- Read the *Avaya Aura™ Contact Center Planning and Engineering* (NN44400-210) guide.
- Read the *Avaya Aura™ Contact Center Routine Maintenance* (NN44400-514) guide.
- Understand the features that you purchased.
- Install, upgrade, or migrate your Avaya Aura™ Contact Center Release 6.0/6.1 software.
- Commission your Contact Center Release 6.0/6.1 software, see *Avaya Aura™ Contact Center Commissioning* (NN44400-312) and *Avaya Aura™ Contact Center SIP Commissioning* (NN44400-511).

Navigation

- Troubleshooting fundamentals (page 15)
- Troubleshooting planning (page 17)
- General troubleshooting (page 19)
- Installation troubleshooting (page 25)

Troubleshooting fundamentals

This section contains the fundamental concepts required to troubleshoot the server software in Avaya Aura™ Contact Center Release 6.0/6.1.

Navigation

- Handling errors (page 15)
- Monitoring log files (page 15)

Handling errors

For all errors, record the error messages, the system configuration, and actions taken before and after the error occurred. If the problem persists, contact your Avaya customer support representative.

Monitoring log files

You need to review log files to determine where errors occur and how to address them. You require this information if you need to contact Avaya to assist with troubleshooting.

Troubleshooting planning

This section describes the information required for you to locate users and applications that can require troubleshooting in Avaya Aura™ Contact Center Release 6.0/6.1.

You can troubleshoot problems better by planning for events in advance and having up-to-date information available when network or device problems occur and troubleshooting is required

Prerequisites for Troubleshooting planning

- Know your network configuration.
- Understand the normal behavior of your network.

Navigation

- Site network map (page 17)
- Logical connections (page 17)
- Device configuration information (page 17)
- Other important network data (page 17)
- Determining baseline information for your network (page 18)

Site network map

The site network map identifies where each device is physically located. This helps you locate the users and applications that are affected by a problem. You can use the map to systematically search each part of your network for problems.

Logical connections

With virtual LANs (VLANs), you need to know how your devices are connected logically as well as physically.

Device configuration information

Maintain online and paper copies of device configuration information. Make sure that all online data is stored with your site's regular data backup. If your site does not have a backup system, copy the information onto a backup disc (CD, DVD, or Zip disk) and store it offsite.

Other important network data

For a complete picture of your network, have the following information available:

- **All passwords**: Store passwords in a safe place. Keep previous passwords in case you restore a device to a previous software version and need to use the old password that was valid for that version.

- **Device inventory**: The inventory allows you to see the device type, IP address, ports, MAC addresses, and attached devices at a glance. Software tools, such as Transcend Central, can help you keep track of the 3Com devices on your network. Using Transcend Central, you can group devices by type and location and have this information on hand for troubleshooting.
- **MAC address-to-port number list**: If your hubs or PABXs are not managed, you must keep a list of the MAC addresses that correlate to the ports on your hubs and PABXs. Generate and keep a paper copy of this list, which is crucial for deciphering captured packets, using Address Tracker.
- **Change control**: Maintain a change control system for all critical systems. Permanently store change control records.
- **Contact details**: Store, online and on paper, the details of all support contracts, support numbers, engineer details, and telephone and fax numbers.

Determining baseline information for your network

You can use a baseline analysis, which is an important indicator of overall network health, to identify problems. A baseline can serve as a useful reference of network traffic during normal operation, which you can then compare to captured network traffic while you troubleshoot network problems. A baseline analysis speeds the process of isolating network problems.

By running tests on a healthy network, you compile normal data to compare against the results that you get when your network is in trouble. For example, Ping each node to discover how long it typically takes you to receive a response from devices on your network.

Certain applications enable you to collect days and weeks of data and set a baseline for comparison to a network with performance issues or outages.

General troubleshooting

This section describes the general troubleshooting procedures that you should perform when investigating basic problems in Avaya Aura™ Contact Center Release 6.0/6.1.

Prerequisites for general troubleshooting

- Ensure that the power is on.
- Ensure that the PABX is operational and that all components are securely seated in the chassis.
- Ensure that all power leads and data cables are firmly connected at both ends.
- Ensure that the ports are properly configured.
- Ensure that all servers and their services are running.

Navigation

Troubleshooting hardware problems

All hardware diagnostics are the responsibility of the platform manufacturer. No hardware procedures are documented in this guide.

Procedure steps

Step	Action
1	Check the manufacturer’s instructions and recommendations. Contact the manufacturer if necessary.

--End--

Troubleshooting hardware errors

You can try to resolve some hardware errors by disconnecting the system, simplifying the setup, and restarting the system.

Procedure steps

Step	Action
1	Log users off the LAN and turn off the server.
2	Disconnect the power cord and unplug the telephone cables.
3	Simplify the server configuration to one monitor, one floppy and one hard disk drive, and one keyboard and mouse.
4	Remove all third-party options.
5	Reinstall options one at a time, checking the system after each installation.
6	Reconnect the power cord and telephone cables.
7	Restart the system. If the system does not function, see Troubleshooting when the system does not turn on (page 20).

--End--

Troubleshooting when the system does not turn on

You can check a number of things when the system does not turn on. There can be several reasons why the server is not functioning.

Procedure steps

Step	Action
1	Ensure that all cables and power cords are firmly plugged into their proper receptacles.
2	Ensure that all parts of the system are turned on and properly adjusted.
3	If the server is plugged into a switched multiple-outlet box, ensure that the switch on the outlet box is turned on.
4	Plug a different electrical device (such as a printer) into the power outlet, and turn it on.
5	Unplug the power cord, wait 20 seconds, plug it in again, and restart the system.
6	If the system still does not function, contact the server manufacturer.

--End--

Troubleshooting operating system start-up errors

Operating system start-up errors are often related to memory and hard disk drive capacity issues.

Procedure steps

Step	Action
1	Determine if the server has enough memory and hard disk drive capacity.

--End--

Troubleshooting connection errors

Connection errors involve loose or absent connections.

Procedure steps

Step	Action
1	Verify that all cables and boards are securely plugged into their appropriate connectors or slots.

--End--

Removing added options

You can have difficulty troubleshooting server issues if there are conflicts with added options.

Procedure steps

Step	Action
1	Remove all added options, and change only one component at a time.

--End--

Troubleshooting power cord errors

You can resolve many power errors by unplugging and plugging in the power cords.

Procedure steps

Step	Action
1	Unplug the server's power cords.
2	Wait 20 seconds.
3	Plug the power cords in.
4	Restart the system.

--End--

Resolving a failed ping

If you test the contact center server subnet and ELAN subnet connection using the ping command, and the test fails, then follow these steps to verify that the server ELAN subnet and contact center server subnet cards are configured and identified correctly.

Procedure steps

Step	Action
1	Plug the crossover network cable into the network card in the Client PC.
2	Plug the other end into the ELAN subnet card in the server.
3	If you must restore the IP address information of the client PC after this procedure, then record the TCP/IP address, subnet mask, and gateway of the client PC.
4	Configure the client PC with an IP address that is part of the same subnet as the IP address assigned to the ELAN subnet card. For example, if the server ELAN subnet card has the IP address 1.1.1.1, then assign the client PC an IP address of 1.1.1.2.
5	Set the client PC to have an subnet mask of 255.0.0.0. Leave the gateway blank.
6	Open an MS-DOS prompt window on the client PC and try to ping the server ELAN subnet card. For example, if the server ELAN subnet card has the IP address 1.1.1.1, then type ping 1.1.1.1 and press Enter. *If the ping test succeeds, then you know that you have correctly identified the ELAN subnet card in the network control panel. The other network card, if present, must be the contact center server subnet card.*
7	From the server, repeat the steps described in the procedure Retesting the ELAN subnet and contact center server subnet network connection (page 92). If the test fails, then verify that the network is set up correctly.

--End--

Refreshing your servers

If a new license file was issued and accepted by Contact Center Manager Server, or if you connect to a different License Manager (that is, a new or standby License Manager server), you must refresh your servers.

If you changed the password of sysadmin in the Server Utility, you must change the password in that server.

When you refresh a server, you refresh Contact Center Manager Server data associated with that server in Active Directory Lightweight Directory Services (AD-LDS), such as release number, feature list, and networking information.

Prerequisites

- Ensure that you log on as webadmin, because only the default administrator can add, edit, delete, and refresh servers in Contact Center Manager Server.
- You must log on using the Contact Center Manager Administration server name instead of the IP address, as the SOAP files are configured to use the server name. You can save the Contact Center Manager Administration server address by adding it to your list of Internet Explorer favorites.
- Ensure that you have configured the Contact Center Manager Administration server name as Trusted Site with the relevant Active X Download values selected.
- Ensure that you have installed the client version of SOAP 3.0 on the PC.

Procedure steps

Step	Action
1	Start Internet Explorer.
2	In the **Address** box, type the Contact Center Manager Administration server name. For example, http://<Contact Center Manager Administration Server name>. You must log on using the Contact Center Manager Administration server name instead of the IP address, as the SOAP files are configured to use the server name.
3	Press **Enter**. *The Contact Center Manager Server main logon window appears.*
4	Enter your webadmin user ID and password in the text boxes.
5	Click **Login**. *The Contact Center Manager Administration main window appears.*
6	Select **Configuration**.
7	On the menu bar, click **Server, Refresh All Servers**.
8	Click **Yes**. *The system refreshes all servers in the system tree. A message appears in the information bar at the bottom of the screen which lists the refreshed servers and the*

servers that did not refresh. An entry specifying the servers that you refresh also appears in the Audit Trail.

--End--

Installation troubleshooting

This section describes the procedures required to troubleshoot installation problems in Avaya Aura™ Contact Center Release 6.0/6.1.

Prerequisites for installation troubleshooting

- Read the *Avaya Aura™ Contact Center Installation* (NN44400-311) guide.
- Read the *Avaya Aura™ Contact Center Planning and Engineering* (NN44400-210) guide.

Navigation

Troubleshooting installation

The Avaya Aura™ Contact Center 6.0 (AACC 6.0) installer initiates a series of individual application installations with each one creating its own log file. If an application installation fails, the AACC 6.0 installer identifies which application has failed and notifies the user.

Procedure steps

Step	Action
1	Identify the application that is experiencing the issue.
2	Examine the log files to determine if the error can be corrected.
3	If additional support is required. • Archive the error screenshots.

- Archive all logs below the C:\Avaya\Logs\Sysops folder.
- Send the archived screenshots and logs to the appropriate support personnel.

--End--

Log Files

Installation logs are located in C:\Avaya\Logs\Sysops. The following table shows the AACC 6.0 installation sequence and the paths to related log files.

Installation Log File Paths

Installation Sequence	Log File Location
AACC 6.0 Installer	C:\Avaya\Logs\Sysops
Third party	C:\Avaya\Logs\Sysops\MsiLogs
CC applications	C:\Avaya\Logs\Sysops\MsiLogs
	C:\MA_Logs (MAS application)
CC patches	C:\Avaya\Logs\Sysops\MsiLogs\ProductUpdates

AACC 6.0 Installer Log Files

Log File	Details
CC_Install_Data.xml, CC_Install_Log.xml	• Location: C:\Avaya\Logs\Sysops • Created during contact center application installation • Contains customer configuration data entered during the interview phase • Contains machine specific info, for example the IP address and computer name
Install_success_temp.html, Install_fail_temp.html	• Location: C:\Program Files\Avaya\Resources\HTML\ • Contains a high level summary of application installation status
CC8_ProductInstaller.log	• Location: C:\Avaya\Logs\Sysops • Contains detailed low level commands for the application designer

Third Party Log Files

Application	Msi log file
AD-LDS	CCMAADAM.log
Policy Agent	CCMAIISPolicyAgentComponents.log
Tomcat	ContactCenterTomcatInstall.log
Cache	Cache_x64.msi.log

Third Party Log Files

Application	Msi log file
Crystal RAS 2008	RAS.msi.log
JRE	jre1.5.0_14.msi.log
Primary Interop Assemblies	No log generated
ODBCDriver_2007.1_x86.exe	ODBCDriver_2007.1_x86.exe.log
Sybase Open Client	No log generated
Visual Studio 2008 runtime	No log generated
WebServicesFramework.msi	No log generated

CC Patching Log Files

Log File	Details
CCPatches.log	• Location: C:\Avaya\Logs\Sysops\Product Updates • Contains history of patches installed or uninstalled on the system
PatchScript.log	• Location: C:\Avaya\Logs\Sysops\Product Updates\<ComponentName>\<PatchName> For example, C:\Avaya\Logs\Sysops\Product Updates\CCT\AvayaAura_CCT_6.0.201.0\PatchScript.log • Contains custom actions during patch installation or uninstallation, such as registry creation, service shutdown or startup, generated on patch install or uninstall
Nisoppep.log	• Location: C:\Avaya\Logs\Sysops\Product Updates\<ComponentName>\<PatchName> For example, C:\Avaya\Logs\Sysops\Product Updates\CCT\AvayaAura_CCT_6.0.201.0\nisoppep.log • Contains details of files updated during a patch installation or uninstallation

Troubleshooting error messages during Communication Control Toolkit installation

Error messages appear during Communication Control Toolkit installation.

Procedure steps

Step	Action
1	Take a screenshot of the error message for future reference.
2	Click **OK**. *A CCT exit code (Install Failure) window appears with a path to the log file directory, C:\Avaya\Logs\Sysops\MsiLogs.*
3	Click **OK**. *The Main installation stops. A window appears with a summary of the installation. The Communication Control Toolkit component appears last in the summary with a red 'X' to indicate an error. Successful components appear with a green check mark.*
4	Open CommunicationControlToolkit.log in C:\Avaya\Logs\Sysops\MsiLog.
5	Search CommunicationControlToolkit.log in C:\Avaya\Logs\Sysops\MsiLog for the text for the error message in step 1.
6	Review the log leading up to this message to find information on what caused the error.
7	The end of the log has the statement MainEngineThread is returning <number>. For a successful installation this number is 0. Any other value is an error return code. Use this return code in Installshield experts to determine the cause of the error.
8	For additional help, archive the error screenshots, archive all logs in C:\Avaya\Logs\ Sysops folder and send the archived screenshots and logs to support personnel.

--End--

Troubleshooting when a Contact Center patch does not successfully install

Contact Center patch does not successfully install. A window titled Patch Install Failure appears during installation.

Procedure steps

Step	Action
1	Note the patch name in the message that has failed to install.
2	To proceed with Contact Center installation and install the patch a later time, click **Yes**. *If there are no other errors, the installation will complete and a status window appears.*
3	A red X appears beside the patch installation phase in the status window to indicate the failure.

--End--

Troubleshooting a Contact Center Manager Server Configuration Error

An error occurs during CCMS Config execution.

Procedure steps

Step	Action
1	Check Server Configuration's registry key HKEY_LOCAL_MACHINE\SOFTWARE\Nortel\Contact Center\Product Installation\ServerSetupConfig.
2	If ErrorDescription is ERROR, then an error occurred while running Server Config.
3	Search D:\Avaya\Logs\CCMS\CC_ServerConfig.log for ERROR to identify cause of error. Possible causes of the error include the following: • If the log file contains errors referring to database connection problems, the cache database was not running during CCMS Configuration. • C:\Avaya\Logs\Sysops\CC_Install_Data.xml file is malformed, not present, or missing data.
4	Confirm Cache is running.
5	Run CCMS Server Configuration utility, verify and enter configuration data.
6	Click **Apply All**.

--End--

Troubleshooting error messages during or after server installation

Error messages during or after server installation can occur if files are copied incorrectly. Error messages during installation can also occur if conflicts arise with other programs running on the server during installation.

Procedure steps

Step	Action
1	Close any other programs currently running on the server.
2	Uninstall the software.
3	Reinstall the software.

--End--

Troubleshooting configuration errors after server installation

Configuration errors can occur if values were not entered correctly in the Server Configuration.

Procedure steps

Step	Action
1	From the **Start** menu, choose **All Programs**, **Avaya**, **Contact Center**, **Manager Server**, **Server Configuration**.
2	In the Server Configuration Utility window, enter the correct values for your server.

--End--

Troubleshooting server installation failure with Windows Server 2008 Release 2

Contact Center Multimedia installation can fail when the optional components of Windows Server 2008 Release 2 are installed.

Procedure steps

Step	Action
1	Uninstall Windows Server 2008 Release 2 64-bit Edition.
2	Reinstall Windows Server 2008 Release 2 64-bit Edition, without the optional components on DVD 2 of the Windows Server 2008 Release 2 64-bit Edition installation DVDs.
3	When you are prompted to install DVD 2, click **Cancel** and then click **OK**.

--End--

Migration troubleshooting

This section describes the procedures required to troubleshoot migration problems in Avaya Aura™ Contact Center Release 6.0/6.1.

Windows Server 2008 Release 2 is the only operating system platform supported for Contact Center, so software upgrades using the operating system from previous contact center releases are not supported. A migration procedure migrates the statistical and configuration data from one server to another. You can migrate your existing customer data to Contact Center on a new Windows server. You can migrate all your configuration and statistical data to the new server so no data is lost in the move.

Prerequisites for Migration troubleshooting

- Always back up the server database prior to any maintenance activity.
- Read the *Avaya Aura™ Contact Center Upgrade and Patches* (NN44400-410) guide.

Navigation

- Task Flow Executor does not start after an upgrade (page 31)

Task Flow Executor does not start after an upgrade

If the Task Flow Executor (TFE) does not appear in the UP state after an upgrade, then you must validate all scripts to correct the problem. For more information about validating scripts, refer to the *Avaya Aura™ Contact Center Configuration – Service Creation Environment Application Development* (NN44400-510) guide.

Procedure steps

Step	Action
1	Validate all scripts.

--End--

Server administration troubleshooting

This section describes the troubleshooting procedures that you should perform when handling server administration problems in Avaya Aura™ Contact Center Release 6.0/ 6.1.

Prerequisites for server administration troubleshooting

- Ensure that you know the License file location and Contact Center License Manager IP address.

Navigation

- Resetting the Contact Center License Manager Grace Period (page 33)
- Troubleshooting when the Contact Center Manager Server hosts file contains multiple instances of each site (page 35)

Resetting the Contact Center License Manager Grace Period

In the event of a communication error between the Contact Center Manager Server and the Contact Center License Manager, normal operation of the Contact Center Manager Server runs for the duration of the Grace Period.

The Grace Period duration is equal to 30 days and the Grace Period is cumulative over the lifetime of the product. On the first occurrence of a communication problem between the Contact Center Manager Server and the Contact Center License Manager, there are 30 days available for the Contact Center Manager Server to continue normal operation. For example, if the problem is resolved in 2 days, then on the next occurrence of a communication problem, there will be 28 days available to fix the problem.

When the server enters the Grace Period, an event continues to be generated until either the Grace Period expires or the communication problem between the server and the Contact Center License Manager is resolved.

If, at any stage, the Grace Period expires, Contact Center Manager Server shuts down and Contact Center Manager Server is locked. You cannot restart Contact Center Manager Server without resetting the Grace Period.

The Grace Period can be reset back to 30 days at any time. When a communication error is detected, an event is sent to the Server Utility detailing that there was an error, the time already elapsed in the Grace Period, and a lock code that you must return to Avaya to get the Grace Period reset.

For Contact Center Manager Server, you must apply separate unlocking codes for both CCMS Control Service and ASM Service.

Within the grace period, you have the same capabilities as if you were the only client of the Contact Center License Manager. You can request the maximum licenses that are available from the Contact Center License Manager. When communication is re-established, the licenses are acquired automatically from the Contact Center License Manager (if they are available).

When a licensing error is detected, you must check that the Contact Center License Manager service is running, and verify the status of the Contact Center License Manager server and network communications. During the grace period, alarms are sent every 6 hours notifying the time elapsed in the grace period.

If you reestablish communications during the grace period, notification is sent to the Windows Event Log on the server and the Alarm Monitor. While communication is reestablished, alarms are sent every 6 hours notifying the time elapsed in the grace period.

During the grace period, you can shut down, start up, or restart Contact Center Manager Server without affecting the operation of Contact Center Manager Server.

If you cannot fix the connection between the Contact Center License Manager and Contact Center Manager Server within the 30 day grace period, contact your Avaya Customer Service Representative to determine if an emergency license file may need to be activated on your system.

The emergency license file expires after 30 days and is used only to ensure operation of the Contact Center Manager Server on a temporary basis. You must install the emergency license file through the Contact Center License Manager Configuration tool. If you are using corporate licensing, you may need to change the Contact Center Manager Server Configuration in cases where the Contact Center License Manager is installed on a different server than it was previously.

Prerequisites

- Ensure that you locate the license file in the D:\Avaya\Contact Center\License Manager\bin folder on the server. The license file is called plservrc.
- Ensure that the IP addresses used for the Primary and Secondary Contact Center License Manager are on the same contact center server subnet and the contact center server subnet is at the top of the binding order on the Contact Center Manager Server and Contact Center License Manager servers.

Procedure steps

Step	Action
1	From the Event Viewer, make a copy of the lock code and send this code to Avaya Support. *Avaya Support provides you with an unlock code that you must apply to the Contact Center Manager Server.*

2 Launch the Contact Center License Grace Period Reset application.

3 Enter the unlock code you received from Avaya Support.

4 Click **Apply**.

5 Click **Exit**.

6 Repeat steps 1 through 5 for both Contact Center Manager Server Control Service and ASM Service.

--End--

Troubleshooting when the Contact Center Manager Server hosts file contains multiple instances of each site

If you delete any site entry from the hosts file, then you must restart the MAS configuration manager service to ensure that it updates the database with the changes.

Procedure steps

Step	Action
1	On the Contact Center Manager Server, go to C:\WINDOWS\system32\drivers\etc and open the hosts text file.
2	Delete the multiple entries of the site, and then click **File, Save**.
3	Select **Start, All Programs, Avaya, Contact Center, Manager Server, Server Configuration**.
4	Save and apply all changes.
5	Restart the server.
6	Open the hosts text file and confirm that the file is accurate and there are no multiple instances of any site.

--End--

Database Integration Service troubleshooting

This section describes the troubleshooting procedures that you should perform when handling Database Integration Service problems in Avaya Aura™ Contact Center Release 6.0/6.1.

Navigation

Handling Database Integration Wizard errors

There is a list of errors that you can receive when you are running the Database Integration Wizard (DIW). The Job Aid below lists each of the error messages and gives a brief explanation of how to handle each error.

Procedure steps

Step	Action
1	Review the Database Integration Wizard error messages (page 37) table and determine how to proceed.

--End--

Procedure job aid

Database Integration Wizard error messages

Error message	Description
Already Connected (when setting and testing the HDX connection)	Contact Center Manager Database Integration is already connected to HDX.
Already Connected (when configuring the database)	The selected DSN is already connected.
Authorization Failed	The user details supplied are incorrect. This indicates that the version of Contact Center Manager Database Integration is different than the version of HDX. Contact Avaya Support.

Database Integration Wizard error messages

Error message	Description
Error	The connection cannot be performed. Contact Avaya support.
Incompatible Version	The version information supplied is incorrect. This indicates that the version of Contact Center Manager Database Integration is different than the version of HDX. Contact Avaya support.
Invalid Object	HDX Server object cannot be found. This indicates that the HDX Server service is not running.
Invalid Provider ID	The provider ID entered is invalid. Ensure that the provider ID is within the valid range of 0 to 1999999999.
The Host could not be found.	A server with the host name or IP address given cannot be found on the network. Enter a new host name or IP address.
Too Many Connections	All HDX connections are being used. Deregister another HDX provider to free a connection.

Ensuring you have the correct access permissions to the database

The connection to the database requires access permissions. For example, if the database security is configured to use its own integral user accounts, then a user can be specified in the Database Integration Wizard and the ODBC Data Source Name (DSN). However, if the database security is configured for Domain or Workgroup authentication, then the Contact Center Manager Server Host Application Integration service and the Database Integration Wizard need to use the correct context when connecting.

The Database Integration service runs by default in the local system context and therefore does not have access permissions to the database on another server in the customer network using Domain or Workgroup authentication.

Procedure steps

Step	Action
1	To enable access to the database, follow one of the recommendations below: • Use Local or Domain Policy to assign permissions to the Local System context of the Contact Center Manager Host Application Integration Service.

- Configure the Contact Center Manager Host Application Integration service to start with the <Domain>/<User> context with the appropriate permissions.
- Configure the database permissions for the Contact Center Manager Server computer access context.
- Contact your Customer Network Administrator or your Database Administrator for further information about configuring the correct access permissions for connection to the database.

--End--

Ensuring access to the database over a network

The Database Integration service runs as a Windows service using the predefined Local System account on the server. A service that runs in the context of the Local System account inherits the security context of the Windows Service Control Manager. This account has extensive privileges on the local computer and acts as the computer on the network.This account has limited access to network resources (such as shares) because it has no credentials and must connect to the network using a null security session. For example, the account may not have sufficient security credentials to access a Microsoft Access database owned by an authenticated user over a network share, which was created in the context of the user.

Procedure steps

Step	Action
1	Contact your Network Administrator. *For information on making a remote share available using a null session share, see the Microsoft Web site.*

--End--

Network Control Center troubleshooting

This section describes the troubleshooting procedures that you should perform when handling Network Control Center (NCC) issues in Avaya Aura™ Contact Center Release 6.0/6.1.

Prerequisites for Network Control Center troubleshooting

- Ensure that you are aware of your NCC configuration.

Navigation

Troubleshooting call routing problems

Troubleshoot call routing problems if your server cannot route calls to or receive calls from other sites. You need to review several issues to determine why the server cannot route calls.

If you experience issues with networking calls, Avaya also provides a network trace utility (NtwkTraceMon) that customer support staff can use to help you troubleshoot your problem.

Procedure steps

Step	Action
1	Verify that the source server did not filter the server.
2	Verify that the dialable DN is configured correctly at the source server.
3	Ensure that network skillsets and routing tables are received at the server. If not, see Verifying the connection to the NCC (page 42).

--End--

Verifying the connection to the NCC

Verify the connection to the NCC if calls are not being routed properly.

Procedure steps

Step	Action
1	At the NCC, start the Nbconfig utility. Run **nbconfig -admin**.
2	Check the Address and Site tables to ensure that they are configured correctly: • The IP addresses are unique and correct. • The site names are correct. • The site names in the Site table match the site names in the Sites window on the NCC.
3	Add any missing sites and, if any information is incorrect, remove the affected site and add it again.
4	At the server, start the Nbconfig utility, and verify that the Address table and the Site table match those on the NCC.
5	At the server, use the Nbconfig utility to ensure that the NCC site is defined correctly. If any of this information is incorrect, see Resetting all site and address settings (page 43).
6	At the server, open a DOS window and type the following command: ping nnn.nnn.nnn.nnn where nnn.nnn.nnn.nnn is the CLAN IP address of the NCC. If the NCC cannot be found, then use the tracert command to find out where the error is occurring.
7	Restart the NCC.
8	If the problem continues, contact your Avaya customer support representative.

--End--

Resetting all site and address settings

Reset all site and address settings if the contents of the Address table and Site table are incorrect or if the two servers do not communicate even though they can ping each other. You will need to shut down all Contact Center Manager Server services.

If this procedure does not resolve the problem, run nicomsetup at the NCC and define all sites again using nbconfig -admin.

Procedure steps

Step	Action
1	From the Windows Start menu, choose **Programs, Avaya, Contact Center, Manager Server, Shutdown**.
2	At the DOS prompt, type **cd \Avaya\iccm\bin**.
3	From the bin directory, run **nicomsetup** to reset all communication settings.
4	Restart Contact Center Manager.
5	On the NCC, run **nbconfig -admin**.
6	Select the **Force Synchronization** check box on the Site Table tab, and then click **OK**.

--End--

Troubleshooting when network skillsets are not distributed from the NCC to all sites

This problem can occur for the following reasons:

- **An existing entity has the same name**: If a server has a variable named Sales, then you cannot add a network skillset named Sales. Avaya recommends that skillset names include the characters _sk to identify them as skillsets and to avoid potential conflicts with other entities.
- **The configured limit for number of skillsets was reached**: For more information about historical statistics configuration, see the *Avaya Aura™ Contact Center Manager Administration – Client Administration* (NN44400-611) guide.
- **One or more sites is running** Avaya Aura™ Contact Center **Web Client Release 4.2 or earlier**: Network skillsets configured for longest idle agent or average speed of answer are not propagated to servers running Avaya Aura™ Contact Center Web Client 4.2 or earlier.

Prerequisites

- Determine the reason why network skillsets are not being distributed from the NCC to all sites.

Procedure steps

Step	Action
1	If an existing entity has the same name as a network skillset, contact your network administrator to resolve naming problems.
2	If you have reached the configured limit for number of skillsets, use either client application to check the historical statistics configuration parameters. and change the configured limit of skillsets. If you change the configured limit of skillsets, you must force synchronization of the site information from the NCC.
3	If one or more sites is running Avaya Aura™ Contact Center Web Client 4.2 or earlier, install a supported Web client at any site that requires upgrading.

--End--

Troubleshooting when calls for a network skillset are not sent to other sites

This problem can occur if your scripts are not updated to route calls to the network skillset. When an administrator at the NCC defines a network skillset at the NCC, the NCC propagates the new skillset to all servers in the network. However, scripts are not automatically updated to route calls to the network. Calls continue to be queued to the local copy of the network skillset.

To route calls to other sites, you must add the script command Queue To Network Skillset. For more information about using network skillsets in scripts, see the *Avaya Aura™ Contact Center Configuration – Service Creation Environment Application Development* (NN44400-510) guide.

This error can also occur under the following circumstances:

- The NACD package is not enabled on the telephony switch at the source site.
- A non-ISDN trunk is encountered.
- The dialable DN (set in the Network Communication Parameters window) for the destination is not set to the correct MCDN network CDN.
- A call is abandoned.

Prerequisites

- Determine the reason why calls for a network skillset are not being sent to other sites.

Procedure steps

Step	Action
1	If the NACD package is not enabled on the telephony PABX at the source site, install and configure NACD.

--End--

Troubleshooting when filtering is preventing calls from being sent to a destination site

This problem can occur for the following reasons:

- The NACD package is not enabled on the telephony PABX at the source or at the destination site.
- The dialable DN for the destination site is configured incorrectly.
- The MCDN network CDN is not configured correctly at the destination site. The MCDN network CDN must be configured on the telephony PABX as a CDN (see *Avaya Aura™ Contact Center Configuration – Avaya CS1000 Integration* (NN44400-512)), and it must be configured and acquired as an MCDN network CDN on the server.
- The server at the destination site is not active.
- The network skillset at the destination site is in Night Service mode or Transition Service mode. The site is filtered until an agent with the skillset logs on and the queue at the destination site is active.
- The number of failed attempts set in the Number of Retries box for a skillset is reached. When this happens, the source site removes the destination site from all routing tables for the time configured in the Filter Timer period (minimum of 5 minutes, maximum of 12 hours). After the Filter Timer period, the destination site is no longer filtered.

Prerequisites

- Determine the reason why filtering is preventing calls from being sent to a destination site.

Procedure steps

Step	Action
1	If the NACD package is not enabled on the telephony PABX at the source or at the destination site, install and configure NACD.
2	If the dialable DN for the destination site is configured incorrectly, reconfigure the network communication parameters.
3	If the MCDN network CDN is not configured correctly at the destination site, reconfigure the MCDN network CDN as a CDN.
4	If the server at the destination site is not active, ask the contact person at the remote site whether the server is up.

5	If the network skillset at the destination site is in Night Service mode or Transition Service mode, wait until an agent with the skillset logs on and the queue at the destination site is active.
6	If the number of failed attempts set in the Number of Retries box for a skillset is reached and the source site removes the destination site from all routing tables for the time configured in the Filter Timer period, wait until the Filter Time period is reached or, if the problem is resolved before the Filter Timer period is reached, manually stop filtering the site.

--End--

Troubleshooting problems collecting network call-by-call statistics

This problem can occur for the following reasons:

- **The server or NCC does not have enough disk space**: The historical statistics configuration calculation determines if you have adequate storage space to save the amount of call-by-call data you choose. When historical data is stored and consolidated, each server (including the NCC) checks every 15 minutes to ensure that you have adequate storage space. This is applicable at each server, including the NCC. Call-by-call data is purged when data reaches the age you configure (in the Historical Statistics Configuration window) or when disk space becomes insufficient. This enables more recent call-by-call data to be stored; but if you have less disk space than calculated, it can result in less long-term data stored. An event is logged in Fault Management if this occurs. An event is also logged in Fault Management if network call-by-call data transfer to the NCC takes longer than 15 minutes.

  Attention: If the NCC goes down for an extended period, pegging occurs at each local server that is storing network call-by-call data. This can use a substantial amount of resources at each local server.

- **The call-by-call information is not sent to the NCC**: If you recently changed your call-by-call storage options, the change does not take effect until the information is sent to the NCC and propagated to all sites. This can take several minutes after making a change.

Prerequisites

- Determine the reason why your system is having problems collecting network call-by-call statistics.

Procedure steps

Step	Action
1	If the server or NCC does not have enough disk space, reconfigure storage information in the Historical Statistics Configuration window.

2	If the call-by-call information is not being sent to the NCC because you recently changed your call-by-call storage options, wait a few minutes for the change to take effect.

--End--

Troubleshooting incorrect times on reports

Troubleshoot incorrect times on reports when errors occur because the times set at multiple servers are not synchronized.

Whether sites are in the same time zone or in multiple time zones, if the times at various telephony PABXs are not synchronized, the network call-by-call report does not display accurate information. In some cases, for example, destination events can appear to occur before source events. You must regularly check the time set at each telephony PABX and change the date and time when necessary, to ensure exact synchronization.

Prerequisites

- Check the time set at each telephony PABX regularly to ensure that the times are synchronized.
- Verify that each site on the Sites page of the Configuration component in Contact Center Manager Administration has the relative time to GMT configured correctly.
- If you change the time zone through the Date/Time control panel, restart each server in Contact Center Manager.

Procedure steps

Step	Action
1	Log on to the PABX console.
2	Enter **ld 2**.
3	Type **ttad** to display the date and time.
4	To change the date or time, type **stad**, and then enter the correct date and time in the following format: DD-MM-YYYY 00:00. Use the 24-hour clock format for the time.
5	Press **Enter**.
6	Log off the PABX console.

--End--

Troubleshooting call routing problems when agent reservations are canceled before network calls are presented

The number of times an agent is reserved must be approximately equal to the number of NACD and network calls answered by the agent. If it is not, then your Agent Reserve Timer may be set too low.

Normally, when an agent is reserved for a call, but the call is answered locally or routed to another server, the local server notifies the remote server, and the remote server cancels the agent reservation. However, if a communication problem prevents notification of the remote server, the agent remains in the reserved state indefinitely. To prevent this from happening, the remote server cancels the reservation after a period of time configured on the Agent Reserve Timer.

If the Agent Reserve Timer is too low, the agent can be unreserved before the call is presented to the agent, but after the call arrives at the remote server. When that happens, the agent's ReservedForCall statistic is incremented, but the agent's NetworkCallsAnswered statistic is not.

Procedure steps

Step	Action
1	If agent reservations are being cancelled before network calls are presented, check the Agent Reserve Timer and increase the period of time configured.

--End--

Troubleshooting call routing problems with Landing Pads in Universal Networking

Every site that is licensed for Universal Networking can configure CDN or DNIS Landing Pads. When a request is received at a target network node, a Landing Pad is taken from the idle list and reserved for that call until the source site routes the call to it. Landing Pads are required for the duration of a network call. When the call arrives at the target Landing Pad, the Landing Pad is returned to the idle list to wait for the next call. A relatively small number of Landing Pads should be sufficient to receive several incoming Universal Networking calls at a target node.

There are several possible call routing problems that can occur with Landing Pads in Universal Networking:

- **All Landing Pads are busy**: If the incoming network call rate exceeds the available Landing Pads, then Event 49033 is logged to the Event Browser at the source site stating All Landing Pads Busy at <TargetSiteName>. The Network Communication Parameters page in Contact Center Manager Administration for the source site displays a similar message for the configurable time that the target is filtered. This

message is an indication that not enough Landing Pads are configured for the target site in question. This applies to both CDN and DNIS Landing Pads. CDN Landing Pads must be acquired before Contact Center Manager Server can user them.

- **No DNIS Network CDN is available**: To route a Universal Networking call with a DNIS Landing Pad to a target network node, the DNIS Network CDN at the target network node must be configured and acquired. If the DNIS Network CDN at the target network node is not configured and acquired, then Event 49034 is logged to the Event Browser at the source stating No DNIS Network CDN available at <TargetSiteName>. The Network Communication Parameters page in Contact Center Manager Administration for the source site displays a similar message for the configurable time that the target is filtered.
- **General problems with Universal Networking**: If no Universal Networking calls are routed or if other problems with Universal Networking calls occur, it may be related to the state of the dependent NT Services.
- **Acquisition status errors are occurring for Landing Pad CDNs and the DNIS Network CDN**: The Contact Center Manager Administration CDNs (Route Points) page has an acquired Status column for Landing Pad CDNs and the DNIS Network CDN. This column displays the status of the CDN on the telephony PABX. Possible values are Acquired, Acquire Pending, Not Acquired, or Acquired Failed. If the telephony PABX properly acquires the CDN in question, but one of the Contact Center Manager Server components is not aware of the acquisition, then an acquisition status error can occur. A Landing Pad CDN or the DNIS Network CDN status is Acquired, but there is a problem with the operation of the CDN (for example, after system restarts). In this case, an event appears in the Event Browser indicating UNE_Service is not aware of the acquisition status of CDN <CDN_Number>.

Prerequisites

- Determine the type of call routing problem that is occurring with Landing Pads in Universal Networking.

Procedure steps

Step	Action
1	If the error message All Landing Pads Busy at <TargetSiteName> appears, check that all CDN Landing Pads are acquired.
2	If the Event Browser displays Event 49034 stating No DNIS Network CDN available at <TargetSiteName>, configure and acquire the DNIS Network CDN at the target network node.
3	If general problems are occurring with Universal Networking, open the NT Services manager and verify that the following services are up: • CCMS ASM_Service • CCMS TFE_Service • CCMS NBMSM_Service • CCMS OAMCMF_Service

- CCMS UNE_Service

If you cannot start these services manually from the NT Services manager, you may need to reboot the system to solve the problem.

4 If acquisition status errors are occurring for Landing Pad CDNs and the DNIS Network CDN, deacquire and reacquire the CDN <CDN_Number> noted in the error message.

--End--

Contact Center Multimedia troubleshooting

This section describes the troubleshooting procedures that you should perform when handling Contact Center Multimedia problems in Avaya Aura™ Contact Center Release 6.0/6.1.

Prerequisites for Contact Center Multimedia troubleshooting

- Verify your selected servers before installing Contact Center Multimedia. This verification includes making sure the computers conform to the specifications listed in *Avaya Aura™ Contact Center Planning and Engineering* (NN44400-210).
- Ensure that the operating system is installed and functioning properly.
- Ensure that both the Contact Center Multimedia server and the Redundancy server are set with the current local date and time for installation and switching Primary servers to work correctly.
- Ensure that server names and IP addresses match.
- Ensure that the US English option is selected in the Windows 2008 Server Regional Options control dialog box (on the Regional Options tab and the Advanced tab).
- Ensure that you get technical support for all hardware issues. Hardware diagnostics are the responsibility of the hardware vendor.
- Ensure that you verify the manufacturer's instructions before you perform any hardware-related procedure.

Navigation

Troubleshooting Multimedia licensing configuration errors

The Contact Center License Manager server contains the files required to determine what features and functionality are enabled in the contact center. If licensing is working properly, the enabled bit in the cls.Licenses table for the Contact Center Multimedia caché database is 1.

Procedure steps

Step	Action
1	Verify the Multimedia services are started.
2	Check the contents of the license registry.
3	Check the connection between the Multimedia server and the License server.
4	Check the name of the License server in the Multimedia Administrator.
5	Choose the correct license type.
6	Check the licenses in your contact center.
7	Review the license log files.

--End--

Verifying the Multimedia services are started

Verify that the Contact Center Multimedia License Service and the Contact Center Multimedia Starter Service are both Started.

Procedure steps

Step	Action
1	On the Windows **Start** menu of the Multimedia server, choose **Administrative Tools, Services**.
2	Next to CCMM License Service, verify that the **Status** is Started and the **Startup Type** is Automatic.
3	Next to CCMM Starter Service, verify that the **Status** is Started and the **Startup Type** is Automatic.

--End--

Checking the contents of the Contact Center License Manager registry

Check that the contents of the Contact Center License Manager registry on the Contact Center Multimedia server identify the Contact Center License Manager server. See HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Nortel\LM\LSHost.

If the contents of the LSHost registry key are invalid, change the Contact Center License Manager key in the Multimedia Administrator. See Changing the name of the Contact Center License Manager server in Contact Center Multimedia (page 54).

Prerequisites

- Ensure that you are trained and qualified to edit the Contact Center License Manager registry.
- Back up the Contact Center License Manager registry before making any changes.

Procedure steps

Step	Action
1	On the Multimedia server, choose **Start, Run**.
2	In the **Run** box type Regedit.
3	In the Registry Editor application, expand **My Computer**.
4	Expand **HKEY_LOCAL_MACHINE**.
5	Expand **Software**, **Wow6432Node**, **Nortel**, **LM** and **LSHost**. The <IP Address of Contact Center License Manager Real applicaton>:<Contact Center License Manager server name> is displayed in the LSHost data.
6	Note the IP address for the Contact Center License Manager.

--End--

Checking the link to the Contact Center License Manager server

Ping the Contact Center License Manager server identified in the registry key to ensure that no network problems exist. If you cannot ping the Contact Center License Manager server, change the Contact Center License Manager key using the Multimedia Administrator, see Changing the name of the Contact Center License Manager server in Contact Center Multimedia (page 54), or debug the network to see why Contact Center Multimedia cannot contact the Contact Center License Manager server.

Prerequisites

- Ensure that you are trained and qualified to edit the Contact Center License Manager registry.
- Back up the Contact Center License Manager registry before making any changes.

Procedure steps

Step	Action
1	On the Multimedia server, choose **Start, Run**.
2	In the **Run** box type cmd.
3	In the command prompt window, type ping lmservername, where lmservername is the IP address of the Contact Center License Manager server that you determined in step 6 of Checking the contents of the Contact Center License Manager registry (page 53).

--End--

Changing the name of the Contact Center License Manager server in Contact Center Multimedia

Change the name of the Contact Center License Manager server in Contact Center Multimedia only if the Contact Center License Manager server identified in the registry key does not match the Contact Center License Manager server configured in the Multimedia Administrator. These names must match in order for Contact Center to function properly.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration application.
2	Click **Multimedia**.
3	In the left column, click **General Administration**.
4	Click **Server Settings**.
5	In the Server Settings window, click the **Contact Center License Server**.
6	Click **Edit**.

7 Change the name or the port number for the Contact Center License server. The default port number is 3998.

8 In the **Backup Server** box, type the name for the backup Contact Center License Manager server, if you have one.

9 Click **Save**.

10 On the **Start** menu, choose **Administrative Tools, Services**.

11 Stop the CCMM Starter service.

12 Stop the CCMM License service.

13 Start the CCMM License service.

14 Start the CCMM Starter service.

--End--

Changing the license type

Change the license type on the Contact Center Multimedia server only if necessary to ensure that the type of license (Nodal or Corporate) on the Contact Center License Manager server, specified in the registry at HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Nortel\LM\Type, matches the license type defined in Contact Center Multimedia, specified in the registry on the Multimedia server in HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Nortel\LM\Type.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration application.
2	Click **Multimedia**.
3	In the left column, click **General Administration**.
4	Click **General Settings**.
5	Under **License Type** box, choose the license type (NODAL or CORP).
6	Click **Save**.
7	On the **Start** menu, choose **Administrative Tools, Services**.
8	Stop the CCMM Starter service.
9	Stop the CCMM License service.
10	Start the CCMM License service.
11	Start the CCMM Starter service.

--End--

Reviewing the Contact Center License Manager file

Review the Contact Center License Manager file to determine whether the necessary licenses for your Contact Center Multimedia operation are present. If required, add the necessary licenses to the Contact Center License Manager file on the Contact Center License Manager server.

If the license file does not contain the lines LM_MMP or LM_MMS, then Contact Center Multimedia does not work.

Procedure steps

Step	Action
1	On the Start menu of your Contact Center Manager Server, choose **All Programs**, **Avaya**, **Contact Center**, **License Manager**, **Configuration**.
2	In the Contact Center Licensing window, click the **Real Time Usage** tab.
3	Review these entries in the file D:\Avaya\lm\bin\plservrc on the License Manager server. For example, if the file contains hqvD950dcWZqbmxtoc3V3dnaC9uvNHk+WJlxtaimKiihIbkfyGG1Nw5OVl5 aWFg= #CCM 6.0 00:04:75:f8:0b:8d LM_MMPN (1) 60 secs, then the existence of LM_MMPN indicates that Multimedia is licensed nodally.

--End--

Adding licenses to your current Contact Center License Manager file

Add licenses by contacting your distributor to upgrade your license and then change and install your Contact Center License Manager file.

Prerequisites

- Contact your distributor to upgrade your license.
- Ensure that you have your new License Manager file.

Procedure steps

Step	Action
1	On the Start menu, choose **Administration Tools**, **Services**.
2	Stop the CCMM Starter service.
3	Stop the CCMM License service.
4	Start the CCMM License service.
5	Start the CCMM Starter service.

--End--

Reviewing the Contact Center License Manager log files

Review the Contact Center License Manager log files to look for any errors that have occurred. If you are unable to find or diagnose the cause of the errors, contact Avaya technical support.

Procedure steps

Step	Action
1	On the Contact Center License Manager server, review the log file specified in the registry at HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Nortel\LM\Server\Logfile.
2	On the Contact Center Multimedia server, review the log file specified at location D:\Avaya\Logs\Common Components\CC_LMClient_1.log and D:\Avaya\Logs\CCMM\CCMM_LMService_1.log.
3	On the Contact Center Multimedia server, review the CCMM Starter Service log file specified in Avaya\Licensing\CCMMStartService.exe.config in the variable logFilename.

--End--

Resetting the Licensing grace period

If there is a communication error between Contact Center Multimedia and the Contact Center License Manager, normal operation of Contact Center Multimedia server can run for a defined grace period. Normal operations such as shutting down the server, starting up the server, or restarting the services do not affect the grace period

The defined grace period is 30 days. When the 30 days expires, the Contact Center Multimedia services shut down and cannot be restarted until the grace period is reset.

The grace period is decreased whenever a communication error occurs. For example, if the first communication problem is resolved in two days, there are still eight days available to permanently fix the licensing issues.

The Application log section of the Windows Event Viewer shows when grace period time has elapsed. When the grace period expires, the event 61154 Fatal Error appears in the Windows Event Viewer.

You can contact Avaya to reset the grace period. Schedule the grace period reset outside of normal contact center working hours.

Procedure steps

Step	Action
1	On the Contact Center Multimedia Server, choose **Start, Administrative Tools, Event Viewer**.
2	Double-click the event where the grace period has decreased (Error 61151) or expired (Error 61154).
3	In the Event Properties dialog box, copy the lock code. The lock code appears immediately after the text Lock code = in the Description box.
4	Send the Lock code you copied to Avaya Technical Support. *Avaya Technical Support supplies you with an unlock code.*
5	After Avaya Technical Support supplies you with an unlock code, in the Contact Center Multimedia Server, choose **Start, All Programs, Avaya, Contact Center, Common Utilities, Grace Period Reset**.
6	In the Avaya Contact Center License Grace Period Reset application, in the **Enter the code received from Avaya** box, type or copy the code received from Avaya.
7	Click **Apply**.
8	Ensure that the status changes to Code decrypted successfully.
9	Click **Exit**.
10	On the Start menu, choose **Administrative Tools, Services**.
11	Stop the CCMM Starter service.
12	Stop the CCMM License service.
13	Start the CCMM License service.
14	Start the CCMM Starter service.

--End--

Troubleshooting database access errors

If the system cannot access the database, you need to check for several potential issues.

Procedure steps

Step	Action
1	Ensure that the Multimedia services are running.
2	Ensure that you can connect to the database.
3	Check the size of the database in the D:\Avaya\Contact Center\Databases\CCMM\MULTIMEDIA\DATA\Cache.Dat file, where D is the database drive. If the space is at the maximum, archive the data in the database.

--End--

Troubleshooting logon errors

If you cannot log on to Contact Center Multimedia, you need to check that the database is running.

Procedure steps

Step	Action
1	Verify that the database is running.

--End--

Troubleshooting an ODBC error

An ODBC error can occur when there is a delay in the database startup.

Procedure steps

Step	Action
1	Wait a few minutes, and then try to perform the task you were attempting again.

--End--

Reviewing E-mail Manager Event Logs

E-mail Manager Event Logs are the primary tool for dealing with problems that can occur while using E-mail Manager.

Procedure steps

Step	Action
1	On the Multimedia server, select **Start**, **Administrative Tools**, **Event Viewer**.
2	Expand **Custom views**.
3	Review the event messages where the Source is Email.

--End--

Troubleshooting when the E-mail Manager cannot log on to a mailbox

When the E-mail Manager cannot log on to a mailbox, there are several possibilities for this problem to occur.

Procedure steps

Step	Action
1	Log on to the mailbox using an e-mail client.
2	Verify that the domain name, account name, mailbox name, and password match the e-mail server settings.
3	Verify that the e-mail server is running and that it is set up properly.
4	Review the log files.
5	Use telnet to verify the user names on the server.

--End--

Verifying the user names on the server

Verify the user names on the server by logging on to the e-mail server. If the logon is successful, a message appears:

+OK X1 NT-POP3 Server mail009 (IMail 7.04 997957-16)
user billing
+OK send your password
pass abc123
+OK maildrop locked and ready

If the logon is not successful, a message appears:

+OK X1 NT-POP3 Server mail009 (IMail 7.04 998172-17)
user billing
+OK send your password
pass 123abc
-ERR Invalid userid/password

Procedure steps

Step	Action
1	On the **Start** menu of the E-mail Server, choose **Run**.
2	Type telnet <mailserver> 110 (where 110 is the port number for POP3), and then press **Enter**.
3	Log on to the e-mail server.
4	Review the message to determine whether or not the logon is successful.

--End--

Troubleshooting when the Multimedia E-mail Manager Inbox does not receive e-mail

Troubleshoot when the Multimedia E-mail Manager Inbox does not receive e-mail by verifying that the e-mail server is working properly and that the host names of the external mail servers are correctly recorded on the Multimedia server.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration application.
2	Click **Multimedia**.
3	In the left column, click **General Administration**.
4	Click **Server Settings**.
5	Double-click the **Inbound POP3 Server**.
6	Under **Edit Server Details**, change the name of the server and the port number of the server as required.
7	Click **Save**.
8	Double-click the **Outbound SMTP Server**.
9	Under **Edit Server Details**, change the name of the server and the port number of the server as required.
10	Click **Save**.

--End--

Troubleshooting when Asian characters are not supported in e-mail

Troubleshoot to ensure Asian characters are supported in e-mail by installing the Windows Server 2008 Release 2 Multilingual User Interface Language Packs.

Prerequisites

- Download the x64 version of the Windows Server 2008 Release 2 Multilingual User Interface Language pack from www.microsoft.com.

Procedure steps

Step	Action
1	Click **Start, Control Panel, Clock, Language, and Region.**
2	Click the **Keyboards and Languages** tab.
3	Click **Install/uninstall languages**.
4	Click **Install display languages**.
5	Click **Browse** to locate the language pack that you downloaded.
6	Click **Next** to install the language pack.
7	If you are prompted to insert your Windows Server DVD, insert the Windows Server 2008 Release 2 64-bit Edition DVD into the DVD drive.
8	Reboot your server, if required.

--End--

Troubleshooting the corruption of outgoing e-mail

Troubleshoot the corruption of outgoing e-mail by changing the encoding. The E-mail Manager, by default, encodes outgoing e-mail using UTF-8. On some systems, for e-mail message to be sent successfully, the platform encoding needs to be modified to match the encoding of the sending language family.

Acceptable encoding values are available at http://java.sun.com/j2se/1.5.0/docs/guide/intl/encoding.doc.html.

Prerequisites

Determine which one of the following types of coding is required for your system:

- US-ASCII American Standard Code for Information Interchange
- windows-1250 Windows Eastern European
- windows-1251 Windows Cyrillic
- windows-1252 Windows Latin-1
- windows-1253 Windows Greek
- windows-1254 Windows Turkish
- windows-1257 Windows Baltic
- ISO-8859-1 Latin Alphabet No. 1
- ISO-8859-2 Latin Alphabet No. 2
- ISO-8859-4 Latin Alphabet No. 4

- ISO-8859-5 Latin/Cyrillic Alphabet
- ISO-8859-7 Latin/Greek Alphabet
- ISO-8859-9 Latin Alphabet No. 5
- ISO-8859-13 Latin Alphabet No. 7
- ISO-8859-15 Latin Alphabet No. 9
- KOI8-R KOI8-R, Russian
- UTF-8 Eight-bit UCS Transformation Format
- UTF-16 Sixteen-bit UCS Transformation Format, byte order identified by an optional byte-order mark
- UTF-16BE Sixteen-bit Unicode Transformation Format, big-endian byte order
- UTF-16LE Sixteen-bit Unicode Transformation Format, little-endian byte order

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration application.
2	Click **Multimedia**.
3	In the left column, click **Email**.
4	Click **General Settings**.
5	Under **Encoding**, in the **Encoding for agent initiated emails** list, select the type of encoding you want to use.
6	Click **Save**.
7	On the Start menu of the Multimedia server, choose **Administrative Tools, Services**.
8	Right-click CCMM Email Manager service, and then click **Restart**.
9	Close the window.

--End--

Troubleshooting outgoing e-mail errors with MS Exchange 2007

Troubleshoot when outgoing e-mail is not sent when using Microsoft Exchange 2007 to send e-mail from the Contact Center Multimedia agent desktops. If you are using Microsoft Exchange 2007, you must ensure that additional configuration is performed on the Contact Center Multimedia Server and the Microsoft Exchange server.

If you are using Microsoft Exchange 2003, additional configuration is not required.

Prerequisites

- Ensure that you are using Microsoft Exchange 2007 on your e-mail server.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration application.
2	Click **Multimedia**.
3	In the left column, click **General Administration**.
4	Click **Server Settings**.
5	Select the **Outbound SMTP Server**.
6	Click **Edit**.
7	Under **Advanced SMTP Settings**, select **Base 64 Encoded Authentication**.
8	Click **Save**.
9	Log on to the Microsoft Exchange 2007 server.
10	Open the Exchange Management Console.
11	Click **Server Configuration, Hub Transport, Receive Connectors Tab**.
12	Right-click the **Default <Servername>** and click **Properties**.
13	Click the **Authentication** tab.
14	Ensure that only the following options are checked for authentication: • Basic Authentication • Exchange Server Authentication • Integrated Windows Authentication
15	Close the Exchange Management Console.

--End--

Troubleshooting when the system fails to send an auto-acknowledgement or e-mail response to a customer

Troubleshoot to determine the reason why the system failed to send an auto-acknowledgement or e-mail response to a customer by reviewing the possible reasons the error occurred.

Procedure steps

Step	Action
1	Verify the following: • An auto-acknowledgement is configured in the Multimedia Administrator. • The SMTP service is running on the e-mail server. • The Contact Center E-mail Manager service is running on the Contact Center Multimedia server. • The customer's e-mail address is correct.

--End--

Troubleshooting an unsupported authentication mechanism

Troubleshoot an unsupported authentication mechanism if, after submitting the EHLO command, the server responds with error codes 500, 501, or 502. These error codes indicate that SMTP Authentication is not supported on that mail server.

If you receive a message 504 Authentication mechanism unsupported after the AUTH LOGIN command, it is possible that your mail server conducts SMTP Authentication by either not encoding the logon credentials or by using CRAMMD5 encoding.

You must not select TLS encryption if the server responds with these error codes.

Procedure steps

Step	Action
1	Contact your distributor for further details.

--End--

Communication Control Toolkit troubleshooting

This section describes the troubleshooting procedures that you should perform when handling Communication Control Toolkit issues.

Prerequisites for Communication Control Toolkit troubleshooting

- Ensure that you are aware of the configurations of your Communication Control Toolkit server software before you begin.
- Communication Control Toolkit configuration is one of the following:
  - Communication Control Toolkit on Avaya Communication Server 1000 - contact center
  - Communication Control Toolkit on Avaya Communication Server 1000 - Knowledge Worker
  - Communication Control Toolkit with Microsoft Office Communication Server
  - Communication Control Toolkit with the Avaya Aura™ Unified Communications platform - contact center

Navigation

- Troubleshooting when you cannot stop the Telephony service (page 68)
- Troubleshooting when you cannot add the Administrator to the Communication Control Toolkit console (page 68)
- Troubleshooting when the CCT Administrator Snap-in cannot connect to the Communication Control Toolkit database (page 68)
- Troubleshooting when the CCT Administrator Snap-in cannot import XML data to the CCT database (page 69)
- Troubleshooting when the CCT Web Administration page does not launch from CCMA (page 69)
- Troubleshooting when the CCT Web Administration page launches without any data (page 70)
- Troubleshooting when the Agent Desktop does not display CCT resources (page 70)
- Troubleshooting when the hotdesking does not work (page 70)
- Troubleshooting when after a migration, agents in CCMA do not have users associated with them (page 71)
- Troubleshooting when an agent on a call cannot log off after a switchover (page 71)
- Troubleshooting errors when importing contact center users (page 72)

- Troubleshooting following a power outage (page 72)
- Troubleshooting when the cache service is unavailable after a server reset (page 73)

Troubleshooting when you cannot stop the Telephony service

When you cannot stop the Telephony service on a CCT server on an Avaya Communication Server 1000 platform, you must disable remote access and restart the server.

Procedure steps

Step	Action
1	Disable the Remote Access connection manager and Remote Access Auto connection manager services.
2	Restart the server for these changes to take effect.

--End--

Troubleshooting when you cannot add the Administrator to the Communication Control Toolkit console

If you receive an error when you try to add the Administrator to the Communication Control Toolkit console, do not attempt to make any changes.

Procedure steps

Step	Action
1	Contact your Avaya support prime for assistance.

--End--

Troubleshooting when the CCT Administrator Snap-in cannot connect to the Communication Control Toolkit database

The CCT Administrator Snap-in may not be able to connect to the CCT database if Terminal Server and Terminal Server Licensing were installed before you installed CCT. The installation of Terminal Services interferes with communication between Communication Control Toolkit and its database.

Procedure steps

Step	Action
1	Uninstall and reinstall all components in the following order: • Communication Control Toolkit • Terminal Server • Terminal Server Licensing

--End--

Troubleshooting when the CCT Administrator Snap-in cannot import XML data to the CCT database

The CCT Administrator Snap-in may not be able to import XML data into the Communication Control Toolkit database if the format selected in the CCT Administrator Snap-in Data Import/Export tool is not correct.

Procedure steps

Step	Action
1	In the CCT Administrator Snap-in, in the Data Import/Export tool, check the format selected matches the format of the input file.

--End--

Troubleshooting when the CCT Web Administration page does not launch from CCMA

The CCT Web Administration may not load if Tomcat is not running or the internet browser has not been configured correctly.

Procedure steps

Step	Action
1	Check Tomcat is running.
2	Check if the browser has been configured to allow javascript.
3	Check if the firewall is on, the Avaya Aura™ Contact Center firewall policy to open contact center ports has been applied.

--End--

Troubleshooting when the CCT Web Administration page launches without any data

The CCT Web Administration may not display data if the relevant services are not running.

Procedure steps

Step	Action
1	Check the CCT DAL service is running in the SCMU utility.
2	Check if Caché is running.

--End--

Troubleshooting when the Agent Desktop does not display CCT resources

Agent Desktop may not display CCT terminals due to CCT configuration issues.

Procedure steps

Step	Action
1	Check the agent, user, terminal and address resource assignment in the CCT Web Administration.
2	If the configuration is standalone, ensure the deployment type is configured in CCT Administrator Snap-in.
3	Ensure there are no PABX issues.

--End--

Troubleshooting when the hotdesking does not work

If hotdesking is not working check the configuration in the CCT Web Administration.

Procedure steps

Step	Action
1	Check the agent is created in the CCMA server and is assigned to a CCT domain user.
2	Check the correct addresses are assigned to each terminal in CCT Web Administration.
3	Check each terminal is assigned to a workstation in CCT Web Administration.
4	Check the terminals for hotdesking are assigned to a terminal group in CCT Web Administration.

5 Check windows users for hotdesking are assigned to a user group in CCT Web Administration.

6 Check the terminal group is assigned to the user group in CCT Web Administration.

--End--

Troubleshooting when after a migration, agents in CCMA do not have users associated with them

If there are agents visible in CCMA after a migration without users associated to them, then there is possibly a mismatch between the first name and last name of the user and the first name last name of the agent.

In the current release, when an agent is created, CCMA uses the CCT windows user first name and last name as the agent's first name and last name. Therefore in a migration from a previous release when this one to one mapping of user first name and last name and agent first name and last name was not used, CCMA will display agents without their associated windows user.

Procedure steps

Step	Action
1	Check the first name and last name of the windows user matches the first name and last name of the agent.
2	If it does not match edit the names to match or create new users to match the agent details.

--End--

Troubleshooting when an agent on a call cannot log off after a switchover

If an Agent is on a call when a switchover occurs, the call does not appear on Agent Desktop after the switchover is complete. The result is the Agent can see that the call is missing, but cannot log off until after the call is finished. The agent cannot log off while on a call. The log off request remains pending in the Avaya Communication Server 1000 until the call ends.

Procedure steps

Step	Action
1	The Agent attempts to log off.
2	The Agent waits until the call is finished and then the agent is automatically logged off.

--End--

Troubleshooting errors when importing contact center users

Contact center users are imported from the Communication Control Toolkit console. If users cannot be imported, do not attempt to configure them manually. Check for various issues that may be causing problems when importing users.

Prerequisites

- Ensure that the Contact Center Manager Server and Contact Center Manager Administration server are configured and active.
- Ensure that the CCMS_OAMCMF service is running.
- Ensure that the OpenQ feature is enabled.
- Ensure that Deployment Type of Communication Control Toolkit is configured correctly in Communication Control Toolkit Console.

Procedure steps

Step	Action
1	Check that the agent can be logged in on a telephone.
2	Check that the correct skillsets have been assigned to the agent and that licenses for these agents are available. Licensing errors can be viewed in the Event Viewer.

--End--

Troubleshooting following a power outage

Following a power outage, view the Windows event logs to determine if any service did not stop gracefully during the power outage.

Procedure steps

Step	Action
1	On the Communication Control Toolkit server, open the Windows Event Viewer.
2	Determine if any events were created to indicate a service failure by reviewing the following logs: • DrWatson • hdmp • mdmp

- Java hotspot

3 Follow up on any specific errors described in the event logs.

--End--

Troubleshooting when the cache service is unavailable after a server reset

The cache service is grayed out after the server is reset during a restoration of the Communication Control Toolkit database.

Procedure steps

Step	Action
1	On the Communication Control Toolkit server, stop the Cache service.
2	Delete the file D:\Avaya\Cache\CacheSys\mgr\CACHE.WIJ.
3	Start Cache service. The cache service is available although CCT services did not successfully start. You cannot restore the CCT database.

--End--

Using CCT Reference Client for troubleshooting

In addition to using the Reference Client to verify the Communication Control Toolkit installation, you can use the Communication Control Toolkit Reference Client as a diagnostic tool with Avaya Aura™ Contact Center Release 6.0/6.1. The Reference Client application is designed to troubleshoot your client applications.

If the Reference Client does not demonstrate the functionality you require, then there is a problem in your client application. Otherwise, there is a problem with the Communication Control Toolkit server software.

You can use the Reference Client application to do the following:

- Verify the server settings, if required.
- View agent, device, or contact details.
- View the event log.
- Test telephone functions.

Navigation

- Logging on to the Reference Client (page 76)
- Viewing agent, device, and contact details (page 76)
- Viewing the event log during a call (page 77)
- Viewing server details (page 77)
- Making the phone busy (page 77)
- Forwarding a call (page 78)
- Turning the message waiting feature on or off (page 78)
- Generating DTMF digits while on a call (page 78)
- Attaching contact data (page 79)
- Calling a supervisor (page 79)
- Calling a supervisor while on an ACD or CDN call (page 79)
- Setting an activity code (page 80)
- Troubleshooting when the Reference Client cannot make a call (page 80)

Logging on to the Reference Client

Log on to the Reference Client to diagnose problems with the client application.

Procedure steps

Step	Action
1	Log on to the server with the Local Administrator user ID and password.
2	From the Start menu, choose **All Programs, Avaya,** Communication Control Toolkit**, RefClient**.
3	Click **OK**.
4	From the Session menu, choose **Connect**.
5	In the **User ID** box, enter your user ID.
6	In the **Domain** box, enter the host name of your Communication Control Toolkit server or the domain name for your user ID.
7	In the **Password** box, enter your password.
8	Click **OK**.
	The available devices list displays a list of lines and their associated DNs.

--End--

Viewing agent, device, and contact details

You can view information about the agents in the contact center, the associated devices, and the current contact using the Reference Client. The agent details show the information about the agent that is configured in Contact Center Manager Administration.

Procedure steps

Step	Action
1	On the View menu of the Reference Client application, click **Agent Details** to view the agent details.
2	On the View menu of the Reference Client application, click **Device Details** to view information about your current device.
3	On the View menu of the Reference Client application, click **Contact Details** to view information about the current contacts using the Reference Client during a call.

--End--

Viewing the event log during a call

You can view the event log during a call to help diagnose any issues you experience when you connect to your phone.

Procedure steps

Step	Action
1	Log on to the Reference Client.
2	From the **View** menu, choose **Event Log**.
3	Keep the Event Log dialog box open while you make a call using the Reference Client.
4	In the **Available Desktop Devices** box, choose a terminal that you configured.
5	Choose the address from which you want to make a call.
6	In the **Destination Address** box, enter the address you want to call.
7	Click **Originate**.

--End--

Viewing server details

You can view your server settings using the Reference Client.

Procedure steps

Step	Action
1	Log on to the Reference Client.
2	From the **Preferences** menu, choose **Server Settings**.

--End--

Making the phone busy

You can make the phone busy using the Reference Client.

Procedure steps

Step	Action
1	Log on to the Reference Client.
2	Click **DND** (do not disturb).
3	Click **Set "do not disturb"**.

--End--

Forwarding a call

You can forward a call using the Reference Client.

Procedure steps

Step	Action
1	Log on to the Reference Client.
2	Click **FWD**.
3	Click **Set/Change Forwarding Instructions…**.

--End--

Turning the message waiting feature on or off

You can turn the message waiting feature on or off using the Reference Client.

Procedure steps

Step	Action
1	Log on to the Reference Client.
2	Click **MSG**.

--End--

Generating DTMF digits while on a call

You can use the Reference Client to generate DTMF digits while on a call.

Procedure steps

Step	Action
1	Log on to the Reference Client.
2	Click **DTMF**.

--End--

Attaching contact data

You can use the Reference Client to attach contact data while on a call.

Procedure steps

Step	Action
1	Log on to the Reference Client.
2	Click **Data**.

--End--

Calling a supervisor

You can call a supervisor using the Reference Client.

Procedure steps

Step	Action
1	Log on to the Reference Client.
2	Click **Supervisor**.

--End--

Calling a supervisor while on an ACD or CDN call

You can use the Reference Client to call a supervisor while on an ACD or CDN call.

Procedure steps

Step	Action
1	Log on to the Reference Client.
2	Click **Emergency**.

--End--

Setting an activity code

You can set an activity code using the Reference Client.

Procedure steps

Step	Action
1	Log on to the Reference Client.
2	Click **Activity Code**.

--End--

Troubleshooting when the Reference Client cannot make a call

Troubleshoot using the following procedure if the Reference Client application receives the signaling when a phone is taken off the hook, but the Reference Client fails when an attempt is made to make a call from the phone.

Procedure steps

Step	Action
1	Ensure that the SECU prompt on the PABX is set to yes in LD17.

--End--

Agent Desktop troubleshooting

Troubleshooting Agent Desktop must be done to address errors that occur when the agent is working on the application.

Prerequisites for Agent Desktop troubleshooting

- Read the *Avaya Aura™ Contact Center Server Administration* (NN44400-610) guide.

Navigation

Troubleshooting logon problems to the Agent Desktop

Troubleshoot when you encounter problems logging on to the Agent Desktop by reviewing the possible reasons for the error.

Procedure steps

Step	Action
1	Verify that IIS is running.
2	Verify that ASP and ASP.NET are enabled.
3	Verify that the user has access rights to the Web applications.
4	Verify that the services on the Contact Center Multimedia server are running.

5 Verify that the software for .NET Framework and .NET service pack 3.5 is installed on the clients.

6 Verify that the agent ID is valid.

7 Verify that the agent password is valid, or is the default password.

8 Verify that you have not exceeded the number of Agent Desktop or Outbound Campaign Management Tool licenses in your Contact Center.

9 Verify that Domain Naming Service (DNS) is working.

10 Verify that you can ping the Contact Center Multimedia server (multimedia solution) or the Communication Control Toolkit server (voice only solution) by name.

11 Verify that you have a two way trust with the Contact Center Multimedia server domain (multimedia solution) or the Communication Control Toolkit server domain (voice only solution).

--End--

Troubleshooting when an agent does not remember password

Troubleshoot when an agent forgets his or her password by resetting the password to the default setting. You can use the Multimedia Administrator application to reset the password to the default agent password, which is the agent ID or assign any password.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration application.
2	Click **Multimedia**.
3	In the left column, click **General Administration**.
4	Click **Agent Settings**.
5	Under **Edit Current Agents**, select the agent for the password change or reset.
6	Under **Edit Agent Details**, click **Set Password** and type the new password in the **New Password** and **Confirm Password** boxes.
7	Click **Save**.

--End--

Troubleshooting problems connecting to the CCT server

Troubleshoot if there are problems on the Communication Control Toolkit server and you see the error message Cannot connect to CCT Server. You need to review the possible reasons why you may be having a problem connecting to the CCT server.

Procedure steps

Step	Action
1	On the Communication Control Toolkit server, check that the CCT Server service is started. For more information, see *Avaya Aura™ Contact Center Commissioning* (NN44400-312).
2	In the Multimedia Administrator application, check that the Communication Control Toolkit server is correct. If you must change the name of the Communication Control Toolkit server, you must also change the CCTSERVER key in the ccad.exe.config file in the Avaya\Contact Center Multimedia\Agent Desktop directory on the Contact Center Multimedia server.
3	Make sure that ASP.NET is enabled on the Contact Center Multimedia server. For more information, see *Avaya Aura™ Contact Center Commissioning* (NN44400-312).

--End--

Troubleshooting an Invalid Credentials error

Troubleshoot if you receive an error message indicating Invalid Credentials. The windows user is not configured for Communication Control Toolkit authentication.

Procedure steps

Step	Action
1	Ensure that you have followed the Communication Control Toolkit configuration steps in this guide.
2	If the user is outside the Communication Control Toolkit domain, then use a local account on the Communication Control Toolkit server to launch the Agent Desktop. You must add the local Communication Control Toolkit user to the resources and map the resources.

--End--

Troubleshooting when an agent cannot login to CCMS

Troubleshoot the error "Cannot login to CCMS" if a voice agent cannot login to CCMS because another agent is already logged on to that telephone.

Procedure steps

Step	Action
1	Log off the first agent, or map the current agent to a different terminal.

--End--

Troubleshooting when the Login button shows no agent

Troubleshoot when the Login button shows no agent by first determining the cause for this error. There are two possible reasons why the Login button shows no agent:

- The agent is not mapped to a contact center user.
- Agent objects are not replicated.

Procedure steps

Step	Action
1	If the agent is not mapped to a contact center user, you must map the Windows user to a contact center user for handling contacts.
2	If the agent objects are not replicated, you must ensure that Server Configuration and Contact Management Framework are both configured on the Contact Center Manager Server and on the Communication Control Toolkit server when new patches are installed.

--End--

Troubleshooting when the Originate key is disabled

If the Originate key is disabled on the telephony toolbar in the Agent Desktop, a terminal is not mapped to the logged-on agent, or the mapped terminal is out of service.

Procedure steps

Step	Action
1	If a terminal is not mapped to the logged-on agent, map the user to the terminal.
2	If the mapped terminal is out of service, restart the TAPI connector, and restart the Telephony service on the Communication Control Toolkit server.

--End--

Troubleshooting when the Emergency and Supervisor keys on the phone do not work

If the Emergency and Supervisor keys are disabled, the keys used for Emergency and Supervisor calls on phones are not configured or the telephony port property of Supervisor is incorrect.

Procedure steps

Step	Action
1	Configure two keys on the agent phone: ASP (call supervisor) and EMR (emergency).
2	Ensure that the supervisor phone is configured as a supervisor phone, and then configure two keys: AAG (answers the call from the agent ASP key) and AMG (answers the call from the agent EMR key).
3	Configure the telephony port property to be the position ID of the supervisor phone. In Contact Center Manager Administration, right-click Supervisor, and then choose Supervisor details.

--End--

Troubleshooting disabled Transfer and Conference buttons on the telephony toolbar

Troubleshoot disabled buttons by enabling then using the line features available during Communication Control Toolkit installation or maintenance procedures.

Procedure steps

Step	Action
1	Enable transfer and conference functions using the TN details.

--End--

Troubleshooting agent statistics

Troubleshoot disabled agent and skillset related statistics. Agent Desktop displays live agent and skillset related statistics.

Procedure steps

Step	Action
1	Ensure that you have a Contact Center Web Statistics (CCWS) license.

--End--

Troubleshooting opening an attachment in Agent Desktop statistics

Troubleshoot opening an inbound attachment with Agent Desktop in the Email Display section.

Procedure steps

Step	Action
1	Open Internet Explorer.
2	Select **Tools**, **Internet Options**, **Programs**.
3	Confirm the default web browser is Internet Explorer.

--End--

High Availability troubleshooting

Troubleshooting High Availability must be done to address errors that occur when the active servers does not switch over as expected or when the standby server fails to shadow the active server.

Prerequisites for High Availability troubleshooting

- Read *Avaya Aura™ Contact Center Commissioning* (NN44400-312).
- Read *Avaya Aura™ Contact Center Server Administration* (NN44400-610).

Navigation

- Troubleshooting failure to shadow (page 87)
- Troubleshooting failure to switch over (page 88)
- Troubleshooting active server resources (page 89)

Troubleshooting failure to shadow

Troubleshoot when the standby server does not shadow the active server. The standby set of Avaya Aura™ Contact Center applications monitors and shadows the active applications in the system and does not process calls. The standby CCMS monitors the active CCMS. The standby CCT monitors the active CCT. The standby CCMM monitors the active CCMM. Each active and standby pair of applications forms a resilient or replication pair. If any of the active applications fail, the standby applications recognize the failure and start processing contacts.

Procedure steps

Step	Action
1	Verify that the standby server is installed exactly the same as the active server. The standby and active servers must have the exact same patch level and the same hard disk drive partitions.
2	Verify that Cache is running on the standby server.
3	Verify that you have installed a Standby Server license to enable High Availability.
4	Verify that the standby server can communicate with the active server by name and IP address.
5	Verify that you can ping the Managed IP address of the active server from the standby server and from a client computer.
6	Verify that the static IP address of the active and standby servers are configured correctly in the High Availability configuration utility.

7	Ensure that the standby server is configured exactly the same as the active server. Backup the active server database and restore this database onto the standby server.
8	Examine the Windows Event Viewer on the active and standby servers for High Availability, network, or Contact Center-related error messages.

--End--

Troubleshooting failure to switch over

Troubleshoot when the active server does not switch over to the standby server. Each active and standby pair of applications forms a resilient or replication pair. If any of the active applications fail, the standby applications recognize the failure and start processing contacts.

Attention: In a campus co-resident CCMS and CCT solution, only a CCMS service failure, hardware, network, or database failure can initiate a switchover. A CCT service failure does not initiate an automatic switchover, CCT simply restarts itself.

Procedure steps

Step	Action
1	Verify that the standby server can shadow the active server.
2	Verify that the switchover check box on both servers is selected.
3	Verify that the standby server is installed exactly the same as the active server. The standby and active servers must have the exact same patch level and the same hard disk drive partitions.
4	Verify that you have installed a Standby Server license to enable High Availability.
5	Verify that the standby server can communicate with the active server by name and IP address.
6	Verify that you can ping the Managed IP address of the active server from the standby server and from a client computer.
7	Verify that the static IP address of the active and standby servers are configured correctly in the High Availability configuration utility.
8	Ensure that the standby server is configured exactly the same as the active server. Backup the active server database and restore this database onto the standby server.
9	Examine the Windows Event Viewer on the active and standby servers for High Availability, network, or Contact Center related error messages.

--End--

Troubleshooting active server resources

Avaya Communication Server 1000 resources acquired by the CCMS are not deacquired at the time of a failure, and the login state of voice agents is maintained when the backup CCMS comes online. This means that in the event of a CCMS outage, there is no need for agents to cycle their voice login state. The standby CCMS will start up and show the correct state of every agent's voice terminal as they were at the time of the active CCMS outage. There is no impact to calls that are in progress between a customer and an agent,

CCMS does not deacquire Avaya Communication Server 1000 resources when stopped by the High Availability utility therefore caution must be exercised when starting a CCMS in a High Availability environment to ensure the Avaya Communication Server 1000 resources are available to it.

CCMS de-acquires Avaya Communication Server 1000 resources when stopped by the System Control and Monitor Utility (SCMU).

Procedure steps

Step	Action
1	Ensure the active Contact Center Manager Server has full control privileges over Avaya Communication Server 1000 resources by using the System Control and Monitor Utility (SCMU) to completely stop all CCMS servers in the contact center.

--End--

Networking troubleshooting

This section describes the procedures required to troubleshoot networking problems in Avaya Aura™ Contact Center Release 6.0/6.1.

Navigation

Troubleshooting network connection problems

If you test the contact center server subnet and ELAN subnet connection using the ping command, and the test fails, then follow these steps to verify that the server ELAN subnet and contact center server subnet cards are configured and identified correctly.

When Contact Center Manager Server is used with Avaya Communication Server 1000, time changes on the Contact Center Manager Server can cause communication issues on the ELAN subnet. This can cause defaulting calls for short durations and can typically self-recover after a number of minutes. For more information, see Disabling the time synchronization features on the operating system (page 93).

Prerequisites

- Ensure that you have a laptop or PC that is near the server and can be connected directly to the server. In this procedure, the laptop or PC is referred to as the client.
- Ensure that you are using a direct connect (crossover) network cable that allows two PCs to be directly connected without a hub between them.

Procedure steps

Step	Action
1	Resolve the failed ping.
2	Retest the ELAN subnet and contact center server subnet network connection.
3	Disable the time synchronization features on the operating system.

--End--

Resolving a failed ping

If you test the contact center server subnet and ELAN subnet connection using the ping command, and the test fails, then follow these steps to verify that the server ELAN subnet and contact center server subnet cards are configured and identified correctly.

Procedure steps

Step	Action
1	Plug the crossover network cable into the network card in the client.
2	Plug the other end into the ELAN subnet card in the server.
3	If you must restore the IP address information of the client after this procedure, then record the TCP/IP address, subnet mask, and gateway of the client.
4	Configure the client with an IP address that is part of the same subnet as the IP address assigned to the ELAN subnet card. For example, if the server ELAN subnet card has the IP address 1.1.1.1, then assign the client an IP address of 1.1.1.2.
5	Set the client PC to have an subnet mask of 255.0.0.0. Leave the gateway blank.
6	Open an MS-DOS prompt window on the client and try to ping the server ELAN subnet card. For example, if the server ELAN subnet card has the IP address 1.1.1.1, then type ping 1.1.1.1 and press Enter. *If the ping test succeeds, then you know that you have correctly identified the ELAN subnet card in the network control panel. The other network card, if present, must be the contact center server subnet card.*
7	From the server, repeat the steps described in the procedure “Retesting the ELAN subnet and contact center server subnet network connection.” If the test fails, then verify that the network is set up correctly

--End--

Retesting the ELAN subnet and contact center server subnet network connection

If you test the contact center server subnet and ELAN subnet connection using the ping command, and the test fails, then follow these steps to verify that the server ELAN subnet and contact center server subnet cards are configured and identified correctly.

Procedure steps

Step	Action
1	Ensure you are logged on to the server as Administrator.
2	From the **Start** menu, choose **All Programs, Accessories, Command Prompt**.
3	In the Command Prompt window, type **ping** followed by the ELAN subnet IP address for the PABX, and then press Enter. For example, enter ping 12.38.3.8

The display indicates whether the ping was successful. If you do not receive a successful ping message, then no connection was made.

4 To test the contact center server subnet card, type **ping** followed by the contact center server subnet IP address of another PC on the contact center server subnet, and then press Enter. For example, enter ping 47.2.13.9

The display indicates whether the ping was successful. If you do not receive a successful ping message, then no connection was made.

5 Type **exit**, and then press **Enter** to close the Command Prompt window

--End--

Disabling the time synchronization features on the operating system

When Contact Center Manager Server is used in the Avaya Communication Server 1000 environment you must disable all time synchronization features of the operating system to avoid potential call processing outages because time synchronization between Contact Center Manager Server and Avaya Communication Server 1000 and not using time modification features of the operating system such as Time servers of daylight savings configuration.

If you disable the Date and Time features after you disable the Windows Time service, the Startup type for the Windows Time service is set to Automatic.

Procedure steps

Step	Action
1	Choose **Start, Control Panel, Clock, Language, and Region**.
2	In the **Date and Time** section, click **Change the time zone**.
3	In the Date and Time dialog box, click the **Change time zone**.
4	Clear the **Automatically adjust clock for Daylight Saving Time** check box.
5	Click **OK**.
6	Click the **Internet Time** tab.
7	Click **Change settings**.
8	Clear the **Synchronize with an Internet time server** check box.
9	Click **OK**.
10	Click **Apply** to save your changes.
11	Click **OK**.

--End--

Troubleshooting network connectivity

Troubleshoot network connectivity errors between the components of the Contact Center suite by reviewing error logs, then determining the appropriate solution to the network connectivity error.

In the CCT_Server_0.log file, various errors indicate that the Contact Management Framework is not responding to requests from Communication Control Toolkit clients, and that there are problems with the network connectivity for all of the Contact Center servers. If you find the following out-of service text in CCT_Server_0.log, the error indicates that the connection between Contact Center Multimedia and Contact Center Manager Server is out of service due to network issues.

[Peer] Service Provider Status Change Event - Provider: CCMM, Status: MasterApplicationFailure

[ActiveProvider CCMM] Service provider has gone out-of-service

[Peer] Service Provider Status Change Event - Provider: ContactManager, Status: MasterApplicationFailure

[ContactManager] Service provider has gone out-ofservice

You can also determine if there are network problems on the site by examining the following files for the text java.net.SocketExemption:

- On the Contact Center Manager Server, review D:\Avaya\Contact Center\Manager Server\Core\CMF\CCMS\<latest version>\logs\OAMContainer0.log, where <latest version> is the latest version of Contact Management Framework software installed.
- On the Communication Control Toolkit server, review D:\Avaya\Contact Center\CMF\CCT\<latest version>\logs\ClientContainer_1.log, where <latest version> is the latest version of Contact Management Framework software installed.
- On the Communication Control Toolkit server, review D:\Avaya\Contact Center\CMF\CCT\<latest version>\logs\SPContainer_1.log, where <latest version> is the latest version of Contact Management Framework software installed.

Procedure steps

Step	Action
1	Check the network cable for faults. Cable faults are often difficult to identify and can be intermittent, therefore replacing the faulty cable with a known good cable is the best solution.
2	Check the network card speed and duplex settings. Communication Control Toolkit to Contact Center Manager Server settings must match the required PABX and hub settings, and be in the same network segment. Also, Contact Center Manager Server and the PABX settings must match the required PABX and hub settings, and be in the same network segment.
3	Check the physical network card for faults.

4 Check the network hub. Check both hardware and software (if applicable) problems in your hub.

5 If your hub is a switched hub, ensure that a virtual LAN separation is not present at a hardware or software level. If a virtual LAN separation is present, the performance of the connection between Communication Control Toolkit and Contact Center Manager Server is minimal.

6 Ensure the ability for Windows to turn off the network card to save power is disabled. Windows Server 2008 has a power management setting for network cards.

7 Ensure the network card has the latest driver software.

--End--

Troubleshooting Contact Center Manager Administration

This section describes procedures required to address various problems relating to Contact Center Manager Administration, including:

- Installation or upgrade problems
- Communication problems between CCMA and CCMS
- General CCMA problems
- Client PC problems
- Simple Object Access Protocol (SOAP) errors
- Real-time Statistics Multicast (RSM) problems
- Real-Time Reporting problems
- Historical reporting problems
- Configuration Tool problems
- Access and Partition Management problems
- Agent Desktop Display problems

Prerequisites for troubleshooting Contact Center Manager Administration

- Ensure that you have downloaded the latest Service Updates for both Contact Center Manager Server and Contact Center Manager Administration. You can download the latest installation or documentation addendum from either www.avaya.com (for end customers), or www.avaya.com/pic (for distributors), and the latest Service Updates from www.avaya.com/espl.
- Ensure that you have registered for the ESPL Web site. To do so, follow the instructions listed at www.avaya.com/register.
- Ensure that you check the Windows Event Viewer log and note any relevant information related to the problem you are handling. You may need this to resolve the problem or to communicate information to Avaya support.
- Ensure that you have installed an Avaya-supported remote access tool on the Contact Center Manager Administration server. Avaya uses Microsoft Remote Desktop Connection as the recommended remote support tool.

Navigation

- Troubleshooting logon problems following installation (page 101)
- Troubleshooting logon problems due to an inconsistency in the IUSR_SWC password (page 103)

Troubleshooting logon problems following installation

Troubleshoot logon problems if you launch SCE and receive an error message indicating that you cannot connect to Contact Center Manager Administration.

You need to create an iceAdmin and IUSR_SWC account on a client if Contact Center Manager Administration is part of a workgroup.

Prerequisites

- Review the *Avaya Aura™ Contact Center Commissioning* (NN44400-312) guide.
- Ensure that Contact Center Manager Administration is part of a workgroup.
- Ensure that you have the passwords for both the IUSR_SWC and iceAdmin user accounts on the Contact Center Manager Administration server.

Procedure steps

Step	Action
1	On the client PC, choose **Start, Administrative Tools, Computer Management**.
2	In the **Computer Management** window, in the left pane, expand **System Tools, Local Users and Groups**.
3	Right-click the **Users** folder, and select **New User**.
4	In the **New User** dialog box, in the **User name** box, type **iceAdmin**.
5	(Optional) In the **Full name** box, type the full name.
6	(Optional) In the **Description** box, type a description.
7	In the **Password** box, type the iceAdmin password.

Attention: The password must match the password on the Contact Center Manager Administration server.

8	In the **Confirm Password** box, type the password again.
9	Clear the **User must change password at next logon** check box.
10	Select the **Password never expires** check box.
11	Clear all other check boxes.
12	Click **Create**.
13	Click **Close** to close the **New user** dialog box.
14	Repeat steps 3 to 13 to add the IUSR_SWC account, if necessary.

--End--

Troubleshooting logon problems due to an inconsistency in the IUSR_SWC password

Troubleshoot the following error when you launch SCE: “Unable to contact CCMA server. Verify that the server is fully configured and available. See the SCE log for more information.” This message occurs when you attempt to log on to Contact Center Manager Administration. An inconsistency in the IUSR_SWC password can cause the error.

To resolve the issue, you must reset the IUSR_SWC password, manually reconfigure Application Pools to run under the IUSR _SWC, and retype the IUSR_SWC password for Authentication and access control for the CCMA Web site.

Procedure steps

Step	Action
1	Change IUSR_SWC password.
2	Click **Application Pools** in Internet Information Services (IIS) Manager.
3	Right-click each application pool, and select **Properties**.
4	Select the **Identity** tab to reconfigure the pool running under IUSR_SWC.

Attention: If the pool was configured to run under IUSR_SWC, retype password for IUSR_SWC.

5	Right-click CCMA Website, and select **Properties**.
6	Click the **Directory Security** tab.
7	Click **Edit** for **Authentication and access control**, and retype IUSR_SWC password.

--End--

Troubleshooting logon problems due to AD-LDS password encryption error

Troubleshoot when you receive a failed to login message when attempting to log on to Contact Center Manager Administration.

If, during Contact Center Manager Administration installation, AD-LDS installation failed and error messages occurred following the iceAdmin password prompt, this can indicate that the EncryptPasswordForCCMAUsers setting is set to restrict accessibility only to the user account that created the certificate during installation.

To address this problem, you need to change the policy setting under the Security options on the Contact Center Manager Administration server and provide access to the RSA Machine Keys to all users in the administrators group.

Procedure steps

Step	Action
1	Review the certificate created during installation of the Contact Center Manager Administration in C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\RSA\MachineKeys.
2	Under the Security options, set the local policy for Default owner for objects created by members of the administrator group to all members of the administrator group.
3	Save the certificate.
4	Uninstall and reinstall Contact Center Manager Administration.

--End--

Troubleshooting when logon problems result in computer requires restart error message

Troubleshoot when you attempt to log on to Contact Center Manager Administration and you receive an error message prompting you to restart the computer.

This problem can be caused when the browser tries to download a new version of the HRCtrl ActiveX control or any control that has an existing version installed which is different than the version attempting to be downloaded.

Procedure steps

Step	Action
1	Click **Cancel** to reject the request to restart the computer.
2	Close all Internet Explorer browser windows.
3	Open a new Internet Explorer browser window.
4	Go to the same Contact Center Manager Administration URL that resulted in the prompt to restart the computer. *The control downloads and no prompt to restart the computer appears.*

--End--

Troubleshooting when Citrix server performance is slow

Troubleshoot when you use a Citrix server and the server performance and speed are slow.

This problem can be caused by numerous agents launching Agent Desktop Display. Each Agent Desktop Display uses 20 MB of RAM. If the server is performing slowly, you may need to increase the amount of RAM available on the Citrix server.

Prerequisites

- Review the *Avaya Aura™ Contact Center Planning and Engineering* (NN44400-210) guide.

Procedure steps

Step	Action
1	Determine the RAM requirements for the Citrix server.
2	Upgrade the RAM available on the Citrix server.

--End--

Refreshing servers

Troubleshoot if CCMA does not function correctly after upgrading from SWC or after making a change to the Contact Center Manager Server, such as performing an upgrade, installing or uninstalling a service pack, receiving a new license file, or making a change to a standby CCMS. For example, if pages and tabs load incorrectly, new components and features are unavailable, or scripting errors occur, you may need to refresh your Contact Center Manager Servers. To troubleshoot these errors, you need to refresh one or all servers in the system tree.

Although Contact Center Manager Administration automatically refreshes all servers every 12 hours, Avaya recommends that you manually refresh servers following an upgrade, to ensure that Contact Center Manager Administration functions correctly.

When you refresh a server, you refresh Contact Center Manager Server data associated with that server in Active Directory Lightweight Directory Services (AD-LDS), such as the release number, feature list, and networking information.

If you change the password of sysadmin in the Server Utility, you must also change the password in that server.

Use the Refresh All Servers option to refresh all servers at the same time when:

- You upgrade from Avaya Aura™ Contact Center Web Client 4.5 SP0601 v1 or later, or you upgrade from a previous version of Contact Center Manager Administration.
- You change the Contact Center Manager Administration server to connect to a standby Contact Center Manager Server.
- There is a feature change to the Contact Center Manager Server. This is because the change is not reflected in the browsers until all browsers using CCMA are refreshed.

Use the Refresh Server option to refresh only the Contact Center Manager Server that incurred a change when:

- You upgrade the Avaya Aura™ Contact Center Contact Center Server or Contact Center Manager Server.
- You install or uninstall a Service Pack (SP) on the Contact Center Manager Server.

- A new license file is issued and accepted by Contact Center Manager Server, or you connect to a different License Manager server (that is, a new or standby License Manager server).

Prerequisites

- Ensure that you have logon privileges as an administrator, who has permissions to add, edit, delete and refresh servers in Contact Center Manager Server.
- Ensure that you determine whether you need to refresh all servers in the system tree or just a single server in the system tree, based on the reasons described above.

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration.
2	Select **Configuration**.
3	If you want to refresh all servers in the system tree: • On the menu bar, choose **Server, Refresh All Servers**.
4	If you want to refresh a single server in the system tree: • On the system tree, click the server that you want to refresh. • On the menu, choose **Server, Refresh Server**.
5	Click **Yes**.
6	Click **Yes**. *The system refreshes the selected servers. A message appears in the information bar at the bottom of the screen that lists the servers that successfully refreshed and the servers that did not refresh. An entry specifying the servers that were successfully refreshed also appears in the Audit Trail.*

--End--

Troubleshooting if CCMA starts slowly when downloading ActiveX controls

Troubleshoot if downloading ActiveX controls causes the Contact Center Manager Administration web client to load slowly. This can occur when the client PC cannot contact the Verisign Web site. The ActiveX controls are digitally signed and the system attempts to verify that the digital signature is valid by accessing the Verisign Web site. If verification is not possible, the attempt times out and the download of the ActiveX controls should proceed normally.

The ActiveX controls can be distributed to a client PC during installation, using the ActiveXControl MSI package.

Procedure steps

Step	Action
1	When starting Contact Center Manager Administration, if a delay of longer than a minute occurs during the download of ActiveX controls, contact Avaya Technical Support.

--End--

Troubleshooting CCMA replication errors related to problems with AD-LDS

Troubleshoot if Contact Center Manager Administration replication fails and if you selected Enable Active Directory - Lightweight Directory Services (AD-LDS) replication during installation but did not provide the name of the AD-LDS instance, for example Avaya Aura™ Contact Center WC, for replication during AD-LDS setup.

AD-LDS is installed during the installation of Contact Center Manager Administration. AD-LDS is not removed during the uninstallation of Contact Center Manager Administration because AD-LDS is a windows component that is incorporated into the operating system and uninstallation of AD-LDS can cause the operating system to fail.

The DVD Controller manages all contact center uninstallation processes. The AD-LDS Instance, CCMA Database, is removed from the system during the uninstallation of Contact Center Manager Administration, if the user does not choose to preserve customer data. However, the AD-LDS Instance is not removed from the system and Contact Center Manager Administration replication does not work if you do not provide the name of the AD-LDS instance for replication during AD-LDS setup.

Procedure steps

Step	Action
1	If Contact Center Manager Administration replication fails and if you selected Enable AD-LDS replication during installation but did not provide the name of the AD-LDS instance, for example Avaya Aura™ Contact Center WC, for replication during AD-LDS setup, manually uninstall AD-LDS.

--End--

Troubleshooting IIS worker process errors after you reboot CCMA

On Contact Center Manager Administration server, after you install software updates and reboot the server, a dialog box appears indicating that the IIS worker process closed due to a Windows error. These types of errors are informational and indicate that the IIS

worker process crashed. The server stores the errors and the IIS worker reports them when a user logs on after a reboot. These errors may have occurred in the past and may appear several times, with times and dates for previous time periods.

There is no impact to the Contact Center Manager Administration installation or application.

Procedure steps

Step	Action
1	In the dialog box, click **Don't Send**.
2	If not previously reported, report the IIS Lockups specified in the error dialog box to Avaya Technical Support.

--End--

Troubleshooting configuration errors for ASP.NET in IIS

If you do not configure ASP.NET correctly prior to installing Contact Center Manager Administration, problems can occur. You need to ensure that ASP.NET web services are allowed.

Procedure steps

Step	Action
1	Click **Start, Administrative Tools, Internet Information Services (IIS) Manager**.
2	In the left pane of the Internet Information Services (IIS) Manager, navigate to the **Web Service Extensions** folder.
3	In the right pane, ensure that the following Web Service Extensions are present and that the status for each is **Allowed**. • ASP.NET v1.1.4322 • ASP.NET v2.0.50727
4	If the status for either Web Service Extension is Prohibited, select the web service, and then click **Allow**.
5	Close the Internet Information Services (IIS) Manager.

--End--

Troubleshooting Server Error in /RCW Application error message when previewing reports

Troubleshoot when you receive the error message “Server Error in ‘/RCW’ Application” when you attempt to preview a report through the Report Creation Wizard.

This error occurs when the RCW ASP.NET framework is set to the incorrect version. You need to change the ASP.NET version and reset IIS.

Procedure steps

Step	Action
1	On the Contact Center Manager Administration server, choose **Start, Administrative Tools, Internet Information Services (IIS) Manager**.
2	In the left pane of the Internet Information Services (IIS) Manager, navigate to the **Websites\Default Web Site\RCW** folder.
3	Right-click and select **Properties**.
4	In the **RCW Properties** window, click the **ASP.NET** tab.
5	Change the **ASP.NET version** to **1.1.4322**.
6	Click **OK** and close the Internet Information Services (IIS) Manager.

--End--

Troubleshooting errors after CCMA server is added to Domain Server

Troubleshoot errors that can occur after a Contact Center Manager Administration server is added to a Domain Server with a strict security policy.

Prerequisites

- Ensure that you have read the *Avaya Aura™ Contact Center Server Administration* (NN44400-610) guide.

Procedure steps

Step	Action
1	If you cannot see the Login screen, ensure that you have WRITE permissions on the Windows\Temp folder.
2	If you cannot log on to Contact Center Manager Administration server, ensure that you have IUSR_SWC READ access to the <x:>\Program Files\Avaya directory.
3	If you cannot run the Configuration Report for CDN (Route points) because the screen freezes, ensure that you have Network Service or Users Group READ\Execute access to <x:>\Sybase\ODBC folder and Program Files\Common Files\Crystal Decisions\2.5.

4 If you cannot load Supervisors when you click on the Contact Center Manager Administration server in the tree menu, ensure that you have IUSR_SWC READ\ Execute access to <x:>\Sybase\ODBC folder and <x:>\Sybase\ini\sql.ini.

5 If you cannot submit a change to filter the Real-time displays, ensure that you have IUSR_SWC READ access to <x:>\Windows\System32\msxml4r.dll.

6 If you cannot launch the Report Creation Wizard, ensure that you have Users Group or Network Service or IUSR_SWC READ permissions on the Windows\assembly directory.

7 If you cannot import a report created by the Report Creation Wizard, ensure that you have Network Service or Users group READ access to the <x:>\Program Files\Avaya directory.

8 If the Report Creation Wizard is performing slowly, ensure that you have Network Service READ/Execute access to <x:>\Program Files\Avaya directory. Ensure that you add Network Service or Users Group or IUSR_SWC READ permissions to Program Files\Crystal Decisions\Report Application Server 11\clientSDKOptions.xml.

--End--

Troubleshooting communication errors with Contact Center Manager Server

Troubleshoot communication errors with Contact Center Manager Server by testing for the various issues that can cause the communication errors and, after testing, taking appropriate action as required.

Procedure steps

Step	Action
1	Check to ensure that the Contact Center Manager Server IP address being used is valid.
2	Ping the Contact Center Manager Server, by name and by IP address.
3	Contact your system administrator if you are unable to successfully ping the Contact Center Manager Server.
4	Check your cabling.
5	Check the IP addresses for the Contact Center Manager Administration servers and the servers in Contact Center Manager Server.
6	Check the versions on the servers in Contact Center Manager Server, and confirm that they are compatible with Contact Center Manager Administration

--End--

Changing the computer name of the Contact Center Manager Server on the CCMA server

Change the computer name of the Contact Center Manager Server on the Contact Center Manager Administration server if you:

- change the computer name and/or IP address of the Contact Center Manager Server
- change to a standby Contact Center Manager Server with a new name

You must reconfigure the Contact Center Manager Administration server to connect to a secondary Contact Center Manager Server, with a different computer name and IP address. Contact Center Manager Administration can then continue to communicate with a new standby Contact Center Manager Server and retrieve all of the data stored in the application server for that server.

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration as the webadmin user.
2	Open the **Configuration** component.
3	In the left pane, right-click the server with altered network settings.
4	Click **Edit Properties**. This enables the text fields for the servers name, IP address, logon ID and password.
5	Enter the new details and click **Submit**.

--End--

Troubleshooting connection errors following a computer name change on a standalone CCMA server

If you change the computer name of the Contact Center Manager Administration server, you must reset the name so that the Contact Center Manager Server and the Contact Center Manager Administration function properly.

You must update your Domain Name Server (DNS) or HOSTS table to reflect the new name of the Contact Center Manager Administration server for your Contact Center Manager Administration to function correctly.

Prerequisites

Ensure that you have administrator privileges.

Procedure steps

Step	Action

1	Run the iceAdmin PasswordChange utility and reset the iceAdmin password.

--End--

Troubleshooting connection errors following a computer name change on a co-resident CCMA server

On a co-resident server, after you change the computer name, you must perform the following tasks to reset the name so that Contact Center Manager Server and Contact Center Manager Administration function properly.

You must update your Domain Name Server (DNS) or HOSTS table to reflect the new name of the Contact Center Manager Administration server for your Contact Center Manager Administration to function correctly.

Prerequisites

Ensure that you have administrator privileges.

Procedure steps

Step	Action
1	Run the Contact Center Manager Server Computer Name Sync utility.
2	Run the iceAdmin PasswordChange utility and reset the iceAdmin password.

--End--

Resetting the iceAdmin password after a CCMA server name change

You must update your Domain Name Server (DNS) or HOSTS table to reflect the new name of the Contact Center Manager Administration server for your Contact Center Manager Administration to function correctly.

Prerequisites

Ensure that you have administrator privileges.

Procedure steps

Step	Action
1	Click **Start, All Programs, Avaya, Contact Center, Manager Administration, Configuration**.
2	In the left pane, click **Avaya**.

3 In the **Avaya Applications Configuration** window, click **IceAdmin Password Change**.

4 In the **Old Password** box, type the old password.

5 In the **New Password** box, reenter the old password for the iceAdmin user account. This resets the iceAdmin password.

6 In the **Confirm Password** box, type the password again.

7 If your Contact Center Manager Administration server is a member of an active domain, the **Domain Account** option is enabled on the **iceAdmin Password Change** window.

8 If the domain account button is disabled, proceed to step 15.
OR
To export scheduled reports to a domain network PC, proceed to step 9.

9 Click **Domain Account**.

10 In the **Optional Domain Account Setup** window, from the **Select Domain Name** list, select the name of the domain to add.

11 In the **Enter Domain Account** box, type the domain account. Obtain the domain account name and password from your network administrator.

12 In the **Enter Domain Account Password** box, type the domain account password. You must enter the correct domain account password. If the password is incorrect, the system does not proceed.

13 In the **Confirm Domain Account Password** box, retype the domain account password.

14 Click **OK**.

The iceAdmin Password Change window reappears and activates all scheduled reports using the domain account instead of the local iceAdmin account

15 Click **OK**.

The system verifies that you typed the same password both times, and then resets the password for both iceAdmin and IUSR_SWC.

--End--

Troubleshooting client PC communication problems with the CCMA server

There are a number of issues that can cause client PCs to be unable to communicate with the Contact Center Manager Administration server. You must identify the source of your problem before determining the solution.

Prerequisites

Ensure that you have administrator privileges and that your username and password are valid.

Procedure steps

Step	Action
1	Test the communication from the client to the Contact Center Manager Administration server.
2	Verify that Web users have permissions on all directories in the Contact Center Manager Administration Web site. When Contact Center Manager Administration is installed, it uses the default settings stored in IIS. If Web users do not have permissions, contact your site administrator for details about changing the settings in IIS.
3	If you configure a Domain Name Server (DNS), verify that the computer name of the Contact Center Manager Administration server is registered on the DNS. If the computer name is not registered on your DNS, then Contact Center Manager Administration does not function properly.
4	If you did not configure a DNS server, verify that you added the computer name of the Contact Center Manager Administration server to the HOSTS table on each client PC that accesses Contact Center Manager Administration.
5	Check if Internet Explorer uses a proxy server.
6	Ensure that the IIS service is running on the Contact Center Manager Administration server.
7	Ensure that Active Directory Application Mode is installed on the Contact Center Manager Administration server.
8	Confirm that the event viewer logs are configured correctly on the Contact Center Manager Administration server.

--End--

Testing communication from the client to the CCMA server

If the client cannot connect to the Contact Center Manager Administration server, and you have already checked to make sure that the Contact Center Manager Administration username and password are valid, you need to test communication.

Procedure steps

Step	Action
1	Ping the Contact Center Manager Administration server.
2	Check the IP addresses for the Contact Center Manager Administration servers and the servers in Contact Center Manager Server.
3	Check your cabling.
4	Make sure the Web site is active on the Contact Center Manager Administration server.
5	Make sure the computer name of the Contact Center Manager Administration server is registered on the DNS server.

6 If the Web site is active, the IP addresses are valid, and you are unable to successfully ping the Contact Center Manager Administration server, contact your system administrator.

--End--

Checking if Internet Explorer uses a Proxy Server

If the client cannot connect to the Contact Center Manager Administration server, check whether Internet Explorer uses a Proxy Server.

Procedure steps

Step	Action
1	On the Internet Explorer menu bar, choose **Tools, Internet Options, Connections, Lan Settings**.
2	If the **Use a proxy server for your LAN** check box is selected, contact your Proxy Server administrator to verify that there are no restrictions preventing you from accessing the Contact Center Manager Administration server.

--End--

Adding the computer name of the CCMA server to the HOSTS table on each client PC (if you have not configured a DNS)

Avaya recommends that the Contact Center Manager Administration server host name be resolved by the corporate DNS. However, if you did not configure a name resolution server during the operating system installation, then the client PCs that connect to Contact Center Manager Administration cannot find the Contact Center Manager Administration server. If this occurs, you must manually update the HOSTS table on each client PC with the name and contact center server subnet network interface IP address of the Contact Center Manager Administration server.

When you use server names to connect to a Contact Center Manager Administration server in TCP/IP networks, the server name must be associated with an IP address. The HOSTS table carries out this association, which is called host name resolution.

The HOSTS table consists of a list of IP addresses followed by a computer name: 123.4.56.100 webclient.Avaya.com. At the end of the file, type the IP address and computer name of the Contact Center Manager Administration server. Separate the two values by using the space or tab key. HOSTS tables are case-sensitive. After you edit

and save the HOSTS file, the system automatically reads your new settings. If you edit the sample HOSTS file, then save the file with no extension to enable the system to recognize your changes.

Based on the operating system installed on the client PC, sample host tables are located in various directories. With the Windows 2008 Release 2 installation, for example, sample HOSTS tables are provided in the following directory: [x]:\WINDOWS\system32\drivers\etc.

Prerequisites

- Ensure that you carefully review the detailed information about HOSTS in the supporting Microsoft documentation. Incorrectly modifying a HOSTS table on the client PC can cause extensive network problems.

Procedure steps

Step	Action
1	On each client PC, use a text editor to modify the HOSTS tables by entering the computer name and IP address of the Contact Center Manager Administration server.

Attention: You do not have to use HOSTS tables for name resolution if the name of the Contact Center Manager Administration server is registered on a DNS server

--End--

Verifying that IIS is running on the Contact Center Manager Administration server

Verify that IIS is running on the Contact Center Manager Administration server.

Procedure steps

Step	Action
1	On the Contact Center Manager Administration server, choose **Start, Administrative Tools, Services**.
2	In the right pane of the **Services** window, select the **IIS Admin Service**.
3	In the **Status** column, verify that the IIS Admin Service is **Started**.

--End--

Verifying that AD-LDS is installed on the Contact Center Manager Administration Server

Verify that Microsoft Active Directory Lightweight Directory Services (AD-LDS) is installed on the Contact Center Manager Administration Server.

Procedure steps

Step	Action
1	Click **Start, Control Panel, Programs** .
2	Click **Programs and Features**.
3	In the **Programs and Features** window, verify that **AD LDS Instance SymposiumWC** is displayed.

--End--

Resolving trust relationship error when installing AD-LDS

Resolve the trust relationship error that occurs when installation of AD-LDS fails and the trust relationship between the domain and the workstation is broken.

Prerequisites

- Ensure you read *Avaya Aura™ Contact Center Installation* (NN44400-311).

Procedure steps

Step	Action
1	Use the DVD controller to uninstall Contact Center Manager Administration.
2	Remove the workstation from the domain and add it to a workgroup.
3	Add the workstation to the domain, to re-establish the trust relationship between the domain and the workstation.
4	Use the DVD controller to install Contact Center Manager Administration.

--End--

Identifying the source of Internet Explorer problems

Identify the source of Internet Explorer problems by checking various items. Depending on the source of the problem, you may need to reinstall the correct version of Internet Explorer on the client PC or you may need to reconfigure Internet Explorer on the client PC.

Procedure steps

Step	Action
1	Check that Internet Explorer Version 6.0 or Internet Explorer Version 7.0 is installed with the latest supported Service Pack on the client PC.
2	Check that you configured security in Internet Explorer correctly.

3	If you receive error messages from Internet Explorer indicating that your Web site cannot run Out of Process components, enable Out of Process components.
	• Create a script called AspAllowOutOfProcComponents.vbs using any text editor. Insert the following commands:
	• `Set objWebService = GetObject ('IIS://LocalHost/w3svc')`
	`' Enable AspAllowOutOfProcComponents. objWebService.Put`
	`'AspAllowOutOfProcComponents', True`
	`' Save the changed value to the metabase.`
	`objWebService.SetInfo`
	• Save the script.
	• In Windows Explorer, double-click the script.

4	If all of the above steps do not resolve the problem, reinstall Internet Explorer on the client PC.

--End--

Troubleshooting when CCMA Web interface is distorted

Troubleshoot when the display of the Contact Center Manager Administration Web interface is distorted. Distortion occurs when your display settings are not optimized for the Contact Center Manager Administration Web interface. You need to check the display settings on your computer and, if required, resize the font.

Procedure steps

Step	Action
1	Click **Start, Control Panel, Appearance**.
2	In the **Appearance** window, click **Display**.
3	Click **Adjust resolution**.
4	In the **Resolution** list, select at least **1024 x 768** pixels.
5	Click **Make text and other items larger or smaller**.
6	Ensure **Smaller - 100% (default)** is selected.
7	Click **Apply**.
8	In Internet Explorer, on the **Page** menu, click **Text Size, Medium**.

9	If the text or content display in Internet Explorer is too large, select **Text Size, Smaller**.

--End--

Disabling pop-up blockers

Troubleshoot when you cannot launch a window in Contact Center Manager Administration and a message displays indicating that Pop ups were blocked on this page. For all components of Contact Center Manager Administration to function correctly, you must disable pop-up blockers on Internet Explorer.

Procedures to disable pop-up blockers vary, depending on the type of pop-up blocker you have. If the procedure here does not disable your pop-up blocker, contact the pop-up blocker provider.

Procedure steps

Step	Action
1	Open Internet Explorer.
2	If you use Google, on the Google toolbar, click on the **Popup blocker** icon and confirm that the icon indicates **Site popups allowed**.
3	If you use Yahoo, on the Yahoo toolbar, click on the button that displays the tooltip Pop-Up Blocker Is On or Pop-Up Blocker Is Off. In the expanded menu, ensure that the option **Enable Pop-Up Blocker** is unchecked.
4	If you use Windows XP Service Pack 2, click on **Tools, Pop-up Blocker, Turn Off Pop-up Blocker**.

--End--

Troubleshooting when CCMA logon screen displays ERROR:UNKNOWN!

Troubleshoot when you attempt to launch Contact Center Manager Administration and the logon screen displays ERROR:UNKNOWN! You need to ensure that the display settings for Internet Explorer are configured for Western European (ISO).

Procedure steps

Step	Action
1	Open Internet Explorer.
2	In the **Internet Explorer** browser window, select **View, Encoding**.
3	In the **Encoding** selection menu, ensure that **Western European (ISO)** is selected.

4	Close all windows.

--End--

Troubleshooting when CCMA logon page displays Connect Login prompt

Troubleshoot when attempting to launch the Contact Center Manager Administration logon screen, and the Connect to <CCMA server name> logon window appears, prompting you for a username and password. This indicates that the IUSR_SWC password configured in IIS does not match the specified password for your user account in Computer Management. You need to re-run the iceAdmin password change utility to reset the IUSR_SWC password.

Procedure steps

Step	Action
1	Run the iceAdmin PasswordChange utility and reset the iceAdmin password.

--End--

Troubleshooting when CCMA Web services fail to execute

Troubleshoot when you attempt to log on to Contact Center Manager Administration and Web services fail and an error message appears. This error can occur when the client PC has Windows/System32/vbscript.dll version 5.6 installed, but it is not the registered version of vbscript.dll, which is version 5.0.

Procedure steps

Step	Action
1	Register Windows/System32/vbscript.dll.

--End--

Troubleshooting when you forget the iceAdmin password

Troubleshoot when you forget the iceAdmin password by resetting it. This is a two-step procedure, since you must reset the password in Windows, and then you must reset the password using the iceAdmin Password Change utility that is provided with Contact Center Manager Administration.

Prerequisites

- Ensure that you are logged on as an administrator.
- If you want to export scheduled reports to a domain account or use the domain account setup function to reset the domain account password, obtain the domain account name and password from your network administrator.

Procedure steps

Step	Action
1	On the Contact Center Manager Administration server, choose **Start, Administrative Tools, Computer Management**.
2	In the left pane of the **Computer Management** window, click the plus sign (+) beside **Local Users and Groups**.
3	Click the **Users** folder.
4	Right-click the **iceAdmin** user.
5	On the menu, select **Set Password**.
6	In the **Set Password** window, type the new password and confirm the password.
7	Click **OK**.
8	Close all windows.
9	Click **Start, All Programs, Avaya, Contact Center, Manager Administration, Configuration**.
10	In the left pane, click **Avaya**.
11	In the **Avaya Applications Configuration** window, click **IceAdmin Password Change**.
12	In the iceAdmin **Password Change** window, in the **Old Password** box, type the same password that you typed in step 6.
13	In the **New Password** box, type a new password for the iceAdmin user account.
14	In the **Confirm Password** box, type the new password again.
15	If your Contact Center Manager Administration server is a member of an active domain, the Domain Account option is enabled on the iceAdmin Password Change window. If you want to export scheduled reports to a domain account or use the domain account setup function to reset the domain account password, click **Domain Account**. OR If you do not want to export scheduled reports to a domain account, or if the Domain Account button is disabled, go to step 21.
16	In the **Optional Domain Account Setup** dialog box, from the **Select Domain Name** list, select the name of the domain to add.
17	In the **Enter Domain Account** box, type the domain account name that you obtained from the network administrator.
18	In the **Enter Domain Account Password** box, type the domain account password.

19 In the **Confirm Domain Account Password** box, retype the domain account password.

20 Click **OK**.

The iceAdmin Password Change window reappears and activates all scheduled reports using the domain account instead of the local iceAdmin account.

21 Click **OK**.

The system verifies that you typed the same password both times and registers the new password in all required components.

--End--

Refreshing all servers in the system tree

Troubleshoot when no Agent Real-time display appears in a Terminal Services environment. This occurs because only one user can log on at a time for unicast reporting. Enabling Unicast in a Terminal Services environment results in an error if you launch the same Real-time display on a duplicate Terminal Services session.

If you want to use unicast transmission for statistics from the Contact Center Manager Server to the Contact Center Manager Administration server for reporting purposes, you must disconnect the Terminal Services session.

An alternative for using unicast transmission in a Terminal Services environment is using multicast transmission. This must be selected on the Contact Center Manager Administration server, under Transmission.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration server.
2	Click **Start, Administrative Tools, Terminal Services Manager**.
3	In the **Terminal Services Manager** window, in the right pane, click the **Sessions** tab.
4	In the right pane, right-click the session to disconnect and select **Disconnect** from the menu.
5	Click **OK**.
6	Close the Terminal Services Manager window.

--End--

Troubleshooting Terminal Services Real-time display errors

Troubleshoot when no Agent Real-time display appears in a Terminal Services environment. This occurs because only one user can log on at a time for unicast reporting. Enabling Unicast in a Terminal Services environment results in an error if you launch the same Real-time display on a duplicate Terminal Services session.

If you want to use unicast transmission for statistics from the Contact Center Manager Server to the Contact Center Manager Administration server for reporting purposes, you must disconnect the Terminal Services session.

An alternative for using unicast transmission in a Terminal Services environment is using multicast transmission. This must be selected on the Contact Center Manager Administration server, under Transmission.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration server.
2	Click **Start, Administrative Tools, Terminal Services Manager**.
3	In the **Terminal Services Manager** window, in the right pane, click the **Sessions** tab.
4	In the right pane, right-click the session to disconnect and select **Disconnect** from the menu.
5	Click **OK**.
6	Close the Terminal Services Manager window.

--End--

Troubleshooting when the Real-Time Data Collector service does not update

Troubleshoot when a nodal server is removed and added again to the Network Control Center, but the Real-Time Data Collector service does not update the change. If this happens, the old site ID is not deleted and multicast information occurs for two site IDs. The Contact Center Manager Administration server Windows Event Viewer displays event number 500 and Contact Center Manager Administration runs slowly. All Contact Center Manager Server computers configured on Contact Center Manager Administration are affected until the Real-Time Data Collector service on affected.

Procedure steps

Step	Action
1	In Windows Event Viewer, note all event number 500 references and note the Contact Center Manager Server computers affected.

2 Restart the Real-Time Data Collector service on each of the Contact Center Manager Server computers affected.

3 Restart the iceRTD service on the Contact Center Manager Administration server.

--End--

Troubleshooting RTD data errors following backup and restore on a Stratus server

Troubleshoot when you have performed a backup and restore on a Stratus server and the Real-time Display is not displaying correct data.

This problem occurs because the Real-time Display displays all of the agents in the merged filter belonging to both servers and the data results are incorrect.

Procedure steps

Step	Action
1	Create one filter for each server. Do not merge data from two servers in one filter.

--End--

Troubleshooting when LMService license grant and release events are not logged

Troubleshoot when Contact Center Manager Administration LMService events 18002, 18003, 18004 and 18005 are not logged to the Windows security event log on Contact Center Manager Administration when the user opens or closes a Report Creation Wizard browser session. This problem occurs if the Audit Object Access security policy was not configured to audit the success and failure attempts.

Procedure steps

Step	Action
1	On the Contact Center Manager Administration server, choose **Start, Administrative Tools, Local Security Policy**.
2	In the left pane of the **Local Securities Settings** window, expand the **Local Policies** folder by clicking the plus (+) sign next to Local Policies.
3	In the left pane of the **Local Policies** folder, click the **Audit Policy** subfolder. *A list of audit policies appears in the right pane.*
4	In the right pane of the **Local Policies** folder, double-click **Audit Object Access**.

5 In the **Audit Object Access Properties** window, select **Success**.

A check mark appears next to the Success option.

6 In the **Audit Object Access Properties** window, select **Failure**.

A check mark appears next to the Failure option.

7 Click **Apply**.

8 Click **OK**.

9 Close all windows.

--End--

Troubleshooting when the browser is preventing ActiveX controls from installing

Troubleshoot when errors occur because the Internet Explorer security setting for Automatic prompting for ActiveX controls is set to Disable.

Procedure steps

Step	Action
1	Open Internet Explorer.
2	From the menu, select **Tools, Internet Options**.
3	Select the **Security** tab.
4	Click the **Trusted Sites** icon.
5	Click **Custom Level**.
6	In the **Security Settings** window, under the **ActiveX controls and plug-ins** heading, for **Automatic prompting for ActiveX controls**, select **Enable**.
7	Click **OK**.
8	Click **Yes**.
9	Restart Internet Explorer. *After the security setting is set to Enable and Internet Explorer restarts, when the browser encounters an ActiveX control, a dialog box appears, asking the user if they want to install the control. To install the control, click Install.*

--End--

Troubleshooting when you cannot open technical documentation .pdf files through CCMA

Troubleshoot when you have copied the latest user guides to the Contact Center Manager Administration server but you cannot open the user guides through Contact Center Manager Administration. You must change the security permissions of the folder where the guides are stored.

Procedure steps

Step	Action
1	On the Contact Center Manager Administration server, browse to the folder where the guides are stored: <drive>:\Avaya\Contact Center\Manager Administration\Apps\documentation\guides.
2	Right-click the `guides` folder and select **Properties**.
3	In **Properties**, select the **Security** tab.
4	Click **Advanced**.
5	In **Advanced Security Settings for guides**, select **Replace all child object permissions with inheritable permissions from this object**.
6	Click **OK**.
7	Close all windows.

--End--

Troubleshooting when performance issues occur when you install Microsoft Service Packs or Hot Fixes

Troubleshoot when you have installed Microsoft Service Packs or Hot Fixes and performance issues occur. These issues can occur if Automatic Private IP Addressing (APIPA) is enabled on the Contact Center Manager Administration server. You need to disable APIPA.

APIPA is a feature available with Windows 2000 and Windows 2008 operations systems that automatically assigns an IP address to an unconfigured network card. The assigned IP address is in the range 169.254.0.0 to 169.254.255.255.

APIPA is automatically disabled in Contact Center Manager Administration Release 6.0 SP0202 and up. When you install Microsoft Service Packs or Hot Fixes, it is possible that the APIPA setting is overwritten.

If APIPA is enabled on the Contact Center Manager Administration server and the server contains an unconfigured network card, the server is assigned an IP address for that network card. The Contact Center Manager Administration server can then provide this IP address to Contact Center Manager Server. This results in Contact Center Manager Server attempting to send notifications to the Contact Center Manager Administration server on an invalid IP address. The notifications time out and the following can occur:

- Contact Center Manager Server does not acquire TNs
- ASM and TFE services remain in the Starting state

- Performance on Contact Center Manager Server degrades
- OAM Service does not respond to update requests from client

The following information message appears in the system event log:

- `<date time> Dhcp Warning None 1007 N/A WCHICAP`
  `Your computer has automatically configured the IP address for the Network Card with network address <###>. The IP address being used is 169.254.###.###.`

If the IPAutoconfigurationEnabled entry is not present, a default value of 1 is assumed, which indicates that APIPA is enabled.

Procedure steps

Step	Action
1	On the Contact Center Manager Administration server, choose **Start, Run**.
2	In the **Run** dialog box, in the **Open** field, type `regedit`, and then click **OK**.
3	In the Registry Editor, navigate to: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`.
4	Right-click the **Parameters** folder and select **New, DWORD Value**.
5	Type `IPAutoconfigurationEnabled` as the name.
6	Right-click `IPAutoconfigurationEnabled` and click **Modify**.
7	In the **Edit DWORD Value** dialog box, in the **Value Data** box, type `0` (zero).
8	In the **Base** section, select the **Hexadecimal** option.
9	Click **OK**.
10	Restart the Contact Center Manager Administration server.

--End--

Troubleshooting Real-time Statistics Multicast from the CCMA server

Troubleshoot Real-time Statistics Multicast (RSM) from the Contact Center Manager Administration server by checking various causes for errors. The source of errors can originate in the following network components:

- the client PC
- the Contact Center Manager Administration server
- the Contact Center Manager Server

Prerequisites

- Ensure that you check with your network administrator for acceptable IP multicast addresses for your network. The IP multicast addresses that you select for RSM sending and receiving must be within the 224.0.1.0 and 239.255.255.255 range.

Procedure steps

Step	Action
1	Ensure that the LAN or WAN supports multicast traffic. Contact your network administrator to confirm that the routers have multicast capabilities.
2	Verify that you can send and receive data between Contact Center Manager Server, the Contact Center Manager Administration server, and the Contact Center Manager Administration clients.
3	Confirm that the Real-time Statistics Multicast components send data to the same IP multicast address.
4	Ensure that the IP Receive address for the Contact Center Manager Administration server matches the IP Send multicast address setting in Contact Center Manager Server.

--End--

Using ICERTDTrace to trace IP multicast data

Use ICERTDTrace to trace IP multicast data, to assist you in determining whether your network is configured properly for IP multicasting, and to help you identify where Real-Time Reporting or Agent Desktop Display problems originate. ICERTDTrace.exe is a diagnostic tool provided with Real-Time Display configurations of Contact Center Manager Administration.

Use ICERTDTrace.exe to test that the Contact Center Manager Administration server is sending and receiving multicast to and from the Contact Center Manager Server.

Procedure steps

Step	Action
1	On the Contact Center Manager Administration server, at the command prompt, navigate to the Contact Center Manager Administration folder C: \> `cd [x]:\Avaya\Contact Center\Manager Administration\Server` where [x] is the driver letter for the hard drive on which the operating system is installed.
2	To trace data sent from Contact Center Manager Server to the Contact Center Manager Administration server, type the following command: `icertdtrace -r IPreceive <IP Multicast receive address> -s <CCMS site name> -t <statistic type>` where <statistic type> is an agent, application, skillset, ivr, nodal, or route statistic. The multicast address must be specified if the -s or -t options are used. The -s or -t options can be used separately.

The output log file is printed to the screen at run time to a text file at the following location: <drive>:\Avaya\Contact Center\Manager Administration\Server\IPRcvLog.txt.

3 On the Contact Center Manager Administration server, at the command prompt, navigate to the Contact Center Manager Administration folder C: \> `cd [x]:\Avaya\Contact Center\Manager Administration\Server` where [x] is the driver letter for the hard drive on which the operating system is installed.

4 To trace data sent from Contact Center Manager Administration server to clients, type the following command: `icertdtrace -r IPSend <IP Multicast send address> -s <CCMS server name> -t <statistic type>` where <statistic type> is an agent, application, skillset, ivr, nodal, or route statistic. The multicast address must be specified if the -s or -t options are used. The -s or -t options can be used separately.

The output log file is printed to the screen at run time to a text file at the following location: <drive>:\Avaya\Contact Center\Manager Administration\Server\IPSndLog.txt.

--End--

Troubleshooting when the server is receiving, but not sending, multicast

Troubleshoot when the server is receiving, but not sending, multicast by checking that the ICERtd Service is running and by checking for event log errors relating to machine names or IP addresses.

Procedure steps

Step	Action
1	Check that the ICERtd Service is running.
2	In the Windows Event Viewer, check the application event log for errors relating to machine names or IP addresses.
3	Verify that the configured Contact Center Manager Servers can be reached by their specified names by pinging each individual name and verifying that the IP address that the system uses in the ping is the same as the one that appears in the CContact Center Manager Administration Configuration window.

--End--

Troubleshooting Server Utility Event Browser failure

If Server Utility Event browser fails to retrieve events for an application, verify the Windows Event Viewer application settings. In the case of Windows Event Viewer failure, you receive the error message: Failed to Retrieve; Fault Management Server Error.

Procedure steps

Step	Action
1	Click **Start**, **Administrative Tools**, **Event Viewer**.
2	Select the required application.
3	On the **Event Viewer** menu bar, select **Action**, **Properties**.
4	Click the **General** tab.
5	In the **Log** size section, verify that the value in **Maximum log size** is not set to high.
6	In the **When maximum log size is reached section**, select **Overwrite events as needed**.
7	Click **Apply**.
8	Click **OK**.

--End--

Testing the RSM service on Contact Center Manager Server

Test the RSM service using the Multicast Receive utility (mRcv.exe), if you are having problems with real-time displays. The mRcv.exe utility displays statistical information according to the settings specified in a configuration tool called mRcv.ini.

Because the mRcv.exe utility tests the RSM service send capabilities one port at a time, you must specify the IP address and port utility that monitor the MCast section of the mRcv.ini file. The only portion of the mRcv.ini file that can be modified is the [MCast] section at the bottom of the file. The port numbers listed within the section bordered by the number (#) symbols in the mRcv.ini file are for reference only and list all of the acceptable port numbers that you can use in your test.

The IP address field must be the multicast IP address of the Contact Center Manager Server. The port number corresponds to the port number of the statistic that you want to test.

For example, to test receipt of Skillset - Interval to date data using mRcv.exe, check the port number for Skillset - Interval to date in the mRcv.ini file, and then change the port number for Skillset - Interval to date in the mRcv.ini file, and then change the

Port=setting in the [MCast] section to that port number. If Skillset - Interval to date = 6040 in the mRcv.ini file, the [MCast] section of the mRcv.ini file must be modified as follows:

```
[MCast]
IP=234.5.6.7
Port=6040
```

Procedure steps

Step	Action
1	On Contact Center Manager Server, choose **Start, All Programs, Accessories, Windows Explorer**.
2	Navigate to the folder <drive>:\Avaya\Contact Center\Manager Server\iccm\bin\mRcv.ini.
3	Using a text editor, open mRcv.ini.
4	In the mRcv.ini file, modify the IP address or the port number or both.
5	Save the mRcv.ini file.
6	Click **Start, All Programs, Accessories, Windows Explorer**.
7	Navigate to the folder <drive>:\Avaya\Contact Center\Manager Server\iccm\bin.
8	Double-click mRcv.exe. *The mRcv.exe utility opens in a console window. If data is multicasted out, the command prompt window is populated with incoming data from the port and IP address that you specified in the mRcv.ini file. All non-RSM data is identified as "Not recognized by RSM."*
9	If you want to save the mRcv.exe utility data, run mRcv.exe from the command prompt (<drive>:\Avaya\Contact Center\Manager Server\iccm\bin\mRcv.ini>log.txt). *The log file with the name log.txt is saved in the same folder as mRcv.exe.*

--End--

Troubleshooting if no data is multicasted out

Troubleshoot if no data is multicasted out by ensuring that all types of statistics are selected in the MulticastCtrl.exe file.

Procedure steps

Step	Action
1	Select **Start, All Programs, Accessories, Windows Explorer**.
2	Navigate to the folder <drive>:\Avaya\Contact Center\Manager Server\iccm\bin.
3	Double-click **MulticastCtrl.exe**.

4 In the **RTD Multicast controller** window, ensure that all types of statistics are selected.

5 Click **Apply**.

--End--

Interpreting Real-time Statistics Multicast error messages on the client PC

Troubleshoot when error messages appear on the client PC by reviewing and interpreting the message.

When you first launch a display and the system is retrieving data, an icon appears on the display, indicating whether the Contact Center Manager Administration server supports multicast clients, unicast clients, or both.

A unicast session is defined as a single data stream between the CCMA server and the client.There are a maximum of twelve possible sessions between the server and a client, two for each of the data types agent, skillset, application, nodal, IVR and route. The two sessions available are interval-to-date and moving window. Multiple displays that use the same data stream running on a client share a stream e.g a skillset tabular and skillset graphical display share a session.

Multicast communication transmits messages to multiple recipients at the same time. Multicast transmits only one stream of data to the network where it is replicated to many receivers.

After the display is launched, the icon indicates the transmission mode that is being used to launch the display.

Procedure steps

Step	Action
1	Review the error message and interpret it, using Real-time Statistics Multicast error messages (page 134).

--End--

Procedure job aid

Real-time Statistics Multicast error messages

Error message	Description
No unicast sessions available	This error normally appears on a client when an attempt to open a unicast channel fails and the client is not receiving multicast data. The absence of a unicast icon indicates that the unicast connection was not successfully established and the client PC is not receiving data packets. You need to close the display and try to launch it again later. If the problem persists, you may need to increase the number of unicast connections that the Contact Center Manager Administration server allows, if prior engineering analysis permits this.
No relevant data	This error normally appears on a client computer when it is receiving data, but the data is not relevant for the current display (for example, when the information is not available within the user partitions or the current filter blocks the data from the display). The presence of the unicast icon indicates that a unicast connection was successfully established and the client PC is receiving data packets.
No data is available on the network	This window appears on a client when it is not receiving any data. There is no icon at the top of the window, indicating that the display is not receiving any data. The Transmit Mode = Multicast note implies that the server supports only multicast, but, in this case, the client PC is not receiving multicast data. This may be the result of a network problem, or it may mean that the server can support unicast, but it has not been enabled. Report the problem to your administrator to check the Contact Center Manager Administration server settings and enable unicast, if necessary.
The characters * and 0 appears in the display	Occasionally, the statistics in a real-time display may stop updating and the characters * and 0 appear instead of the variable fields. In a unicast environment, this indicates that the server has stopped sending data to this client. You must close and reopen the display. In a multicast environment, this can indicate that the server is no longer sending the multicast stream. If the problem persists, you need to run a trace on the Contact Center Manager Administration server.

Troubleshooting when no Agent Real-time display appears when using a Gigabit NIC card

Troubleshoot when no Agent Real-time display appears due to problems with the Gigabit NIC card. A Real-time display issue occurs when the Receive Side Scaling (RSS) feature is enabled on the Gigabit NIC card. Multicast data cannot be received by Contact Center Manager Administration. You need to disable the RSS feature to view the Agent Real-time display.

Prerequisites

- Ensure that your contact center is not busy; if possible, perform this procedure when your contact center is not open.

Procedure steps

Step	Action
1	On the Contact Center Manager Administration server, choose **Start, Control Panel, Network and Internet, Network Sharing Center**.
2	Click **Change adapter settings**.
3	Right-click the Gigabit NIC card and click **Properties**.
4	In the **Local Area Connection Properties** window, on the **Networking** tab, click **Configure**.
5	In the Gigabit NIC card properties page, click the **Advanced** tab.
6	Click **Receive Side Scaling**, and confirm that it is **Disabled**.
7	Click **OK**.

--End--

Troubleshooting when Real-time displays do not display any data

Troubleshoot when opening a Real-time display and no data appears.

You need to check the following:

- On the Contact Center Manager Administration server, the Contact Center Manager Server IP address can be resolved correctly to the server name.
- On the Contact Center Manager Administration server, the Contact Center Manager Server name can be resolved correctly to the expected IP address.
- On the Contact Center Manager Server, the RSM Compression option has not been selected in the RTD Multicast Controller window. If this option is selected during configuration, real-time displays and Agent Desktop Displays will not function in Contact Center Manager Administration.

Procedure steps

Step	Action
1	On the Contact Center Manager Administration server, click **Start, Run**.
2	Type `cmd`.
3	Click **OK**.
4	In the **Command Prompt** window, type `ping <`Contact Center Manager Server `name>`.
5	Press **Enter**. *The Contact Center Manager Server IP address and the packets sent and received are displayed. If unexpected results are returned, check your DNS setting and the local host file on the server for incorrect entries.*
6	In the **Command Prompt** window, type `ping <`Contact Center Manager Server `IP address>`.
7	Press **Enter**. *The Contact Center Manager Server name and the packets sent and received are displayed. If unexpected results are returned, check your DNS setting and the local host file on the server for incorrect entries.*
8	On the Contact Center Manager Server, choose **Start, All Programs, Avaya, Contact Center, Manager Server, Multicast Stream Control**.
9	In the **RTD Multicast Controller** window, deselect the **RSM Compression** option.
10	Click **Apply**.
11	Click **OK**.
12	Close all windows.
13	Stop and start the Statistical Data Propagator (SDP) service, to activate the new RSM settings on the Contact Center Manager Server.

--End--

Troubleshooting when you cannot launch Real-time displays

Troubleshoot if you cannot launch Real-time displays on a client PC. In Contact Center Manager Administration, to enable the Real-time displays to start properly, the system downloads and registers a new RTDControl to the client PC when you launch a Real-time display for the first time. If you cannot launch a Real-time display, it can be because you enforced user policies that deny access to the registry on the PC, and, therefore, you are preventing the system from downloading and registering the new RTDControl.

To download the RTDControl, you can download the control manually or you can download the Multicast Trace Tool.msi on the client PC.

This procedure describes how to download the RTDControl manually. To download the Multicast Trace Tool.msi on the client PC, see Downloading the Multicast Trace Tool.msi on the client PC (page 137).

Prerequisites

- Ensure that you have administrator privileges for Contact Center Manager Administration.

Procedure steps

Step	Action
1	Log on to the client PC as the local administrator.
2	Open Contact Center Manager Administration.
3	Open the Real-Time Reporting component.
4	Launch a real-time display. *The system downloads and registers the required RTDControl to the client PC. Regular users can now log on to the client PC and launch Real-time displays.*
5	Perform steps 1 through 4 on each client PC where Real-time displays are launched.

--End--

Downloading the Multicast Trace Tool.msi on the client PC

Download the Multicast Trace Tool.msi on the client PC if you cannot launch Real-time displays on a client PC because you enforced user policies that deny access to the registry on the PC, and, therefore, you are preventing the system from downloading and registering the new RTDControl.

To download the RTDControl, you can download the Multicast Trace Tool.msi on the client PC or you can download the control manually.

This procedure describes how to download the Multicast Trace Tool.msi on the client PC. To download the RTDControl manually, see Troubleshooting when you cannot launch Real-time displays (page 136).

Prerequisites

- Ensure that you have administrator privileges for Contact Center Manager Administration.
- Ensure that you have access to the Contact Center Manager installation DVD.

Procedure steps

Step	Action
1	Log on to the client PC as the local administrator.
2	Insert the Contact Center installation DVD into the PC, and then navigate to the root directory.
3	In the root directory, double-click the file Multicast Trace Tool.msi to begin the installation. *The Windows Installer window appears briefly, followed by the Welcome window.*
4	In the **Welcome** window, click **Next**.
5	In the **Destination Folder** window, click **Next** to install to the default folder or click Change to install to a different folder.
6	In the **Ready to Install the Program** window, click **Install**.
7	Click **Finish**.
8	From the MS-DOS command prompt, change the directory to the folder on the client PC where the Multicast Trace Tool.msi files were copied by typing, for example: `cd c:\Program files\Avaya\Contact Center\Multicast Trace Tool`
9	From the MS-DOS command prompt, check if data is being received by the client PC by typing the following command: `icertdtrace -r IPSend <IP Multicast send address> -s <CCMS server name> -t <agent/application/skillset/ivr/nodal/route statistic type>` *If the client PC is receiving statistics from the Contact Center Manager Administration server, the data appears on the monitor. Data is displayed by server name and statistic type, making it possible to view a particular data stream from a particular server.*
10	To stop the information from scrolling, press CTRL+C. *You can also view the log file that captures the information, IPSndLog.txt, in the same directory as the Multicast Trace Tool.msi files.*

--End--

Troubleshooting when Real-time displays cannot launch and other displays display negative values or long data strings

Troubleshoot when Real-time displays cannot launch and other displays that can launch display negative values or long data strings. If you select the RSM Compression check box when you configure Contact Center Manager Server, Real-time displays and Agent Desktop Displays do not function in Contact Center Manager Administration. On the Contact Center Manager Server, ensure that the RSM Compression check box is clear in the RTD Multicast Controller window.

Procedure steps

Step	Action
1	On the Contact Center Manager Server, choose **Start, All Programs, Avaya, Contact Center, Manager Server, Multicast Stream Control**.
2	In the **RTD Multicast Controller** window, in the **Compression** section, deselect the **RSM Compression** option.
3	Click **Apply**.
4	Click **OK**.
5	Close all windows.
6	Stop and start the Statistical Data Propagator (SDP) service, to activate the new RSM settings on the Contact Center Manager Server.

--End--

Troubleshooting when no names appear in Real-time displays

Troubleshoot when no names (for example, agent names, answering skillset names, route names, IVR queue names, skillset and application names) appear in Real-time displays. Names may appear as *UNKNOWN* or they may appear incorrectly in the Real-time displays. If this happens, there may be a problem with one or more of the following:

- permissions in IIS
- network settings
- configuration of the DNS server
- delays in the network
- information storage in the RTD cache

Procedure steps

Step	Action
1	Verify that Contact Center Manager Server is running. Check the Windows Event Viewer log for network errors.
2	Check that IIS permissions are correctly configured. See Checking that IIS permissions are correctly configured (page 140).
3	Set the IP address field in IIS to All Unassigned. See Setting the IP address field in IIS to All Unassigned (page 141).
4	Check address configurations for Host Headers. See Checking address configurations for Host Headers (page 142).
5	Ensure the anonymous user account has the correct permissions. See Ensuring the anonymous user account has the correct permissions (page 142).

6	Verify that the information cache stored in the Contact Center Manager Administration server exists and contains the correct information. See Verifying the RTD information cache is storing correct information (page 143).

--End--

Troubleshooting when new agents appear as *UNKNOWN* in Real-time displays

Troubleshoot when a new agent is added but appears as *UNKNOWN* in Real-time displays.

This problem occurs if you install Veritas Backup Exec and use the default settings. The default installation of Veritas Backup Exec uses the TCP port 10000, which is the default port that the Avaya Aura™ Contact Center Web Client Toolkit NameService uses. This port conflict results in Web Client errors that require you to restart the ICERTDService to refresh the cache. To avoid this port conflict, you must change the default port that Veritas Backup Exec uses before you use the application.

Prerequisites

- Ensure that you know the ports that are being used by all Avaya and third-party products installed on your network.

Procedure steps

Step	Action
1	Change the default port in use by Veritas Backup Exec to a port that is not being used by any Avaya or third-party product installed on your network.
2	Verify that a port conflict no longer exists by using Veritas Backup Exec and then viewing the Real-time displays. If new agents still appear as *UNKNOWN*, contact Avaya support.

--End--

Checking that IIS permissions are correctly configured

Check that IIS permissions are correctly configured if names are not appearing in Real-time displays.

Procedure steps

Step	Action
1	On the Contact Center Manager Administration server, type the following in the Internet Explorer address bar: `http://localhost` *If IIS is configured correctly, you see the logon page. If the following error appears, IIS permissions are configured incorrectly, and you need to go to step 2 of this procedure:* `HTTP 403.6 - Forbidden: IP address rejected.`
2	If an error message appeared after Step 1, choose **Start, Administrative Tools, Internet Information Services (IIS)**.
3	In the left pane of the **Internet Information Services (IIS) Manager** window, click the plus (+) sign next to `<Computer_Name>` for the local computer. *The heading expands and a series of folders appears.*
4	Right-click **CCMA Web Site** and then select **Properties** from the menu.
5	In the **CCMA Web Site Properties** window, click the **Directory Security** tab.
6	In the **IP Address and Domain Name Restrictions** section of the window, click Edit.
7	In the **IP Address and Domain Name Restrictions** window, ensure that the local host address 127.0.0.1 is added to the list of allowed computers.
8	Click **OK**.

--End--

Setting the IP address field in IIS to All Unassigned

Set the IP address field in IIS to All Unassigned if names are not appearing in Real-time displays.

Procedure steps

Step	Action
1	On the Contact Center Manager Administration server, choose **Start, Administrative Tools, Internet Information Services (IIS) Manager.**
2	In the left pane of the **Internet Information Services (IIS) Manager** window, click the plus (+) sign next to `<Computer_Name>` for the local computer. *The heading expands and a series of folders appears.*
3	Right-click **CCMA Web Site** and then select **Properties** from the menu.
4	In the **CCMA Web Site Properties** window, in the IP address list, ensure that **All Unassigned** is selected.
5	Click **OK**.

--End--

Checking address configurations for Host Headers

Check address configurations for Host Headers if names are not appearing in Real-time displays.

Procedure steps

Step	Action
1	On the Contact Center Manager Administration server, choose **Start, Administrative Tools, Internet Information Services (IIS) Manager**.
2	In the left pane of the **Internet Information Services (IIS) Manager** window, click the plus (+) sign next to `<Computer_Name>` for the local computer. *The heading expands and a series of folders appears.*
3	Right-click **CCMA Web Site** and then select **Properties** from the menu.
4	In the **CCMA Web Site Properties** window, click **Advanced**.
5	In the **Advanced Web Site Identification** window, in the **Multiple identities for this Web site** list, an entry appears for the Default address only and the Host Header field is empty. If the Host Header field is populated, or if entries for IP addresses other than Default appear, you must have an entry for localhost.
6	Click **OK**.

--End--

Ensuring the anonymous user account has the correct permissions

Ensure that the anonymous user account has the correct permissions if names are not appearing in Real-time displays. If your anonymous user account was modified, this can cause *UNKNOWN* to appear in standard agent display. If the user specified is not the Default user, then the new user must have access to all of the files under the Program Files\Avaya Networks\WClient\Apps folder. The user must be able to access the “common\soaplisten” files.

Procedure steps

Step	Action
1	On the Contact Center Manager Administration server, choose **Start, Administrative Tools, Internet Information Services (IIS) Manager**.
2	In the left pane of the **Internet Information Services (IIS) Manager** window, click the plus (+) sign next to `<Computer_Name>` for the local computer. *The heading expands and a series of folders appears.*
3	Right-click **CCMA Web Site** and then select **Properties** from the menu.
4	In the **CCMA Web Site Properties** window, click the **Directory Security** tab.
5	Under **Authentication and access control**, click **Edit**.

6 Ensure that the anonymous user is a member of one of the groups with access to the required files, specifically common\soaplisten files.

7 Click **OK**.

--End--

Verifying the RTD information cache is storing correct information

Verify that the RTD information cache stored on the Contact Center Management Administration server is storing the correct information if names are not appearing in Real-time displays.

Procedure steps

Step	Action
1	Log on to the Web client as the webadmin user.
2	In Internet Explorer, go to http://<app_srv_name>/supportutil/rtdcache.asp where <app_srv_name> is the URL of the application server.
3	Enter the name of the Contact Center Manager Administration server. *The following information populates the window:* *- a list of active unicast clients* *- details of the data in the agent cache* *- details of the agent template cache* *- details of the skillset template cache* *- details of the application template cache* *- details of the IVR template cache* *- details of the route template cache* *- details of the nodal template cache*
4	If the correct information is not displayed, there is a problem with the RTD cache. Contact your administrator. OR If the correct information is displayed, the RTD cache is not the problem. Contact Avaya support.

--End--

Troubleshooting when a site does not appear in Network Consolidated Real-Time Displays

Troubleshoot when a networked site does not appear in the Network Consolidated Real-Time Display.

This can occur if a server is added by IP address instead of by name. If a server is added by IP address, the nodal displays for the site do not function correctly.

Another reason for this problem could be that the Network Consolidated Real-Time Displays do not display data for a Contact Center Manager site configured on the Contact Center Manager Administration server with a fully qualified hostname (for example, CCMS_test1.enterprise.europe.Avaya.com).

Procedure steps

Step	Action
1	If necessary, modify the server configuration to ensure that the server is added by name.
2	If necessary, modify the server configuration to use a non-fully qualified hostname (for example, CCMS1_test1).

--End--

Troubleshooting when the number of contacts waiting in an RTD does not match a query result

Troubleshoot if the number of contacts waiting in an application or skillset Real-time display does not match the Agent Desktop Contact Query result. This can occur for several reasons.

- If a contact is routed to a site where no agents are logged in for a skillset, then the contact counts against the application but not against the skillset.
- If a contact is rescheduled by an agent so it is no longer queueing to any skillset, then it counts against the application but not against the skillset.
- The contact may have been transferred by an agent to a different skillset than initially set by Contact Center Multimedia rules.
- The contact may not "queue to skillset", but may "queue to agent" in the script or application.
- The script or application may be queuing to multiple skillsets.

Procedure steps

Step	Action
1	To determine the number of calls or e-mail messages waiting, view the appropriate application or skillset Real-time display.

--End--

Managing memory leaks in Agent RTD when running Internet Explorer 8.0.

A memory leak occurs in the iexplore.exe file when you are running traffic and generating Agent Real-time displays when you use Internet Explorer 8.0.

Procedure steps

Step	Action
1	In Internet Explorer 8, choose **Tools**, **Internet Options**.
2	Click the **Advanced** tab.
3	Clear the check box beside **Disable Script Debugging (Internet Explorer)**.
4	Clear the check box beside **Disable Script Debugging (Other)**.
5	Click **OK**.

--End--

Launching multiple RTD displays

When your first browser launches a RTD display, the second browser cannot launch the same type RTD display (private or public). The error code 4097 - Transmission error appears in the second browser window.

Unicast has this limitation. It supports only one instance of the browser. The second instance of the browser attempts to use the IP from the first instance.

Procedure steps

Step	Action
1	Only use one browser to review unicast data in your system.

--End--

Troubleshooting when the report viewer is blank when launching an ad hoc report

Troubleshoot when you launch an ad hoc report and the report viewer is blank.

Procedure steps

Step	Action
1	On the client PC, install the required third-party files for the Crystal Reports viewer to function properly.

--End--

Troubleshooting when you cannot connect to the data source

Troubleshoot when you try to run historical reports and you receive an error message in the ad hoc report preview window indicating “There is a problem connecting to the data source.”

This problem can occur if the bindings order of the ELAN subnet network card and the contact center server subnet network card on the Contact Center Manager Server are not set up correctly. This problem can also occur if you do not refresh your server.

Procedure steps

Step	Action
1	Ensure that you configure the bindings order of the network interface cards so that the contact center server subnet card comes first, then the ELAN subnet card, and then the virtual adapters for remote access.
2	If necessary, refresh your server. See Refreshing servers (page 105).

--End--

Editing the sysadmin password in Contact Center Manager Administration

Edit the sysadmin password in Contact Center Manager Administration using the following procedure.

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration.
2	Open the **Configuration** component.
3	In the left pane, right-click the Contact Center Manager Server that is experiencing the problem.
4	Click **Edit Properties**.
5	In the **Login ID** box, change the Login ID to `sysadmin`.
6	In the **Password** box, type the same sysadmin password that is defined on the Avaya Aura™ Contact Center Server Classic Client.
7	Click **Submit**.
8	Refresh the same Contact Center Manager Server.
9	On the system tree, click the Contact Center Manager Server.
10	On the menu bar, select **Server, Refresh Server**.
11	Click **Yes**.
12	Click **Yes**.
13	On the Launchpad, select **Logout**.
14	Log back on to Contact Center Manager Administration.

--End--

Editing the sysadmin password using Server Utility

Edit the sysadmin password using Server Utility with the following procedure.

Procedure steps

Step	Action
1	Using the Server Utility, log on to Contact Center Manager Server.
2	Double-click **User Administrator, Users** screen.
3	Double-click on the name of the user that logs on to the server through Contact Center Manager Administration. The Login ID of this user is configured in the Desktop tab and is the same as the Login ID configured in the Server Properties page on Contact Center Manager Administration.

4 Click the **Desktop** tab, and note the access class of the user.

5 Use Server Utility to delete this user.

6 Redefine this user, using the same Login ID, Password, and access class.

7 Log on to Contact Center Manager Administration.

8 Open the **Configuration** component.

9 Refresh the same Contact Center Manager Server.

10 On the system tree, click the Contact Center Manager Server.

11 On the menu bar, select **Server, Refresh Server**.

12 Click **Yes**.

13 Click **Yes**.

14 On the Launchpad, select **Logout**.

15 Log back on to Contact Center Manager Administration.

--End--

Troubleshooting when you cannot print scheduled reports

Troubleshoot when you cannot print scheduled reports from the Historical Reporting component.

Prerequisites

- Ensure that you are logged on as a user with administrator privileges.

Procedure steps

Step	Action
1	On the Contact Center Manager Administration server, add and configure a local printer.

--End--

Troubleshooting when you cannot synchronize user-imported reports because network drive access is denied

Troubleshoot when you cannot synchronize user-imported reports and network drive access is denied. This problem occurs because the Contact Center Manager Administration IIS directory security account (IUSR_SWC) is not able to read the report template on the network drive.

This can occur for either of the following reasons:

- The source report folder on the network drive is not shared with read permissions for IIS directory security account.
- The Contact Center Manager Administration is on a workgroup and the network PC is on a domain, or vice-versa.

You need to verify network access. This is done differently if Contact Center Manager Administration is on a workgroup than if Contact Center Manager Administration is on a domain.

Prerequisites

- Ensure that you know whether Contact Center Manager Administration is on a workgroup or on a domain.

Procedure steps

Step	Action
1	If Contact Center Manager Administration is on a workgroup, on the Contact Center Manager Administration server, go to the MS-DOS prompt and run the net use command as follows: `NET USE \\<computername>\<sharename> password of IUSR_SWC /USER:IUSR_SWC` If you cannot map the network drive, check the permission on the report folder on the network drive. If you can map a network drive, but synchronization status displays the message Access denied on the network drive, contact Avaya support.
2	If Contact Center Manager Administration is on a domain and the IIS directory security account is also using the domain account, go to the MS-DOS prompt and run the net use command as follows: `NET USE \\<computername>\<sharename>password of IIS domain account /USER:domain name\IIS Domain Account Name` If you cannot map the network drive, check the permission on the report folder on the network drive. If you can map a network drive, but synchronization status displays the message Access denied on the network drive, contact Avaya support.

--End--

Troubleshooting when you cannot synchronize user-imported reports because cannot copy to CCMA server

Troubleshoot when you cannot synchronize user-imported reports and you cannot copy to the Contact Center Manager Administration server.

This can occur for either of the following reasons:

- The report is being run while you are trying to synchronize it.
- The report template file that was copied during the last successful synchronization had read-only attributes on the network folder.

Procedure steps

Step	Action
1	Ensure that the report is not running.
2	Change the attributes of the report template on the network drive to ensure that it is not read-only, and then save the report in Crystal software.
3	On Contact Center Manager Administration server, run the Synchronize User Imported Report Templates again.

--End--

Troubleshooting when you cannot import user-created report templates because of ASP script timeout error

Troubleshoot when you cannot import user-created report templates because of an ASP script timeout error. If the report templates were created in Crystal Reports 8.5 or earlier, and because Crystal Reports 9 onwards are Unicode-compliant, this may cause a delay or failure when importing and generating reports on Contact Center Manager Administration.

If you receive an ASP script timeout error when you attempt to import user-created report templates, you need to resave any report templates that cannot be imported.

Procedure steps

Step	Action
1	On a PC other than the Contact Center Manager Administration Server, install Crystal Reports 11 software.
2	On the same PC on which you installed Crystal Reports 11, create a new directory named `OldVersionTemplates`.
3	Copy all custom report templates created in Crystal Reports 8.5 or earlier versions into the directory `OldVersionTemplates`.
4	On the same PC on which you installed Crystal Reports 11, create a new directory named `Crystal11Templates`.
5	Open the Crystal Reports 11 software.
6	Click **File, Open**.
7	Go to the `OldVersionTemplates` directory and select one of the report templates.

8 Click **Open**.

9 Click **File, Save As** to save the report template into a Crystal Reports 11 report template in the `Crystal11Templates` directory.

10 Repeat steps 6 through 9 for each of the report templates in the `OldVersionTemplates` directory.

11 After you have resaved all of the old report templates into the `Crystal11Templates` directory, copy the `Crystal11Templates` folder to the desired PC from which you want to import the report templates.

--End--

Troubleshooting when Historical Reports cannot retrieve a large number of agents

Troubleshoot when you access the Historical Reporting component and attempt to retrieve a large number of agents in the selection criteria and a blank list is returned.

Procedure steps

Step	Action
1	In the Real-Time Reporting settings, increase the OAM Timeout value (for example, set the OAM Timeout value to 40000 for 4000 configured agents).

--End--

Troubleshooting when you cannot obtain a license to open a Report Creation Wizard session

Troubleshoot when you cannot obtain a license to open a Report Creation Wizard session. Check the License Manager Service configuration and look for Windows Event log entries with an LMService source.

For a co-resident server with Contact Center Manager Administration and Contact Center Manager Server, check with the Contact Center Manager Server administrator for the License Manager interface log file name and location.

Procedure steps

Step	Action
1	Click **Start, All Programs, Avaya, Contact Center, Manager Administration, Configuration**.
2	Click **LMService Configuration**.

3 Verify that the License Manager Server IP address and port numbers are correct.

4 Click **OK** to submit your changes, if any.

5 In the Windows event log, look for any entries with a source of `LMService`.

6 From the Contact Center Manager Administration install directory (or the directory indicated by the Contact Center Manager Server administrator), and using a text editor, open the log file `CCMA_LMService_1.log`.

7 Review and note any entries.

8 Close the `CCMA_LMService_1.log` file.

--End--

Troubleshooting when you cannot find Access and Partition Management information

Troubleshoot when you cannot find Access and Partition management information after you restore your backup file of Contact Center Manager Administration data. This occurs when you use the Windows Backup Utility to create your backup file and two of the AD-LDS files do not back up successfully.

You must ensure that the following AD-LDS files are included for all users in the Windows Backup Utility, and then you must backup and restore your Contact Center Manager Administration data again:

- `<x>://Program Files/Microsoft ADAM/InstanceName/data/adamntds.dit`
- `<x>://Program Files/Microsoft ADAM/InstanceName/data/ebd*.log`

Procedure steps

Step	Action
1	Click **Start, All Programs, Accessories, System Tools, Backup**. *The Backup and Restore Wizard appears.*
2	Click **Advanced Mode**.
3	Click the **Restore and Manage Media** tab.
4	In the **Restore and Manage Media** window, in the left-hand pane, expand the backup file that you use to restore your Contact Center Manager Administration data files by clicking the plus (**+**) sign next to the media item.
5	In the expanded list of the Contact Center Manager Administration backup files, ensure that the following files are listed: • <x>://Program Files/Microsoft ADAM/InstanceName/data/adamntds.dit • <x>://Program Files/Microsoft ADAM/InstanceName/data/ebd*.log

6 If the two AD-LDS files in step 5 appear in the expanded list, go to step 12.
If the two AD-LDS files in step 5 do not appear in the expanded list, go to step 7.

7 In the Windows Backup Utility, click **Tools, Options**.

8 In the **Options** window, click the **Exclude Files** tab.

9 In the **Exclude Files** window, under **Files excluded for all users:**, select the following AD-LDS files and click **Remove**:

- <x>://Program Files/Microsoft ADAM/InstanceName/data/adamntds.dit
- <x>://Program Files/Microsoft ADAM/InstanceName/data/ebd*.log

10 Click **OK**.

11 Close all windows to exit the Windows Backup Utility.

12 Create a new backup file of your Contact Center Manager Administration data files, and restore the backup file again. Ensure that the following two files are selected when you perform the backup:

- <x>://Program Files/Microsoft ADAM/InstanceName/data/adamntds.dit
- <x>://Program Files/Microsoft ADAM/InstanceName/data/ebd*.log

--End--

Troubleshooting when you cannot view agents or skillsets

Troubleshoot when you cannot view available agents and skillsets in the User Defined Partition view. If a server that is not fully operational is listed for this partition, then agent or skillset information for remaining servers may not display properly.

Procedure steps

Step	Action
1	Ensure that all servers configured on Contact Center Manager Administration are fully operational.

--End--

Troubleshooting when User Defined Historical Reports shows data for the day instead of the selected interval

Troubleshoot when a user defined historical report shows data for the day instead of the selected interval. This can happen when the data field used for data range filtering is a Date field and not a DateTime field. This can happen for the following reasons:

- The report was imported as an interval report, but the timestamp field selected is not a DateTime field.
- The report is using the Convert DateTime to Date feature which is no longer supported.

You must verify the issue is caused by the data field being a Date Field instead of a DateTime field. Reimport the report. Change the report to not use Convert DateTime to DateSelect a Report Data Range other than Interval or select another a DateTime field.

Procedure steps

Step	Action
1	On the Contact Center Manager Administration server, select **Start**, **Administrative Tools**, **Event Viewer**.
2	Expand the **Windows Logs** folder.
3	Select application.
4	Find **Event ID 61714** from **Source CCMADisplayReport** or **CCMAReportSevice**. The event provides the Date Field, Report Name, Report Group, Report User and Server Name.
5	Import the report selecting a **Report Data Range** other than **Interval** OR Select another a **DateTime** field as the **Timestamp** field.
6	Open the report in Crystal Reports.
7	Select **File**, **Report Options**.
8	In **Report Options**, select **To Date-Time** in the **Convert Date-Time** list.
9	Select the valid **ODBC Data Source** for the report.
10	If needed, provide a **User ID** and **Password** to access the data source.
11	Create a new formula to convert the datetime field back to date. For example, if the field used is the Timestamp from the iApplicationStat table, the formula would be CDate({iApplicationStat .Timestamp})
12	Replace the current database field on the report with the new formula.
13	If groups are based on the same field, change the group to use the new formula field.
14	Confirm all servers configured on Contact Center Manager Administration are fully operational.

--End--

Troubleshooting when Contact Center Management No Supervisors Defined error messages occur

Troubleshoot when you receive No Supervisors Defined error messages after you add supervisors in Contact Center Management, exit the component, return to the component, and select the same server in Contact Center Manager Server on which you defined the supervisors, but the supervisors are not there.

This problem can occur when the bindings order of the ELAN subnet network card and the contact center server subnet network card on the server in Contact Center Manager Server are not set up correctly. You must configure the bindings order of the network interface cards so that the contact center server subnet card comes first, then the ELAN subnet card, and then the virtual adapters for remote access. Ensure that all Contact Center Manager Administration procedures are on the Contact Center Manager Server.

Procedure steps

Step	Action
1	On the Contact Center Manager Server, choose **Start, Control Panel, Network and Internet**.
2	Click **Network and Sharing Center**.
3	Click **Change adapter settings**.
4	In the **Network Connections** window, press **Alt**. A hidden menu displays.
5	From the **Advanced** menu, click **Advanced Settings**.
6	In the **Connections** box, ensure that the contact center server subnet connection is listed first. If it is not listed first, adjust the order to ensure that it appears first in the list.
7	Save your changes and close all windows.
8	Restart the Contact Center Manager Server.

--End--

Troubleshooting when Column Names text and data run over the line in historical reports

Troubleshoot when you run a historical report and the Column Names text and data run over the line, making the report unreadable.

This problem is caused when the generic text printer installed on the Contact Center Manager Administration server conflicts with the historical report formatting.

Procedure steps

Step	Action
1	On the Contact Center Manager Administration server, remove the generic text printer.
2	Install a printer driver that is compatible with Crystal Web (for example, the HP LaserJet 4000 Series).

--End--

Troubleshooting when the last column is cut off when you run a historical report

Troubleshoot when you run an Agent Performance report and the last column of the report is cut off in the Ad hoc Crystal Report Viewer.

This problem is caused because the report does not fit on letter-size paper.

Procedure steps

Step	Action
1	Create a new default printer and change the paper size to Legal.
2	Print the Agent Performance report using the new default printer.

--End--

Troubleshooting when historical reports Selection Criteria is slow to display the list of agent IDs

Troubleshoot when it takes a very long time for the list of agent IDs in the Selection Criteria pane to populate.

This problem can occur when the contact center server subnet address and the ELAN subnet address are both listed in the DNS entries for the Contact Center Manager Server.

Procedure steps

Step	Action
1	Check the DNS entries for the Contact Center Manager Server.

2 If both the contact center server subnet address and the ELAN subnet address are listed, remove the ELAN subnet address.

--End--

Troubleshooting when the scheduled report export fails on the network drive

Troubleshoot when the scheduled report export fails on the network drive. This problem occurs because the Contact Center Manager Administration scheduled report account (iceAdmin or the domain account) cannot write to the specified folder in the output file text box. This occurs for one of the following reasons:

- The scheduled report account or account password used for the shared folder on the client does not match the scheduled report account or account password on the Contact Center Manager Administration server.
- You specified an invalid path when scheduling the report.
- The network directory folder does not have read/change permissions.
- A network problem occurs when connecting to the directory folder.

To resolve the problem, use the iceAdmin Password Change Utility to reset the scheduled report account or account password. This resets all of the scheduled reports to use the correct account name and password when exporting reports.

To verify network access from Contact Center Manager Administration, use the scheduled report account (iceAdmin or the domain account) and password for this account to map the network drive to which the report is to be exported. Alternatively, you can use the net use command to verify whether you can map to the directory folder on the network drive from the Contact Center Manager Administration server.

Procedure steps

Step	Action

1	On the Contact Center Manager Administration server, go to the MS-DOS prompt and run the net use command as follows.
	If you use iceAdmin as your scheduled report folder, type:
	`NET USE \\<computername>\<sharename> password of iceAdmin /USER:iceAdmin`
	If you use the domain account as your Scheduled report folder, type:
	`NET USE \\<computername>\<sharename>password of iceAdmin /USER:<domain account name>`

2	If you cannot map the network drive, check the permission on the report folder on the network drive. If you can map the network drive, try to create a file on the network folder.

3	If you cannot create a file on the network folder, check the share permissions on the network folder from the network PC. It must be set to Read/Change for the account that you have set up on the network PC. If you can create a file on the network folder, but the scheduled report export still fails, contact Avaya support.

--End--

Troubleshooting when you cannot activate scheduled reports

Troubleshoot when you cannot activate scheduled reports in Contact Center Manager Administration.

This problem occurs when the Internet Information Services (IIS) default security account under anonymous access is not a member of the backup operators group, or if you need to reset your scheduled report account (iceAdmin or the domain account) password.

Procedure steps

Step	Action
1	Ensure that the IIS default security account under anonymous access is a member of the backup operators group. See Ensuring that IIS default security account under anonymous access is a member of backup operators (page 158).
2	Reset the scheduled report account or account password using the iceAdmin Password Change utility. See Resetting the scheduled report account or account password using the iceAdmin Password Change utility (page 159).

--End--

Ensuring that IIS default security account under anonymous access is a member of backup operators

Ensure that the IIS default security account under anonymous access is a member of the backup operators group, if you cannot activate scheduled reports in Contact Center Manager Administration.

Procedure steps

Step	Action
1	On the Contact Center Manager Administration server, choose **Start, Administrative Tools, Internet Information Services (IIS) Manager**.

2 In the **Internet Information Services (IIS) Manager** window, in the system tree, click the plus (**+**) sign beside the Web Sites folder.

3 In the expanded folder, right-click **CCMA Web Site**, and then click **Properties** on the menu.

4 In the **CCMA Web Site Properties** window, click the **Directory Security** tab.

5 Under the **Authentication and access control** heading, click **Edit**.

6 In the **Authentication Methods** dialog box, ensure that **Enable Anonymous Access** is selected, and note the user account that is listed in the User Name box.

7 Close all windows.

8 Click **Start, Administrative Tools, Computer Management**.

9 In the left pane, click the **Local Users and Groups** heading.

10 In the right pane, double-click the **Groups** folder.

11 From the list of groups in the right pane, double-click **Backup Operators**, and ensure that the IIS default security account under anonymous access is listed under backup operators.

12 If the IIS default security account under anonymous access is listed, proceed to Resetting the scheduled report account or account password using the iceAdmin Password Change utility (page 159).
OR
If it is not listed, click **Add**.

13 Enter the domain account as `<domainname>\account name`, and then click **OK**.

14 If you cannot see the domain account on the Contact Center Manager Administration server, contact your network administrator.

15 Close all windows.

--End--

Resetting the scheduled report account or account password using the iceAdmin Password Change utility

Reset the scheduled report account or account password using the iceAdmin Password Change utility, if you cannot activate scheduled reports in Contact Center Manager Administration.

Prerequisites

- If you have a domain account, ensure that you know the domain account name and password. If necessary, contact your network administrator for this information.

Procedure steps

Step	Action
1	On the Contact Center Manager Administration server, choose **Start, All Programs, Avaya, Contact Center, Manager Administration, Configuration**.
2	In the left pane, click **Avaya**.
3	In the **Avaya Applications Configuration** window, click **IceAdmin Password Change**.
4	In the **iceAdmin Password Change** window, in the **Old Password** box, type the old password.
5	In the **New Password** box, retype the old password for the iceAdmin user account. This resets the iceAdmin password.
6	In the **Confirm Password** box, type the password again. *If your Contact Center Manager Administration server is a member of an active domain, the Domain Account option is enabled on the iceAdmin Password Change window.*
7	If you do not want to export scheduled reports to a domain account, or if the Domain Account button is disabled, go to step 12. OR If you want to export scheduled reports to a domain account, and the Domain Account button is enabled, click **Domain Account**.
8	From the **Select Domain Name** list, select the name of the domain to add.
9	In the **Enter Domain Account** box, type the domain account provided by your network administrator.
10	In the **Enter Domain Account Password** box, type the domain account password provided by your network administrator.
11	In the **Confirm Domain Account Password** box, type the domain account password again.
12	Click **OK**. *The system verifies that you typed the same password both times, and then resets the password in all required components.*
13	Close all windows.

--End--

Troubleshooting when historical reports display and print only in portrait orientation

Troubleshoot if the historical reports always display and print in portrait orientation even if the report template is designed for landscape mode. This can result in report data columns being truncated.

This problem is caused by a printer driver on the Contact Center Manager Administration server.

Procedure steps

Step	Action
1	On the Contact Center Manager Administration server, choose **Start, Devices and Printers**.
2	Select the **Microsoft Office Document Image Writer** printer, right-click and select **Remove device** from the menu.

--End--

Troubleshooting when exporting large reports to PDF results in error message

Troubleshoot when you attempt to export a large report to PDF and the following error message appears: The report was not exported. The selected export format may be disabled on the server.

This error message appears if you attempt to export a report to PDF that is more than 360 pages long. To export a report to PDF with more than 360 pages, you must use the page selection fields and export the report in batches of 360 pages or less.

Procedure steps

Step	Action
1	When exporting a report to PDF that is longer than 360 pages, export the first batch to PDF using pages 1 to 360.
2	Export the next batch to PDF using pages 361 to no more than page 720.
3	Continue exporting to PDF in batches of 360 pages or less until the entire report is exported.

--End--

Troubleshooting when fonts are missing in Report Creation Wizard

Troubleshoot when there are fonts missing from the font list on the Configuration Settings page and the Report Layout page in Report Creation Wizard.

The fonts that are available in Report Creation Wizard are the fonts that are installed on the Contact Center Manager Administration server. There are restrictions on the type of fonts available in Report Creation Wizard and fonts that do not meet these requirements are not available.

Procedure steps

Step	Action
1	Verify with the administrator that the fonts installed on the Contact Center Manager Administration server meet the following requirements: • The font must be a TrueType font. • The font must support the following styles: Regular, Bold, Italic, Underlined, and Strikethrough. • The font must support ANSI or Symbol character sets. The font can also support other character sets.

--End--

Troubleshooting Configuration Tool problems

Troubleshoot Configuration Tool problems by ensuring that you do not exceed the restrictions and limits set in the Parameters tab of the Historical Statistics window in Contact Center Manager Server. For example, if you have a limit of 240 configured CDNs in the Historical Statistics, you cannot upload more than 240 CDNs using the Contact Center Manager Server Configuration Tool spreadsheet.

Procedure steps

Step	Action
1	On the Contact Center Manager Server, open the **Historical Statistics** window and note the limits set on the **Parameters** tab.
2	If you use a client PC to upload or download configuration data, ensure that the Contact Center Manager Administration application can be accessed from the client with the Contact Center Manager Administration Server Name.
3	Ensure that you are aware of the number of worksheet columns that your version of Microsoft Excel supports (for example, 256 columns). The number of agent to skillset assignments and agent to supervisor assignments that you can upload from the Configuration Tool spreadsheets is restricted to the maximum number of worksheet columns available in Microsoft Excel.
4	Open **Tools, Macro, Security** and ensure that the **Security level** is set to **Medium** and that **Macros** are enabled.

--End--

Troubleshooting when e-mail notifications are not received

Troubleshoot when e-mail notifications are not received after a scheduled report succeeds or fails. The e-mail address is defined for each report.

If the e-mail was not sent, then the failure will be logged in the Event Viewer on the Contact Center Manager Administration server.

Prerequisites

- Ensure that you know the SMTP Server details. If necessary, contact your network administrator for this information.

Procedure steps

Step	Action
1	On the Contact Center Manager Administration server, select **Start**, **Administrative Tools**, **Event Viewer**.
2	In the left pane of the **Event Viewer** window, expand **Windows Logs** and select **Application**.
3	Select the event with the following details: Level: Warning Source: CCMAReportService Event ID: 61706
4	In **Event Properties**, on the **General** tab, look for Email = <status> - <email To Address>, where that status can be **OK** or **Failed**.
5	If the e-mail status is OK, confirm that the <email to Address> is correct.
6	If the e-mail <status> is Failed, look for Error = Email: Failed to send email notification, which should be followed by an error message. The following table provides details for known errors:

Error message	Description
The remote name could not be resolved	Confirm that the SMTP Server entered is correct.
Unable to connect to remote server	Confirm that the SMTP Server and port entered are correct. If the CCMA server was entered as the SMTP Server, ensure the SMTP Server is installed and configured.

Error message	Description
The SMTP server requires a secure connection or the client was not authenticated. The server response was: 5.7.0 Must issue a STARTTLS command first.	The SMTP Server requires SSL. Update the e-mail notification settings such that SSL Required is selected.
Mailbox unavailable. The server response was: 5.7.3 Requested action aborted; user not authenticated.	The User Name or Password entered for accessing the SMTP Server are invalid. Update the e-mail notification settings with a valid e-mail account and ensure the password is correct.

7 Repeat steps 3 to 6 for each event.

--End--

Troubleshooting when you cannot upgrade Agent Desktop Display

Troubleshoot when you cannot upgrade Agent Desktop Display from Avaya Aura™ Contact Center Web client to Contact Center Manager Administration on client PCs.

This problem can occur if you have proxy settings turned on when you attempt to upgrade Agent Desktop Display. You need to ensure that proxy settings are turned off before you upgrade Agent Desktop Display. If your network security policy requires, you must turn proxy settings back on after you complete the Agent Desktop Display upgrade.

Procedure steps

Step	Action
1	On Internet Explorer, choose **Tools, Internet Options**.
2	In the **Internet Options** window, on the **Connections** tab, click **LAN Settings**.
3	In the **Local Area Network (LAN) Settings** window, clear the checkbox next to **Use a proxy server for your LAN**.
4	Click **OK**.
5	Close all windows.

--End--

Troubleshooting when Agent Desktop Displays do not show any data

Troubleshoot when you launch Agent Desktop Display and no data appears.

This problem can occur if you select the RSM Compression option in the RTD Multicast Controller window when you configure Contact Center Manager Server. If you select the RSM Compression option, real-time displays and Agent Desktop Displays will not function in Contact Center Manager Administration.

Procedure steps

Step	Action
1	On the Contact Center Manager Server, choose **Start, All Programs, Avaya, Contact Center, Manager Server, Multicast Stream Control**.
2	In the **RTD Multicast Controller** window, in the **Compression** section, deselect **RSM Compression**.
3	Click **Apply**.
4	Click **OK**.
5	Close all windows.
6	Stop and start the Statistical Data Propagator (SDP) service.

--End--

Installing Sybase Open Client 12.5

Install Sybase Open Client 12.5 to access and control the content of the Contact Center Manager Administration database.

Prerequisites

- Ensure that you have administrator privileges in Windows Server 2008.
- Use the same administrator account to log on to the Contact Center Manager Administration server each time you install a Contact Center Manager Administration component.

Procedure steps

Step	Action
1	Log onto Contact Center Manager Administration server as the administrator.
2	Insert the Contact Center installation DVD into the DVD drive.
3	If the Contact Center DVD installer main menu appears, click **Cancel**.
4	Using Windows Explorer, browse in the DVD folder to **ThirdParty**, **Sybase Open Client**.
5	In the **Sybase Open Client** folder, double-click **setup.exe**.

6 Select **Standard Install**.

7 Click **Next**.

8 In the **Choose the installation directory** box, accept the default location.

9 On the **Choose Directory** dialog box, click **Next**.

10 On the **Summary** dialog box, click **Next**.

11 On the **Create Directory** dialog box, click **Yes** to confirm the name of the directory to which to copy the files.

12 If you upgrade to Sybase version 12.5, the system asks if you want to overwrite the following existing Sybase.DLL files. Click **Yes** when prompted to replace or reinstall these Sybase files:

- Replace mchelp.dll version 12.0 with version 12.5.0.0
- Replace mclib.dll version 12.0 with version 12.5.0.0
- Replace Language Modules version 12.0 with version 12.5
- Reinstall Component Sybase Central 3.2.0

13 If the system prompts you to replace the optional Power Dynamo file, click **Yes**. Replace the optional Power Dynamo file, replace version 3.0.0 with version 3.5.2.

14 If the system prompts you to replace any other DLLs, including system DLLs, such as msvcrt40.dll version 4.20, click **No**. Do not replace any system DLLs.

15 A message box appears that states the system does not need this update. Click **OK**.

16 On the **Sybase Installer Confirmation** dialog box, click **Yes** to restart the system before you configure the installed components.

17 Click **OK**.

18 Close the Control Panel window.

--End--

Updating the Sybase ODBC driver

Update the Sybase Database Connectivity (ODBC) driver to ensure that you use the latest version.

Prerequisites

- Install Sybase Open Client 12.5.

Procedure steps

Step	Action
1	Click **Start, Run**.
2	In the **Open** box, type **cmd**.

3 Click **OK**.

4 At the prompt, type **iisreset**.

5 Press **Enter**.

6 At the **MS-DOS** prompt, navigate to the root directory of the Sybase folder on the DVD. For example, <x>: \ThirdParty (<x> is the location of the DVD).

7 Change to the directory containing the Sybase Open Client hotfixes. For example, cd Sybase Open Client — Hotfixes.

8 Type the following xcopy command:

```
xcopy EBF11113\*.* %SYBASE% /S /E /V /Y > C:\EBF11113.TXT
```

9 Press **Enter**.

--End--

Variable definitions

Command	Description
EBF11113	The directory containing the Sybase ODBC driver.
<SYBASE>	The environment variable containing the directory location of the Sybase Open Client 12.5 software installed on the Contact Center Manager Administration server (for example, c:\sybase).
C:\EBF11113.TXT	The log file that you can use to verify that all the files are copied correctly.

Verifying that the system successfully updated the driver

Verify that the system successfully updated the Sybase ODBC driver to ensure that the Contact Center Manager Administration server software can interact with the database.

Perform this step only if you plan to use a Contact Center Manager Server Release 6.0 to report statistics.

Prerequisites

- Update the Sybase ODBC driver. See Updating the Sybase ODBC driver (page 166)

Procedure steps

Step	Action
1	On the target server, browse to **C:\Windows\SysWOW64**.

2 Double-click **ODBC Data Source Administrator** to start the 32-bit version of the driver.

3 In the **ODBC Data Source Administrator** dialog box, click the **Drivers** tab.

4 On the **Drivers** page, scroll down until you locate the correct **Sybase ASE ODBC** driver, which is **4.10.00.49**.

5 Click **OK**.

6 If the ODBC driver version is not 4.10.00.49, open the log file C:\EBF11113.txt to see any error messages were recorded during the xcopy command.

--End--

Avaya Communication Server 1000 PABX troubleshooting

This section describes the troubleshooting procedures that you should perform when handling Avaya Communication Server 1000 PABX issues in Avaya Aura™ Contact Center Release 6.0/6.1. This section provides information about how and where to check for the status of the various configuration elements and parameters mentioned in the checklists.

Prerequisites for Contact Center PABX troubleshooting

- Read the *Avaya Aura™ Contact Center Configuration – Avaya CS1000 Integration* (NN44400-512) guide.

Navigation

Verifying that the server is up

Verify that the server is up to determine where subsystem link problems are occurring. Problems may be related to the Contact Center Manager Server, the PABX, or on the Contact Center Manager Administration server.

Procedure steps

Step	Action
1	On the Contact Center Manager Server, in the SCMU utility, check that all components have the status Started.
2	On the PABX, check that the ELAN subnet connection to the PABX is functioning. See Verifying the ELAN subnet connection between the server and PABX (page 170).
3	Verify that you can successfully log on to the Contact Center Manager Administration server

--End--

Verifying the ELAN subnet connection between the server and PABX

Verify that the ELAN subnet connection between the server and the PABX is functioning.

Procedure steps

Step	Action
1	On the PABX, in LD 48, enter the following command: stat ELAN.
2	Verify that the status for the ELAN subnet connected to the server is ACTIVE, EMPTY and APPL ACTIVE.
3	If there are multiple ELAN subnets, check the ELAN subnet connection for each IP address.

--End--

Example

```
>ld 48
LNK000
.stat elan
SERVER TASK: ENABLED
ELAN #: 16
APPL_IP_ID: 47.166.111.14
LYR7: ACTIVE EMPTY APPL ACTIVE
ELAN #: 17
APPL_IP_ID: 47.166.111.13
LYR7: ACTIVE EMPTY APPL ACTIVE
```

Verifying the ACCESS Link between the Contact Center Manager Server and Avaya CallPilot™

Verify that the ACCESS Link between the Contact Center Manager Server and Avaya CallPilot™ is functioning.

Procedure steps

Step	Action
1	On CallPilot, select **System Utilities, Support Tools, CallPilot Processing Utilities, Trace Viewer <nbtview>**.
2	In Trace Control, on Meridian Link Services (MLS), select **MLink_Trace** for messages on Meridian Link Services (MLS).
3	Select **NBAPE** for messages on ACCESS Link.
4	On the Contact Center Manager Server, select **Start, Run**, enter **tsm_oam**, and then select option 3.
5	For VSM and MLSM session traces: • From the OAM menu, select option 2, and then enter 0 at the prompt. • Note the Session ID for VSM_Service and Meridian Link Services (MLS) SP (CallPilot Application). • Press Return to go back to the OAM menu. • Select option 5, enter the Session ID, and then respond to the prompts as appropriate.
6	For AML traces:

- From the OAM menu, select option 7.
- From the AML Trace menu, select option 4.

7 For Access Protocol traces:

- From the OAM menu, select option 9.
- Select option 3 to enable the trace.

8 For Access Protocol Debug traces:

- From the OAM menu, select option 10.
- Select option 3 to enable the trace.

--End--

Verifying the PABX loop, shelves, and cards

Verify that the PABX loop, shelves, and cards are functioning.

Procedure steps

Step	Action
1	On the PABX, in LD 32, use the following command: **stat n1 n2 n3** where n1 is the loop, n2 is the shelf, and n3 is the card that contains either agents or voice ports.
2	The status for real agents must be LOG IN or LOG OUT, depending on the state of the agent.
3	The status for CallPilot voice ports must always be LOG IN. If it is not, disable and enable the port on CallPilot to trigger the auto-logon.

--End--

Example

Command on the PABX**:**

Loop

ld 32

NPR000

.stat 24

SUPER LOOP

000 DSBL 038 BUSY

Real agents status (2500 set agents):

.stat 24 0 0

00 = UNIT 00 = IDLE (L500 LOG IN)

01 = UNIT 01 = IDLE (L500 LOG IN)

02 = UNIT 02 = IDLE (L500 LOG IN)

03 = UNIT 03 = IDLE (L500 LOG IN)

04 = UNIT 04 = IDLE (L500 LOG IN)

05 = UNIT 05 = IDLE (L500 LOG IN)

06 = UNIT 06 = IDLE (L500 LOG IN)

07 = UNIT 07 = IDLE (L500 LOG IN)

08 = UNIT 08 = IDLE (L500 LOG IN)

09 = UNIT 09 = IDLE (L500 LOG IN)

10 = UNIT 10 = IDLE (L500 LOG IN)

11 = UNIT 11 = IDLE (L500 LOG IN)

12 = UNIT 12 = IDLE (L500 LOG IN)

13 = UNIT 13 = IDLE (L500 LOG IN)

14 = UNIT 14 = IDLE (L500 LOG IN)

15 = UNIT 15 = IDLE (L500 LOG IN)

Voice Ports status (SL1 sets):

.stat 4 0 3

00 = UNIT 00 = IDLE (BCS LOG IN)

01 = UNIT 01 = IDLE (BCS LOG IN)

02 = UNIT 02 = IDLE (BCS LOG IN)

03 = UNIT 03 = IDLE (BCS LOG IN)

04 = UNIT 04 = IDLE (BCS LOG IN)

05 = UNIT 05 = IDLE (BCS LOG IN)

06 = UNIT 06 = IDLE (BCS LOG IN)

07 = UNIT 07 = IDLE (BCS LOG IN)

Verifying that CallPilot™ ports are enabled

Verify that the CallPilot ports are enabled.

Procedure steps

Step	Action
1	On the CallPilot client, navigate to CallPilot Manager.
2	Select **Channel Monitor** link.
3	Verify that the channels are in **Idle** state. *ACCESS channels appear in blue and Give IVR channels appear in green.*

--End--

Verifying that the CDN is acquired

Verify that the CDN is acquired.

Procedure steps

Step	Action
1	Go to **Contact Center Manager Administration Launchpad, Configuration**.
2	Select **CDN (Route Points)**.
3	Verify that the CDN status is **Acquired**.
4	On the PABX, in LD 23, enter the command **REQ PRT**.
5	Enter the command **TYPE CDN**. *The following values appear on the printout:* • AACQ = YES • ASID = ELAN connected to Contact Center Manager Server • CNTL = YES

--End--

Example

```
ld 23
ACD000
MEM AVAIL: (U/P): 3591770 USED: 405925 TOT:
3997695
DISK RECS AVAIL: 2682
ACD DNS AVAIL: 23758 USED: 242 TOT: 24000
REQ PRT
TYPE cdn
CUST 0
CDN 2003
TYPE CDN
CUST 0
CDN 2003
FRRT
SRRT
FROA NO
MURT
DFDN 7700
CEIL 2047
OVFL NO
TDNS NO
RPRT YES
AACQ YES
ASID 16
SFNB 1 2 3 4 5 6 9 10 11 12 13 15 16
17 18 19
USFB 1 2 3 4 5 6 7 9 10 11 12 13 14 15
CALB 0 1 2 3 4 5 6 7 8 9 11
CNTL YES
VSID
HSID
```

CWTH 1

BYTH 0

OVTH 2047

STIO

TSFT 20

Verifying that the correct script is activated

Verify that the correct script is activated.

Prerequisites

- SCE is installed on the client and server.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration.
2	Click **Scripting**.
3	From the **Service Creation** Menu, choose **Launch Service Creation**. *The SCE Contact Center list opens.*
4	In the SCE Contact Center pane, expand **Contact Center Manager Administration server name**, **Contact Center Manager Server name**, **Application [Full Control]**. *A list of existing scripts on that Contact Center Manager Server appears.*
5	Verify that the script is in Active state, as indicated by a green checkmark on the script icon.
6	If the script is not active, right-click on the script and select **Activate**. *The system activates the script. The script status changes to Active when the activation process finishes successfully.*

--End--

Verifying that the IVR ACD-DN is acquired

Verify that the IVR ACD-DN is acquired.

Procedure steps

Step	Action

1. Log on to the Contact Center Manager Administration.
2. Click **Configuration**.
3. Select **IVR ACD-DN**.
4. Verify that the IVR ACD-DN status is **Acquired**.
5. On the PABX, in LD 23, enter the command **REQ PRT**.
6. Enter the command **TYPE ACD**.

   The following values appear on the printout:

   - AACQ = YES
   - ASID = ELAN connected to Contact Center Manager Server
   - IVR = YES
   - TRDN = default treatment DN, if any

Example

```
ld 23
ACD000
MEM AVAIL: (U/P): 3591770 USED: 405925 TOT: 3997695
DISK RECS AVAIL: 2682
ACD DNS AVAIL: 23758 USED: 242 TOT: 24000
REQ PRT
TYPE acd
CUST 0
ACDN 7725
TYPE ACD
CUST 0
ACDN 7725
MWC YES
IMS YES
CMS YES
IMA YES
IVMS YES
EES NO
VSID 7
MAXP 48
SDNB NO
BSCW NO
AACQ YES
ASID 16
SFNB 1 2 3 4 5 6 9 10 11 12 13 15 16 17 18 19
USFB 1 2 3 4 5 6 7 9 10 11 12 13 14 15
CALB 0 1 2 3 4 5 6 7 8 9 11
ALOG YES
RGAI NO
ACAA NO
FRRT
```

...

CCBA NO

IVR YES

TRDN 3600

CWNT NONE

Verifying that Give IVR voice ports are acquired by the TN in CallPilot™

Verify that the Give IVR voice ports are acquired by the TN in CallPilot.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration.
2	Select **Phonesets and Voice Ports**.
3	Verify that the Voice Ports status is **Acquired Login**.
4	In the CallPilot Manager, select **Channel Monitor link**.
5	Verify that the Give IVR channels are in **Idle** state.
6	On the PABX, in LD 20, use the following commands: **REQ TNB** and **TYPE 2008**. *The following values appear on the printout:* • ACQ AS = TN • ASID = ELAN connected to Contact Center Manager Server

--End--

Example

DES CLPLT

TN 024 1 13 26

TYPE 2008

CDEN 8D

CTYP XDLC

CUST 0

FDN

TGAR 1

LDN NO

NCOS 3

RNPG 0

SCI 0

SSU

XLST

SCPW

CLS CDT ...

CPND_LANG ENG

HUNT

SPID NONE

AST 00 01

IAPG 0

AACS YES

ACQ AS: TN,AST-DN,AST-POSID

ASID 16

SFNB 1 2 3 4 5 6 11 12 13 18 22

SFRB

USFB 1 2 3 4 5 6 7 9 10 11 12 13 14 15

CALB 0 1 2 3 4 5 6 8 9 10 11 12

FCTB

ITNA NO

DGRP

PRI 01

DNDR 0

DTMK

KEY 00 ACD 5990 0 5356

AGN

01 SCN 5386 0 MARP

CPND

NAME CallPilot

XPLN 27

DISPLAY_FMT FIRST,LAST

02 MSB

03 NRD

04 TRN

05 AO3

06

07

Verifying that ACCESS voice ports are acquired by the TN and CallPilot™ class ID or channel

Verify that the ACCESS voice ports are acquired by the TN and CallPilot class ID or channel.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration.
2	Select **Phonesets and Voice Ports**.
3	Verify that the Voice Ports status is **Acquired Login**.
4	On the CallPilot client, in the CallPilot Manager, select **Channel Monitor link**.
5	Verify that the ACCESS channels are in **Idle** state.
6	On the PABX, in LD 20, use the following commands: • **REQ TNB** • **TYPE 2008**

The following values appear on the printout:

- ACQ AS = TN
- ASID = ELAN connected to Contact Center Manager Server

--End--

Verifying that the system default Treatment DN is configured correctly

Verify that the system default Treatment DN is configured correctly.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration.
2	Click **Configuration**.
3	Verify that the default treatment DN specified in the Global Settings window is configured correctly.

--End--

Verifying that treatment DNs are defined in the CallPilot SDN table

Verify that treatment DNs are defined in the CallPilot SDN table.

Procedure steps

Step	Action
1	In CallPilot, in the **Configuration Manager**, select **System, Service Directory Number**.
2	Verify that the table contains an entry for each treatment DN, in which the Application Name is the name of the application created in Application Builder.

--End--

Verifying that IVR ACD-DNs match on the PABX, Contact Center Manager Administration, and the voice-processing system

Verify that the IVR ACD-DNs match on the PABX, Contact Center Manager Administration, and the voice-processing system. The ACD-DNs must match in the following locations:

- Channel Information page in CallPilot Manager
- PABX DN
- Contact Center Manager Administration script
- IVR ACD-DNs window in Contact Center Manager Administration

Prerequisites

- In CallPilot, ensure that you have configured the ACCESS IVR ACD-DN in the Service DN table in CallPilot Manager.

Procedure steps

Step	Action
1	In CallPilot Manager, select **System, Service Directory Number** and check the value specified in the **Service DN** field.
2	On the PABX, in LD 20, enter the following command: **REQ DNB**.
3	On Contact Center Manager Administration, verify that the Give Controlled Broadcast script command specifies the DN defined in the CallPilot SDN table: **Give Controlled Broadcast 4604**.
4	Navigate to **Contact Center Manager Administration Launchpad, Configuration, IVR ACD-DNs**, and verify the following: • The IVR ACD-DN number matches the ACD-DN defined on the PABX and in the CallPilot SDN table. • The status for the IVR ACD-DN is **Acquired**.

--End--

Verifying that voice port TNs match on the PABX, Contact Center Manager Administration, and the voice-processing system

Verify that the voice port TNs match on the PABX, Contact Center Manager Administration, and the voice-processing system. The configuration of the TNs belonging to the ACD-DNs must match in the following locations:

- Channel Information page in CallPilot Manager
- PABX DN

- IVR ACD-DNs acquired by Contact Center Manager Administration

Procedure steps

Step	Action
1	In CallPilot Manager, select **Configuration Wizard**, and then click.
2	Select **CallPilot Individual Feature Configuration (Express Mode)**, and then click **Next**.
3	Choose **Switch Configuration**, and then click **Next**.
4	Note the value in the **TN** column.
5	On the PABX, in LD 20, enter the following command: **REQ DNB**.
6	Navigate to **Contact Center Manager Administration, Phonesets and Voice Ports**, and verify the following: • The **Channel** column for the voice port contains a unique number. • The status for the IVR ACD-DN is **Acquired Login**.

--End--

Verifying that channels for ACCESS voice ports match on the server and the voice-processing system

Verify that the channels for the ACCESS voice ports match on the server and the voice-processing system. The channel number for a specific TN must match the channel number for the same TN in the Voice Ports window on Contact Center Manager Administration. The channel number is the number shown in the Class ID column in the CallPilot Channel Monitor.

Procedure steps

Step	Action
1	In CallPilot Manager, select **Configuration Wizard**.
2	Select **CallPilot Individual Feature Configuration (Express Mode)**, and then click **Next**.
3	Choose **Switch Configuration**, and then click **Next**.
4	Note the value in the **Class ID** column.
5	Navigate to **Contact Center Manager Administration, Phonesets and Voice Ports**, and verify the following: • Each TN has a unique number in the Channel column. • The status for the voice port is **Acquired Login**.

--End--

Alarms, logs, traps and system messages

This section describes various alarms, logs, traps and system messages in Avaya Aura™ Contact Center and how they can be used to assist with troubleshooting system problems.

Prerequisites for alarms, logs, traps and system messages

- Read *Avaya Aura™ Contact Center Server Administration* (NN44400-610).

Navigation

- Using the Log Archiver utility (page 185)
- Troubleshooting call routing problems (page 188)

Using the Log Archiver utility

Use the Log Archiver (LA) utility to ensure that all active log files are archived on the Contact Center server. Use the LA utility to view both current and archived logs to diagnose problems on the server.

The log files for Contact Center Manager Server, Contact Center Manager Administration, Contact Center Multimedia and the Communication Control Toolkit are preconfigured in the LA. You can also add any other log files from the server to the LA utility.

Prerequisites

- Ensure that there is enough space at the archive location to store the archive files.
- If you are using a network archive location, ensure that there is automatic logon privileges for the selected location.

Procedure steps

Step	Action
1	On the Contact Center Manager Server, select **Start**, **All Programs**, **Avaya**, **Contact Center**, **Common Components**, **CC Log Archiver**.
2	To add a log file to one of the tabs, in the Contact Center Log Archiver window, click **Add**. In this example, on the CCMS tab, the Add New Rule to CCMS dialog box opens.
3	Select the log file to add using the **Browse** buttons for the **Directory to watch** and **File or wildcard pattern** fields.
4	Select **A matching file is renamed** from the **Take action when a matching file is** list.

5 Select **Archive the file** from the **Action to take** list. These two settings apply to the majority of Contact Center log files.

Attention: If you select **A matching file is changed or created** from the **Take action when** list, you can generate an excessive amount of archive files.

6 Click **Add**.

7 Click the **Settings** tab.

8 In the **Archive Location** field, click **Browse** to select the location where archive files are stored.

9 In the **Archive Management** group, click the **Cleanup Settings** button.

10 To configure archive management, set disk space restriction and schedule file deletion. Avaya recommends you use the default settings, unless the archive files take up too much disk space.

11 Click **OK**.

12 Click **Mirror Settings**.

13 You can configure a DVD drive or an FTP server to mirror archive files.

14 To save changes on all tabs, click **Save All.**

--End--

Procedure job aid

Contact Center Log Archiver Settings tab description

Field name	Description
Archive Location	The location where archived files are saved. Confirm there is enough space to store archived log files at this location. The Log Archiver service must have automatic logon privileges if you use a network Archive Location. The default Archive Location is D:\Avaya\Logs\Archive.
Refresh	Refresh the displayed information. The Current Location shows available disk space and space required by the Log Archiver based on Cleanup Settings. The Saved Location shows the total number and size of archives at the Archive Location. If you change the Archive Location, the Current Location can be different from the Saved location.

Contact Center Log Archiver Settings tab description

Field name	Description
Cleanup Settings	Cleanup Settings provide three ways to purge archive files. Maximum Archive Size: Total disk space of archive files can not exceed the specified value. The default is 10GB. When the total disk space reaches the Maximum Archive Size, files are deleted as defined by the Reduce total size by value. The default is 2GB. Minimum Free Disk Space: Archive files will never reduce the free disk space below the specified value. The default is 10% of the total disk space. When the limit is reached, files are deleted as defined by the Total free space desired value. The default is 15%. If both Maximum Archive Size and Minimum Free Disk Space are enabled, the setting that provides the most free disk space is used. The Log Archiver only increases disk space by deleting archive files. It cannot increase disk space for other applications. Periodical: Run a scheduled cleanup task. The default settings schedule the cleanup late in the evening, to avoid peak server activity; repeat every day; and delete archives older than two weeks.
Mirror Settings	You can configure Mirror Settings to archive to an FTP server and a DVD drive. Select Automatic FTP Mirroring or Automatic Disc Mirroring to archive files to the specified location. Use the Manual Copy tab to make copies of archive files.
View Archive Location	Open the Archive Location in Windows Explorer.
Delete	Delete all archives older than the specified date.
Archive All Files Now	Create an archive of all active log files. Select Include previous logs to include backup log files as well as the active files.
Set Events	Open the Events window to enter Windows Event Log Message IDs. When one of these events is triggered, the Log Archiver runs Archive All Files Now. For example, it will create an archive of all active log files.
Disable Archiving	Disable all automatic archiving operations.

Troubleshooting call routing problems

Troubleshoot call routing problems if your server cannot route calls to or receive calls from other sites. You need to review several issues to determine why the server cannot route calls.

If you experience issues with networking calls, Avaya also provides a network trace utility (NtwkTraceMon) that customer support staff can use to help you troubleshoot your problem.

Procedure steps

Step	Action
1	Verify that the source server did not filter the server.
2	Verify that the dialable DN is configured correctly at the source server.

--End--

SIP Contact Center troubleshooting on an Avaya Communication Server 1000 platform

This section describes the troubleshooting procedures that you should perform when handling SIP issues in an Avaya Communication Server 1000 Avaya Aura™ Contact Center.

Prerequisites for Communication Control Toolkit troubleshooting

- Ensure SIP Contact Center software is installed correctly, see *Avaya Aura™ Contact Center Installation* (NN44400-311).
- Ensure SIP Contact Center software is configured correctly, see *Avaya Aura™ Contact Center SIP Commissioning* (NN44400-511).

Navigation

Troubleshooting when there is no response when dialing a Route Point

When a Route Point is dialed, the customer is placed on a conference call in the Media Application Server (MAS) and ringback is the first treatment. If a Route Point is dialed and there is no audible response or error code, check the Route Point has been acquired on the Contact Center Manager Administration server.

Prerequisites

- Ensure the Contact Center Manager Administration server is configured.

Procedure steps

Step	Action
1	Check the Route Point is acquired. For more information, see Configuring and acquiring a CDN (route point). For more information, see *Avaya Aura™ Contact Center Manager Administration – Client Administration* (NN44400-611)

--End--

Troubleshooting when an agent cannot login to Agent Desktop

When an agent cannot login to Agent Desktop, the agent is presented with an internal server error message. There can be many reasons for this error, however one resolution is to check the transport type for the SIP CTI Proxy Server is correct. Ensure the SIP settings in the server configuration utility are correct.

Procedure steps

Step	Action
1	Check the transport type for the SIP CTI Proxy setting in the Server Configuration utility is not set to TLS. For more information, see Configuring the Signalling Server for SIP CTI in the *Avaya Aura™ Contact Center SIP Commissioning* (NN44400-511) guide.

--End--

Troubleshooting when an agent cannot answer a call

When an agent can login to Agent Desktop, can login to the phone however the agent is unable to answer a call. The Avaya Communication Server 1000 is not responding to the Contact Center communication.

Procedure steps

Step	Action
1	Contact the Avaya Communication Server 1000 expert to identify where the problem is.

--End--

Troubleshooting when multiple agents receive an acquisition failure error connecting to Communication Control Toolkit after an HA switchover

Agents can receive an acquisition failure error connecting to Communication Control Toolkit after an HA switchover, when all the CSTA sessions for agent's DN are used. This happens to agents who did not receive voice calls during the switchover.

You must increase the number of sessions for DNs on Avaya Communication Server 1000. The default is 3 sessions for a DN.

Procedure steps

Step	Action
1	Contact the Avaya Communication Server 1000 expert to make a change to the number of sessions for a DN.

--End--

Troubleshooting when hold/unhold causes calls to be dropped after seventy seconds

If hold/unhold causes calls to be dropped after seventy seconds, there is a problem with the SIP terminal configuration.

Procedure steps

Step	Action
1	Check the agent's SIP terminal configuration in the Contact Center Manager Administration server.

--End--

Troubleshooting when ringback is played into an active call

If ringback or an announcement is played in an active call, there is a problem with the SIP terminal configuration

Procedure steps

Step	Action
1	Check the agent's SIP terminal configuration in Contact Center Manager Administration server.

--End--

Troubleshooting when call processing fails due to suspected Media Application Server failure

If there is an issue with call processing which has been narrowed down to Media Application failure, follow these sequence of steps.

Procedure steps

Step	Action
1	First ping the MAS to ensure it is on the network.
2	If it is on the network, log on to the MAS and ensure there are no alarms in the Alarms window in Element Manager.
3	If there are no alarms, ensure the MAS handled the INVITE correctly. Turn on logging and check the timestamp of the failed call in the sipmcDebug.txt file.
4	If there is no INVITE in the logs, there is a problem with the lower level components of the MAS (i.e. the SIP stack).

--End--

Troubleshooting when there is no ringback on a call and message 486 Busy Here is in the CCMS_SGM_SIPMessages.log

If there is no ringback on a call and message 486 Busy Here is in the CCMS_SGM_SIPMessages.log, the CCMS cannot establish communication with the MAS.

Procedure steps

Step	Action
1	Ensure the Firewall is turned off on the MAS. MAS cannot function correctly with a Firewall turned on.
2	Ensure Domain policies are correct as per defined by your system administrator.

--End--

Troubleshooting when there is no ringback on a call and message 404 Not Found is in the CCMS_SGM_SIPMessages.log

If there is no ringback on a call and message 404 Not Found is in the CCMS_SGM_SIPMessages.log, the CCMS cannot establish communication with the MAS. This indicates that the MAS services have not been installed correctly.

Procedure steps

Step	Action
1	Verify the Contact Center Services (Announcement, Conference, Dialog) exist in Packaged Applications in the Element Manager. If they do not exist the Contact Center Services installer was not run, or failed to run successfully.
2	Run the Contact Center Services installer.

--End--

Troubleshooting when here is no ringback on a call and message 480 Temporarily Unavailable is in the CCMS_SGM_SIPMessages.log

If there is no ringback on a call and message 480 Temporarily Unavailable is in the CCMS_SGM_SIPMessages.log, the Contact Center Manager Server cannot establish communication with the MAS. This is due to an one of the following licence issues with MAS:

- Not licensed
- Licensed incorrectly
- Licensed but the licence is not saved and confirmed.

Procedure steps

Step	Action
1	To verify this look for any alarms in the MAS Alarms window. If there are no issues there, use the MAS logs to pinpoint the problem.
2	Apply a licence to the MAS, save and Confirm the licence.

--End--

Contacting Technical Support

This section describes the information that you need to locate before contacting Avaya Technical Support. You should contact Technical Support only if you are unable to resolve the issue using the information and steps provided in this guide.

Navigation

- Gathering information for Technical Support (page 195)

Gathering information for Technical Support

Gather all relevant information and have it available before contacting Avaya Technical Support. For all errors, record the error messages, the system configuration, and actions taken before and after the error occurred. If the problem persists, contact your Avaya customer support representative.

Be prepared to answer the following questions:

- When did the problem begin?
- How often does the problem occurs?
- Is this a new install?
- Has the solutions database been searched? If so, were any related solutions found?
- Is there currently a workaround for this issue?
- Have you made any recent changes or upgrades to the system or network (for example, a modification to the configuration or code)? If so, when exactly were these changes made? Who made these changes (provide first and last name, if possible)?

Ensure that you can provide the following information to Avaya Technical Support:

- a copy of your configuration files
- a copy of the .000 file from the PCMICIA
- a detailed network topology diagram
- log files
- output of show tech command (available for MERS8600 and ESU18xx only)