Avaya Contact Center Select Business Continuity

Release 7.0.3
Issue 02.04
July 2018

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

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

Hosted Service

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

Licenses

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

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License type(s)

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

Heritage Nortel Software

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

Contents

Chapter 1: Introduction

This document describes Avaya Contact Center Select Business Continuity.

Purpose

This document contains high-level feature descriptions and provides details about the characteristics, capabilities, capacities and feature interactions for each feature.

Intended audience

This document is intended for people who want a high-level understanding of the product features and capabilities.

Related resources

The following are some additional Avaya Contact Center Select related resources.

Avaya Contact Center Select Documentation

The following table lists the documents related to Avaya Contact Center Select. Download the documents from the Avaya Support website at http://support.avaya.com.

Title	Use this document to:	Audience
Overview		
Avaya Contact Center Select Solution Description	This document provides a technical description of Avaya Contact Center Select. It describes the product features, specifications, licensing, and	Customers and sales, services, and support personnel

Table continues…

Title	Use this document to:	Audience
	interoperability with other supported products.	
Avaya Contact Center Select Documentation Catalog	This document describes available Avaya Contact Center Select documentation resources and indicates the type of information in each document.	Customers and sales, services, and support personnel
Contact Center Performance Management Data Dictionary	This document contains reference tables that describe the statistics and data in the historical and real-time reports generated in Contact Center.	System administrators and contact center supervisors
Implementing		
Deploying Avaya Contact Center Select DVD	This document contains information about Avaya Contact Center Select DVD installation, initial configuration, and verification. This document contains information about maintaining and troubleshooting the Avaya Contact Center Select server.	Implementation personnel
Deploying Avaya Contact Center Select Software Appliance	This document contains information about Avaya Contact Center Select Software Appliance (VMware) preparation, deployment, initial configuration, and verification. This document contains information about maintaining and troubleshooting the software appliance.	Implementation personnel
Deploying Avaya Contact Center Select Hardware Appliance	This document contains information about Avaya Contact Center Select Hardware Appliance (physical server) installation, initial configuration, and verification. This document contains information about maintaining and troubleshooting the hardware appliance.	Implementation personnel
Avaya Contact Center Select Business Continuity	This document contains information about deploying Avaya Contact Center Select Business Continuity.	Implementation personnel
Upgrading and patching Avaya Contact Center Select	This document contains information about upgrading and patching Avaya Contact Center Select.	Implementation personnel and system administrators
Administering		
Administering Avaya Contact Center Select	This document contains information and procedures to configure the users, skillsets, and contact center configuration data. This document contains information about	System administrators and contact center supervisors

Table continues…

Title	Use this document to:	Audience
	creating Avaya Contact Center Select real-time and historical reports.	
Avaya Contact Center Select Advanced Administration	This document contains information about managing the Avaya Contact Center Select server, licensing, and multimedia configuration.	System administrators
Using Contact Center Orchestration Designer	This document contains information and procedures to configure script and flow applications in Contact Center Orchestration Designer.	System administrators
Maintaining		
Contact Center Event Codes	This document contains a list of errors in the Contact Center suite and recommendations to resolve them. This document is a Microsoft Excel spreadsheet.	System administrators and support personnel
Using		
Using Agent Desktop for Avaya Contact Center Select	This document provides information and procedures for agents who use the Agent Desktop application to accept, manage, and close contacts of all media types in Contact Center.	Contact center agents and supervisors
Using the Contact Center Agent Browser application	This document provides information and procedures for agents who use the Agent Browser application to log on to Contact Center and perform basic tasks.	Contact center agents

Finding documents on the Avaya Support website

Procedure

1. Navigate to http://support.avaya.com/.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list displays the documents only from the selected category.
7. Click **Enter**.

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Chapter 2: Changes in this release

The following sections describe the new features and changes in this release.

Features

New features in the Release 7.0 base build

See the following sections for information about new features in the Release 7.0 base build:

Avaya Contact Center Select supports Microsoft Windows Server 2012 R2

Avaya Contact Center Select Release 7.0 is supported on the Microsoft Windows Server 2012 R2 operating system. Avaya Contact Center Select Release 7.0 is not supported on Microsoft Windows Server 2008 R2. Customers upgrading to Avaya Contact Center Select Release 7.0 must migrate to a new Microsoft Windows Server 2012 R2 server.

Contact Center Manager Administration support for Caché database

In Contact Center Release 7.0, Contact Center Manager Administration (CCMA) stores information in a Caché database. Contact Center Release 7.0 stores agent, user, statistical, scheduling, and reporting information in Caché databases. This simplifies Contact Center data management, migration, and maintenance. This also simplifies the resiliency configuration processes.

In Contact Center Release 7.0, Contact Center Manager Administration (CCMA) does not store information using Active Directory Lightweight Directory Services (AD-LDS) or Microsoft Access databases.

Other changes

Other changes in the Release 7.0 base build

See the following sections for information about changes that are not feature-related in the Release 7.0 base build:

- Avaya Media Server changes on page 14
- Windows Server 2008 is no longer supported on page 15

Other changes in Release 7.0 Feature Pack 3

See the following sections for information about changes that are not feature-related in Release 7.0 Feature Pack 3:

- Avaya Aura Media Server update on page 14

Avaya Aura® Media Server update

Contact Center Release 7.0 Feature Pack 3 supports Avaya Aura® Media Server Release 7.8.

From Contact Center Release 7.0 Feature Pack 3, installing the Windows version of Avaya Aura® Media Server co-resident with a Voice and Multimedia Contact Server is no longer supported. When you deploy a Voice and Multimedia Contact Server with Avaya Aura® Media Server, Contact Center installs the Linux version of Avaya Aura® Media Server on a Hyper-V instance on your Voice and Multimedia Contact Server.

This process is fully automated by the Contact Center software installer for fresh installs, and by the Contact Center Release Pack Installer (RPI) for upgrades. In both cases, you can use the Update Configurator utility to update Avaya Aura® Media Server to the latest supported version and apply all necessary configuration. After a reboot following an install or upgrade, the Update Configurator utility launches.

Avaya Media Server changes

Avaya Media Server is now called Avaya Aura® Media Server. Avaya Contact Center Select Release 7.0 supports only Avaya Aura® Media Server Release 7.7.

Avaya Contact Center Select Release 7.0 no longer requires or uses the Contact Center Services For Avaya Media Server (CCSA) component. Avaya Contact Center Select Release 7.0 integrates directly with Avaya Aura® Media Server Release 7.7 using Media Server Markup Language (MSML) based communication.

Avaya Contact Center Select and Avaya Aura® Media Server use the MSML language to control how Route Point calls are anchored and treated. Avaya Contact Center Select also uses MSML to control Route Point call features such as Barge-in, Observe, Zip Tone, and Whisper Skillset announcements.

In Contact Center Manager Administration (CCMA) *Media Services and Routes* configuration, Avaya Aura® Media Server Release 7.7 instances now provide a new MSML-based service type named ACC_APP_ID. This new ACC_APP_ID service type replaces the CONF service type provided by Avaya Media Server Release 7.6.

The following features, previously configured in Avaya Media Server Element Manager, are now configured in Contact Center Manager Administration (CCMA).

- Barge-in tone
- Observation tone
- Call Force Answer Zip tone
- Custom Zip tones
- Whisper Skillset announcement

Enable or disable Barge-in and Observation tones in CCMA *Global Settings*.

Upload the tone and announcement .WAV files in CCMA *Prompt Management*.

Configure Call Force Answer Zip Tone and Whisper Skillset in CCMA *Call Presentation Classes*.

Avaya Aura® Media Server supports only the following deployment options:

- Co-resident with Avaya Contact Center Select on a Windows Server 2012 R2 server
- Standalone on a Red Hat Enterprise Linux 6.x 64–bit server

Avaya Aura® Media Server is also available as an Open Virtual Appliance (OVA) package. You can use this OVA file to create an Avaya Aura® Media Server virtual appliance on a VMware host.

Windows Server 2008 is no longer supported

Avaya Contact Center Select Release 7.0 is supported only on Microsoft Windows Server 2012 R2. Avaya Contact Center Select Release 7.0 is not supported on Microsoft Windows Server 2008 R2. Customers upgrading to Avaya Contact Center Select Release 7.0, must migrate to a new Microsoft Windows Server 2012 R2 server.

Chapter 3: Overview

Avaya Contact Center Select (ACCS) supports contact center Business Continuity when using an IP Office Server Edition system.

IP Office Server Edition (SE) solutions support voice platform resilience when an IP Office Secondary Server is added to the solution.

Avaya Contact Center Select Release 7.0 and IP Office Server Edition support the following deployment options.

Number of Avaya Contact Center Select servers	Number of IP Office Server Edition servers	Business Continuity
1	1 (One Primary Server)	A single ACCS server connected to a single IP Office SE voice platform. This deployment does not provide ACCS Business Continuity or IP Office resiliency.
1	2 (One Primary Server and one Secondary Server)	A single ACCS server connected to a resilient IP Office SE voice platform. This deployment provides resiliency only for the IP Office voice platform. ACCS does not provide application or server resiliency in this deployment.
2	1 (One Primary Server)	A pair of Business Continuity-enabled ACCS servers connected to single IP Office SE voice platform. This deployment provides application and server resiliency only for the ACCS servers. The IP Office voice platform is not resilient in this deployment.
2	2 (One Primary Server and one Secondary Server)	A pair of Business Continuity-enabled ACCS servers connected to a resilient IP Office SE voice platform. This deployment provides Business Continuity resiliency for ACCS and system resiliency for the IP Office voice platform.

Avaya Contact Center Select supports the following types of Business Continuity:

- **Campus Business Continuity**. In a campus Business Continuity environment the active and standby ACCS servers are in the same location and network subnet. The active and standby servers have different static IP addresses, but share a common virtual Managed IP address. The active server attaches the Managed IP address to its network interface. The active server processes customer contacts. All contact center applications and clients connect to the active server using the Managed IP address. If the active server fails, the standby server starts up

and becomes the active server. The standby server assumes this same Managed IP address and *automatically* takes over call processing. In a campus environment, a switchover from the active to the standby server using the Managed IP address appears as a server restart to client applications such as Agent Desktop.

- **Geographic Business Continuity**. In a geographic Business Continuity environment the active and standby ACCS servers are in different network subnets and/or campus locations. The active server processes customer contacts. In a geographic solution, the standby server is called a Remote Geographic Node. All contact center clients connect to the active server. If the active server fails, you must *manually* start the Remote Geographic Node and redirect client applications such as Agent Desktop to use the Remote Geographic Node server. Geographic Business Continuity solutions do not use a Managed IP address.

The following Avaya Contact Center Select deployment types offer support for Avaya Contact Center Select Business Continuity:

- **Avaya Contact Center Select DVD**; The Avaya Contact Center Select DVD contains the application software. The Avaya Contact Center Select DVD deployment option supports Platform Vendor Independence (PVI). The customer supplies the Microsoft Windows 2012 R2 operating system license and server hardware that meets one of the Avaya Contact Center Select PVI server specifications.
- **Avaya Contact Center Select software appliance**; The Avaya Contact Center Select software appliance is a set of VMware virtual machines; an Avaya Contact Center Select virtual machine, an Avaya Aura® Media Server Open Virtual Appliance (OVA), and a WebLM OVA. The customer supplies the VMware resources and operating system licenses for the VMware virtual machines. To support Business Continuity, your virtualized solution needs two Avaya Contact Center Select virtual machines, two Avaya Aura® Media Server virtual machines, and two WebLM virtual machines.
- **Avaya Contact Center Select hardware appliance**; The Avaya Contact Center Select hardware appliance is a physical server with the application software already loaded and partially preconfigured. Avaya supplies the server hardware and a license for the Microsoft Windows 2012 R2 operating system.

ACCS Business Continuity does not support ACCS and IP Office virtualized on the same VMware host server. To implement a virtualized ACCS Business Continuity solution:

- ACCS and IP Office must be virtualized on two separate VMware host servers.
- The active and standby ACCS must be virtualized on two separate VMware host servers.
- The active and Remote Geographic Node (RGN) ACCS must be virtualized on two separate VMware host servers.
- If using IP Office Resilience, the IP Office Primary Server and IP Office Secondary Server must be virtualized on two separate VMware host servers.

ACCS and IP Office are not supported on a single VMware host server.

Avaya Contact Center Select Business Continuity is supported only with an IP Office Server Edition voice platform.

Avaya Contact Center Select Business Continuity is not supported with an IP Office 500V2 voice platform.

Note:

Avaya Contact Center Select does not support changing the server name or IP address of Avaya Contact Center Select servers configured for Business Continuity. Configure the final production name and IP address of the Avaya Contact Center Select servers before configuring Business Continuity.

Campus Business Continuity

Avaya Contact Center Select (ACCS) supports an Active/Standby campus Business Continuity model. The ACCS active server processes customer contacts. The ACCS standby server automatically takes over if the active server fails or is shut down for maintenance. In a campus ACCS Business Continuity environment the standby and active servers must be in the same campus location, Windows domain, and LAN network subnet.

The standby server is constantly retrieving logical records of database updates from the active server so that the standby server always has a near real-time copy of the active database. This process is called database shadowing, the standby server is shadowing the active server's database. The standby server is configured with the most recent data and it can automatically take over from the active ACCS server if necessary.

When the standby ACCS starts up, it attempts to connect to the IP Office Primary Server. If the standby ACCS cannot connect to the IP Office Primary Server, it then attempts to connect to the IP Office Secondary Server.

Avaya Contact Center Select provides unified administration for contact center agents and IP Office users. The users (agents and supervisors) that you configure in ACCS are automatically mirrored to the connected IP Office. When the standby ACCS is active and connected to the IP Office Primary Server, the standby ACCS supports user data synchronization with the IP Office Primary Server.

To support Business Continuity resiliency, the Avaya Contact Center Select agents must each have an associated Windows domain user account in the same Windows domain as the active and standby servers. Avaya Contact Center Select agents are also supported in domains with a two-way trust relationship with the Avaya Contact Center Select servers' domain.

The following error conditions trigger an ACCS Campus Business Continuity automatic switchover:

- ACCS server hardware failure
- Prolonged network outage
- An ACCS database error
- Contact Center Manager Server (CCMS) or Communication Control Toolkit (CCT) critical service failure
- Avaya Aura® Media Server unavailable

The standby ACCS must match the active ACCS:

- If the active ACCS server is a Hardware Appliance, the standby ACCS server must also be a Hardware Appliance.
- If the active ACCS is a Software Appliance, the standby ACCS must also be a Software Appliance.
- If the active ACCS is a single-server DVD deployment, the standby ACCS must also be a single-server DVD deployment. The standby server must have the exact same hard disk partitions, the same amount of memory and the same CPU type. The standby server must have the Contact Center software installed on the same partitions as the active server.
- The active and standby servers must have the same ACCS patch level and the same operating system updates.

Avaya Contact Center Select supports the following campus deployment options.

- ACCS and non-resilient IP Office on page 19
- ACCS with IP Office resilience on page 20
- ACCS Business Continuity with non-resilient IP Office on page 20
- ACCS Business Continuity with IP Office resilience on page 21

ACCS and non-resilient IP Office

Avaya Contact Center Select continues to support non-Business Continuity solutions. In this solution, one ACCS connects to one IP Office server.

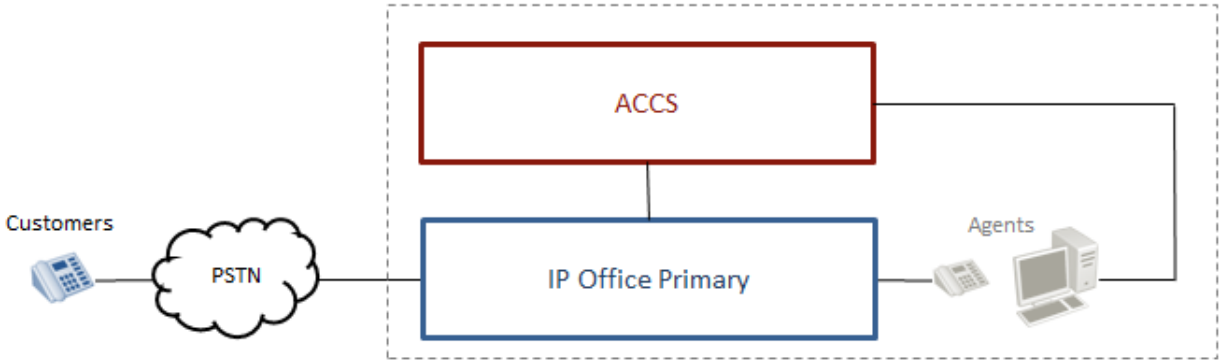


Figure 1: A diagram depicting a non-Business Continuity solution in which one Avaya Contact Center Select connects to one IP Office server

This campus solution type does not provide ACCS Business Continuity or IP Office resiliency, it is listed here for reference and comparison.

ACCS with IP Office resilience

In this solution, one Avaya Contact Center Select connects to an IP Office resilient system.

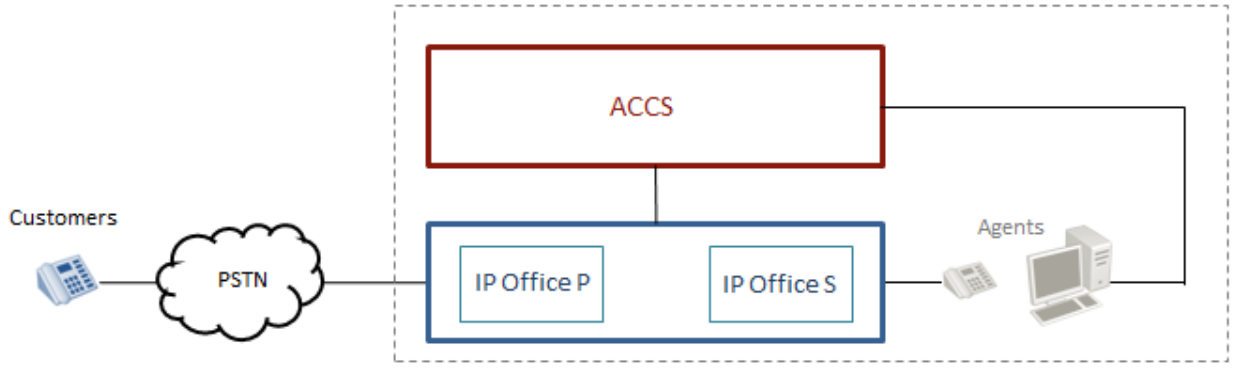


Figure 2: A diagram depicting one Avaya Contact Center Select connecting to an IP Office resilient system

This solution type provides resiliency only for the IP Office voice platform. ACCS does not provide application or server resiliency in this solution

- If the IP Office Primary Server fails, depending on your IP Office implementation, it can take a few minutes for the IP Office Secondary Server to start processing calls. If the IP Office Primary Server fails, ACCS connects to the IP Office Secondary Server.

ACCS Business Continuity with non-resilient IP Office

In this solution, two Business Continuity-enabled Avaya Contact Center Select servers connect to one IP Office server.

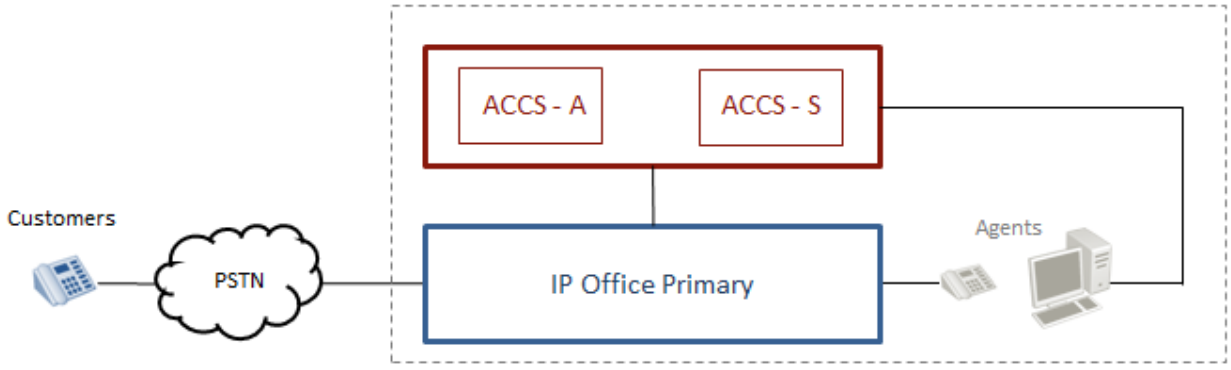


Figure 3: A diagram depicting two Business Continuity-enabled Avaya Contact Center Select server connecting to an IP Office server

This solution type provides Business Continuity resiliency only for ACCS. The IP Office voice platform is not resilient in this solution.

- If the ACCS active server fails, the ACCS standby server automatically takes over and connects to the IP Office voice platform. ACCS client applications such as Agent Desktop automatically reconnect to the standby server.

ACCS Business Continuity with IP Office resilience

In this solution, two Business Continuity-enabled ACCS servers connect to an IP Office resilient system.

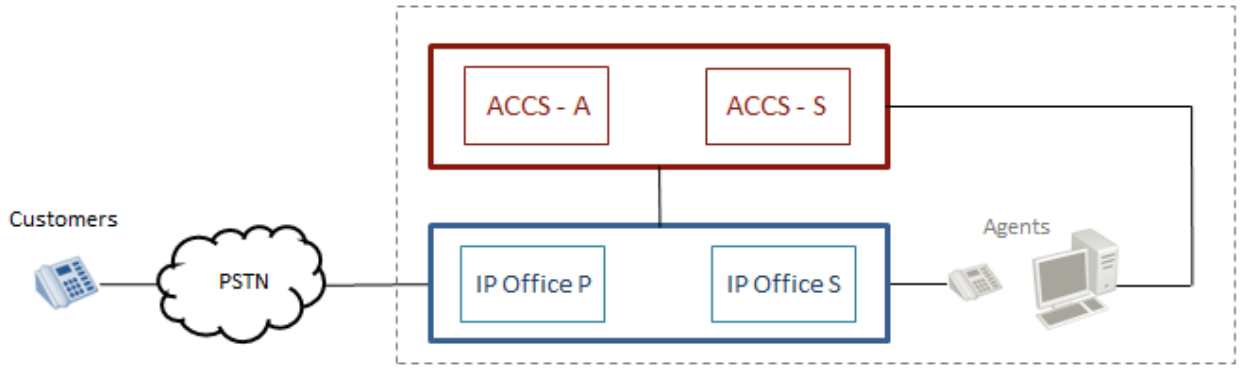


Figure 4: A diagram depicting two Business Continuity-enabled Avaya Contact Center Select connecting to an IP Office resilient system

This solution type provides Business Continuity resiliency for ACCS and system resiliency for the IP Office voice platform.

- If the ACCS active server fails, the ACCS standby server automatically takes over and attempts to connect to the IP Office Primary Server. If the standby ACCS cannot connect to the IP Office Primary Server, it then attempts to connect to the IP Office Secondary Server. ACCS client applications such as Agent Desktop automatically reconnect to the ACCS standby server.
- If the IP Office Primary Server fails, depending on your IP Office implementation, it can take a few minutes for the IP Office Secondary Server to start processing calls. If the IP Office Primary Server fails, ACCS connects to the IP Office Secondary Server.

Managed IP address

Contact Center supports the Active/Standby Business Continuity model. The active server processes contacts. The standby server takes over if the active server fails or is shut down for maintenance.

A Managed IP address is a virtual IP address that is attached to a Network Interface Controller (NIC) on the active server.

Each Avaya Contact Center Select server is assigned a static IP address. After the active server in each replication pair is determined, the active server attaches the Managed IP address to its network interface. The Managed IP address is assigned only to the active server. All other contact center applications and clients connect to that active application using the Managed IP address. The standby server assumes this same Managed IP address, if it takes over processing and becomes the active application. The active server stops hosting the Managed IP when it stops being the active server. When the standby server starts-up to take over call processing, it attaches the Managed IP address to its network interface.

The Managed IP address of the Business Continuity pair, the IP address of the active server, and the IP address of the standby server must all be in the same network subnet IP address range. For example, if the active server IP address is 172.1.1.X and the standby server IP address is 172.1.1.Y, then the Managed IP address for the Business Continuity pair must be 172.1.1.Z. The network subnet IP address range is controlled by the subnet mask.

Managed name

A Managed name can also be configured that maps to the Managed IP address. This Managed name can be configured on a Domain Name System (DNS) or in the hosts file on the servers that are connecting to the Business Continuity servers.

You use the Managed IP address or Managed name when configuring remote IP addresses or server names, do not use the physical name or IP address.

Campus switchover

In a campus environment, a switchover from the active to the standby server using the Managed IP address appears as a server restart to external applications.

You can invoke a switchover manually, or have the switchover triggered automatically when communication is lost or if a service fails. For a switchover to occur, the standby server must shadow the active server and switchover must be enabled on both servers.

The main advantages of Campus Business Continuity are:

- Automatic switchover
- Faster switchover time compared with Geographic Business Continuity
- Minimal switchover steps
- Third-party applications connect to the Managed IP address

Campus Business Continuity caters for Contact Center application or server failures and offers resiliency for local network failures.

Email switchover notification

You can enable automatic email switchover notifications, to alert the Contact Center administrator. When enabled, the specified email address receives an automatic email which provides switchover information to the recipient. This switchover information includes:

- Switchover description — the switchover is manual, is automatic due to a critical service failure, or automatic due to network communication failure.

- Depending on the type of switchover, additional information is provided in the email. In the case of automatic switchovers due to critical service or network failures, information such as event IDs and switchover times are included in the email.
- In the case of automatic switchovers due to service or network failures, the administrator receives two email messages. The first email informs the administrator that a switchover is imminent, and the second email arrives after successful completion of the switchover.

Campus network configuration

You can use Managed IP addresses for campus redundancy. With a Managed IP address, both the active and standby servers have the same IP address.

To eliminate network points of failure in the Contact Center solution, you must use Link Aggregation Control Protocol (LACP), NIC Teaming and Virtual Router Redundancy Protocol (VRRP).

Link Aggregation Control Protocol:

Link Aggregation Control Protocol (LACP) provides a method to control the bundling of several physical ports together to form a single logical channel. LACP allows a network device to negotiate an automatic bundling of links by sending LACP packets to the peer (directly connected device that also implements LACP).

NIC teaming:

NIC teaming is the process of grouping together several physical NICs into one single logical NIC, which can be used for network fault tolerance and transmit load balance. The process of grouping NICs is called teaming. By teaming more than one physical NIC to a logical NIC, resiliency is maximized. Even if one NIC fails, the network connection does not cease and continues to operate on other NICs.

Virtual Router Redundancy Protocol (VRRP):

Virtual Router Redundancy Protocol (VRRP) is a redundancy protocol designed to increase the availability of the default gateway servicing hosts on the same subnet. Two or more physical routers, such as Avaya ERS 5520, can be configured to stand for a virtual router. If one physical router fails, another physical router automatically replaces it.

Campus Business Continuity supports LAN environments where the round trip delay is less than 80ms, with less than 0.5% packet loss.

Switchover

In a Business Continuity campus solution, a monitored CCMS or CCT service failure, Avaya Aura® Media Server service failure, hardware, network, or database failure can initiate a switchover but only in the following situations:

- The active server is in a running state.

- The Contact Center services on the standby server are stopped.
- The active server is running. All the critical CCMS and CCT services are monitored and running.
- The active server has Switchover enabled.
- The shadowing latency is less than the latency threshold.
- A database restore is not running on the standby server.
- The active server database and standby server database are synchronized. The standby server database is shadowing the active server database.
- The standby server can communicate with (ping) the Trusted IP address.

If the Contact Center Administrator uses the Windows Service Control Manager (SCM) to stop a monitored service on an active server, a switchover occurs. If the Contact Center Administrator uses System Control and Monitor Utility (SCMU) to stop a monitored service on an active server, a switchover does not occur.

The Shadowing Latency threshold is used to validate how much time the standby server needs to catch up with the active server shadowed database contents. The default value of the Shadowing Latency threshold is 120 seconds. You can review the Shadow Latency information on the Business Continuity utility - System panel. The Shadow Latency must be greater than or equal to zero, but less than the latency threshold. The latency threshold is calculated as 120 seconds plus the Switchover timeout value as configured on the Server Mode panel of the Business Continuity utility.

To reinstate Business Continuity resiliency after a switchover, it is sometimes necessary to restore a database backup onto the new (post-switchover) standby server. The following table shows when a database restore is required to reinstate Business Continuity resiliency after a switchover:

Cause of switchover	Database restore required
Active server critical service outage	No
Manual switchover	No
Active server CLAN (contact center subnet) network outage	Yes
Complete network outage	Yes
Active server crash	Yes
Active server reboot	Yes

After a switchover, you can review the System Control panel of the Business Continuity utility on the (post-switchover) standby server to confirm if a database restore is necessary. In the Business Continuity utility — *System Control* panel, in the *Information* box, look for a notice about restoring the database(s).

Agent experience during a campus switchover

In a Campus Business Continuity solution, Agent Desktop clients are registered with the Managed IP address of the Business Continuity server pair.

In the event of a switchover, once the standby server has transitioned to the active mode and taken over the Managed IP, Agent Desktop clients automatically reconnect to the newly active server. Agents must log back in using Agent Desktop.

Customer calls in progress, answered customer calls, and customer calls that are queuing are lost during the switchover. During a switchover, all logged on agents are logged out. After a switchover, agents must log back in using Agent Desktop. An active personal call with an agent survives the switchover. Alerting personal calls on the agent are dropped during the switchover.

All active multimedia contacts remain in the active state on the answering Agent Desktop. Alerting multimedia contacts on Agent Desktop are removed from Agent Desktop and are reinserted to the Contact Center queue.

Administrator experience during a campus switchover

In a campus Business Continuity solution, the Contact Center Administrator launches Contact Center Manager Administration using the managed name of the server.

If the active Contact Center server fails, the Contact Center Manager Administration client Web browser continues to use the managed name and the Contact Center Administrator continues working by refreshing the Web browser.

Note:

When a switchover occurs, the Contact Center services stop on the active server. As a result, the historical data being collected on the disk for the 15 minute interval is not saved into the historical statistics tables. It is not possible to recover this data.

Geographic Business Continuity

Avaya Contact Center Select (ACCS) supports Geographic Business Continuity for data resiliency and disaster recovery.

In a Geographic Business Continuity solution, the two ACCS servers are in different network subnets. The two ACCS servers can be in different campus locations separated by a Wide Area Network (WAN). Both ACCS servers must be in the same Windows domain.

One of the ACCS servers, called the active server, processes customer contacts. The other ACCS server, called the Remote Geographic Node (RGN), shadows the active server. The RGN server shadows the active server, maintaining a near real-time local copy of the configuration and statistical databases. Therefore, the RGN server is configured with the most recent data and it can take over from the active server if necessary.

If the active ACCS fails, you must manually start up the RGN server and redirect ACCS agents, supervisors, and administrators to use the RGN. When the RGN server starts up, it attempts to connect to the IP Office Primary Server. If the RGN cannot connect to the IP Office Primary Server, it then attempts to connect to the IP Office Secondary Server. When the RGN is active and

controlling the IP Office system, ACCS agents using Agent Desktop client software must manually redirect Agent Desktop to use the Avaya Contact Center Select RGN.

To support Business Continuity resiliency, the Avaya Contact Center Select agents must each have an associated Windows domain user account in the same Windows domain as the active and RGN servers. Avaya Contact Center Select agents are also supported in domains with a two-way trust relationship with the Avaya Contact Center Select server domains.

The RGN ACCS must match the active ACCS:

- If the active ACCS server is a Hardware Appliance, the RGN ACCS server must also be a Hardware Appliance.
- If the active ACCS is a Software Appliance, the RGN ACCS must also be a Software Appliance.
- If the active ACCS is a single-server DVD deployment, the RGN ACCS must also be a single-server DVD deployment. The RGN server must have the exact same hard disk partitions, the same amount of memory and the same CPU type. The RGN server must have the Contact Center software installed on the same partitions as the active server.
- The active and RGN servers must have the same ACCS patch level and the same operating system updates.

ACCS supports the following Geographic Business Continuity solutions.

- ACCS Geographic Business Continuity with non-resilient IP Office on page 26
- ACCS Geographic Business Continuity with IP Office resilience on page 27
- ACCS Geographic Business Continuity with local IP Office resilience on page 28
- ACCS Geographic Business Continuity with remote IP Office resilience on page 29

ACCS Geographic Business Continuity with non-resilient IP Office

In this Geographic Business Continuity solution, the ACCS active server connects to an IP Office Primary Server and processes customer calls. The ACCS RGN is in a different network subnet and shadows the active server. The ACCS RGN is used for data resiliency and disaster recovery.

Figure 5: A diagram depicting an Avaya Contact Center Select Geographic Business Continuity solution in which the ACCS active server connects to an IP Office server

- If the ACCS active server fails, you must manually launch contact center services on the RGN server. The ACCS RGN then registers with IP Office and begins to process contacts. When the RGN is active and controlling the IP Office system, ACCS agents using Agent Desktop client software are redirected to use the Avaya Contact Center Select RGN.

ACCS Geographic Business Continuity with IP Office resilience

In this Geographic Business Continuity solution, the ACCS active server connects to an IP Office Primary Server and processes customer calls. The ACCS RGN is in a different network subnet and shadows the active server.

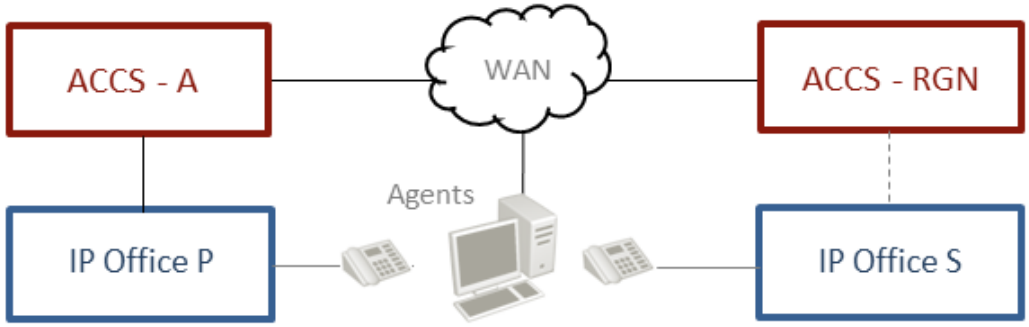


Figure 6: A diagram depicting an Avaya Contact Center Select Geographic Business Continuity solution in which the ACCS active server connects to an IP Office primary server in an IP Office resilient system

- If the ACCS active server fails, you must manually launch contact center services on the RGN server. The ACCS RGN then registers with IP Office and begins to process contacts. If the RGN cannot connect to the IP Office Primary Server, it then attempts to connect to the IP Office Secondary Server.
- If the ACCS active server fails, ACCS agents using Agent Desktop client software must manually redirect Agent Desktop to use the Avaya Contact Center Select RGN.

- If the IP Office Primary Server fails, depending on your IP Office implementation, it can take a few minutes for the IP Office Secondary Server to start processing calls. If the IP Office Primary Server fails, ACCS connects to the IP Office Secondary Server.
- If the ACCS active site fails, you must manually launch contact center services on the RGN server. The ACCS RGN then registers with IP Office and begins to process contacts.

ACCS Geographic Business Continuity with local IP Office resilience

In this solution, the ACCS active server connects to an IP Office Primary Server and processes customer calls. The two ACCS servers are in different network subnets. The ACCS RGN shadows the active server.

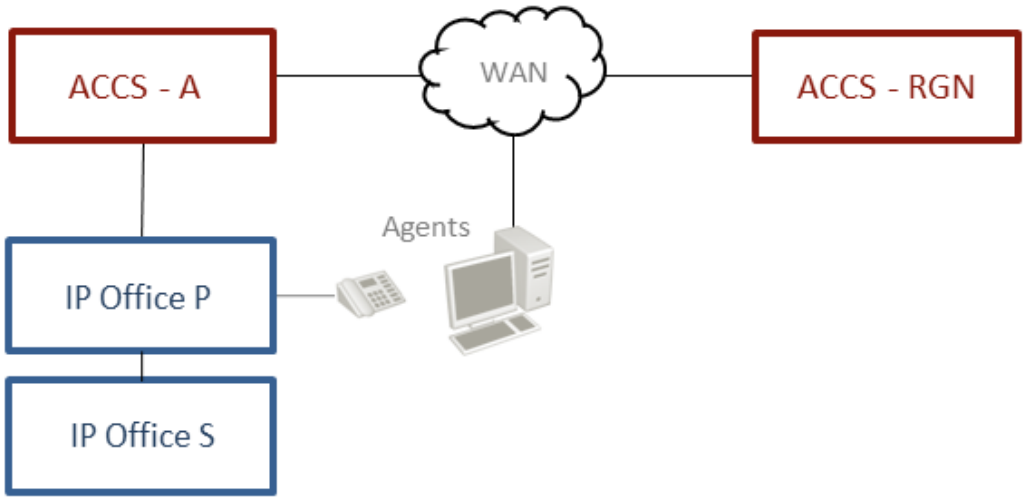


Figure 7: A diagram depicting an Avaya Contact Center Select Geographic Business Continuity solution in which the ACCS active server connects to an IP Office primary server in a local IP Office resilient system

- If the ACCS active server fails, you must manually launch contact center services on the RGN server. The ACCS RGN then registers with IP Office and begins to process contacts. If the RGN cannot connect to the IP Office Primary Server, it then attempts to connect to the IP Office Secondary Server.
- If the ACCS active server fails, ACCS agents using Agent Desktop client software must manually redirect Agent Desktop to use the Avaya Contact Center Select RGN.
- If the IP Office Primary Server fails, depending on your IP Office implementation, it can take a few minutes for the IP Office Secondary Server to start processing calls. If the IP Office Primary Server fails, ACCS connects to the IP Office Secondary Server.

ACCS Geographic Business Continuity with remote IP Office resilience

In this solution, the ACCS active server connects to an IP Office Primary Server and processes customer calls. The two ACCS servers are in different network subnets. The ACCS RGN is used for data resiliency and disaster recovery. The IP Office Primary Server and Secondary Server are in different network subnets. The IP Office Secondary Server can be at a remote location with a properly engineered WAN network connection.

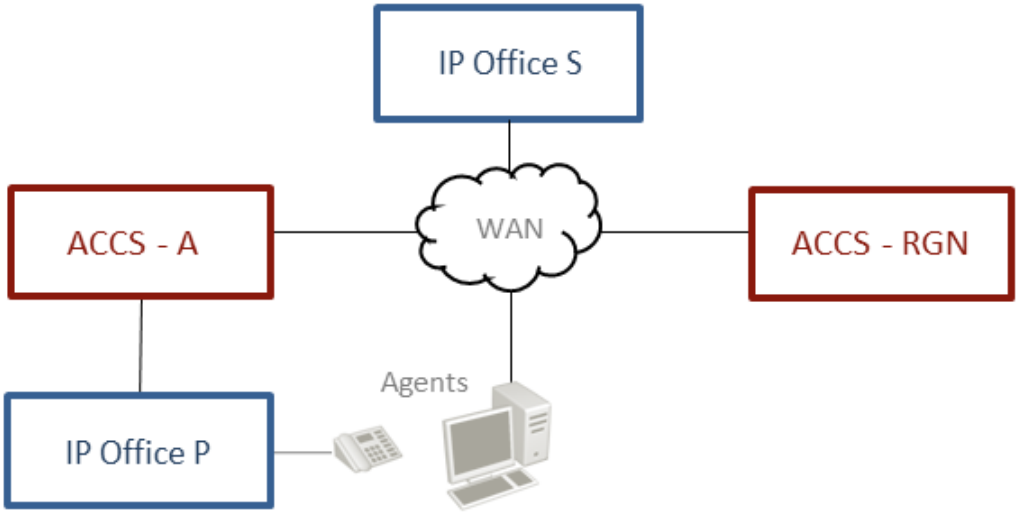


Figure 8: A diagram depicting an Avaya Contact Center Select Geographic Business Continuity solution in which the ACCS active server connects to an IP Office primary server in a remote IP Office resilient system

- If the ACCS active server fails, you must manually launch contact center services on the RGN server. The ACCS RGN then registers with IP Office and begins to process contacts. If the RGN cannot connect to the IP Office Primary Server, it then attempts to connect to the IP Office Secondary Server.
- If the ACCS active server fails, ACCS agents using Agent Desktop client software must manually redirect Agent Desktop to use the Avaya Contact Center Select RGN.
- If the IP Office Primary Server fails, depending on your IP Office implementation, it can take a few minutes for the IP Office Secondary Server to start processing calls. If the IP Office Primary Server fails, ACCS connects to the IP Office Secondary Server.

Geographic network configuration

In a Geographic Business Continuity environment where the servers need not be physically close, configure Business Continuity to perform a full site-by-site switchover.

To eliminate network points of failure in the contact center solution, you must use Link Aggregation Control Protocol (LACP), NIC Teaming and Virtual Router Redundancy Protocol (VRRP).

Link Aggregation Control Protocol:

Link Aggregation Control Protocol (LACP) provides a method to control the bundling of several physical ports together to form a single logical channel. LACP allows a network device to negotiate an automatic bundling of links by sending LACP packets to the peer (directly connected device that also implements LACP).

NIC teaming:

NIC teaming is the process of grouping together several physical NICs into one single logical NIC, which can be used for network fault tolerance and transmit load balance. The process of grouping NICs is called teaming. By teaming more than one physical NIC to a logical NIC, resiliency is maximized. Even if one NIC fails, the network connection does not cease and continues to operate on other NICs.

Virtual Router Redundancy Protocol (VRRP):

Virtual Router Redundancy Protocol (VRRP) is a redundancy protocol designed to increase the availability of the default gateway servicing hosts on the same subnet. Two or more physical routers, such as Avaya ERS 5520, can be configured to stand for a virtual router. If one physical router fails, another physical router automatically replaces it.

Geographic Business Continuity supports WAN environments where the round trip delay is less than 80ms, with less than 0.5% packet loss.

WAN specifications

Successful Avaya Contact Center Select Geographic Business Continuity implementation requires careful up-front Wide Area Network (WAN) planning and engineering.

Avaya recommends that the WAN is resilient.

IP Office voice platform resilience

An IP Office Server Edition solution offers voice platform resilience. To enable IP Office resilience, add an IP Office Secondary Server to the solution and then configure IP Office resilience. The IP Office solution can use the IP Office Secondary Server for redundancy or for shared resource resilience.

If the IP Office Primary Server fails or is stopped for maintenance, the IP Office Secondary Server automatically continues to process voice calls. It can take a few minutes for the H.323 phones, used by Avaya Contact Center Select agents, to reconnect with the IP Office Secondary Server. During this IP Office voice platform switchover, the Avaya Contact Center Select agent phones are unresponsive and calls in progress are lost.

The following diagram shows a typical IP Office resilient solution during normal operation. In this solution, Avaya Contact Center Select (ACCS) is not resilient.

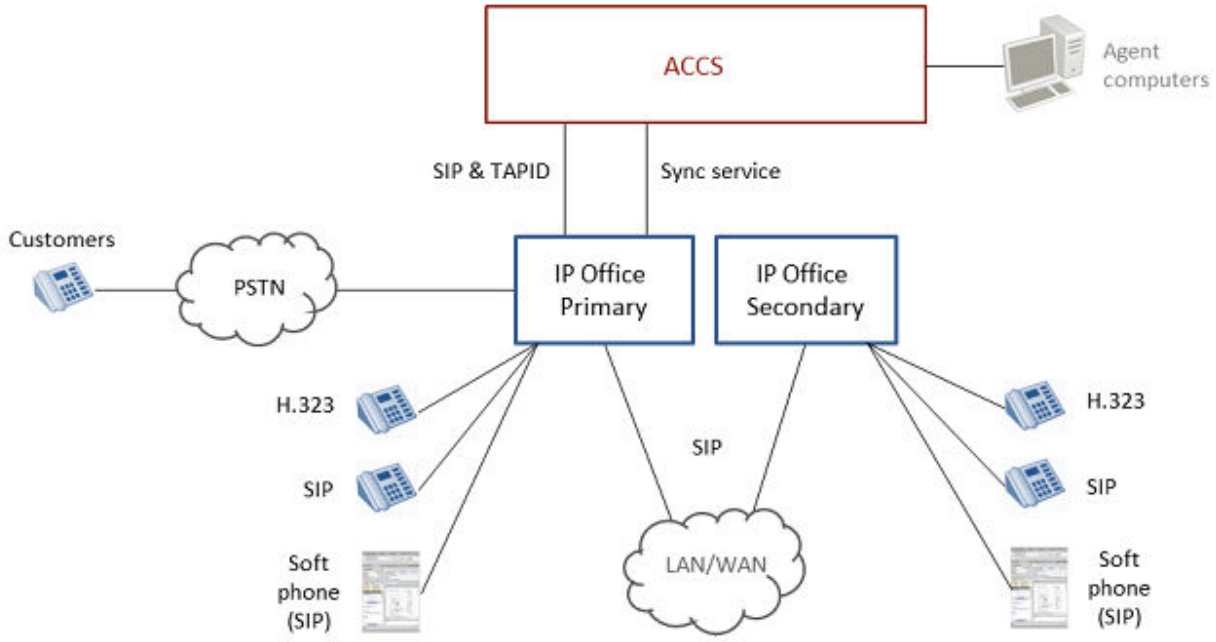


Figure 9: A diagram depicting an IP Office resilient solution during normal operation

The following diagram shows a typical IP Office resilient solution after an IP Office switchover to the IP Office Secondary Server. In this solution, ACCS is not resilient.

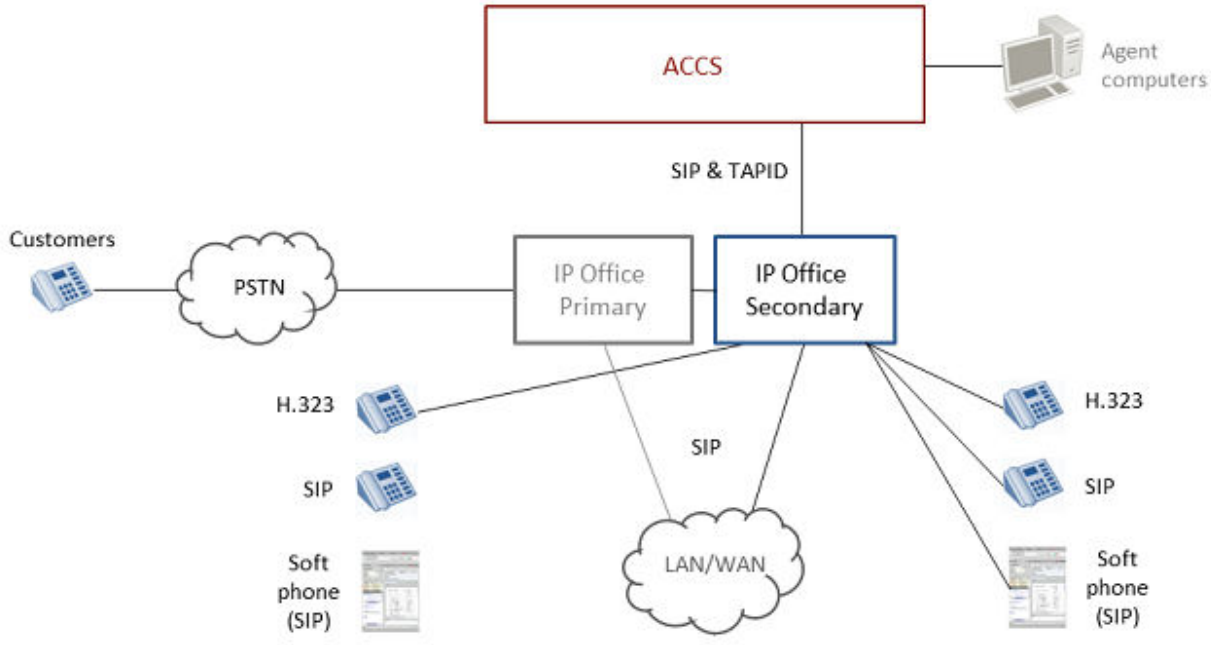


Figure 10: A diagram depicting an IP Office resilient solution after an IP Office switchover to the IP Office secondary server

The following diagram shows a typical IP Office resilient solution during normal operation. In this solution, ACCS implements Business Continuity for server and application resiliency.

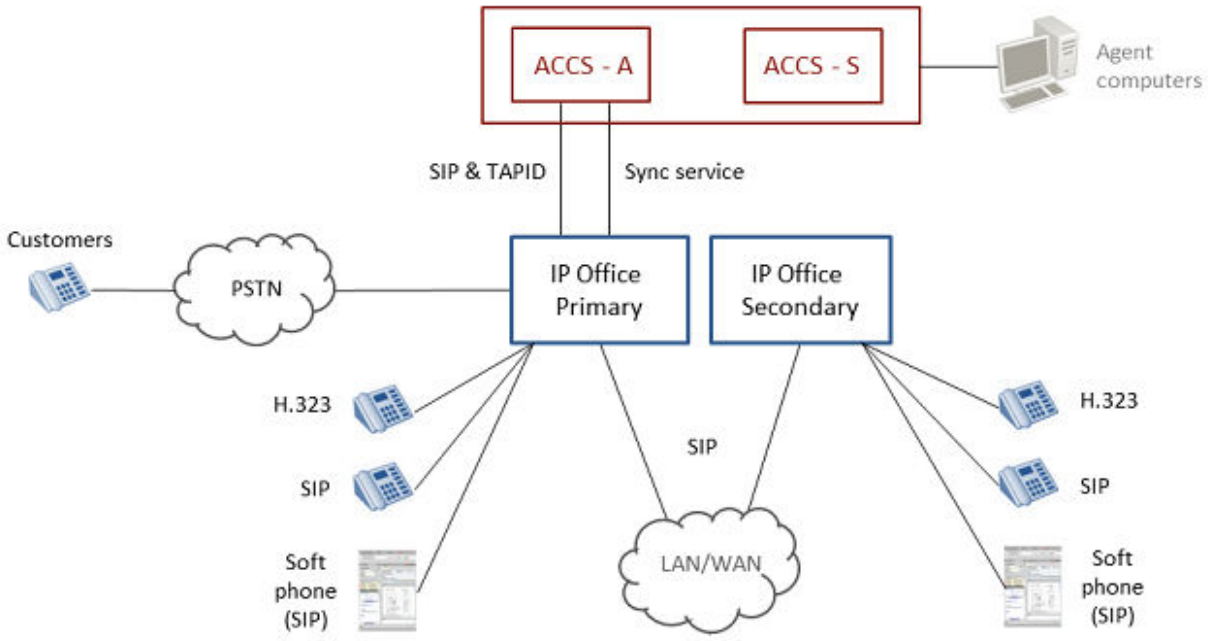


Figure 11: A diagram depicting an IP Office resilient solution during normal operation, with Business Continuity for server and application resiliency

The following diagram shows a typical IP Office resilient solution after an IP Office switchover to the IP Office Secondary Server. In this solution, ACCS implements Business Continuity for server and application resiliency.

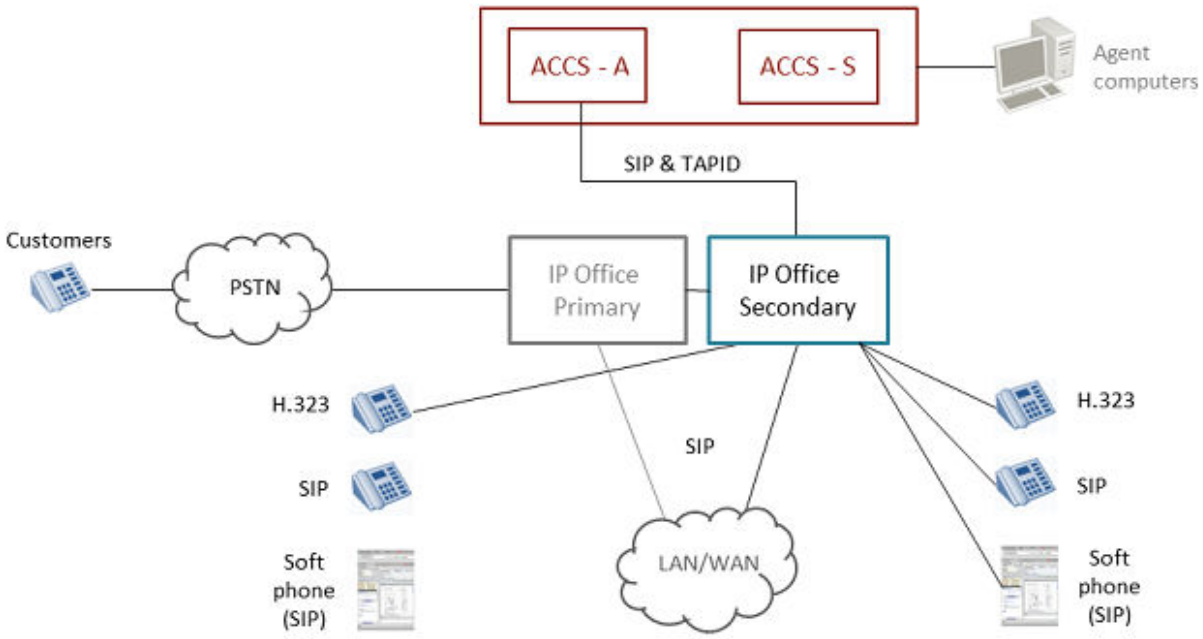


Figure 12: A diagram depicting an IP Office resilient solution after an IP Office switchover to the IP Office secondary server, with Business Continuity for server and application resiliency

The following IP Office components are resilient:

- IP Office Server Edition (fail-over to an IP Office Secondary Server)
- H.323, 16xx, 96xx, and 96x1 endpoints (configured as H.323 endpoints)
- Voicemail Pro Server (After a fail-over, call recording is performed on the IP Office Secondary Server)
- Hunt Groups
- Inter IP Office device links
- Trunks
- Incoming Call Routes

The following IP Office services are not resilient and are not supported following a fail-over:

- Presence/Mobility
- Avaya one-X® Portal
- Avaya Contact Center Select Data Synchronization Service
- Teleworkers

When the customer or agent hangs up the phone, the phone then attempts to connect to the IP Office Secondary Server. This re-connection process can take several minutes.

Phones that re-home from the IP Office Primary Server to the IP Office Secondary Server might not reconnect if the IP Office Secondary Server is restarted while the IP Office Primary Server is off-line.

IP Office call recorder is typically hosted on the IP Office Primary Server. In the event of a fail-over to the secondary IP Office call recording continues, but cannot be accessed until the IP Office Primary Server is brought back into service.

To recover full functionality after a fail-over to the IP Office Secondary Server, reinstate the IP Office Primary Server and then use the ACCS System Management and Monitoring Component (SMMC) system tray to register ACCS with the IP Office Primary Server. The ACCS agents must then redirect their phones to the IP Office Primary Server.

Avaya Contact Center Select automatically detects an IP Office Primary Server outage and transitions CTI connectivity to the IP Office Secondary Server. When this transition is complete, ACCS automatically begins accepting calls from the IP Office Secondary Server.

The IP Office server outage detection is based on a registration timeout failure on the SIP user link between Avaya Contact Center Select and IP Office. This registration timeout failure can take up to 220 seconds.

The ACCS Server Configuration utility has a user configurable delay which allows you to tune fail-over sensitivity to suit your business needs. For the duration of this timer, ACCS continues to attempt to reconnect to the IP Office Primary Server. The *Registration Switchover Delay* is in addition to the SIP registration timeout.

Once an IP Office outage has been detected and a fail-over is triggered, all active and queued ACCS calls are lost. New calls cannot be handled by ACCS until it has completed the transition to the Secondary IP Office Server. When the SIP registration has timed out with the Primary IP Office server, all active and queued calls are lost regardless of the decision to fail-over or not.

ACCS does not maintain active connections to the IP Office Secondary Server while connected to the IP Office Primary Server.

During the ACCS transition from the IP Office Primary Server to the IP Office Secondary Server the following conditions are observed:

- Agent’s physical phones become unresponsive.
- The ACCS Agent Desktop displays a “Link Outage” message box and displays a notice to the agent that they must use the physical set.
- ACCS clears and resets all call states. Existing calls are not preserved.
- For any ACCS calls in progress both agents and customers hear silence, and might hang up.
  - **Note**: The IP Office direct media feature is not supported for ACCS calls (calls from ACCS to the agent phone) because they are anchored on the IP Office server for call recording, and the speech path is bridged between the ACCS SIP connection and the agent’s H.323 phone.
- H.323 desk phones begin connecting to the IP Office Secondary Server. This re-connection can take several minutes.
- New customer calls do not reach the Secondary IP Office until after the PSTN re-routes customer calls to the Secondary IP Office server.

- Agents can continue handling ACCS multimedia contact types during an IP Office fail-over.
- The Secondary IP Office server begins to provide backup or default routing (IP Office Hunt Groups) for new customer calls when the PSTN has rerouted calls and when the Secondary IP Office has detected the Primary Server outage.
- Agent configuration changes made using the ACCS Administration client (CCMA) do not synchronize with IP Office Secondary Server. Changes made using CCMA are not propagated to IP Office until the IP Office Primary Server is brought back into service.

Once ACCS has connected to the IP Office Secondary Server and is in a position to receive calls:

- When the PSTN has switched to alternate routing and IP Office has detected the Primary Server outage, calls are routed to ACCS for treatment and routing
- Agents do not have to perform any action and their voice terminal goes in service automatically if their phone can connect to the IP Office Secondary Server.
- For agents whose phone set has not yet reconnected to the IP Office Secondary Server, their voice terminal remains out of service.

After an IP Office switchover to the IP Office Secondary Server, if the IP Office Secondary Server is rebooted for any reason during this failover period, phones registered to the IP Office Secondary Server do not reconnect back to the IP Office Secondary Server. ACCS agents using these phones remain out-of-service until the IP Office Primary Server system is restored.

Application and platform resiliency

IP Office resilience voice platform fail-over is supported by Avaya Contact Center Select Business Continuity.

With an Avaya Contact Center Select Business Continuity server pair, only one server is active at any time and only one ACCS has an active connection to one IP Office at any given time. Both the active and standby ACCS servers have the ability to detect IP Office Primary Server outages and fail-over to the IP Office Secondary Server.

- The active ACCS server can connect to an IP Office Primary Server and fail-over to an IP Office Secondary Server if the Primary Server fails.
- The standby ACCS server can connect to an IP Office Primary Server and fail-over to an IP Office Secondary Server if the Primary Server fails.

An Avaya Contact Center Select fail-over to the standby ACCS server causes its CTI adapter to initialize and start. On startup, the standby ACCS attempts to connect to the IP Office Primary Server first, if this fails it then attempts to connect to the IP Office Secondary Server.

IP Office Select

IP Office Server Edition offers a Select mode of operation. IP Office Select is a premium version of IP Office Server Edition, offering support for enhanced features. The Select mode is configured in the core IP Office and validated by licensing.

All systems within a Small Community Network (SCN) or Server Edition solution must be of the same type; either all Select or all non-Select.

Feature licenses for Select are available only in the Avaya Product Licensing and Delivery System (PLDS).

Avaya Contact Center Select Business Continuity is supported on IP Office Select and Standard modes.

Business Continuity server hardware requirements

In an ACCS Business Continuity solution, if the active ACCS server fails, the Remote Geographic Node (RGN) or standby ACCS server takes over call processing. The standby or RGN ACCS server must therefore be capable of processing the same number of agent calls as the active server.

In a Campus Business Continuity solution, the standby ACCS must match the active ACCS:

- If the active ACCS server is a Hardware Appliance, the standby ACCS server must also be a Hardware Appliance.
- If the active ACCS is a Software Appliance, the standby ACCS must also be a Software Appliance. The active and standby servers must be virtualized on separate VMware host servers. To support Business Continuity in a virtualized VMware environment, the solution must have two Avaya Contact Center Select virtual machines, two Avaya Aura® Media Server virtual machines, and two WebLM virtual machines. The virtualized Avaya Contact Center Select servers must have the same VMware version and guest (virtual machine) configuration settings.
- If the active ACCS is a single-server DVD deployment, the standby ACCS must also be a single-server DVD deployment. The standby server must have the exact same hard disk partitions, the same amount of memory and the same CPU type. The standby server must have the Contact Center software installed on the same partitions as the active server.
- The active and standby servers must have the same ACCS patch level and the same operating system updates.

In a Geographic Business Continuity solution, the RGN ACCS must match the active ACCS:

- If the active ACCS server is a Hardware Appliance, the RGN ACCS server must also be a Hardware Appliance.
- If the active ACCS is a Software Appliance, the RGN ACCS must also be a Software Appliance. The active and RGN servers must be hosted on separate VMware host servers. To support Business Continuity in a virtualized VMware environment, the solution must have two Avaya Contact Center Select virtual machines, two Avaya Aura® Media Server virtual machines, and two WebLM virtual machines. The virtualized Avaya Contact Center Select servers must have the same VMware version and guest (virtual machine) configuration settings.
- If the active ACCS is a single-server DVD deployment, the RGN ACCS must also be a single-server DVD deployment. The RGN server must have the exact same hard disk partitions, the same amount of memory and the same CPU type. The RGN server must have the Contact Center software installed on the same partitions as the active server.
- The active and RGN servers must have the same ACCS patch level and the same operating system updates.

In solutions using IP Office resilience and ACCS Business Continuity, both ACCS servers can have TLS certificates in place to communicate securely with IP Office.

Licensing

Business Continuity is a licensed feature. It is enabled when you purchase an Avaya Contact Center Select standby server license.

For campus Business Continuity, the license file is based on two MAC addresses, the MAC address of the active server and the MAC address of the standby server. The license file, containing the active and standby MAC addresses, is installed on both servers. If a switchover occurs, the standby server processes calls.

For virtualized campus Business Continuity solutions, the license file is based on two Host IDs, the Host ID of the active WebLM server and the Host ID of the standby WebLM server. The license file, containing the active and standby Host IDs, is installed on both WebLM servers.

For geographic Business Continuity, the license file is based on two MAC addresses, the MAC address of the active server and the MAC address of the Remote Geographic Node server. The license file, containing the active and Remote Geographic Node server MAC addresses, is installed on the active server and on the Remote Geographic Node server.

For virtualized geographic Business Continuity solutions, the license file is based on two Host IDs, the Host ID of the active WebLM server and the Host ID of the RGN WebLM server. The license file, containing the active and RGN Host IDs, is installed on both WebLM servers.

Database Shadowing

Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT), Contact Center Manager Administration (CCMA), and Contact Center Multimedia (CCMM) each store Contact Center information in a Caché database. This Caché database supports database shadowing for fault tolerant solutions such as Avaya Contact Center Select. To use Caché database shadowing, you must have two of each resilient application, an active application server and a corresponding standby application server.

The standby server is constantly retrieving logical records of database updates from the active server so that the standby server always has a near real-time copy of the active database. This process is called database shadowing, the standby server is shadowing the active server's database.

The standby application server shadows the active application server, maintaining a near real-time local copy of the CCMS, CCT, CCMA, CCMM, and administration databases. Therefore, the standby server is configured with the most recent data and it can take over from the active server if necessary.

Trusted IP address

The active and standby servers use the Trusted IP address to verify network connectivity. If the active server cannot communicate with the standby server it attempts to communicate with the Trusted IP address.

If the active server cannot connect to the Trusted IP address on startup then Contact Center services do not start on that server. If the active server cannot communicate with the Trusted IP address, and if shadowing and switchover are enabled, then the active server stops processing contacts and shuts down. The standby server starts processing contacts if it cannot communicate with the active server but can communicate with the Trusted IP address.

You must use the IP address of some part of your IT infrastructure that is always available to respond to a ping request, as the Trusted IP address.

Business Continuity configuration utilities

The Business Continuity feature has the following configuration utilities:

- Business Continuity utility
- SMMC system tray

Use the Business Continuity utility in conjunction with the SMMC system tray.

Business Continuity utility

Configure Business Continuity resiliency for CCMS, CCT and CCMM using the Business Continuity (BC) utility in the Database Utilities. The Business Continuity utility is used to configure which server is the active and which is the standby server. The BC utility also configures the Managed IP of the active server.

The Business Continuity utility on an active server has the following dialogs under the Configuration tab:

- Server Mode
  - Configure the IP address for the active and standby servers
  - Configure the IP address for Trusted servers
  - Configure the IP address for the optional Remote Geographic Node
  - Identify if the server is active or standby
  - Enable Switchover
  - Configure the switchover time-out. This is the wait time if a network outage occurs before an automatic switchover occurs.
- Notifications
  - Configure an email server for email notifications
  - Configure where and how often to send email notifications

  - Configure the email character set
- System
  - Display information on the system status
  - Verify that database shadowing is running

SMMC system tray

The Contact Center System Management and Monitoring Component (SMMC) system tray gives quick access to action items in your Business Continuity environment. The SMMC system tray has the following main menu options and action items:

- Start BC System
- Stop BC System
- Disable Switchover
- Enable Switchover
- System Information
- Database Information
- Disable Next Auto Startup
- Select Standby Auto Startup Mode (Standby server only)
- Re-enable BC system (this option is available only when the active BC server is running but switchovers are disabled)

To access the SMMC system tray menu, right-click the SMMC icon on the Windows taskbar. The SMMC system tray icon displays the status of the Business Continuity feature on the server.

In the SMMC system tray, the available menu options depend on the state of the BC System. For example, the Start BC menu option is available only when the Business Continuity system is in a stopped state. The state of the critical CCT and CCMS services affects the available SMMC system tray menu options. The state of the License Manager, Avaya Aura® Media Server, CCMA, and CCMM services does not affect the available SMMC system tray menu options.

The Contact Center System Management and Monitoring Component (SMMC) system tray icons display the status of the Business Continuity feature on a server, if switchover is enabled or disabled that server, and if the server can communicate with the SMMC component on the remote server.

The following table shows the Business Continuity system status and corresponding SMMC system tray icon.

Business Continuity status	SMMC icon
Non-BC server in stopped state. Business Continuity is not configured on this server.	
Non-BC server in starting state. Business Continuity is not configured on this server.	
Non-BC server in running state. Business Continuity is not configured on this server.	

Table continues…

Business Continuity status	SMMC icon
Non-BC server in stopping state. Business Continuity is not configured on this server.	
Active BC server in stopped state. This server is configured as an active server.	
Active BC server with no connection to remote system. This server is configured as an active server.	
Active BC server running with connection to remote system, fully BC capable system. A switchover is possible.	
Active BC server running, but switchovers disabled. A switchover is not possible.	
Switchover in progress, the active system is switching over to become a standby system. After the switchover, this server becomes a standby server.	
Standby BC server in stopped state. This server is configured as a standby server.	
Standby BC server with no connection to remote system. This server is configured as a standby server.	
Standby BC server running with connection to remote system, fully BC capable system. A switchover is possible.	
Standby BC server running, but switchovers disabled. A switchover is not possible.	
Switchover in progress, the standby system is switching over to become an active system. After the switchover, this server becomes an active server.	
The Remote Geographic Node server BC system is starting.	
The Remote Geographic Node server BC system is stopping.	
The Remote Geographic Node server BC system is stopped.	
The Remote Geographic Node server BC system is shadowing the active server, but the Remote Geographic Node server is not yet synchronized with the active server.	
The Remote Geographic Node server BC system is shadowing and synchronized with the active server.	
The active server from a Geographic BC system is running.	
The active server from a Geographic BC system is preparing to start.	
The active server from a Geographic BC system is starting.	
The active server from a Geographic BC system is not running.	
The active server from a Geographic BC system is stopping.	

Business Continuity utility and SMMC system tray

Use the Business Continuity utility to configure Business Continuity IP addresses and to configure which server is the active server and which is the standby server. Then use the System Management and Monitoring Component (SMMC) system tray to start database shadowing and Business Continuity functionality.

Chapter 4: Configuration process

This work flow shows the sequence of tasks you perform to configure Business Continuity.

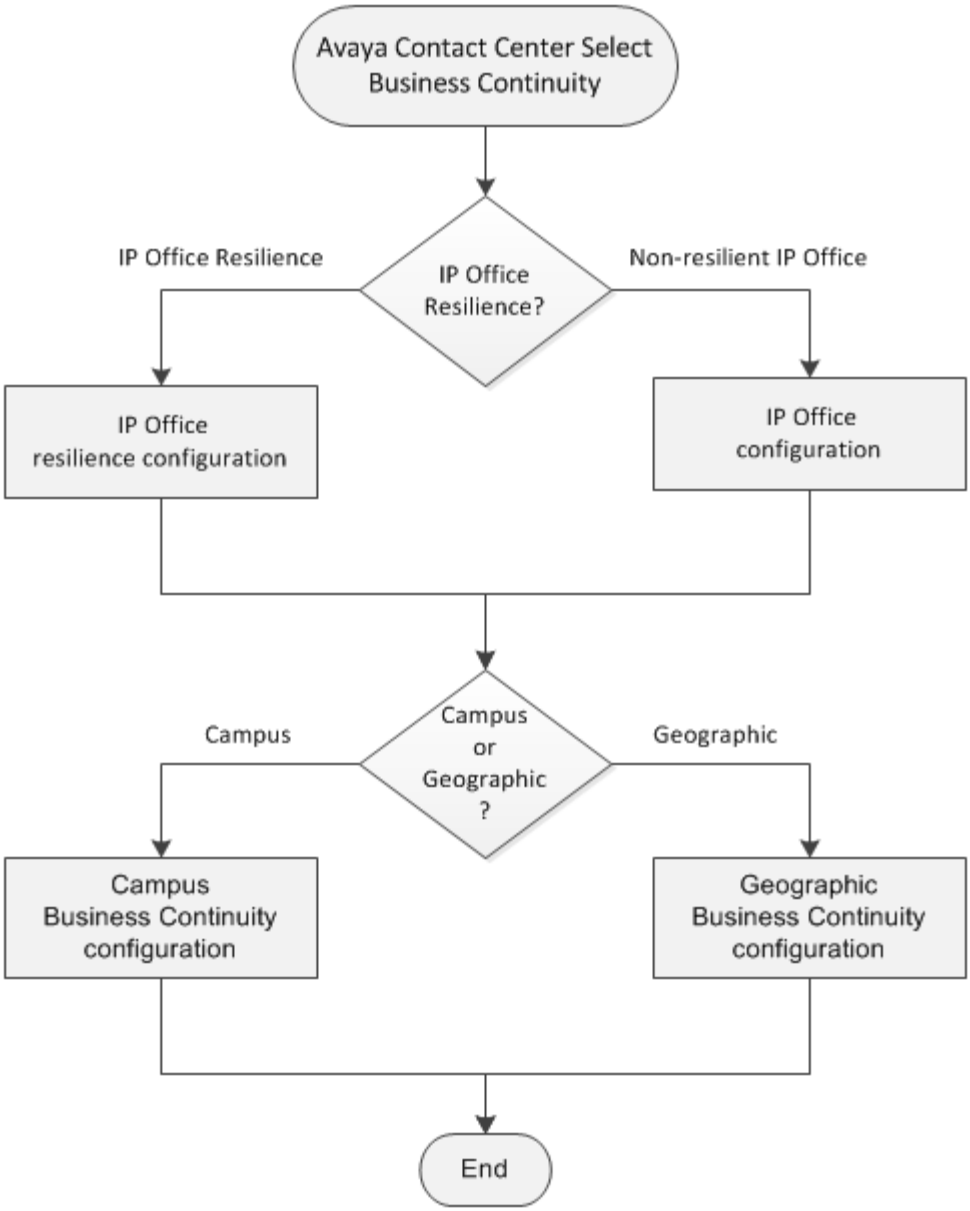


Figure 13: Business Continuity configuration process

Chapter 5: IP Office configuration

This section describes how to configure a non-resilient IP Office Server Edition Primary Server for the following Avaya Contact Center Select solution types:

- Avaya Contact Center Select with Campus Business Continuity
- Avaya Contact Center Select with Geographic Business Continuity

If the Avaya Contact Center Select active server fails or is stopped, the Avaya Contact Center Select standby server registers with the IP Office Server Edition Primary Server and processes customer voice contacts.

Avaya Contact Center Select Business Continuity is supported on a non-resilient IP Office Server Edition system.

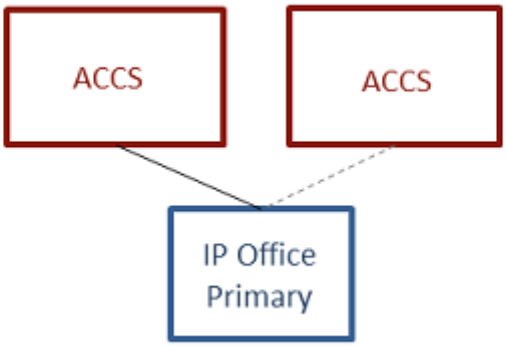


Figure 14: A diagram depicting Avaya Contact Center Select Business Continuity with a non-resilient IP Office Server Edition system

Avaya Contact Center Select Business Continuity is supported with IP Office Server Edition Select and Standard modes.

IP Office configuration prerequisites

- Ensure the IP Office Server Edition Primary Server is configured and licensed.

- Ensure the IP Office Primary Server is configured to support Avaya Contact Center Select. For more information about configuring IP Office to support Avaya Contact Center Select, see one of the following:
  - *Deploying Avaya Contact Center Select DVD*
  - *Deploying Avaya Contact Center Select Software Appliance*
  - *Deploying Avaya Contact Center Select Hardware Appliance*

Using IP Office Manager

Before you begin

- Install the IP Office Manager software on a client computer.
- Ensure the client computer can communicate with the IP Office server.

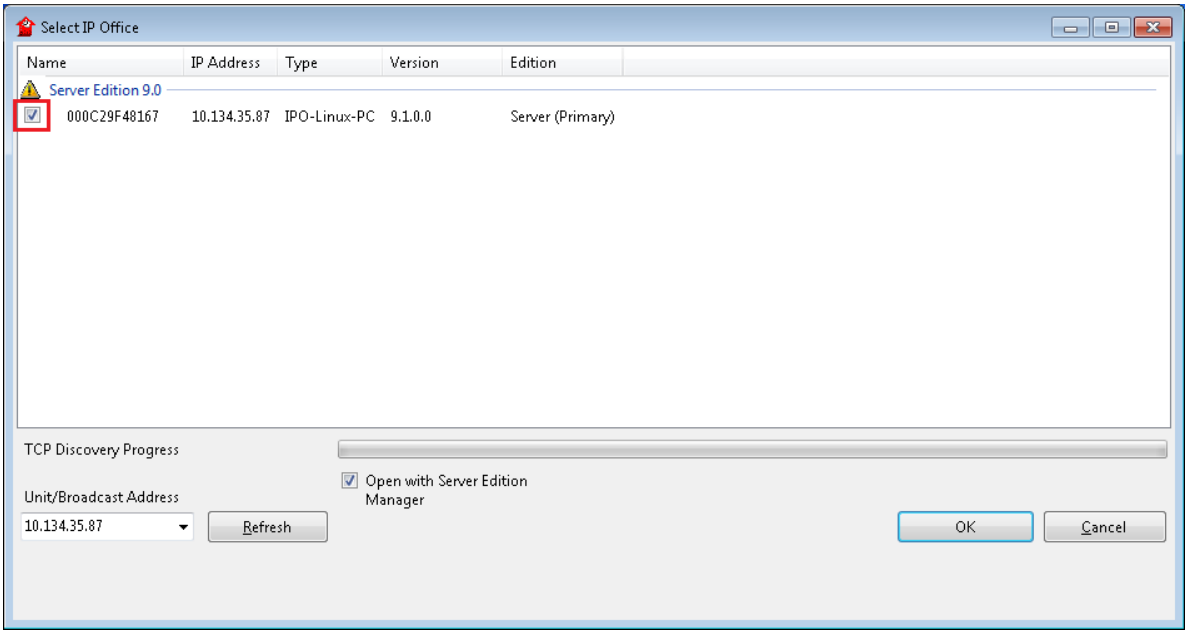
About this task

IP Office Manager is a component of the IP Office administration suite of applications. You use IP Office Manager to configure IP Office. IP Office Manager runs on a Windows computer and connects to the IP Office system using an Ethernet LAN connection.

IP Office Manager is an off-line editor. Use IP Office Manager to connect to your IP Office server and retrieve a local copy of the IP Office current configuration settings. You can then edit the local copy of the IP Office configuration and when you are ready, save your updated configuration data back to the IP Office server.

Procedure

1. On the client computer, select **Start** > **All Programs** > **IP Office** > **Manager**.
2. On the **Configuration Service User Login** message box, in the **Service User Name** box, type the user name. The default name is Administrator.
3. In the **Service User Password** box, type the user password. The default password is Administrator.
4. From the menu, select **File** > **Close Configuration**. This closes any open and potentially out-of-date configurations.
5. To retrieve the current (most recent) IP Office configuration settings, from the menu, select **File** > **Open Configuration**.
6. In the **Select IP Office** window:
   - If the required IP Office server is listed, use the check box to select your IP Office server from the list of available servers.
   - If the required IP Office server is not listed, in the **Unit/Broadcast Address** box type the IP address for your IP Office server. Click **Refresh** to perform a new search. The IP Office server then appears in the list of available servers. Use the check box to select your IP Office server from the list of available servers.



7. Click **OK**.
8. On the **Configuration Service User Login** message box, in the **Service User Name** box, type the user name. The default name is Administrator.
9. In the **Service User Password** box, type the user password. The default password is Administrator.
10. IP Office Manager opens and displays the current configuration data for your IP Office server.

Verifying IP Office licenses

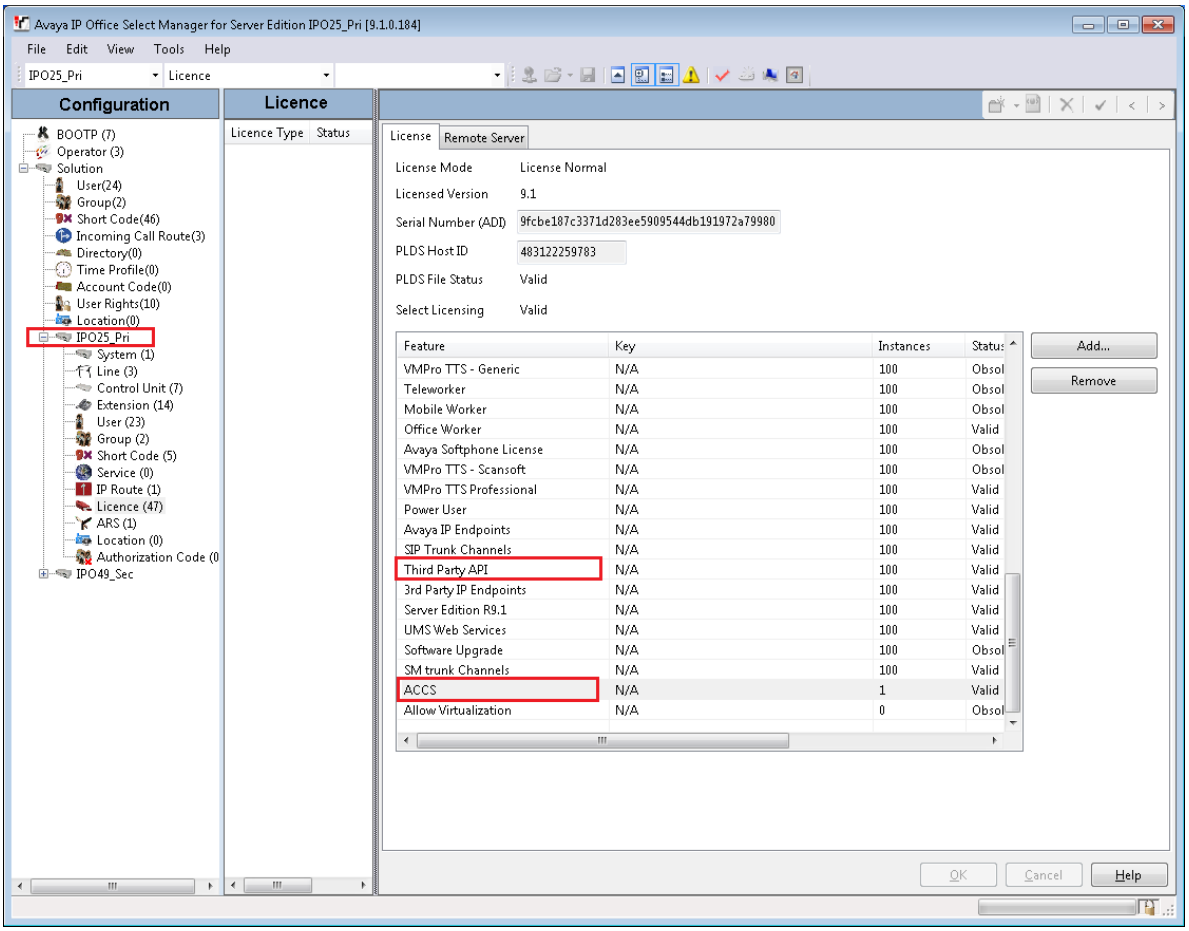
About this task

Verify the IP Office license on the Primary Server.

Procedure

1. Using IP Office Manager, select the IP Office Primary Server in the **Configuration** pane.
2. Click **License**.

3. Verify that the ACCS license is configured on the IP Office Primary Server.



4. Click **OK**.
5. If necessary, reboot the IP Office server.

Configuring the data synchronization user account

Before you begin

- If your solution implements Avaya Contact Center Select Business Continuity, perform this procedure. If your solution does not implement Avaya Contact Center Select Business Continuity, skip this procedure.

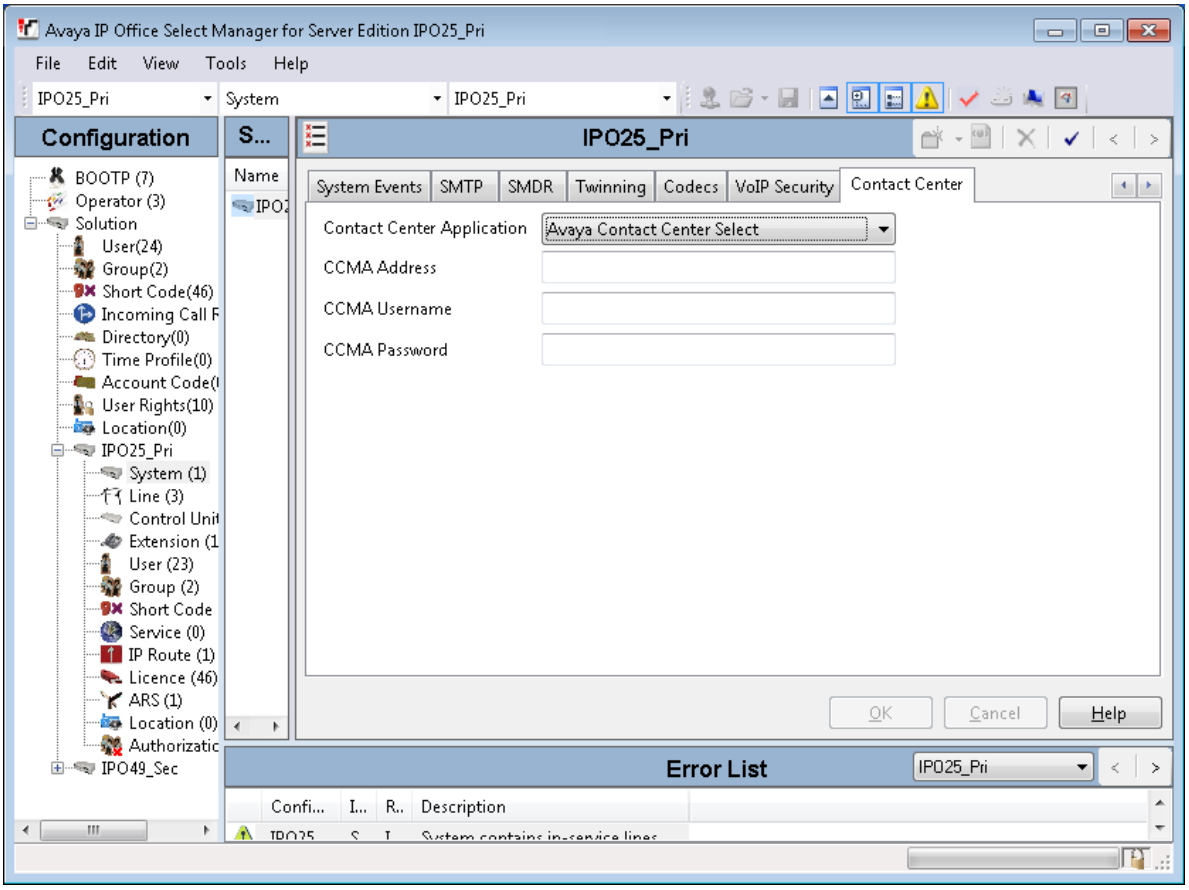
About this task

Configure the user account used by IP Office to maintain data synchronization with Avaya Contact Center Select. The name and password of this account must match the IP Office server details as configured in Contact Center Manager Administration (CCMA) on the Avaya Contact Center Select server.

For user data synchronization, IP Office connects to Avaya Contact Center Select using the Contact Center Manager Administration “accssync” user account details.

Procedure

1. Using IP Office Manager, select the IP Office Primary Server in the **Configuration** pane.
2. In the **Configuration** pane, under the IP Office server, select **System**.



3. Select the **Contact Center** tab.
4. From the **Contact Center Application** list, select **Avaya Contact Center Select**.
5. In the **CCMA Address** box, type one of the following IP addresses:
   - If your solution uses Avaya Contact Center Select Campus Business Continuity, type the Managed IP address of the Business Continuity pair.
   - If your solution uses Avaya Contact Center Select Geographic Business Continuity, type the IP address of the Avaya Contact Center Select active server.
6. In the **CCMA Username** box, type the name of the Avaya Contact Center Select data synchronization user account. The default user name is `accssync`.
7. In the **CCMA Password** box, type the password of the Avaya Contact Center Select data synchronization user account. The default user password is `accssync`.

8. Click **OK**.

Saving the IP Office configuration data

Before you begin

- Install the IP Office Manager software on a client computer that can communicate with the IP Office server.

About this task

Use IP Office Manager to save your configuration changes to the IP Office server.

Procedure

1. In IP Office Manager, in the **Configuration** pane, select your IP Office server.
2. From the main IP Office Manager menu, select **File** > **Save Configuration**.
3. On the **Send Multiple Configurations** window, use the check box to select your IP Office server from the list.
4. Click **OK**.

   IP Office Manager saves the offline configuration file to your IP Office server.

Chapter 6: IP Office resilience configuration

This section describes how to configure IP Office resilience for the following Avaya Contact Center Select solution types:

- Avaya Contact Center Select without Business Continuity
- Avaya Contact Center Select with Campus Business Continuity
- Avaya Contact Center Select with Geographic Business Continuity

An IP Office Server Edition solution offers resilience for IP Office. To enable IP Office resilience, add an IP Office Secondary Server to the solution and then configure IP Office resilience. The IP Office solution can use the IP Office Secondary Server for redundancy or for shared resource resilience. If the IP Office Primary Server fails or is stopped, the IP Office Secondary Server continues to process voice calls.

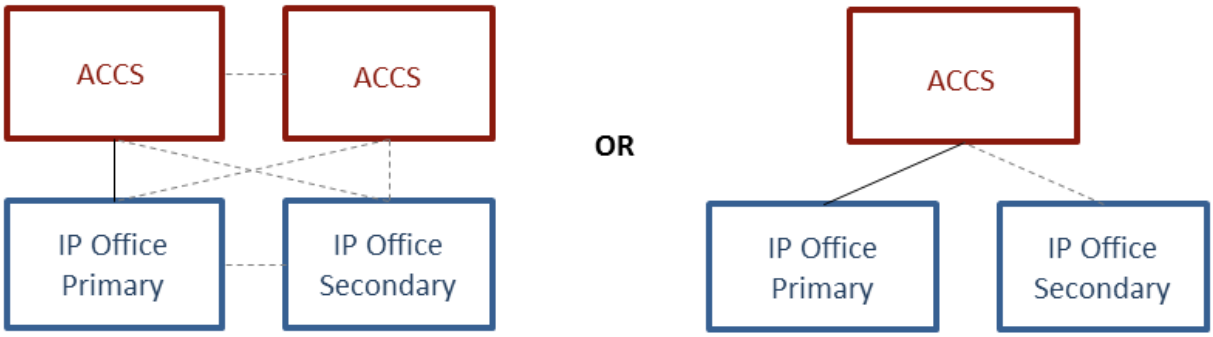


Figure 15: A diagram depicting examples of IP Office resilience in Avaya Contact Center Select solutions

Avaya Contact Center Select Business Continuity is supported only with IP Office Server Edition, Select and Standard modes.

IP Office resilience configuration prerequisites

- Ensure the IP Office Primary Server is configured and licensed.

- Ensure the IP Office Secondary Server is configured and licensed.
- Ensure the IP Office Primary Server is configured to support Avaya Contact Center Select. For more information about configuring IP Office to support Avaya Contact Center Select, see one of the following:
  - *Deploying Avaya Contact Center Select DVD*
  - *Deploying Avaya Contact Center Select Software Appliance*
  - *Deploying Avaya Contact Center Select Hardware Appliance*

Using IP Office Manager

Before you begin

- Install the IP Office Manager software on a client computer.
- Ensure the client computer can communicate with the IP Office server.

About this task

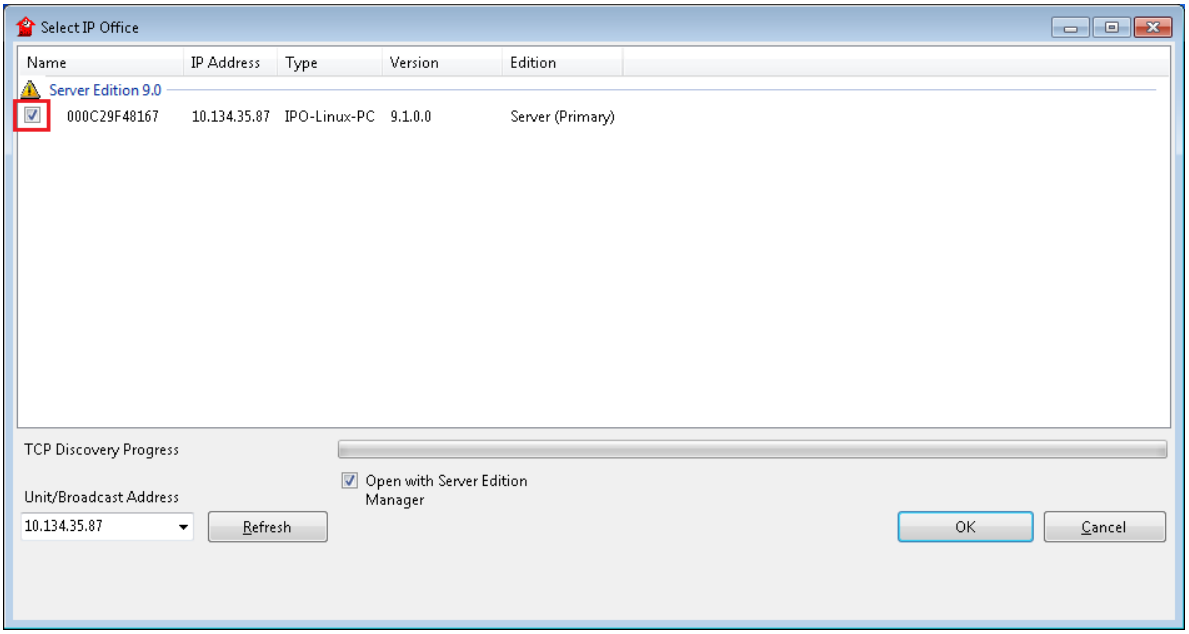
IP Office Manager is a component of the IP Office administration suite of applications. You use IP Office Manager to configure IP Office. IP Office Manager runs on a Windows computer and connects to the IP Office system using an Ethernet LAN connection.

IP Office Manager is an off-line editor. Use IP Office Manager to connect to your IP Office server and retrieve a local copy of the IP Office current configuration settings. You can then edit the local copy of the IP Office configuration and when you are ready, save your updated configuration data back to the IP Office server.

Procedure

1. On the client computer, select **Start** > **All Programs** > **IP Office** > **Manager**.
2. On the **Configuration Service User Login** message box, in the **Service User Name** box, type the user name. The default name is Administrator.
3. In the **Service User Password** box, type the user password. The default password is Administrator.
4. From the menu, select **File** > **Close Configuration**. This closes any open and potentially out-of-date configurations.
5. To retrieve the current (most recent) IP Office configuration settings, from the menu, select **File** > **Open Configuration**.
6. In the **Select IP Office** window:
   - If the required IP Office server is listed, use the check box to select your IP Office server from the list of available servers.
   - If the required IP Office server is not listed, in the **Unit/Broadcast Address** box type the IP address for your IP Office server. Click **Refresh** to perform a new search. The IP

Office server then appears in the list of available servers. Use the check box to select your IP Office server from the list of available servers.



7. Click **OK**.
8. On the **Configuration Service User Login** message box, in the **Service User Name** box, type the user name. The default name is Administrator.
9. In the **Service User Password** box, type the user password. The default password is Administrator.
10. IP Office Manager opens and displays the current configuration data for your IP Office server.

Adding an IP Office Secondary Server

Before you begin

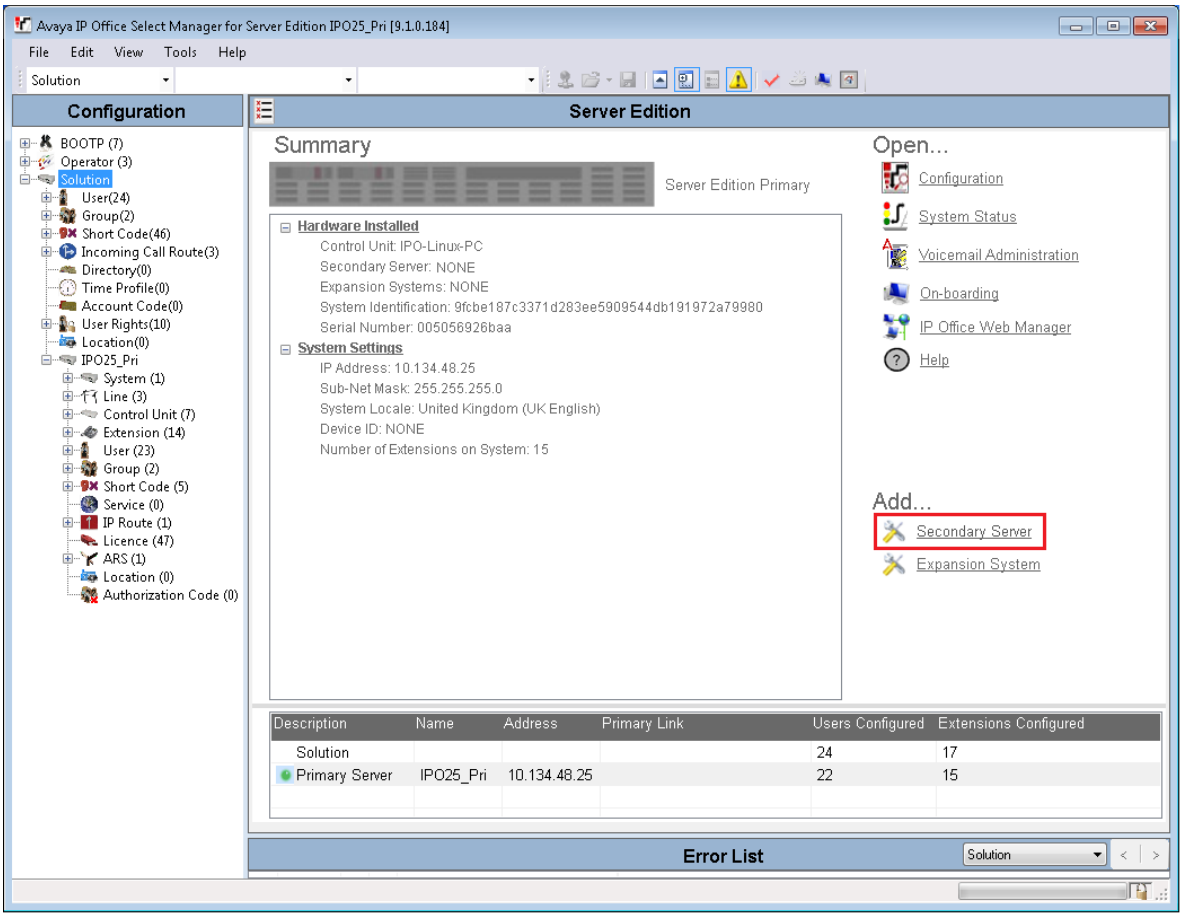
- Install an additional IP Office server. This additional server is later configured as an IP Office Secondary Server.
- Use IP Office Manager to access the configuration of the proposed IP Office Primary Server.

About this task

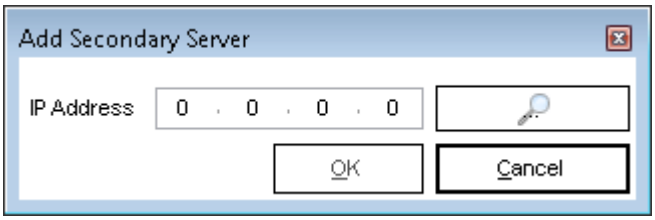
Use the Server Edition Solution View to add an IP Office Secondary Server to the network configuration. This automatically adds the necessary H.323 IP trunks for connection to the new server into the configuration of the other servers already in the network.

Procedure

1. In the **Server Edition Solution View**, under **Add**, select the **Secondary Server** link.

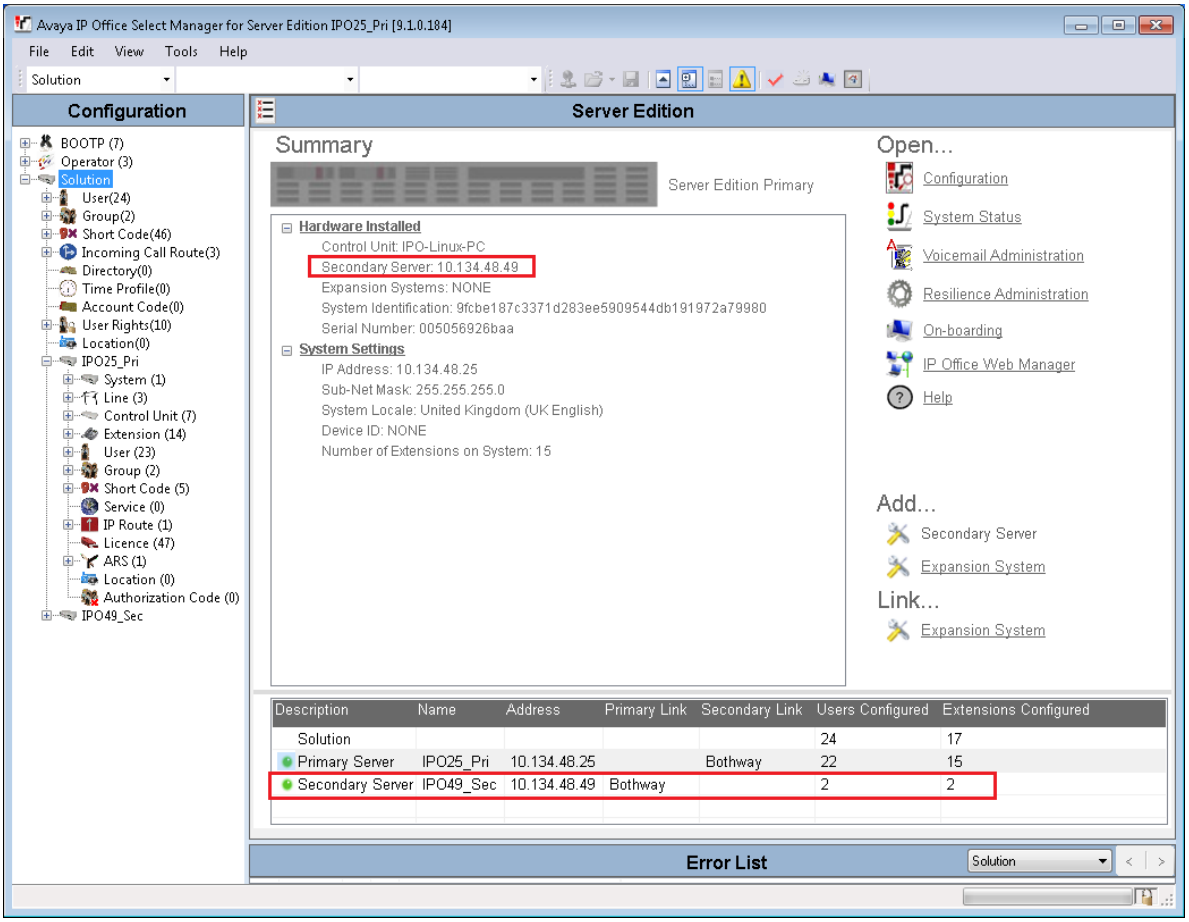


2. Enter the **IP Address** of the secondary server.



3. Click **OK**.
4. The **Initial Configuration** menu is displayed, with the fields pre-filled with the current settings of the existing system. Update the fields as required. For example, you can change the IP address settings.
5. Click **Save**.
6. The system is rebooted. Click **OK**.

7. The icon in the **Description** column alternates between green and grey until the system reboot is complete.



Configuring IP Office resilience settings

Before you begin

- You can activate resilience only if you have configured a Server Edition Secondary in IP Office Server Edition Solution.

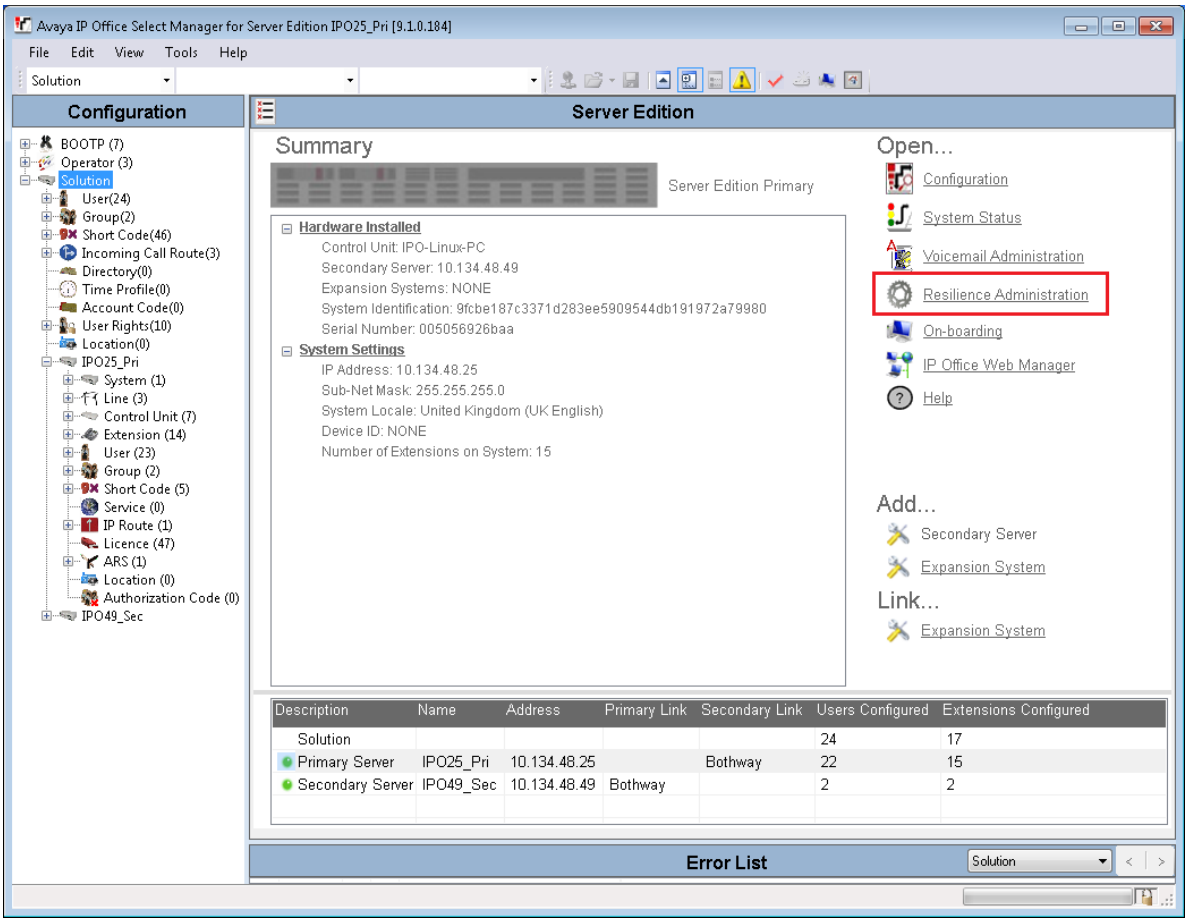
About this task

An IP Office Server Edition solution offers resilience for IP Office. When you add a secondary server to an IP Office Server Edition solution, the resilience for primary and secondary servers is active by default.

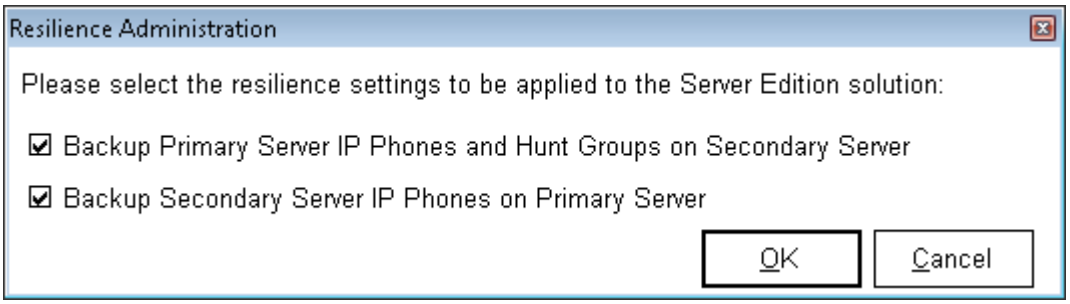
Configure the resilience settings for your IP Office solution.

Procedure

1. In the **Server Edition** window, click **Resilience Administration**.



2. On the **Resilience Administration** window, select the resilience settings to activate.



- **Backup Primary Server IP Phones and Hunt Groups on Secondary Server**. When selected, the Secondary Server supports hunt group operation during any failure of the Primary Server. Also when selected, the Secondary Server supports the continued operation of Avaya IP phones normally registered to the Primary Server.

- **Backup Secondary Server IP Phones on Primary Server**. When selected, the Primary Server supports the continued operation of Avaya IP phones normally registered to the Secondary Server.

3. Click **OK**.

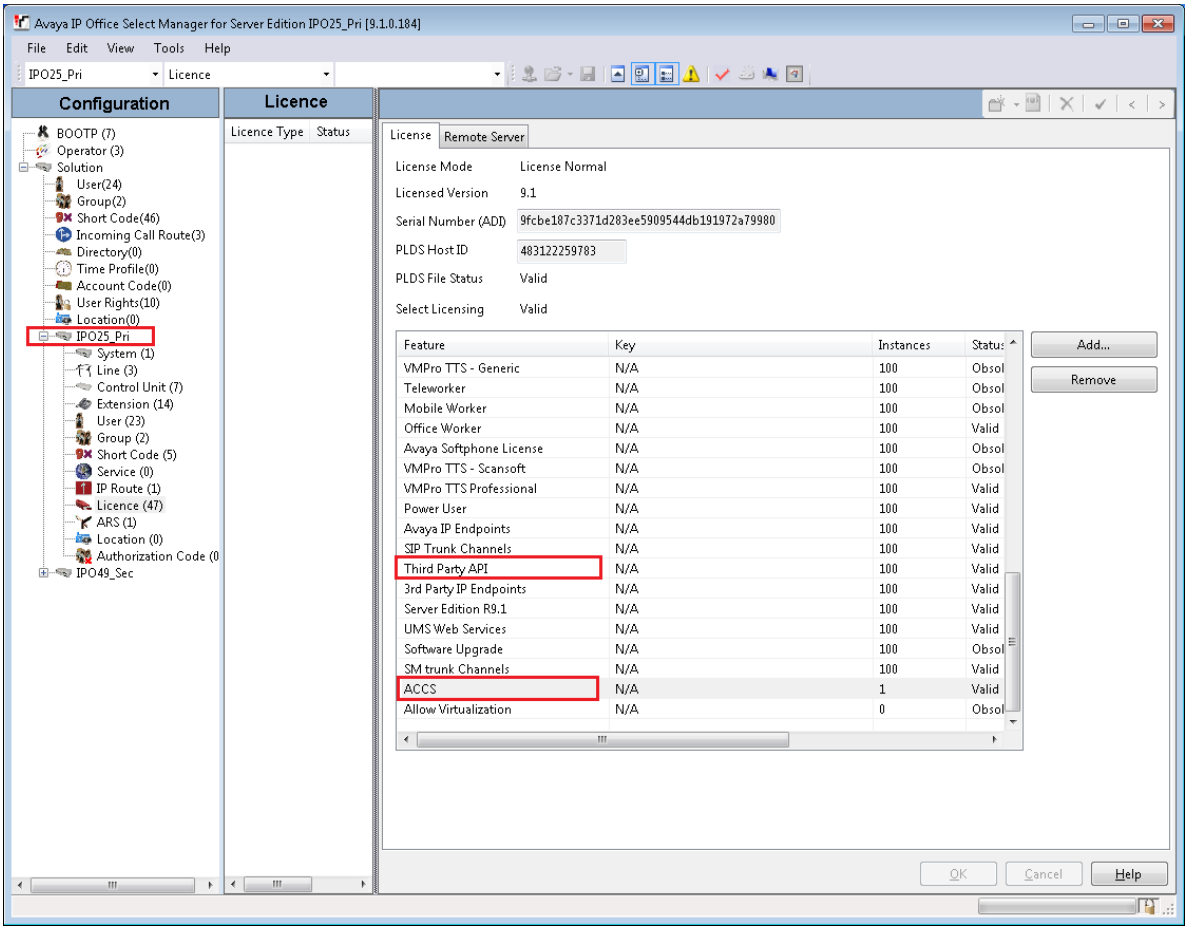
Verifying IP Office licenses

About this task

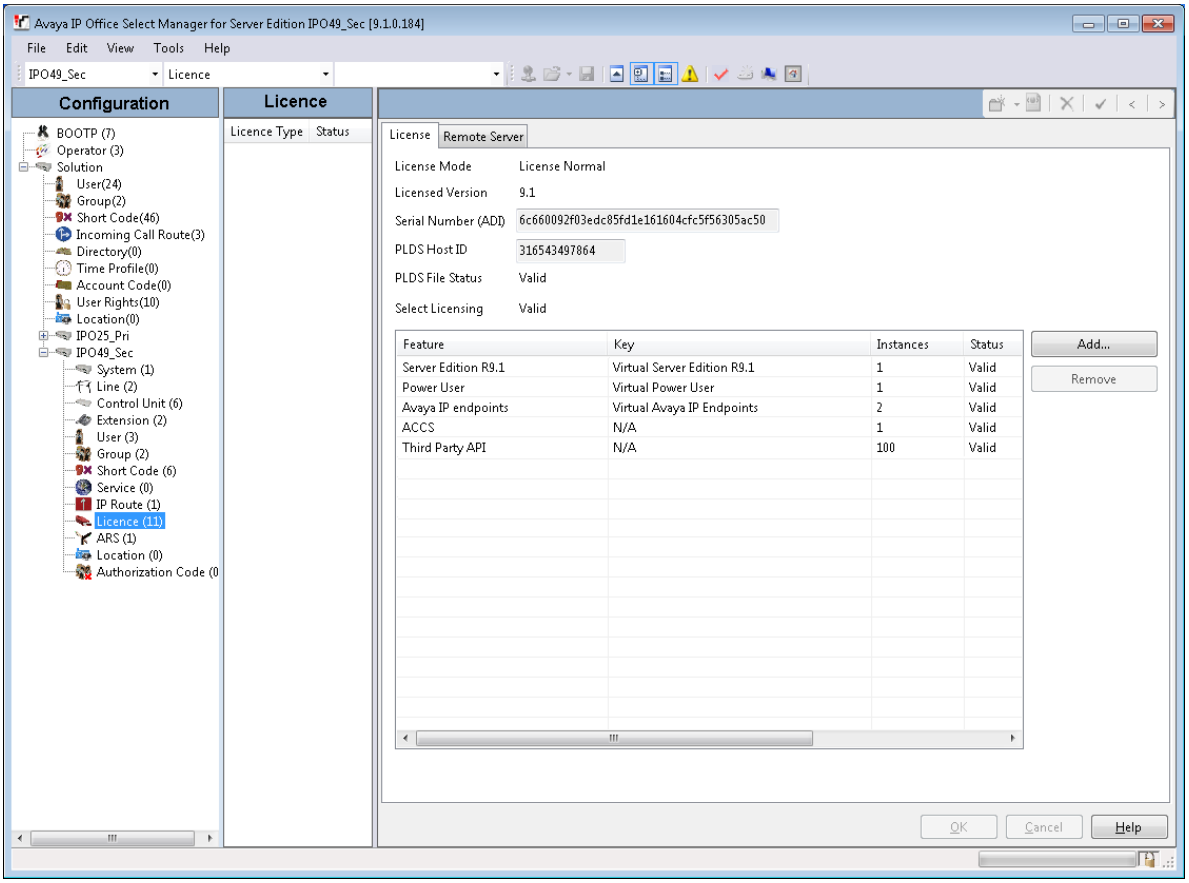
Verify IP Office licenses on the Primary Server and Secondary Server.

Procedure

1. Using IP Office Manager, select the IP Office Primary Server in the **Configuration** pane.
2. Click **License**.
3. Verify that the ACCS license is configured on the IP Office Primary Server.



4. Click **OK**.
5. Using IP Office Manager, select the IP Office Secondary Server in the **Configuration** pane.
6. Click **License**.
7. Verify that the ACCS license is configured on the IP Office Secondary Server.



8. Click **OK**.
9. If necessary, reboot the IP Office servers.

Configuring a Secondary Server SIP User Extension number

About this task

Configure a SIP User Extension number for the IP Office Secondary Server. Avaya Contact Center Select uses this SIP User Extension number and Telephony Supervisor *Login Code* password to register for CTI call control and SIP session messaging.

If the IP Office Primary Server fails or is shut down, Avaya Contact Center Select uses this SIP User Extension for CTI call control and SIP session messaging with the IP Office Secondary Server.

Procedure

1. Using IP Office Manager, select the IP Office Secondary Server in the **Configuration** pane.
2. In the **Configuration** pane, under the IP Office server, select **User**.
3. Right-click on **User**, and select **New**.
4. In the right pane, select the new **User** tab.
5. In the **Name** box, type a descriptive name for the user.
6. In the **Password** box, type a password for the user. For example, type 123456. This password must be a number.
7. In the **Confirm Password** box, re-type the password for the user. For example, type 123456.
8. In the **Extension** box, type the extension number of the user. For example, type 6000.
9. Select the **Telephony** tab.
10. On the **Telephony** tab, on the **Supervisor Settings** sub-tab, in the **Login Code** box, type a password for Avaya Contact Center Select registration. For example, type 123456. This **Login Code** password must be a number. The **Login Code** password must be the same password as used by the SIP User Extension configured on the IP Office Primary Server.
11. Click **OK**.
12. On the **Would you like a new VoIP extension created with this number** message box, select **SIP Extension** and click **OK**.

Verifying the SIP User Extension numbers

About this task

Avaya Contact Center Select uses an IP Office SIP User Extension number and a Telephony Supervisor *Login Code* password to register with IP Office for CTI call control and SIP session messaging.

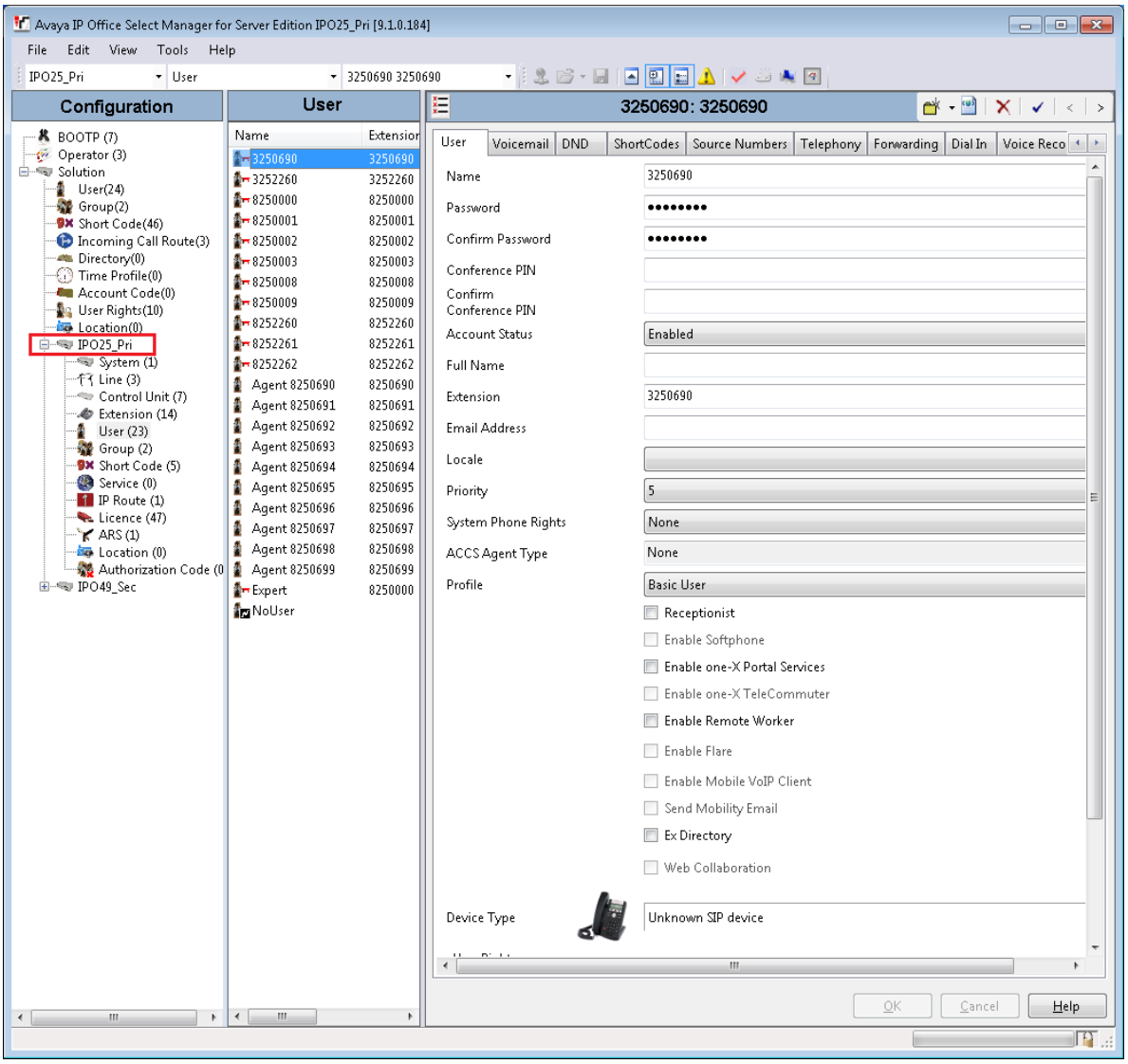
Use IP Office Manager to locate and verify the SIP User Extension number used to register with Avaya Contact Center Select.

If your solution is to have an IP Office Secondary Server, locate and verify the SIP User Extension number used to register the IP Office Secondary Server with the active Avaya Contact Center Select server.

In this worked example, SIP Extension 3250690 is configured on the IP Office Primary Server and SIP Extension 3490690 is configured on the IP Office Secondary Server.

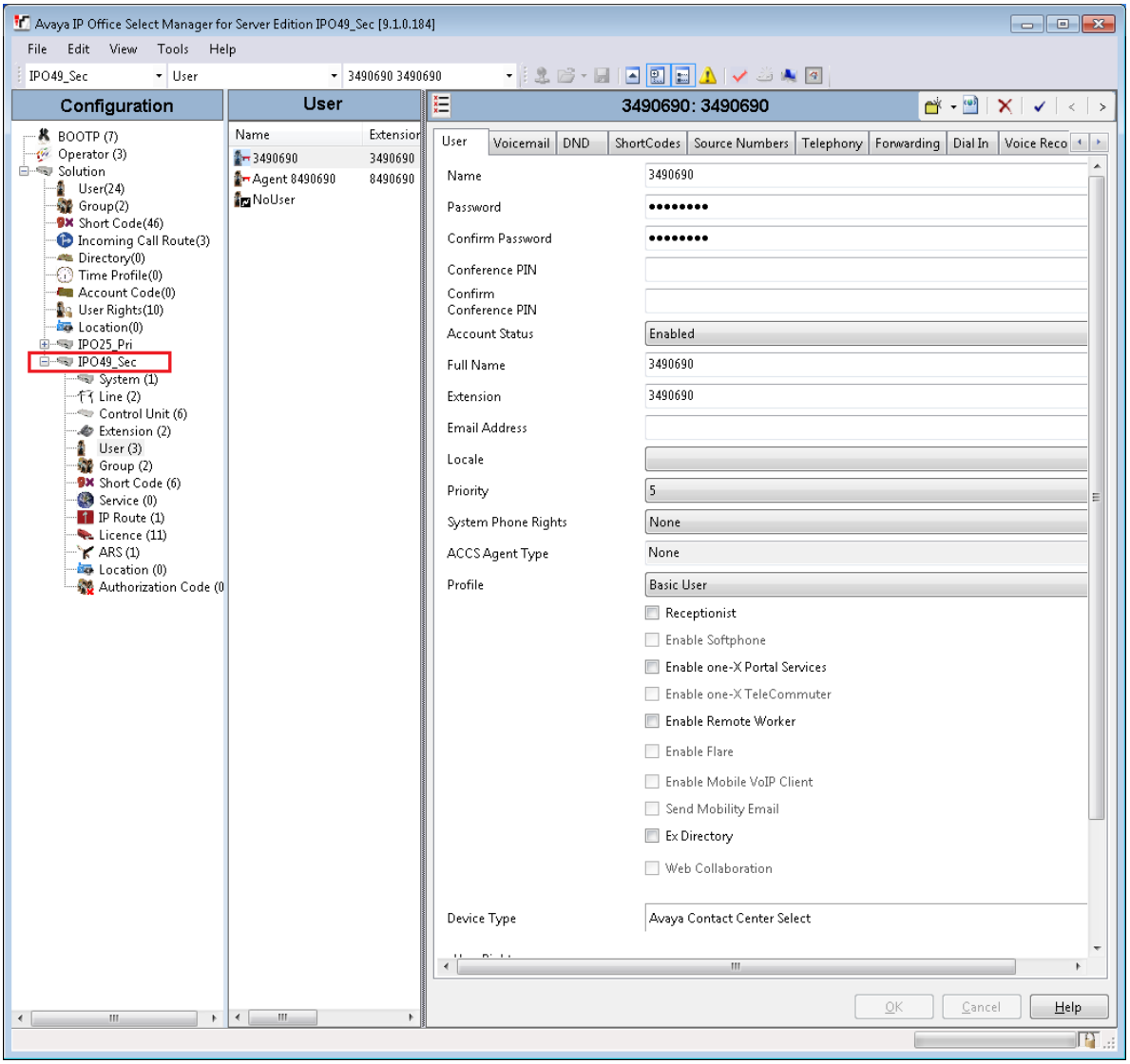
Procedure

1. Using IP Office Manager, select the IP Office Primary Server in the **Configuration** pane.
2. In the **Configuration** pane, under the IP Office server, select **User**.



3. Locate the SIP User Extension number used to register with Avaya Contact Center Select. Note the extension number.
4. If your solution has an IP Office Secondary Server, using IP Office Manager, select the IP Office Secondary Server in the **Configuration** pane.
5. In the **Configuration** pane, under the IP Office server, select **User**.

6. Locate the SIP User Extension number used to register the IP Office Secondary Server with the active Avaya Contact Center Select server. Note the extension number.



Configuring a solution level hunt group

About this task

Configure a solution level hunt group at the IP Office solution level. Configure the hunt group to use the Sequential Ring Mode.

The User List is an ordered list of the users who are members of the hunt group. For Sequential groups it also sets the order in which group members are used for call presentation. The check box next to each member indicates the status of their membership. Group calls are not presented

to members who have their membership currently disabled. However, those users are still able to perform group functions such as group call pickup. The order of the users can be changed by dragging the existing records to the required position.

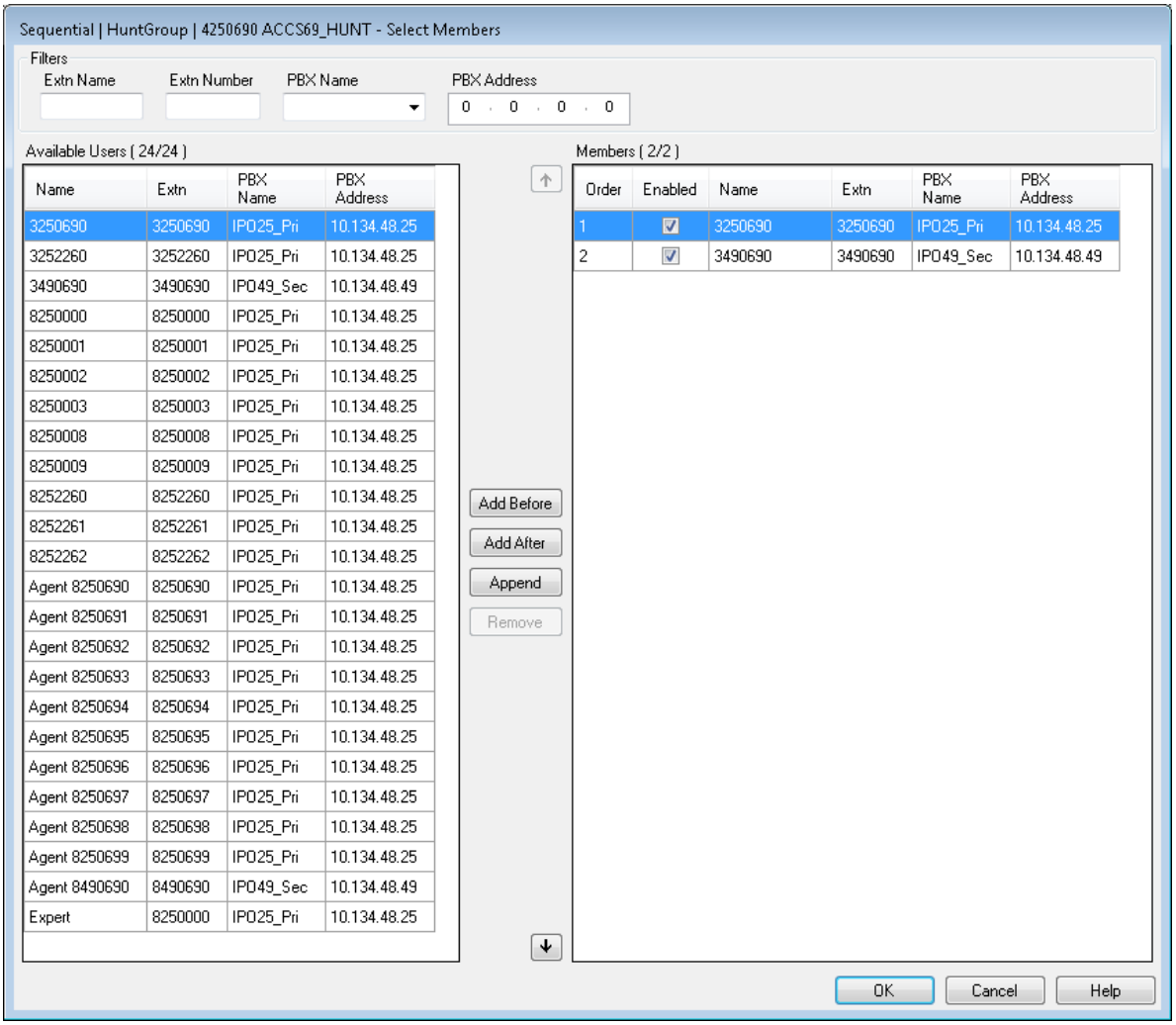
Add the SIP extension number used by the Avaya Contact Center Select server as the first member of the User List.

If your solution has a standby Avaya Contact Center Select server, add the SIP extension number used by the IP Office Secondary Server as the second member of the User List.

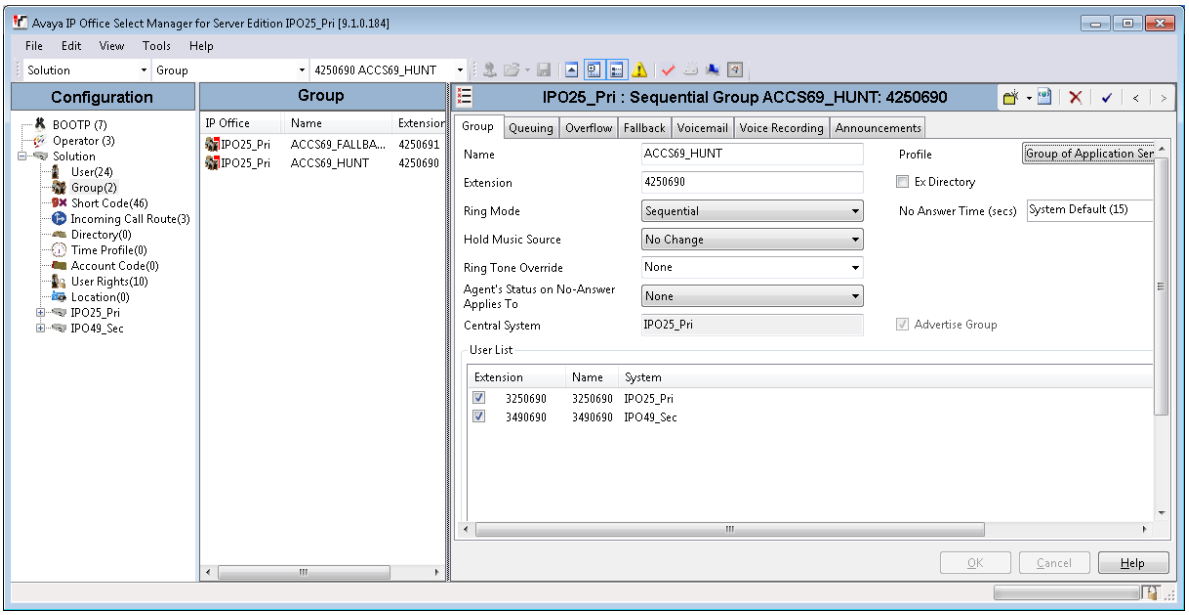
Procedure

1. Using IP Office Manager, select the IP Office server in the Configuration pane.
2. In the **Configuration** pane, under the **Solution** node, select **Group**, right-click and select **New**.
3. In the **Name** box, enter a descriptive hunt group name.
4. From the **Profile** list, select **Group of Application Servers**.
5. In the **Extension** box, enter a number for the hunt group.
6. From the **Ring Mode** list, select **Sequential**.
7. In the **User List** section, click **Edit**.
8. On the **Select Members** window, under **Available Users**, locate and select the SIP extension number used by the Avaya Contact Center Select server.
9. Add this extension to the **Members** list.

10. If your solution is to have a standby Avaya Contact Center Select server, locate and select the SIP extension number used by the standby Avaya Contact Center Select server. Click **Add After**.



11. On the **Select Members** window, click **OK**.



12. Click **OK**.

Configuring a solution level Short Code

About this task

Configure a solution level short code to map the IP Office hunt group used by Avaya Contact Center Select to an Avaya Contact Center Select Route Point CDN range. A short code configures IP Office to perform an action if a specific number is dialed.

For example:

- 225069x is configured in Avaya Contact Center Select as a range of CDNs (Route Points).
- 4250690 is configured in IP Office as a hunt group used by Avaya Contact Center Select.

Create a short code 4250690|>>225069N. All customer calls to number 4250690 are forwarded to extension range 225069N and from there to Avaya Contact Center Select. Avaya Contact Center Select can then treat the customer call and route it to a contact center agent.

A CDN (Route Point) is a logical address used by Contact Center to accept incoming contacts or as a point to which contacts are routed. A Route Point is an address that enables incoming voice contacts (phone calls) to be treated by Contact Center.

You can add multiple short codes and configure each one to map to an Avaya Contact Center Select CDN (Route Point) number. If you create additional short codes to map IP Office calls to Avaya Contact Center Select, you must add the corresponding CDN (Route Point) number in Contact Center Manager Administration on the Avaya Contact Center Select.

Procedure

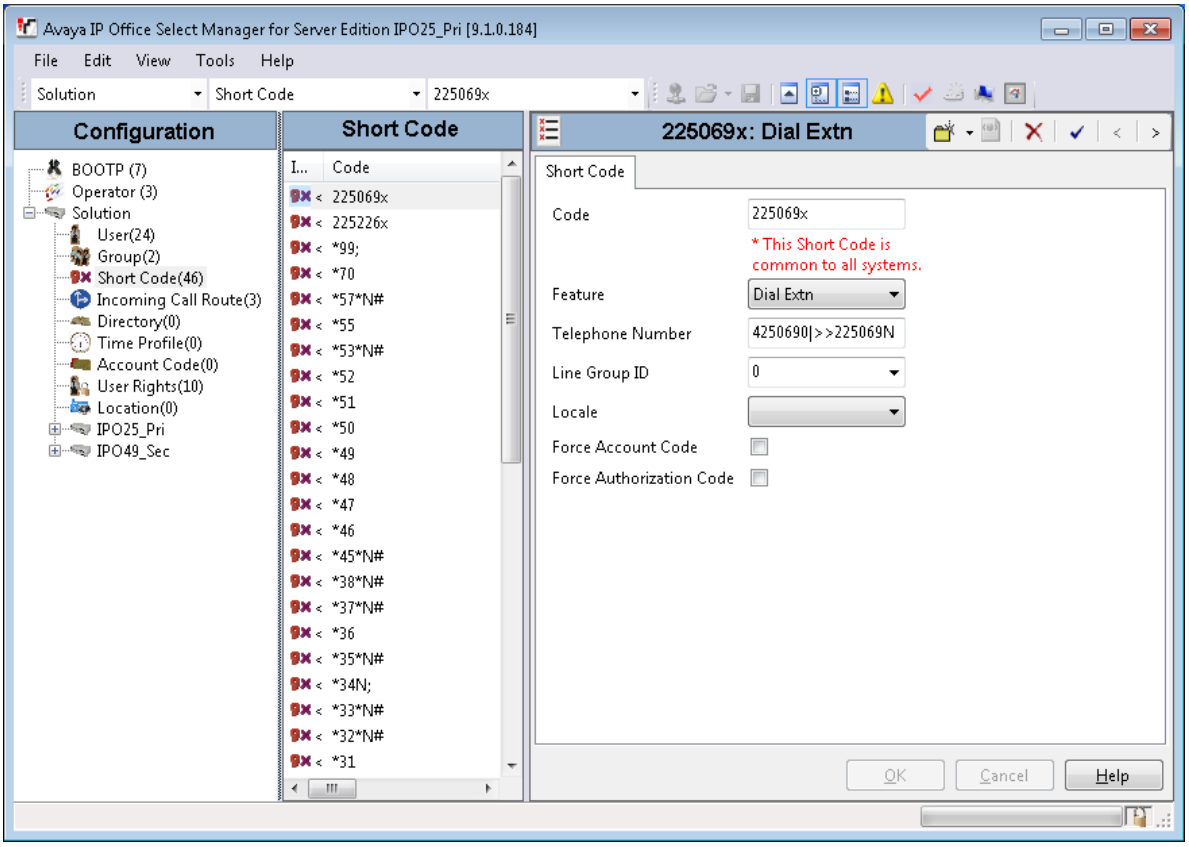
1. Using IP Office Manager, select the IP Office server in the **Configuration** pane.
2. In the **Configuration** pane, under the **Solution** node, select **Short Code**, right-click and select **New**.
3. In the right pane, in the **Code** box, type a range of CDN (Route Point) numbers. When this number is matched, the other short code fields activate. For example, type 225069x, where 225069x is a range of Avaya Contact Center Select CDNs (Route Points).
4. From the **Feature** list, select **Dial Extn**. If you do not see the **Dial Extn** option, ensure that you have selected the Short Code menu item under **Solution**, and not the local Short Code menu item for your IP Office server. The Solution Short Code is common to all systems.
5. In the **Telephone Number** box, type the number output by the short code.

   For example, type the following: 4250690|>>225069x

   - Where 225069N is configured in Avaya Contact Center Select as a range of CDNs (Route Points).
   - Where 4250690 is the Avaya Contact Center Select hunt group.

   Note: Ensure there are no spaces in the **Telephone Number** box.

   If a customer dials 225069x, then 225069x is sent to telephone number 4250690 and Avaya Contact Center Select.



6. Click **OK**.

Configuring the data synchronization user account

Before you begin

- If your solution implements Avaya Contact Center Select Business Continuity, perform this procedure. If your solution does not implement Avaya Contact Center Select Business Continuity, skip this procedure.

About this task

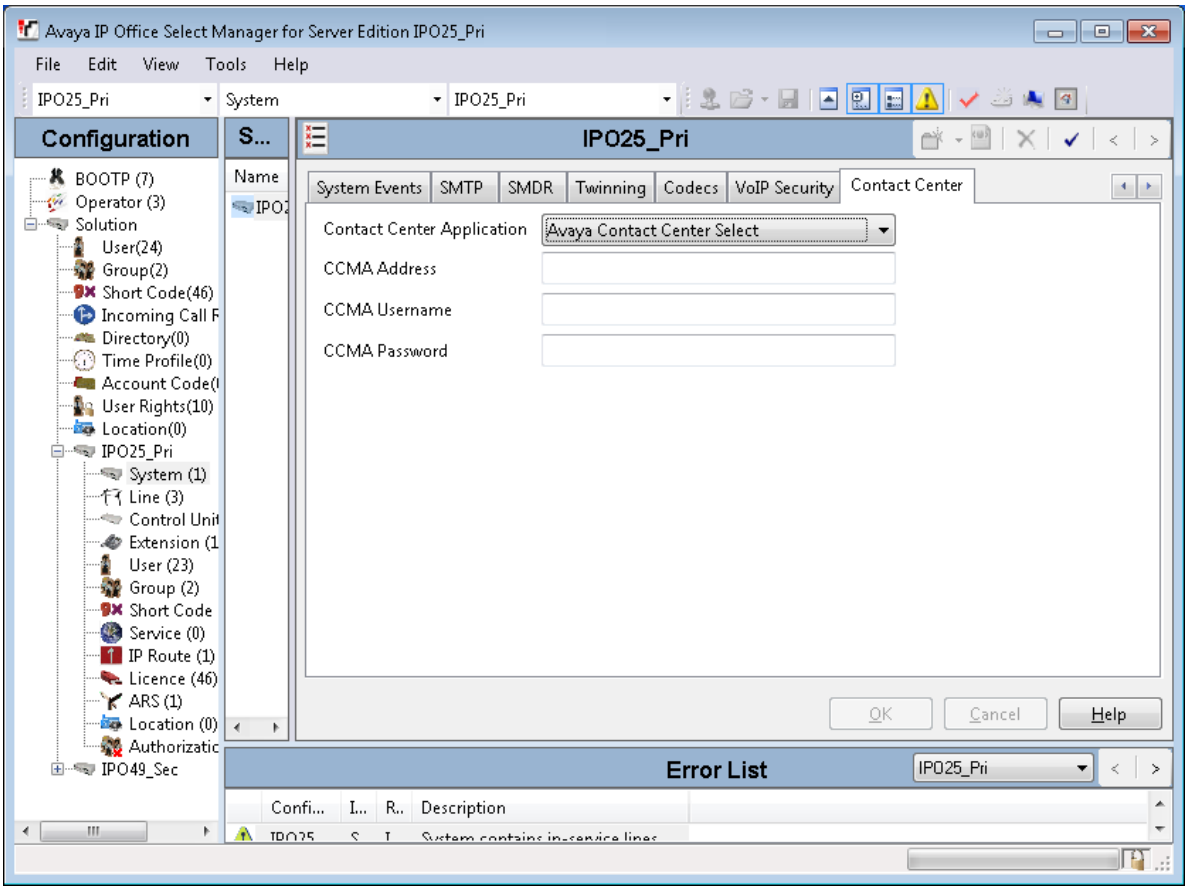
Configure the user account used by IP Office to maintain data synchronization with Avaya Contact Center Select. The name and password of this account must match the IP Office server details as configured in Contact Center Manager Administration (CCMA) on the Avaya Contact Center Select server.

For user data synchronization, IP Office connects to Avaya Contact Center Select using the Contact Center Manager Administration “accssync” user account details.

Procedure

1. Using IP Office Manager, select the IP Office Primary Server in the **Configuration** pane.

2. In the **Configuration** pane, under the IP Office server, select **System**.



3. Select the **Contact Center** tab.
4. From the **Contact Center Application** list, select **Avaya Contact Center Select**.
5. In the **CCMA Address** box, type one of the following IP addresses:
   - If your solution uses Avaya Contact Center Select Campus Business Continuity, type the Managed IP address of the Business Continuity pair.
   - If your solution uses Avaya Contact Center Select Geographic Business Continuity, type the IP address of the Avaya Contact Center Select active server.
6. In the **CCMA Username** box, type the name of the Avaya Contact Center Select data synchronization user account. The default user name is `accssync`.
7. In the **CCMA Password** box, type the password of the Avaya Contact Center Select data synchronization user account. The default user password is `accssync`.
8. Click **OK**.

Saving the IP Office configuration data

Before you begin

- Install the IP Office Manager software on a client computer that can communicate with the IP Office server.

About this task

Use IP Office Manager to save your configuration changes to the IP Office server.

Procedure

1. In IP Office Manager, in the **Configuration** pane, select your IP Office server.
2. From the main IP Office Manager menu, select **File** > **Save Configuration**.
3. On the **Send Multiple Configurations** window, use the check box to select your IP Office server from the list.
4. Click **OK**.

   IP Office Manager saves the offline configuration file to your IP Office server.

Configuring ACCS to use IP Office resilience

Before you begin

- If your IP Office solution does not support IP Office resilience, skip this procedure.

About this task

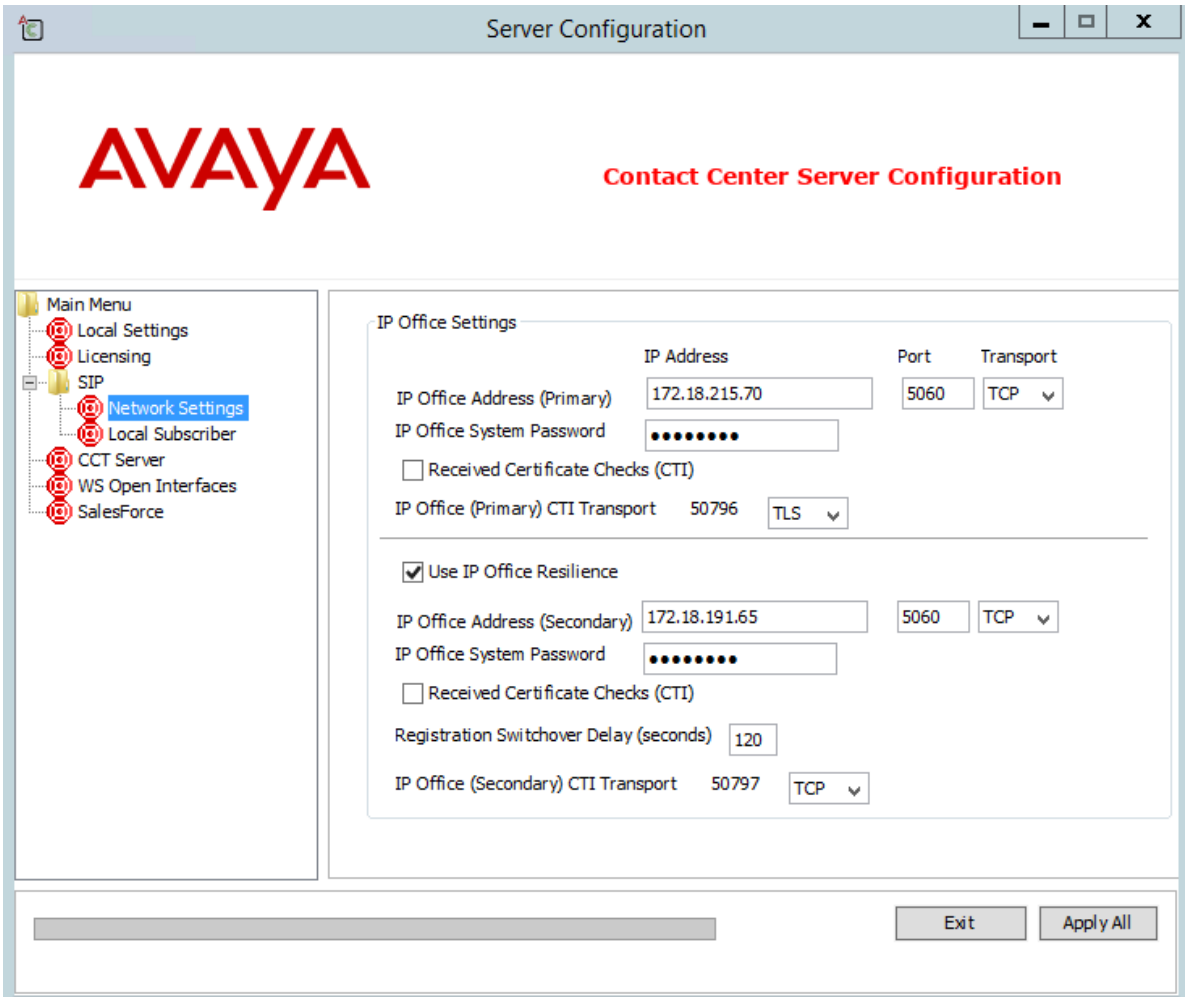
If your IP Office system has an IP Office Secondary Server and if it is configured to support voice platform resilience, configure Avaya Contact Center Select to use the resilient IP Office system.

If your solution uses TLS communication between Avaya Contact Center Select and IP Office, for more information about configuring TLS security certificates, see *Avaya Contact Center Select Advanced Administration*.

Procedure

1. Log on to the Avaya Contact Center Select active server.
2. On the **Apps** screen, in the **Avaya** section, select **Server Configuration**.

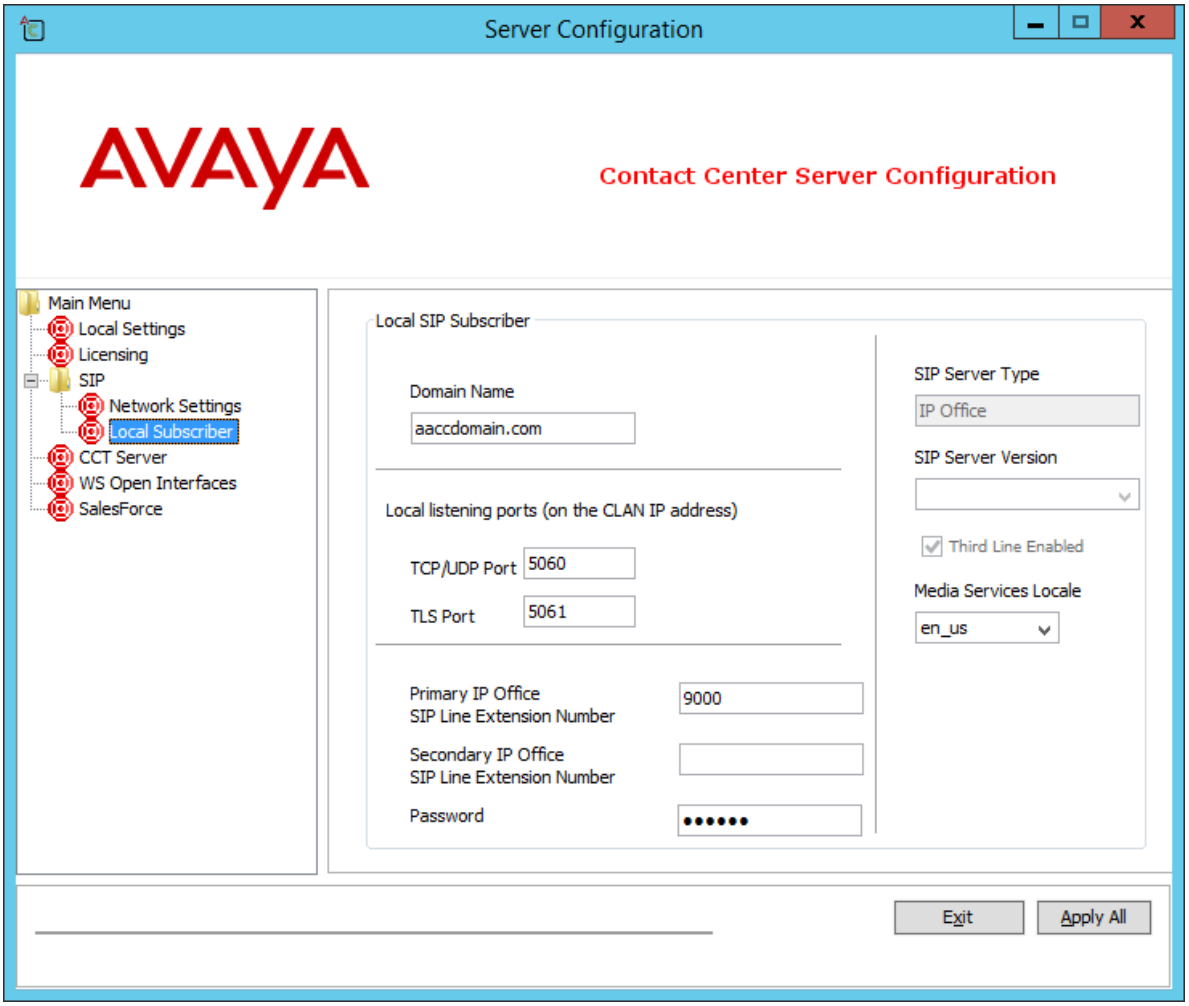
3. In the **Server Configuration** dialog box, under **SIP**, click the **Network Settings** tab.



4. Select **Use IP Office Resilience**.
5. In the **IP Office Address (Secondary)** box, type the IP address of the IP Office Secondary Server.
6. In the Secondary Server **Port** box, type the server listening port. The default port is 5060.
7. From the Secondary Server **Transport** list, select the transport type, **TCP** or **TLS**.
8. In the Secondary Server **IP Office System Password** box, type the system password for your IP Office Secondary Server. Ask your IP Office Administrator for the System Password. If this password changes on the IP Office server, you must update the password in **Server Configuration**.
9. If Avaya Contact Center Select communicates with the IP Office Secondary Server using TLS certification, to enable IP Office Certificate Validation, select **Received Certificate Checks (CTI)**.
10. In the **Registration Switchover Delay (seconds)** box, type the length of time in seconds that the Avaya Contact Center Select server attempts to reconnect to the IP Office Primary

Server before attempting to switchover to the IP Office secondary server. The maximum configurable delay is 600 seconds.

11. From the **IP Office (Secondary) CTI Transport** list, select the CTI transport type, **TCP** or **TLS**.
12. In the **Server Configuration** dialog box, under **SIP**, click the **Local Subscriber** tab.



13. In the **Secondary IP Office SIP Line Extension Number** box, type the IP Office SIP User Extension Number used to register Avaya Contact Center Select with the IP Office Secondary Server.
14. In the **Password** box, type the password of the IP Office SIP User Extension Number for the IP Office server.
15. Click **Apply All**.
16. On the **Restart Required** message box, click **Yes**.

Verifying IP Office resilience

Before you begin

- If your solution is using Avaya Contact Center Select Business Continuity, skip this procedure. Later sections of this document describe verifying IP Office resilience in an Avaya Contact Center Select Business Continuity-enabled solution.

About this task

Verify that when the IP Office Primary Server fails, Avaya Contact Center Select transitions call control from the IP Office Primary Server to the IP Office Secondary Server. If the IP Office Primary Server fails or is stopped, the IP Office Secondary Server continues to process voice calls.

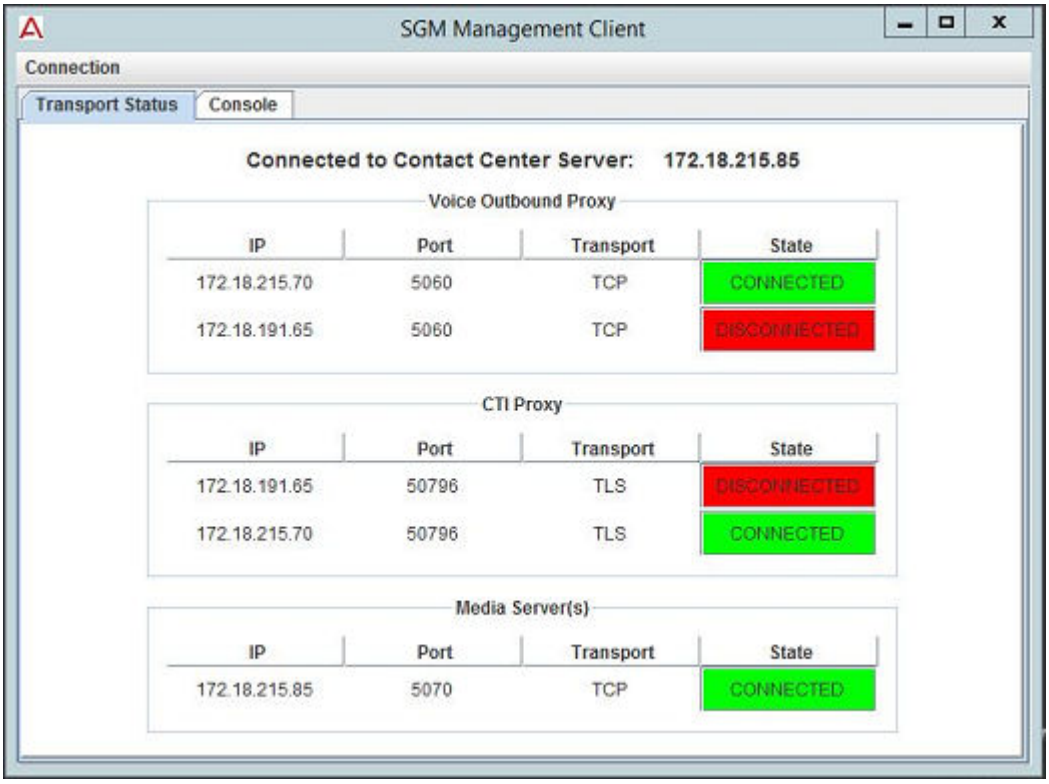
On startup, the Avaya Contact Center Select (ACCS) server registers with the IP Office Primary Server. If the ACCS server is not able to communicate and register with the IP Office Primary Server, after a configurable delay, the ACCS server attempts to register with the IP Office Secondary Server. You can configure this *Registration Switchover Delay* using the ACCS Server Configuration utility.

Note:

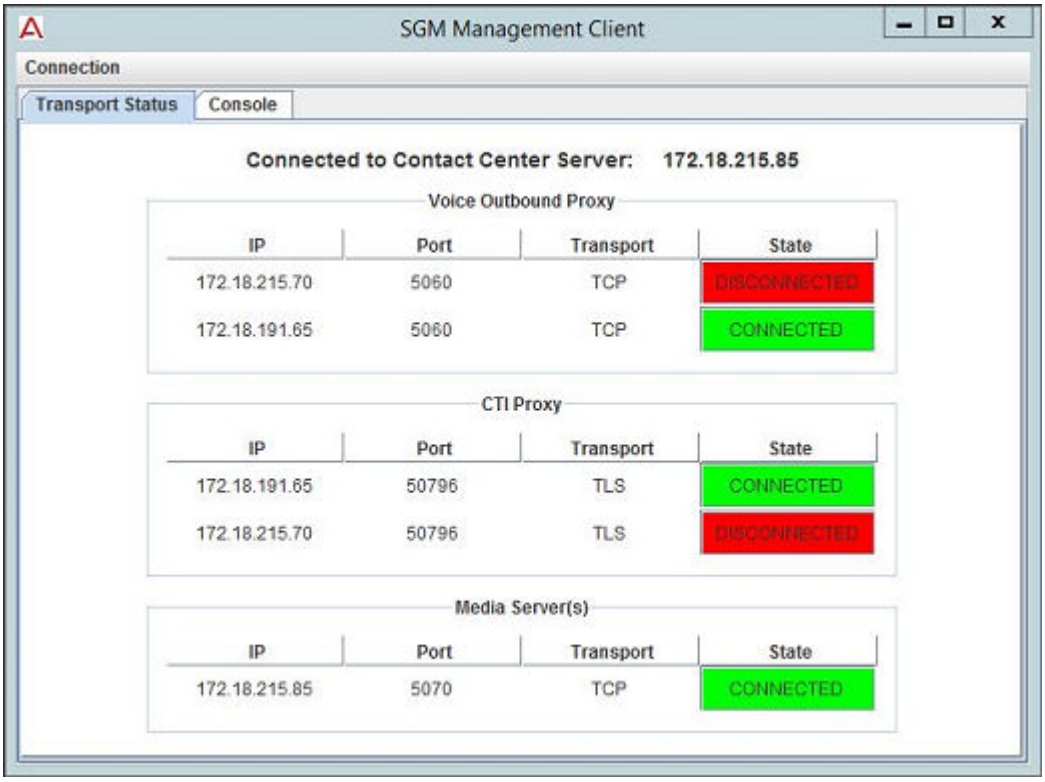
Verify that your IP Office voice platform is resilient before placing the system into production.

Procedure

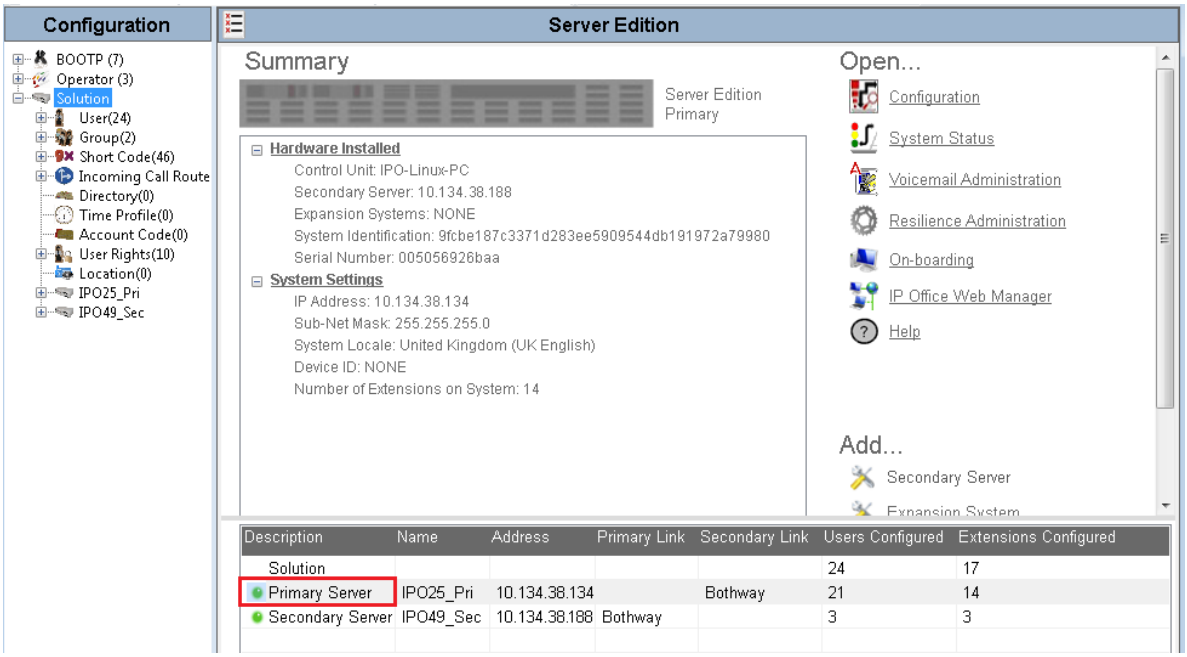
1. Log on to the ACCS server.
2. On the **Apps** screen, in the **Avaya** section, select **SIP Gateway Management Client**.
3. Verify that the ACCS server is registered with the IP Office Primary Server.



4. Disconnect the network cable from the IP Office Primary Server.
5. Verify that ACCS agent H.323 phones register with the IP Office Secondary Server. The phones do not register with the Secondary Server until the existing active calls are dropped. Depending on your solution implementation, it can take several minutes for the phones to register with the IP Office Secondary Server. When the phones have registered with the Secondary Server, they display an **R** on their display.
6. Verify that the IP Office Secondary Server routes Customer calls to ACCS and that ACCS agents can process those Customer calls. At this time, the IP Office system is no longer resilient. The IP Office Primary Server is offline and the IP Office Secondary Server is processing ACCS contacts. The ACCS server is now registered with the IP Office Secondary Server.

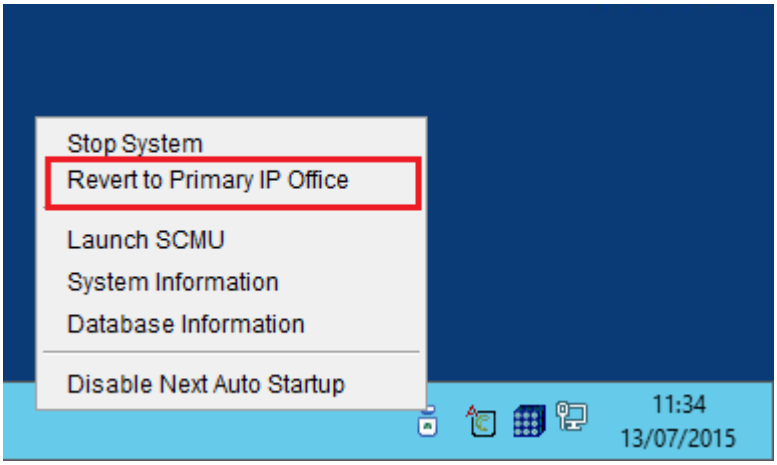


7. Reconnect the network cable to the IP Office Primary Server.
8. Wait for the IP Office Primary Server to start up.

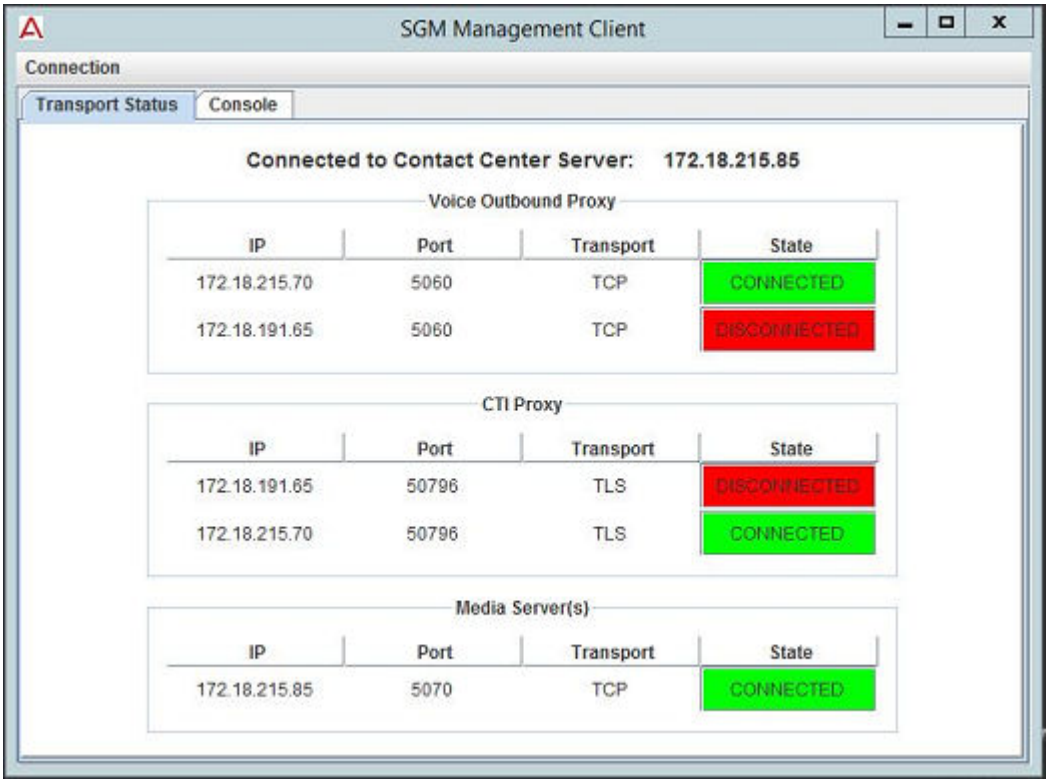


9. Rehome the agent H.323 phones to the IP Office Primary Server.

10. On the ACCS server, on the Windows taskbar, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Revert to Primary IP Office**.



The ACCS server registers with the IP Office Primary Server.



11. The IP Office system is now resilient again.
12. The ACCS server is registered with the IP Office Primary Server and customer call processing continues as normal.

Chapter 7: Campus Business Continuity configuration

This section describes how to configure Avaya Contact Center Select (ACCS) Campus Business Continuity.

The standby ACCS must match the active ACCS:

- If the active ACCS server is a Hardware Appliance, the standby ACCS server must also be a Hardware Appliance.
- If the active ACCS is a Software Appliance, the standby ACCS must also be a Software Appliance.
- If the active ACCS is a single-server DVD deployment, the standby ACCS must also be a single-server DVD deployment. The standby server must have the exact same hard disk partitions, the same amount of memory and the same CPU type. The standby server must have the Contact Center software installed on the same partitions as the active server.
- The active and standby servers must have the same ACCS patch level and the same operating system updates.

Complete all of the procedures in this section in sequential order.

Campus Business Continuity prerequisites

- Ensure your network and solution hardware meets the requirements for Business Continuity. For more information, see *Avaya Contact Center Select Solution Description*.
- Ensure that your Avaya Contact Center Select solution is using a Windows domain. To support Business Continuity resiliency, the Avaya Contact Center Select agents must each have an associated Windows domain user account in the same Windows domain as the active and standby servers. Create Avaya Contact Center Select agents with associated Windows domain accounts.
- Obtain Avaya Contact Center Select standby server licenses.
- Ensure the active and standby server hardware meets the requirements for Business Continuity. For more information, see *Avaya Contact Center Select Solution Description*.

- Install the active and standby Avaya Contact Center Select servers. For more information about installing Avaya Contact Center Select, see one of the following:
  - *Deploying Avaya Contact Center Select DVD*
  - *Deploying Avaya Contact Center Select Software Appliance*
  - *Deploying Avaya Contact Center Select Hardware Appliance*
- Ensure your IP Office system is configured and licensed.

Adding the server to a domain

Before you begin

- Ensure that you have domain administrator privileges, or ask the Domain Administrator to assign you a domain user account for remote access.
- On the server, configure a preferred Domain Name System (DNS) server on the Network Interface Card (NIC).

About this task

Add the server to an existing domain. Ask your System Administrator to add a Domain Name System (DNS) static entry for this server. Each Contact Center server in a domain requires a DNS static entry. Ask your System Administrator to add one DNS static entry for the managed name and associated Managed IP address.

A typical campus Business Continuity solution with a pair of servers requires three DNS static entries; one DNS static entry for the active server, one DNS static entry for the standby server, and one DNS static entry for the managed name and associated IP address. Avaya Contact Center Select Business Continuity solutions do not support Dynamic DNS.

Procedure

1. Log on to the Avaya Contact Center Select server.
2. On the **Start** screen, select **Administrative Tools** > **Server Manager**.
3. In the left pane, select **Local Server**.
4. In the right pane, in the **Properties** section, double-click on the **Domain** value.

   The **System Properties** dialog box appears.
5. In the **System Properties** dialog box, click the **Computer Name** tab.
6. Click **Change**.
7. In the **Member of** section, click the **Domain** option.
8. Type the domain name. You must provide the fully qualified domain name, which includes the prefix and suffix.
9. Click **OK**.

10. Type the domain administrator **User name** and **Password**.
11. Click **OK**.
12. Restart the server when you are prompted to do so.
13. Repeat this procedure for the other Avaya Contact Center Select server.

Installing the third-party networking utility

About this task

Install a third-party utility required by Avaya Contact Center Select to support Business Continuity.

Procedure

1. Log on to the active server.
2. Using Windows Explorer, navigate to <installation drive>:\Avaya\Contact Center\Manager Server\CCSMMC\thirdparty\winpcap.
3. Double-click **WinPcap_4_1_3.exe**.
4. On the WinPcap installer dialog, click **Next**.
5. On the WinPcap installer **Setup Wizard** dialog box, click **Next**.
6. On the WinPcap installer **License Agreement** dialog box, click **I Agree**.
7. On the WinPcap installer **Installation options** dialog box, click **Install**.
8. On the WinPcap installer dialog, click **Finish**.
9. Repeat this procedure on the other Avaya Contact Center Select server.

Resolving the Managed name to the Managed IP Address

About this task

Complete the following procedure to resolve the managed server name to the Managed IP address. Each Contact Center server in a domain requires a DNS static entry.

Important:

Business Continuity solutions do not support Dynamic DNS.

Ask your System Administrator to add a Domain Name System (DNS) static entry for the active and standby servers and one additional DNS static entry for the managed name and associated Managed IP address.

In Business Continuity solutions using local WebLM, the managed IP address must be lower than the active and standby server IP addresses. For example, if the active server IP address is 1.2.3.4 and the standby server IP address is 1.2.3.5, the managed IP address is 1.2.3.3.

A typical Business Continuity campus solution with a pair of servers requires 3 DNS static entries; one DNS static entry for the active server, one DNS static entry for the standby server, and one DNS static entry for the managed name and associated Managed IP address.

Perform this procedure on the active and standby servers.

Procedure

1. Open Windows Explorer.
2. Go to the folder C:\Windows\system32\drivers\etc.
3. Double-click on the **hosts** file, select **Open**, and select **Notepad**.

   The hosts file opens in Notepad.
4. Add the Managed IP address and the managed server name to the hosts file.

   Important:

   The Managed Server name can be a full name or netbios server name.

Configuring Avaya Aura® Media Server replication

About this task

Configure the standby Avaya Contact Center Select Avaya Aura® Media Server to replicate (copy) media files from the Content Store of the active Avaya Contact Center Select Avaya Aura® Media Server.

Content Store replication provides media storage replication. If the solution Administrator adds new media files to the Avaya Aura® Media Server of the active Avaya Contact Center Select, these media files are automatically copied to the Avaya Aura® Media Server of the standby Avaya Contact Center Select system.

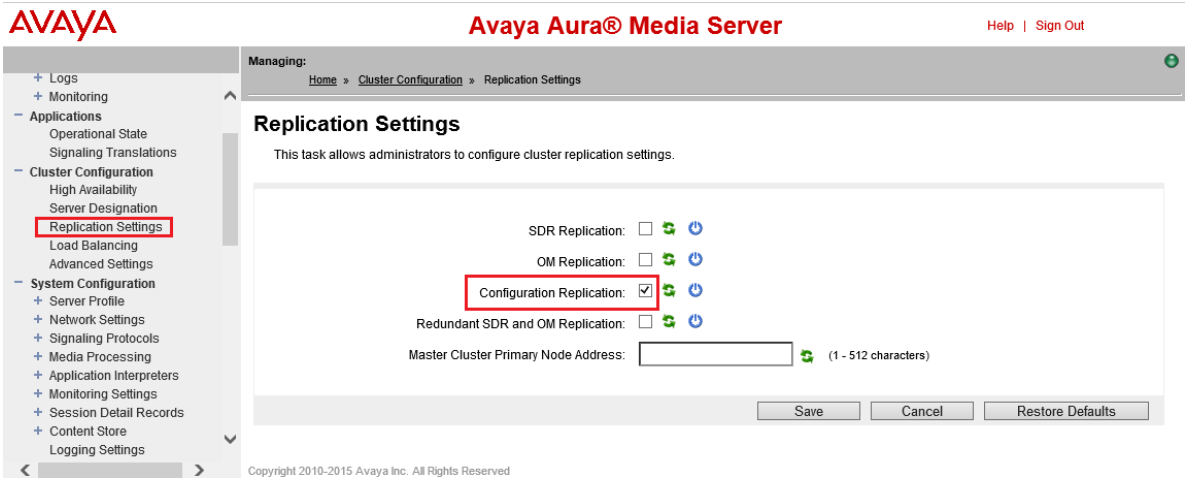
Avaya Aura® Media Server uses a custom password protected account to secure Avaya Aura® Media Server Content Store replication. Configure both Avaya Aura® Media Servers with the same replication account username and password details. The Avaya Aura® Media Server replication account is a custom account used only to secure the Avaya Aura® Media Server Content Store during replication, it is not an operating system account.

Procedure

1. On the Avaya Aura® Media Server of the primary Avaya Contact Center Select system, start a Web browser.
2. In the address box, enter https://SERVER_IP_ADDRESS:8443/em. Where SERVER_IP_ADDRESS is the IP address of the Avaya Aura® Media Server of the primary Avaya Contact Center Select system.

3. In the **User ID** box, type the Avaya Aura® Media Server User ID log on account name. The default Element Manager User ID account name is *cust*.
4. In the **Password** box, type the Avaya Aura® Media Server Element Manager password. The default Element Manager password is the cust password for the Avaya Aura® Media Server server. The Avaya Aura® Media Server replication account is a custom account used only to secure the Avaya Aura® Media Server Content Store during replication, it is not an operating system account.
5. Click **Sign In**.
6. In the navigation pane, click **Cluster Configuration**.
7. Select **Server Designation**.
8. Under **Local Server**, from the **Role** list select **Primary**.
9. Under **Replication Account**, select the **Enable Replication Account** check box.
10. In the **Username** box, type a username for the replication account. This value is arbitrary, but you must use the same value for both Avaya Aura® Media Server servers.
11. In the **Password** box, type a password for the replication account. This value is arbitrary, but you must use the same value for both Avaya Aura® Media Server servers.
12. In the **Confirm Password** box, retype the password.
13. Click **Save**.
14. Click **Confirm**.
15. On the Avaya Aura® Media Server of the standby Avaya Contact Center Select system, start a Web browser.
16. In the address box, enter https://SERVER_IP_ADDRESS:8443/em. Where SERVER_IP_ADDRESS is the IP address of the Avaya Aura® Media Server of the standby Avaya Contact Center Select system.
17. In the **User ID** box, type the Avaya Aura® Media Server User ID log on account name. The default Element Manager User ID account name is *cust*.
18. In the **Password** box, type the Avaya Aura® Media Server Element Manager password. The default Element Manager password is the cust password for the Avaya Aura® Media Server server. The Avaya Aura® Media Server replication account is a custom account used only to secure the Avaya Aura® Media Server Content Store during replication, it is not an operating system account.
19. Click **Sign In**.
20. In the navigation pane, click **Cluster Configuration**.
21. Select **Server Designation**.
22. Under **Local Server**, select **Primary** from the **Role** list.
23. Under **Replication Account**, select the **Enable Replication Account** check box.

24. In the **Username** box, type the username for the replication account that you specified on the Avaya Aura® Media Server of the primary Avaya Contact Center Select system.
25. In the **Password** box, type the password for the replication account that you specified on the Avaya Aura® Media Server of the primary Avaya Contact Center Select system.
26. In the **Confirm Password** box, retype the password.
27. Click **Save**.
28. Click **Confirm**.
29. In the navigation pane, select **Replication Settings**.



30. Select **Configuration Replication**.
31. In the **Master Cluster Primary Node Address** box, type the IP address of the Avaya Aura® Media Server for the primary Avaya Contact Center Select.
32. Click **Save**.
33. Click **Confirm**.

Configuring ACCS to use IP Office resilience

Before you begin

- If your IP Office solution does not support IP Office resilience, skip this procedure.

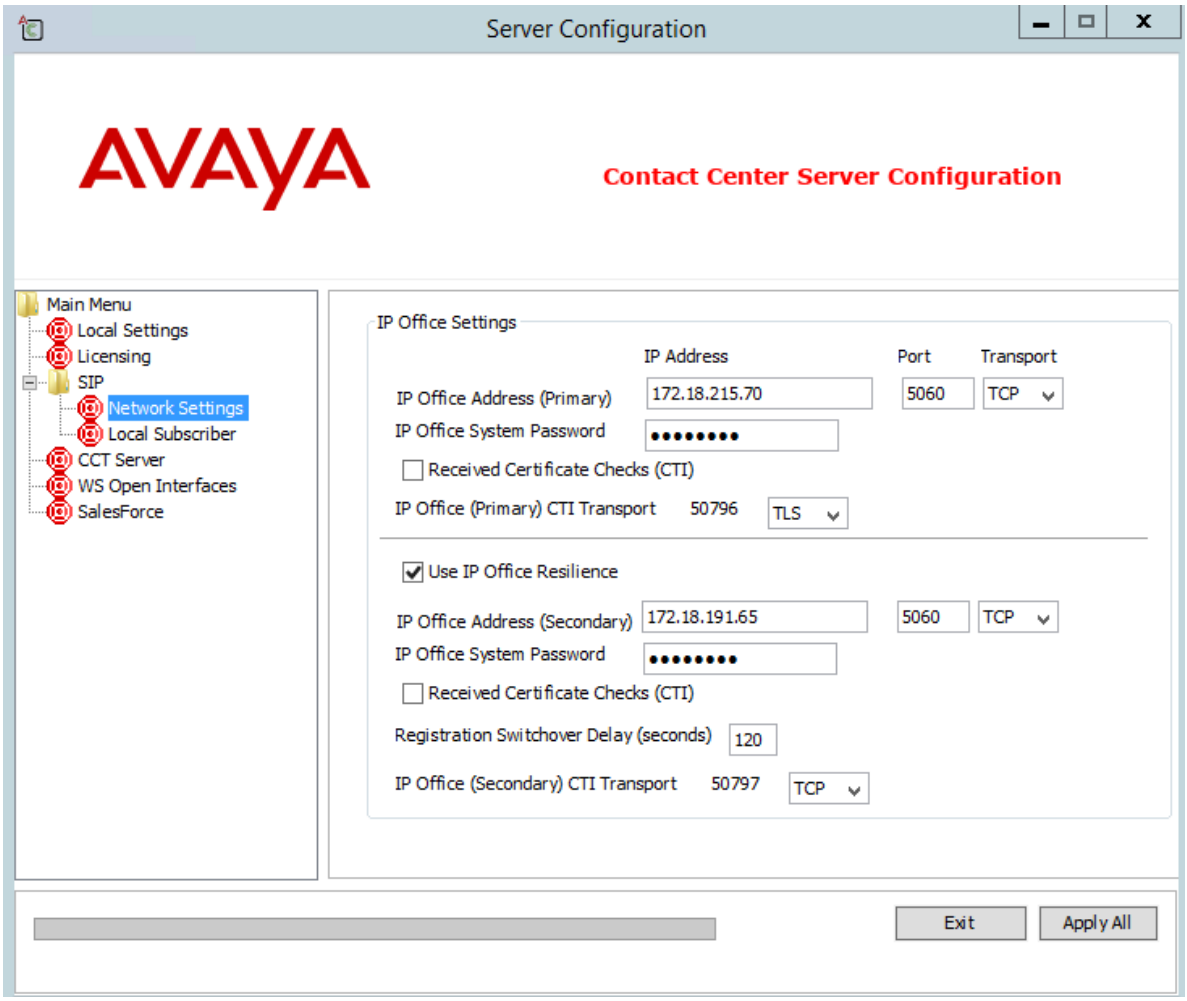
About this task

If your IP Office system has an IP Office Secondary Server and if it is configured to support voice platform resilience, configure Avaya Contact Center Select to use the resilient IP Office system.

If your solution uses TLS communication between Avaya Contact Center Select and IP Office, for more information about configuring TLS security certificates, see *Avaya Contact Center Select Advanced Administration*.

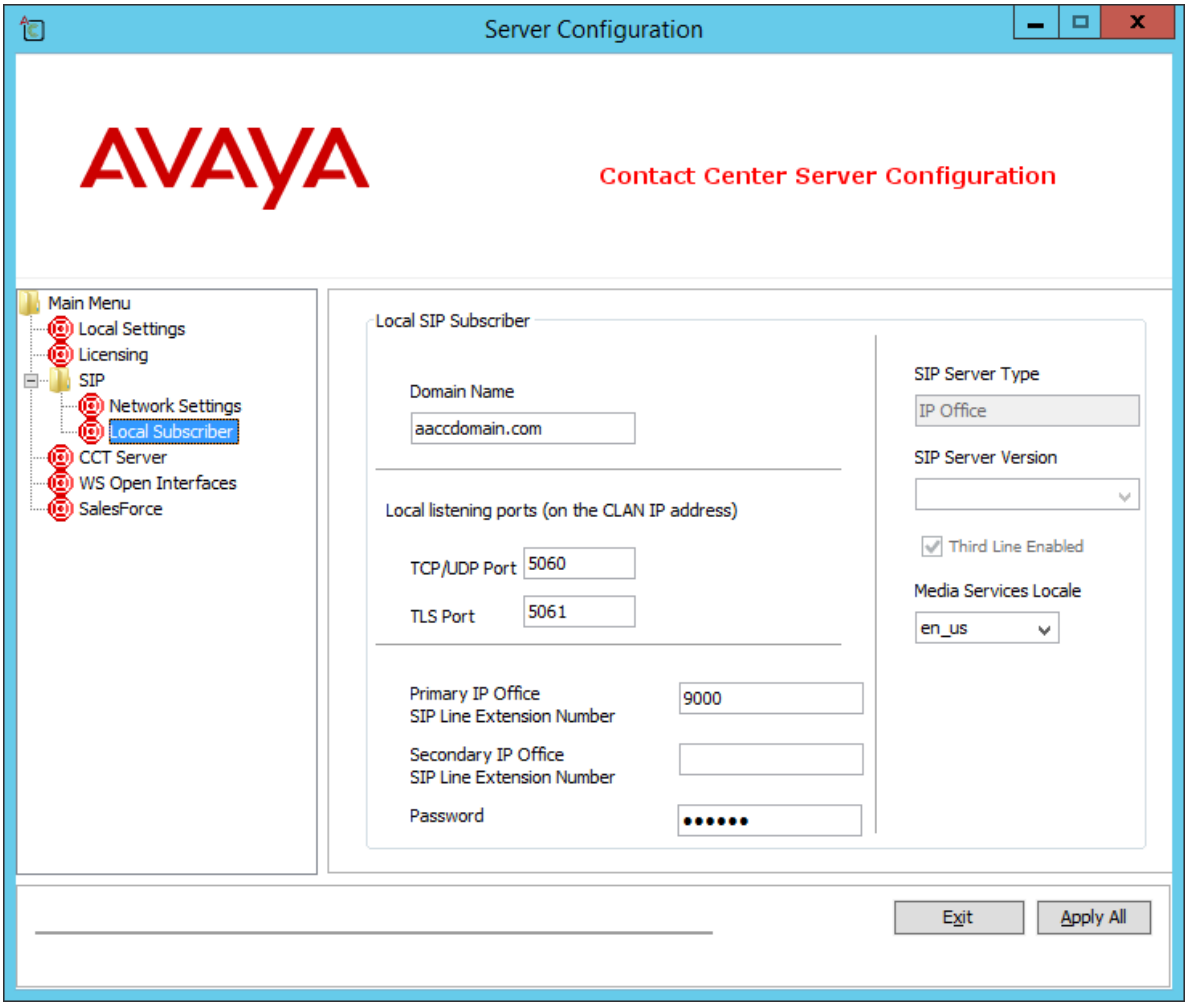
Procedure

1. Log on to the Avaya Contact Center Select active server.
2. On the **Apps** screen, in the **Avaya** section, select **Server Configuration**.
3. In the **Server Configuration** dialog box, under **SIP**, click the **Network Settings** tab.



4. Select **Use IP Office Resilience**.
5. In the **IP Office Address (Secondary)** box, type the IP address of the IP Office Secondary Server.
6. In the Secondary Server **Port** box, type the server listening port. The default port is 5060.
7. From the Secondary Server **Transport** list, select the transport type, **TCP** or **TLS**.
8. In the Secondary Server **IP Office System Password** box, type the system password for your IP Office Secondary Server. Ask your IP Office Administrator for the System Password. If this password changes on the IP Office server, you must update the password in **Server Configuration**.

9. If Avaya Contact Center Select communicates with the IP Office Secondary Server using TLS certification, to enable IP Office Certificate Validation, select **Received Certificate Checks (CTI)**.
10. In the **Registration Switchover Delay (seconds)** box, type the length of time in seconds that the Avaya Contact Center Select server attempts to reconnect to the IP Office Primary Server before attempting to switchover to the IP Office secondary server. The maximum configurable delay is 600 seconds.
11. From the **IP Office (Secondary) CTI Transport** list, select the CTI transport type, **TCP** or **TLS**.
12. In the **Server Configuration** dialog box, under **SIP**, click the **Local Subscriber** tab.



13. In the **Secondary IP Office SIP Line Extension Number** box, type the IP Office SIP User Extension Number used to register Avaya Contact Center Select with the IP Office Secondary Server.
14. In the **Password** box, type the password of the IP Office SIP User Extension Number for the IP Office server.

15. Click **Apply All**.
16. On the **Restart Required** message box, click **Yes**.

Configuring CCMM General Administration

About this task

Agent Desktop communicates with the Communication Control Toolkit (CCT) component of Avaya Contact Center Select to handle voice contacts. Agent Desktop communicates with the Contact Center Multimedia (CCMM) component of Avaya Contact Center Select to handle multimedia based contacts.

Use the CCMM Administration tool to configure standby CCMM and CCT details.

Important:

Changes to the CCMM Server Settings might require a server restart before they take effect.

Procedure

1. Start Internet Explorer.
2. In the **Address** box, type the URL of the Avaya Contact Center Select active server. The default URL is:

   `http://<server name>`

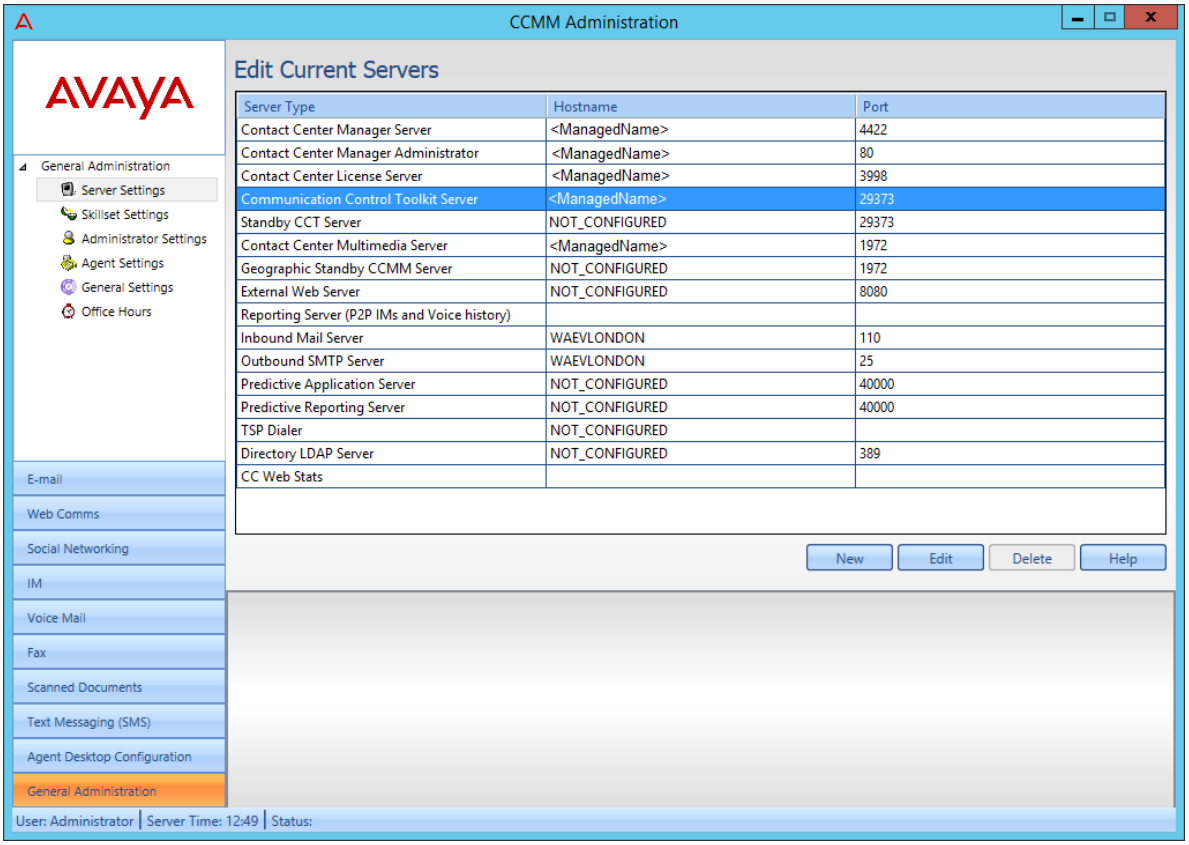
   where <server name> is the host name of the active Avaya Contact Center Select server.
3. Press **Enter**.
4. In the main Contact Center Manager Administration logon window, in the **User ID** box, type the user name. The default user ID is Administrator.
5. In the **Password** box, type the password. The default user password is Administrator.
6. Click **Log In**.

   Contact Center Manager Administration (CCMA) displays the date and time of your last login and also the number of failed login attempts before a successful login.
7. From the **Launchpad**, select **Multimedia**.
8. In the left pane, select the CCMM server to administer.

   The system displays the Multimedia Administration screen in the right pane.
9. Select **Install prerequisite software**.
10. Click **Launch Multimedia Client**.
11. On the **File Download** box, click **Run**.

    The prerequisite software takes some time to install. After the install, the CCMM Administration utility appears.

12. In the left column of the **CCMM Administration** tool, select **General Administration**.
13. Click **Server Settings**.
14. Ensure that **Contact Center Manager Server** is configured with the Managed IP address of the Avaya Contact Center Select Business Continuity pair.
15. Ensure that **Contact Center License Server** is configured with the Managed IP address or managed name of the Avaya Contact Center Select Business Continuity pair.
16. Ensure that **Contact Center Manager Administration** is configured with the managed name of the Avaya Contact Center Select Business Continuity pair.
17. Ensure that **Contact Center Multimedia Server** is configured with the Managed IP address or managed name of the Avaya Contact Center Select Business Continuity pair.
18. Ensure that **Communication Control Toolkit Server** is configured with the Managed IP address of your Avaya Contact Center Select Business Continuity pair.



19. In the left column select **E-mail**.
20. Click **General Settings**.
21. Ensure that the Inbound URL is of the form `http://<ManagedIPAddress>/inboundattachment`.

22. Ensure that the Outbound URL is of the form `http://<ManagedIPAddress>/outboundattachment`.

Verifying services are ready for Business Continuity

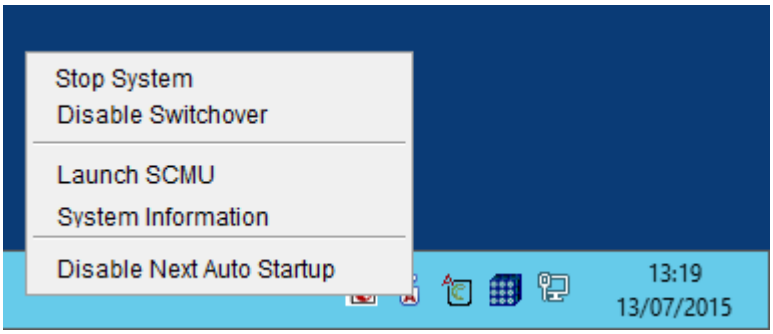
About this task

Verify that all services stop before you configure Business Continuity. This ensures that all resources are available to the active server when it starts.

Perform this procedure using the System Management and Monitoring Component (SMMC) on both Avaya Contact Center Select servers.

Procedure

1. Log on to the active server.
2. On the Windows System Tray, right-click on the System Management and Monitoring Component (SMMC) system tray icon, and select **Stop System**.



3. Repeat this procedure on the other Avaya Contact Center Select server.

Configuring Business Continuity on the active server

About this task

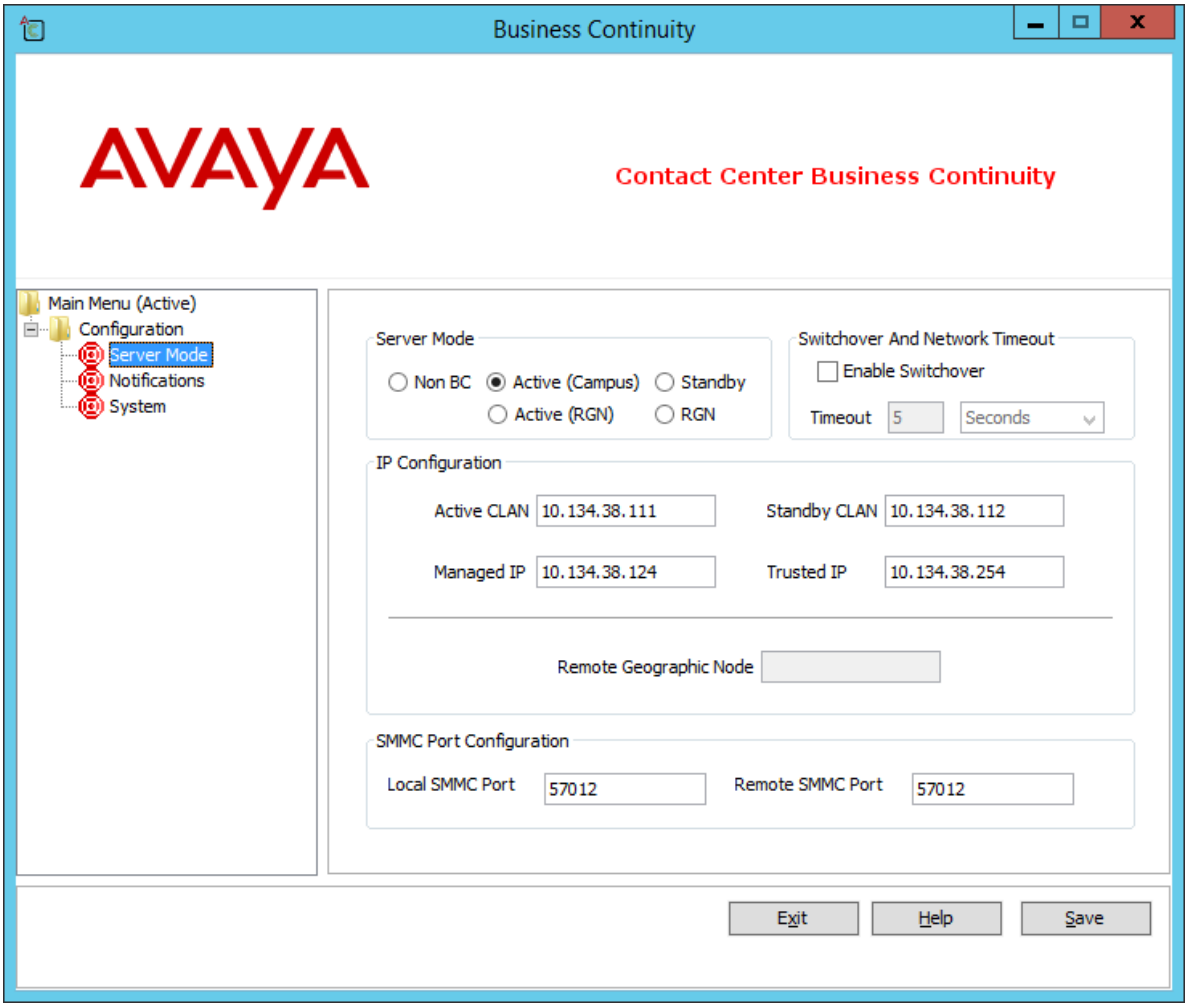
Configure Business Continuity (BC) on the active server using the Business Continuity utility. The active server is the server that normally processes calls. The Business Continuity configuration utility user interface is disabled when the BC system is shadowing.

You might need to restart the server to apply the settings.

Procedure

1. Select one server to be the active server and log on.
2. On the **Apps** screen, in the **Avaya** section, select **Business Continuity**.

3. Expand **Configuration**.
4. Double-click **Server Mode**.
5. Under **Server Mode**, select **Active (Campus)**.
6. Under **Switchover And Network Timeout Configuration**, select **Enable Switchover**.
7. Under **Switchover And Network Timeout Configuration**, in the **Timeout** box, type the maximum length of time the network connectivity tests can continue to fail consecutively before corrective action is considered.
8. Under **Switchover And Network Timeout Configuration**, from the drop down list, select the unit of time for the network connectivity tests.
9. Under **IP Configuration**, in the **Active CLAN** box, type the IP address for the active server.
10. Under **IP Configuration**, in the **Standby CLAN** box, type the IP address for the standby server.
11. Under **IP Configuration**, in the **Managed IP** box, type the managed IP address.
12. Under **IP Configuration**, in the **Trusted IP** box, type the IP address of a trusted server.
13. Under **SMMC Port Configuration**, in the **Local SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the local (active) server.
14. Under **SMMC Port Configuration**, in the **Remote SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the remote (standby) server.



15. Click **Save**.
16. If a **Business Continuity** message box appears requesting a server reboot, click **OK** to reboot the server.

Variable definitions

Name	Description
Timeout	The Business Continuity feature tests network connectivity between BC components by default every 100 milliseconds (100ms). The Timeout value sets the maximum length of time these network connectivity tests can continue to fail consecutively before corrective action is considered. The maximum Timeout value is 30 seconds.

Table continues…

Name	Description
	Avaya recommends that you set Timeout value long enough to be tolerant of normal network latency, but short enough to be responsive if a failure occurs.
Active CLAN	The IP address for the server initially configured in Active mode.
Standby CLAN	The IP address for the server initially configured in Standby mode.
Managed IP	The virtual Managed IP (MIP) address that is used by the active server for campus resiliency. A MIP is used only when the active and standby servers are in the same subnet.
Trusted IP	The active and standby servers use the Trusted IP address to verify network connectivity. If the active server cannot communicate with the standby server it attempts to communicate with the Trusted IP address. If the active server cannot communicate with the Trusted IP address, if shadowing and switchover are enabled, then the active server stops processing contacts and shuts down. The standby server starts processing contacts if it cannot communicate with the active server but can communicate with the Trusted IP address. Avaya recommends that you use the IP address of some part of your IT infrastructure that is always available to respond to a ping request, as the Trusted IP address.
Local SMMC Port	The port number for System Management and Monitoring Component (SMMC) on the local (active) server. The default port number is 57012.
Remote SMMC Port	The port number for System Management and Monitoring Component (SMMC) on the remote (standby) server. The port number entered here must match the port number set on the remote (standby) server. The default port number is 57012.

Configuring email notification on the active server

Before you begin

- If anonymous users are allowed, a user name and password might not be required. Check with the Administrator of the email server for setup configuration.

About this task

If an automatic switchover occurs, the Business Continuity utility can send email messages to configured users at a defined interval.

The default email notification character set is US_ASCII. The following character sets are also supported:

- ISO-8859-1
- UTF-8
- UTF-16BE
- UTF-16LE
- UTF-16

Procedure

1. Log on to the active server.
2. On the **Apps** screen, in the **Avaya** section, select **Business Continuity**.
3. Expand **Configuration**.
4. Double-click **Notifications**.
5. Select the **Email** check box.
6. Type the **SMTP Server** name.
7. Type the **Username**.
8. Type the **Password**.
9. Type the **From Address**.
10. Type the **To Address** or **Addresses**.
11. Click **Save** to save the data.

Variable definitions

Name	Description
Email	Enables or disables email notifications.
SMTP Server	The SMTP Server name, which is automatically verified when saving the data.
Username	Email User log on name.
Password	Email User log on password.
Charset	Email character set to use.
From Address	Email address to send notifications from.
To Address	Email address to send notifications to.

Backing up the database on the active server

About this task

The active server is configured for Business Continuity. Now the standby server must be prepared for Business Continuity. Back up the active server to create a snapshot of the database which is then restored to the standby server. On the active server, all databases must be backed-up.

Important:

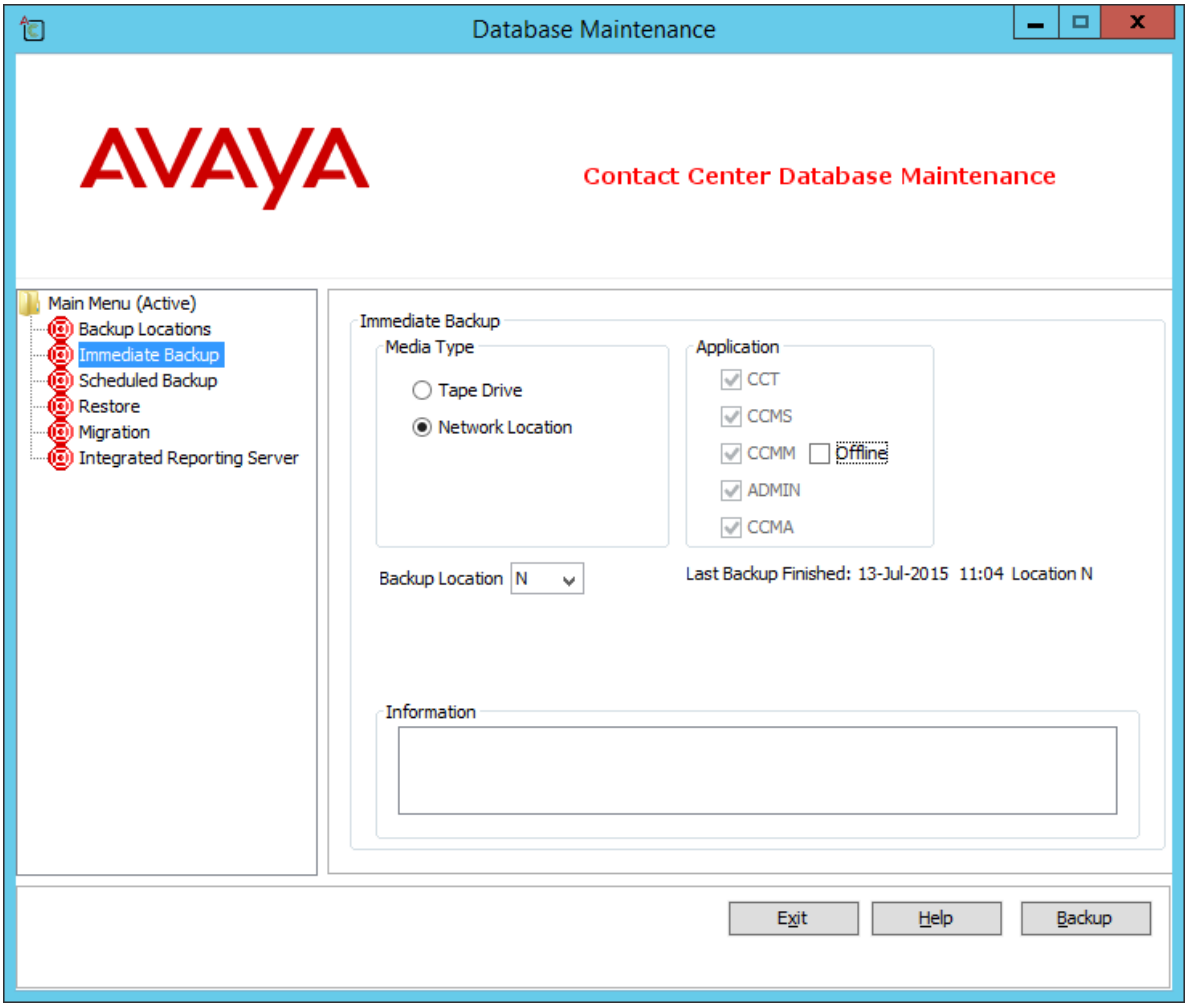
You must back up the active server database, restore it onto the standby server, and enable shadowing within 24 hours. If the difference in time between the active and standby server database content is greater than 24 hours then database shadowing does not work. If shadowing is stopped for more than 24 hours then you must backup the active server database and restore it onto the standby server before re-enabling shadowing. Ensure that the system clock time on the active and standby servers are synchronized.

Important:

Do not use a folder on the active or standby servers as the backup location.

Procedure

1. Log on to the active server.
2. On the **Apps** screen, in the **Avaya** section, select **Database Maintenance**.
3. Click **Backup Locations**.
4. Click **Create**.
5. From the **Driver Letter** list, select the network drive on which you want to store the CCMS, CCT, CCMM, ADMIN, and CCMA databases.
6. In the **UNC Path** box, type the location to store the backup, in the format \\Computer Name \Backup Location. This location must be a shared folder with correct permissions.
7. In the **User Name** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
8. In the **Password** box, type the Windows password.
9. Click **Save**.
10. In the left pane, click **Immediate Backup**.
11. In the **Media Type** section, select **Network Location**.
12. From the **Backup Location** list, select the network drive on which to store the backup.
13. Click **Backup**.



Restoring the database on the standby server

Before you begin

- Know the location of the backup database. Use the Database Maintenance utility to create a backup location on the standby server.
- Ensure no traffic is running on the standby server.
- Stop shadowing if shadowing is running on the standby server.
- Stop all Contact Center services, if services are running.
- Ensure the patch level on the standby server is the same as the active server.

Important:

Not all CCT data is stored in the database; therefore the following data must be configured on the standby server, CCT License, CCT Contact Management Framework, CCT SOA configuration (CCT Web Services), and CCT logging location.

Important:

You must restore all databases on an Avaya Contact Center Select server. Restoring only CCMS and not CCT, CCMM, CCMA, or ADMIN might leave an inconsistent server and Business Continuity cannot shadow data correctly.

Important:

Restoring the ADMIN database can change configuration of Backup locations on the standby server if the active server and standby server backup locations are different. Therefore, after you restore the ADMIN database, close and reopen the Database Maintenance utility.

About this task

Restore the database from the active server to the standby server to ensure the databases are consistent. The Database Maintenance utility can restore all application databases at once. Restore the data for the CCMS, CCMA, CCT, CCMM and ADMIN databases.

You must restore the CCMS, CCMA, CCT, CCMM and ADMIN database onto the standby server.

Important:

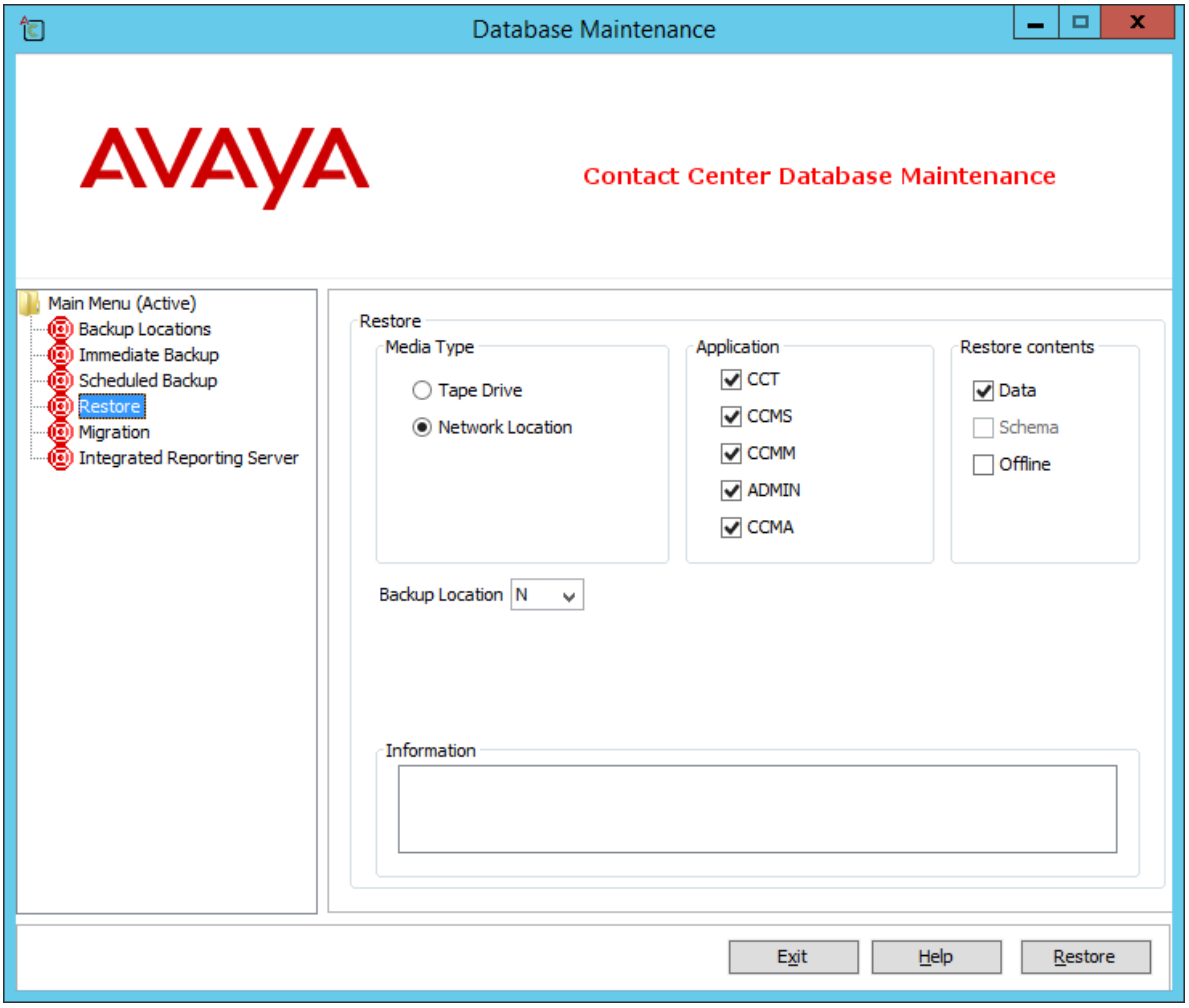
You must back up the active server database, restore it onto the standby server, and enable shadowing within 24 hours. If the difference in time between the active and standby server database content is greater than 24 hours then database shadowing does not work. If shadowing is stopped for more than 24 hours then you must backup the active server database and restore it onto the standby server before re-enabling shadowing. Ensure that the system clock time on the active and standby servers are synchronized.

Procedure

1. Log on to the standby server.
2. On the **Apps** screen, in the **Avaya** section, select **Database Maintenance**.
3. In the **Database Maintenance** dialog box, in the left pane, click **Restore**.
4. In the right pane, under **Media Type**, select the media type on which the backup is restored.
5. If the backup file is on the network drive, in the **Backup Location** list, select the backup location.
6. Under **Application**, select **CCMS**, **CCT**, **CCMM**, **ADMIN**, and **CCMA**.
7. Under **Restore contents**, select **Data**.

   Important:

   Do not select **Schema** or **Offline**.
8. Click **Restore**.



9. Use the **Information** field to monitor the progress of the restoration.
10. Click **Exit** to close the Database Maintenance utility.

Variable definitions

Name	Description
Application	The database and applications of Contact Center that you can back up.
Backup Location	The destination of the network disk. The values are configured in the Backup Locations.
Restore contents	The type of content that is stored in the database. Data is in the database.

Table continues…

Name	Description
	Schema is the data for the database structure, tables and procedures.
Media type	The type of media used for your backup file. You can use a network disk location or a tape drive. If you use a network disk location, you must configure a destination before you can back up the file.

Verifying server details on the standby server

Before you begin

- The active server databases are restored on to the standby server.

About this task

After you restore the active server database on to the standby server, verify that the standby server is configured correctly.

Procedure

1. Log on to the standby server.
2. On the **Apps** screen, in the **Avaya** section, select **Server Configuration**.
3. In the **Server Configuration** dialog box, click the **Local Settings** tab.
4. Verify the standby server local settings.
5. In the **Server Configuration** dialog box, click the **Licensing** tab.
6. Verify the standby server licensing details.
7. In the **Server Configuration** dialog box, under **SIP**, click the **Network Settings** tab.
8. Verify the standby server **SIP Network Settings** details.
9. In the **Server Configuration** dialog box, under **SIP**, click the **Local Subscriber** tab.
10. Verify the standby server **SIP Local Subscriber** details.
11. Click **Apply All**.
12. On the **Restart Required** message box, click **Yes**.
13. Click **Exit**.

Variable definitions

Name	Description
Avaya Server Subnet IP Address	The IP address of the Avaya Contact Center Select server.
IP Office Settings • IP Office Address • IP Office System Password • Port	The networking details for the IP Office voice platform.
Local SIP Subscriber • SIP Line Extension Number • Password	The IP Office SIP User Extension Number used by Avaya Contact Center Select to register for CTI call control and SIP session messaging.
Local SIP Subscriber • Domain Name	Information about the environment of the SIP-enabled contact center and how to identify the server within the network. Associated domain name for the SIP- enabled contact center.
MS Locale	Locale (including language and dialects) of the system environment.
Local Listening Ports	The SIP Communication protocol accepted by the system for incoming calls. TCP/UDP Port default is 5060 TLS Port default is 5061

Configuring the Campus standby Avaya Aura® Media Server

Before you begin

Ensure that Contact Center services are running.

About this task

After restoring the database from the active server to the standby server, the standby server configuration has the details of the active server Avaya Aura® Media Server. On the standby server, in Contact Center Manager Administration, change the Avaya Aura® Media Server details to use the standby server Avaya Aura® Media Server.

Procedure

1. Log on to the standby server.

2. Log on to the Contact Center Manager Administration application with administrative privileges.
3. On the **Launchpad**, click **Configuration**.
4. From the list of servers in the system tree, select the **CC** server.

   The CC server has the active server details.
5. Right-click on **CC**, and select **Edit Properties**.
6. In the **Server Name** box, type the name of the standby server.
7. In the **IP Address** box, ensure that the IP address of the standby server appears.
8. Click **Submit**.
9. From the list of servers in the system tree, expand the **CC** server.
10. Select the **Media Services and Routes** folder.
11. In the **Media Services and Routes** table, select **ACC_APP_ID**.
12. In the **Selected** box, select the active server Avaya Aura® Media Server, and click the left arrow (<).

    The server moves to the **Available** list.
13. Click **Submit**.
14. From the system tree, select the **Media Servers** folder under the **CC** server.
15. In the **Media Servers** list, select the row for the active server Avaya Aura® Media Server, and press Delete.
16. On the Confirm Delete dialog, click **Yes**.
17. In the **Server Name** box, type the name of the standby server Avaya Aura® Media Server.
18. In the **IP Address** box, type the IP address of the standby server Avaya Aura® Media Server.
19. In the **Port** box, type the port of the standby server Avaya Aura® Media Server.

    The port number must match the Avaya Aura® Media Server port number. The default is 5060.
20. Select **Master Content Store**.
21. Click any other row in the table to save your changes.
22. From the system tree, select the **Media Services and Routes** folder under the **CC** server.
23. In the **Media Services and Routes** table, select **ACC_APP_ID**.
24. In the **Available** box, select the standby server Avaya Aura® Media Server that you configured, and click the right arrow (>).

    The server moves to the **Selected** list.
25. Click **Submit**.

Configuring Business Continuity on the standby server

Before you begin

- The active server databases are restored on to the standby server.

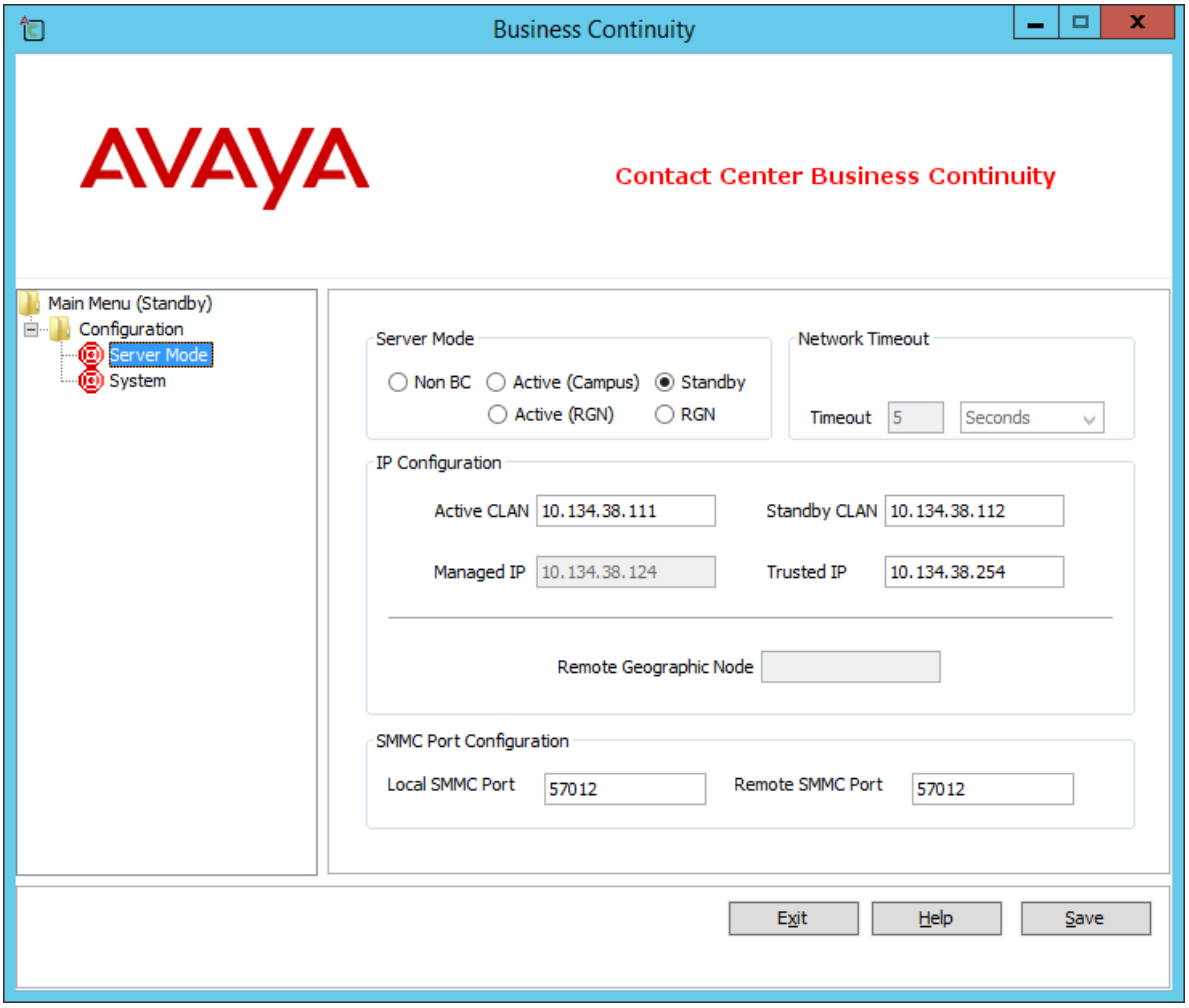
About this task

Configure Business Continuity on the standby server using the Business Continuity utility. The standby server shadows the active server and takes over processing if the active server fails.

You might need to restart the server to apply the new settings.

Procedure

1. Log on to the standby server.
2. On the **Apps** screen, in the **Avaya** section, select **Business Continuity**.
3. Expand **Configuration**.
4. Double-click **Server Mode**.
5. Under **Server Mode**, select **Standby**.
6. Under **IP Configuration**, in the **Active CLAN** box, type the IP address for the active server.
7. Under **IP Configuration,** in the **Standby CLAN** box, type the IP address for the standby server.
8. Under **IP Configuration**, in the **Managed IP** box, ensure the Managed IP address appears.
9. Under **IP Configuration**, in the **Trusted IP** box, type the IP address of a trusted server.
10. Under **SMMC Port Configuration**, in the **Remote SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the remote (active) server.
11. Under **SMMC Port Configuration**, in the **Local SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the local (standby) server.



12. Click **Save**.
13. If a **Business Continuity** message box appears requesting a server reboot, click **OK** to reboot the server.

Variable definitions

Name	Description
Active CLAN	The IP address for the server initially configured in active mode.
Standby CLAN	The IP address for the server initially configured in standby mode.
Managed IP	The virtual Managed IP (MIP) address that is used by the active server for campus resiliency.

Table continues…

Name	Description
	A MIP is used only when the active and standby servers are in the same subnet.
Trusted IP	The active and standby servers use the Trusted IP address to verify network connectivity. If the active server cannot communicate with the standby server it attempts to communicate with the Trusted IP address. If the active server cannot connect to the Trusted IP address on startup then no Contact Center services start on that server. If the active server cannot communicate with the Trusted IP address, if shadowing and switchover are enabled, then the active server stops processing contacts and shuts down. The standby server starts processing contacts if it cannot communicate with the active server but can communicate with the Trusted IP address. Avaya recommends that you use the IP address of some part of your IT infrastructure that is always available to respond to a ping request, as the Trusted IP address.
Local SMMC Port	The Network Management port number for System Management and Monitoring Component (SMMC) on the local (standby) server. The default port number is 57012.
Remote SMMC Port	The Network Management port number for System Management and Monitoring Component (SMMC) on the remote (active) server. The port number entered here must match the port number set on the remote (active) server. The default port number is 57012.

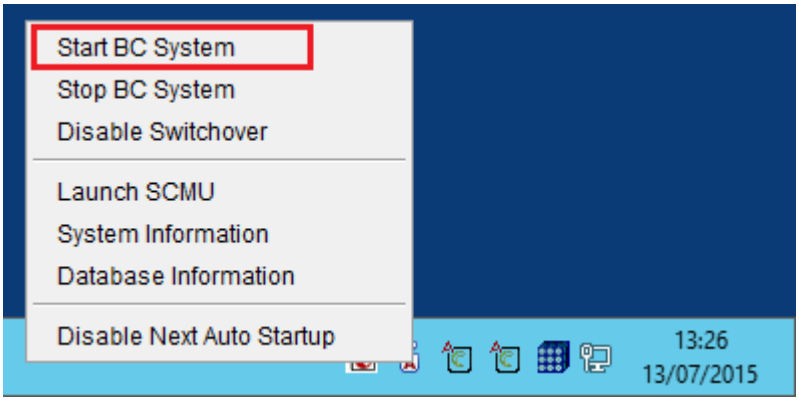
Starting the active server

About this task

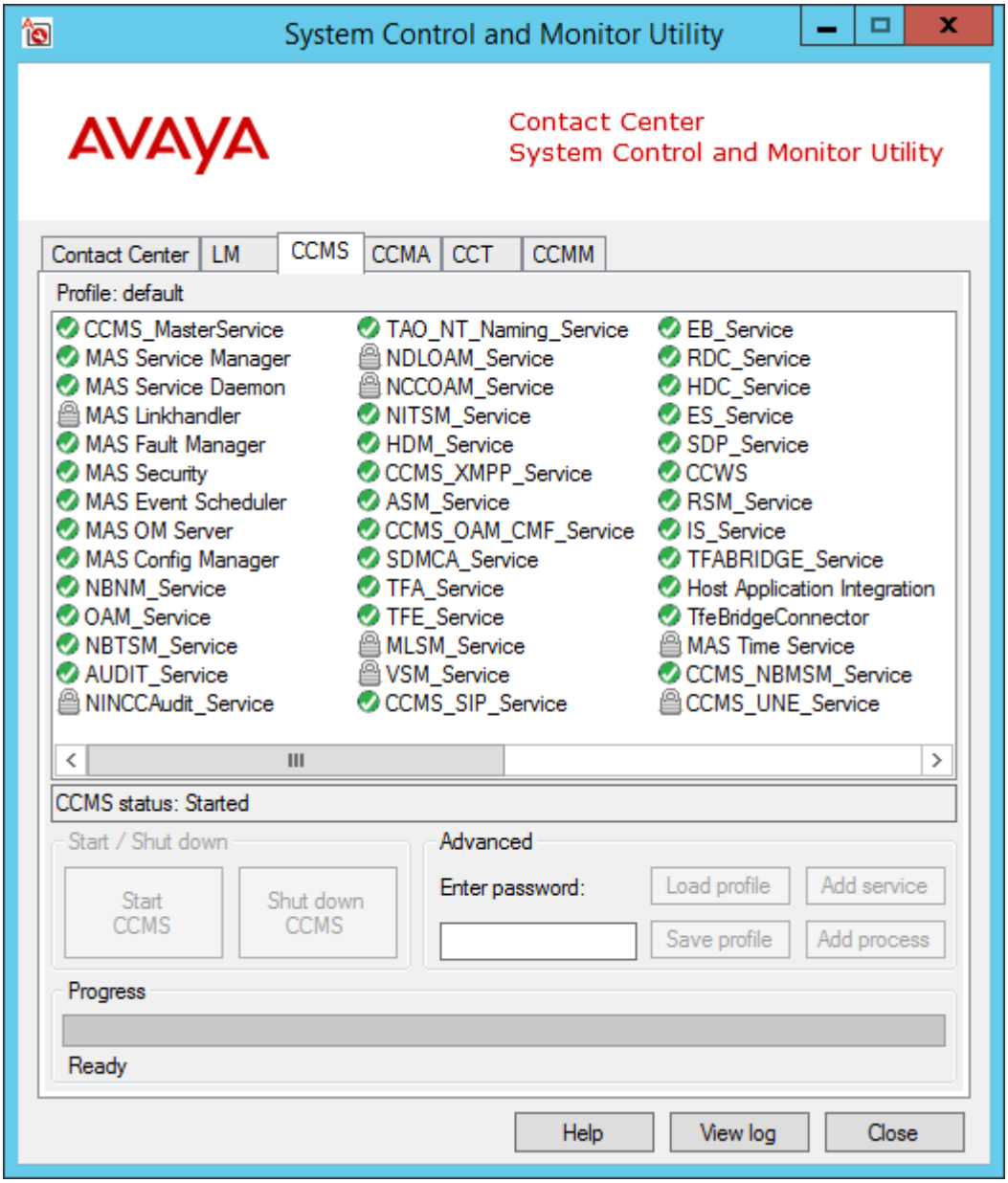
Start the active server using the System Management and Monitoring Component (SMMC) system tray. Starting the active server starts Contact Center applications and system processes.

Procedure

1. Log on to the active server.
2. On the Windows taskbar of the active server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Start BC System**. If the active server was previously rebooted, the system might already be started.



3. Using the System Control and Monitor Utility (SCMU), verify that the Contact Center services are running.



Starting shadowing on the standby server

About this task

Start shadowing on the standby server using the System Management and Monitoring Component (SMMC) system tray.

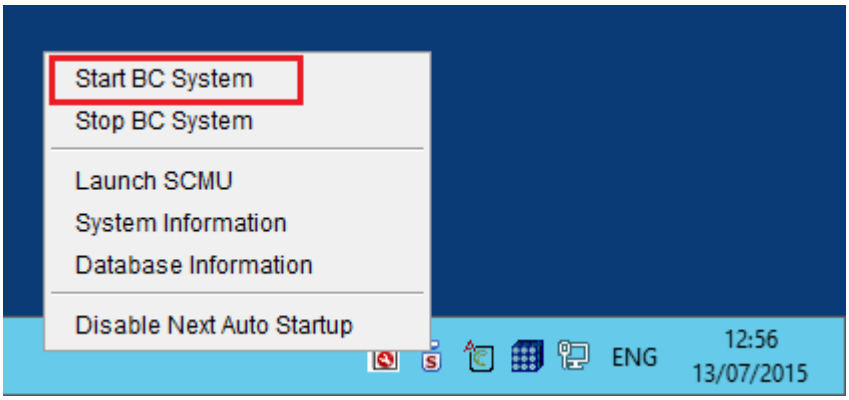
The standby server shadows the active server, maintaining a near real-time local copy of the Contact Center applications and Administration databases. Therefore, the standby server is configured with the most recent data and it can take over from the active server if necessary.

Important:

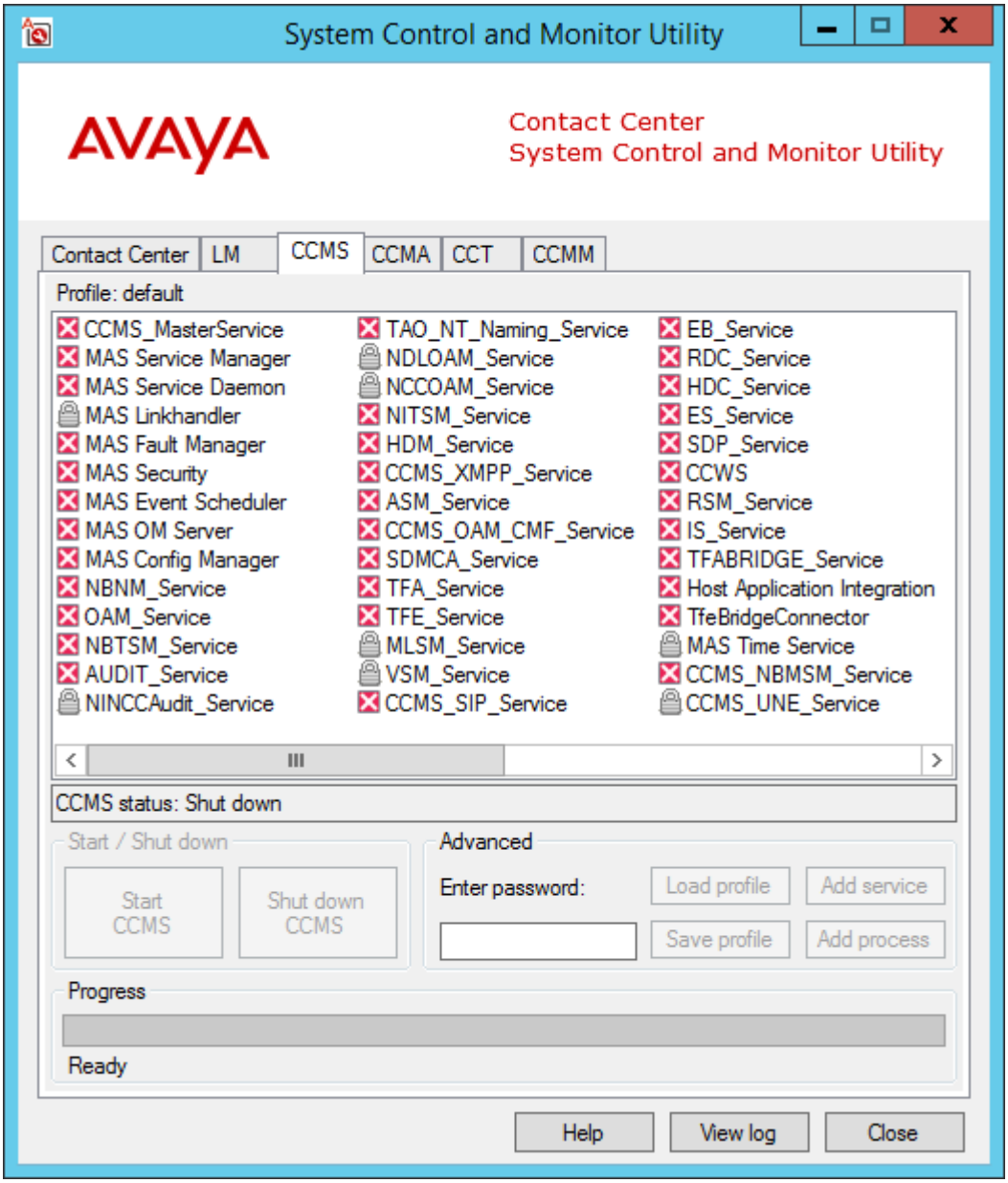
You must backup the active server database, restore it onto the standby server, and enable shadowing within 24 hours. If the difference in time between the active and standby server database content is greater than 24 hours then database shadowing does not work. If shadowing is stopped for more than 24 hours then you must backup the active server database and restore it onto the standby server before re-enabling shadowing. Ensure that the system clock time on the active and standby servers are synchronized.

Procedure

1. Log on to the standby server.
2. On the Windows taskbar of the standby server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Start BC System**.



3. On the **Apps** screen, in the **Avaya** section, select **System Control and Monitor Utility**.
4. Verify that the Contact Center services are not running using the SCMU. Check that the Contact Center services are stopped.



Verifying Business Continuity is running

About this task

Verify that the standby server is shadowing the active server using the Business Continuity utility. The System dialog box of the Business Continuity utility displays system information about the active and the standby servers.

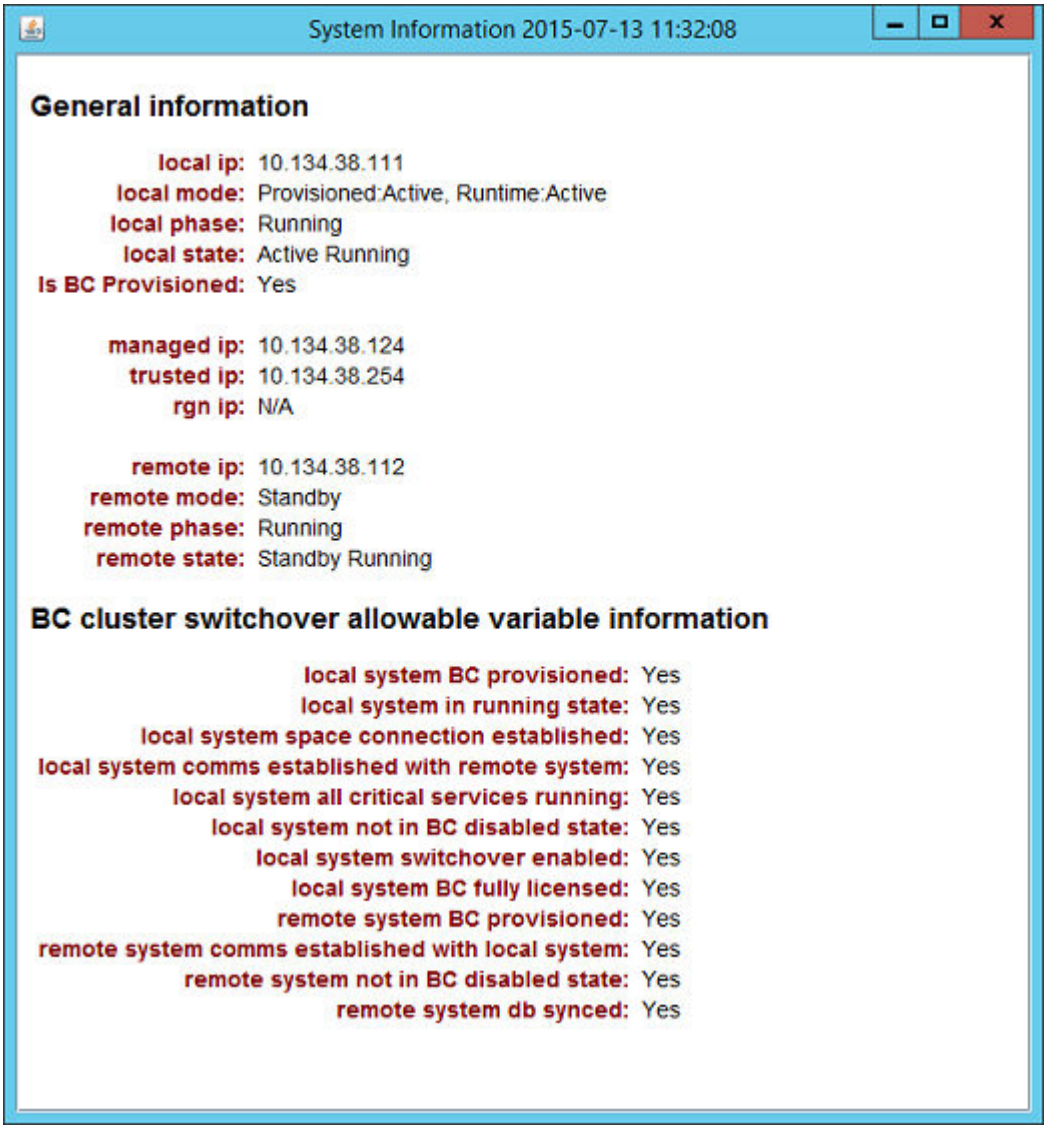
The dialog box displays the followings information categories:

- Computer name and operating system version
- Server mode
- Server configuration type
- Port information
- Remote server connection status
- Remote server port information
- License information
- Databases shadowed
- Time of last record shadowed
- Database namespaces
- Local and remote information on system status, switchover, shadowing and network
- CC Application install information
- Database space and journaling information
- Database processes information

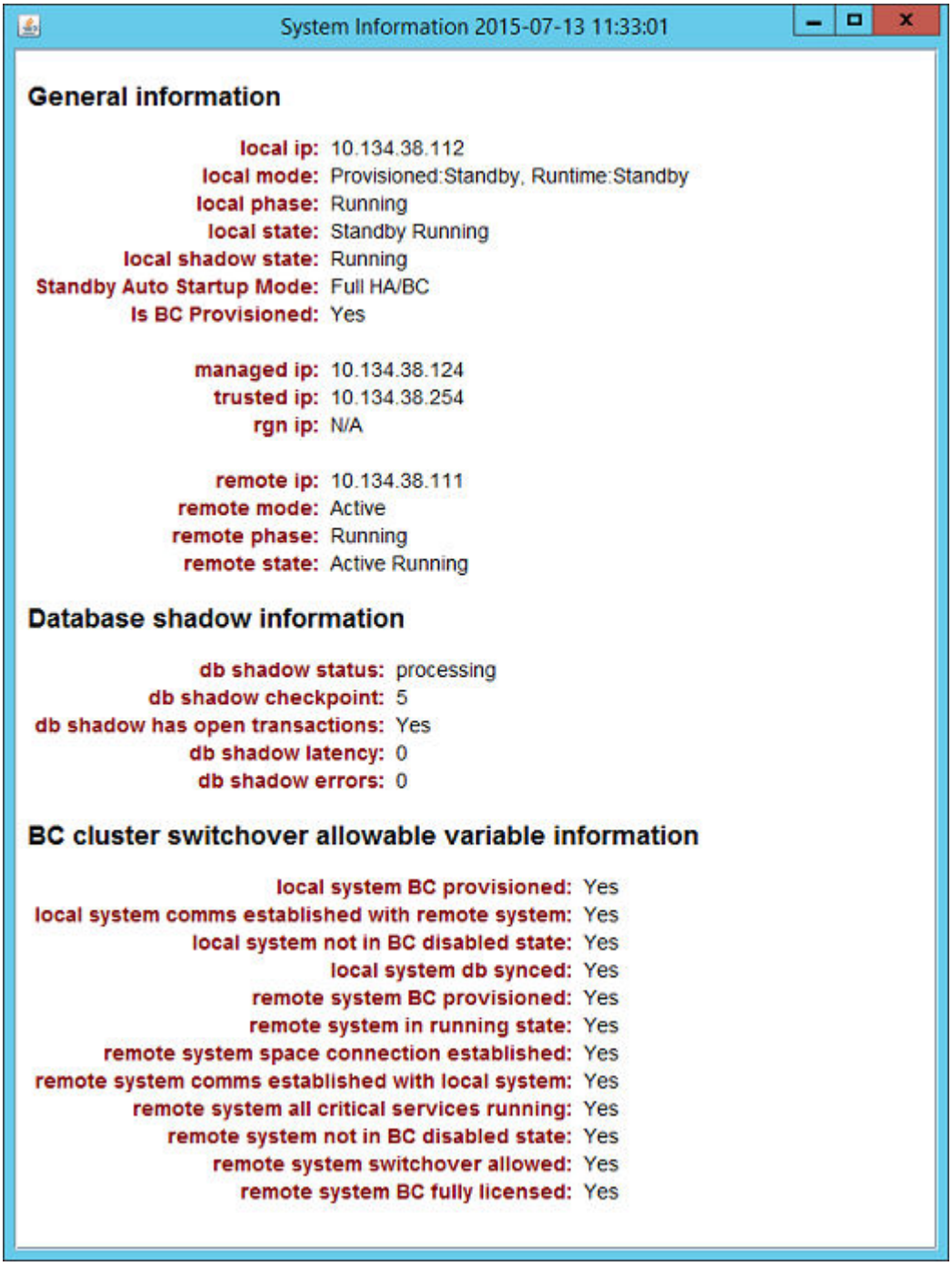
Procedure

1. Log on to the active server.
2. On the **Apps** screen, in the **Avaya** section, select **Business Continuity**.
3. In the left pane, expand **Configuration**.
4. Select **System**.
5. Select **Get System Configuration**.

   The most recent system information appears.
6. On to the active server, on the Windows taskbar, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **System Information**. The System Information window displays the current status of Business Continuity on the active server.



7. On to the standby server, on the Windows taskbar, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **System Information**. The System Information window displays the current status of Business Continuity on the standby server.


System Information 2015-07-13 11:33:01
General information
local ip: 10.134.38.112
local mode: Provisioned:Standby, Runtime:Standby
local phase: Running
local state: Standby Running
local shadow state: Running
Standby Auto Startup Mode: Full HA/BC
Is BC Provisioned: Yes
managed ip: 10.134.38.124
trusted ip: 10.134.38.254
rgn ip: N/A
remote ip: 10.134.38.111
remote mode: Active
remote phase: Running
remote state: Active Running
Database shadow information
db shadow status: processing
db shadow checkpoint: 5
db shadow has open transactions: Yes
db shadow latency: 0
db shadow errors: 0
BC cluster switchover allowable variable information
local system BC provisioned: Yes
local system comms established with remote system: Yes
local system not in BC disabled state: Yes
local system db synced: Yes
remote system BC provisioned: Yes
remote system in running state: Yes
remote system space connection established: Yes
remote system comms established with local system: Yes
remote system all critical services running: Yes
remote system not in BC disabled state: Yes
remote system switchover allowed: Yes
remote system BC fully licensed: Yes

Example

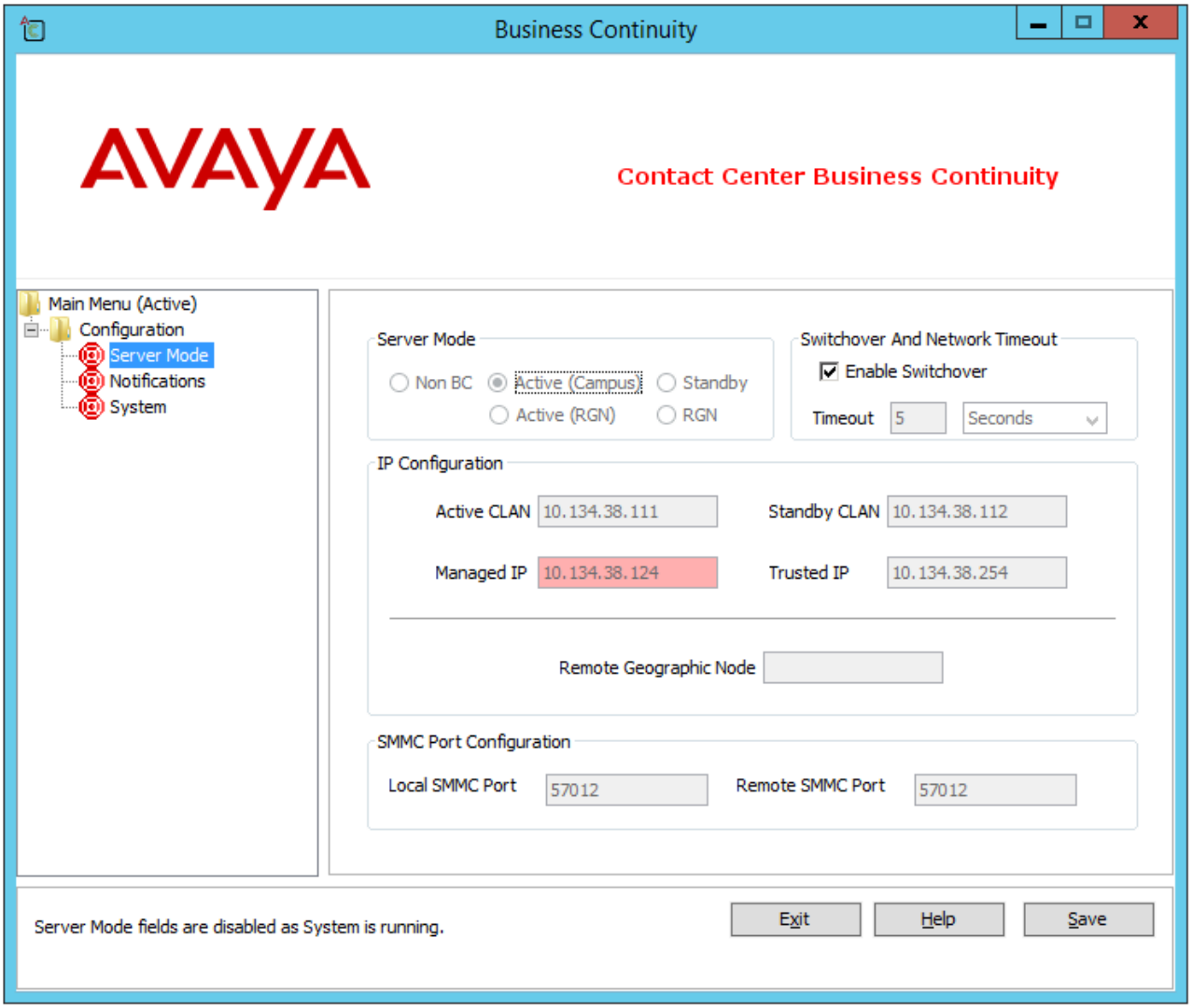


Figure 16: A screenshot showing an active server with the Business Continuity system running

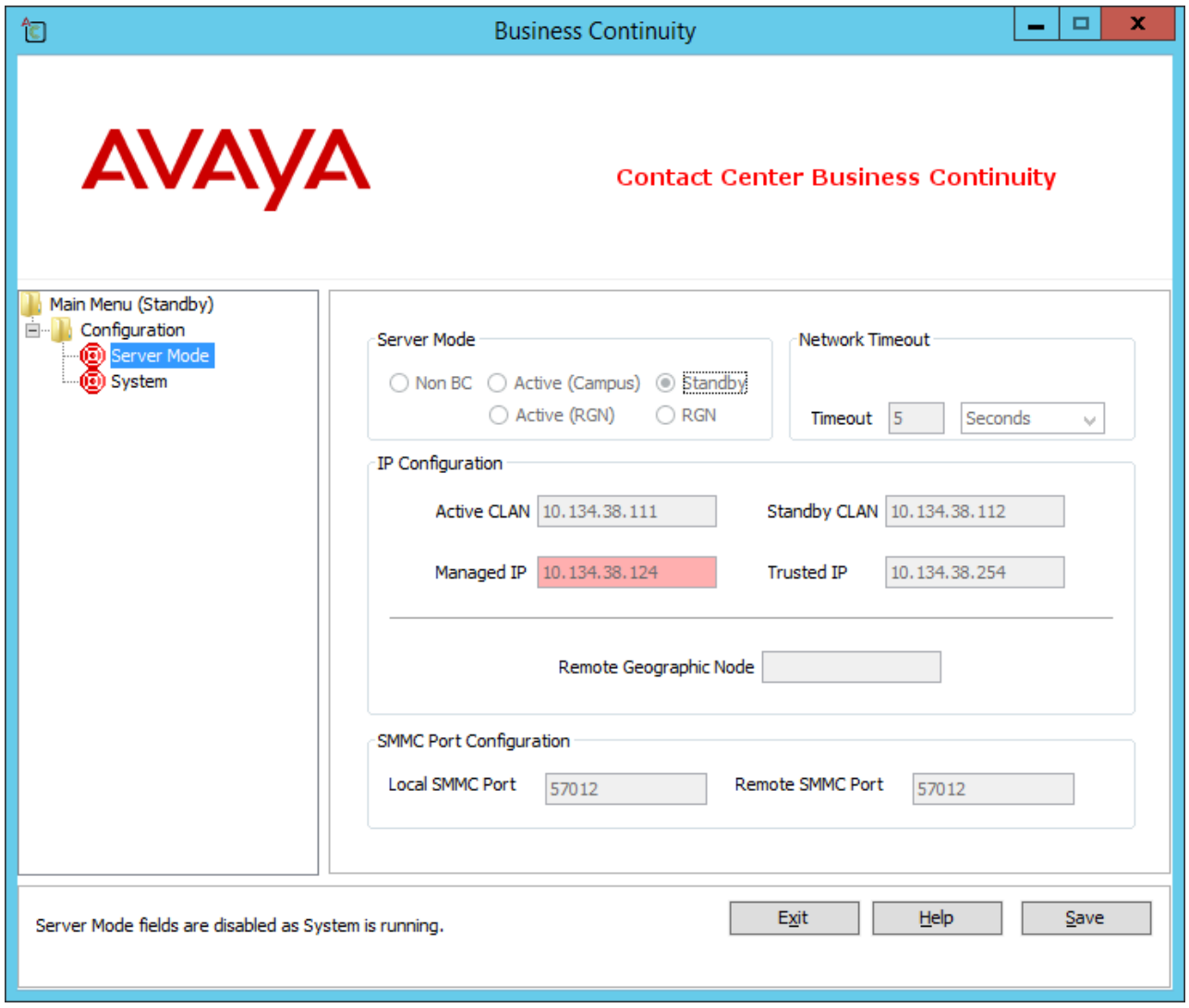


Figure 17: A screenshot showing an active server with the Business Continuity system running

Note the **Server Mode fields are disabled as System is running** notice on the Business Continuity user interface.

On the standby server, on the Windows taskbar, right-click on the System Management and Monitoring Component (SMMC) system tray, note that the **Manual Switchover** option is now available. This confirms that database shadowing is working and that switchovers are enabled.

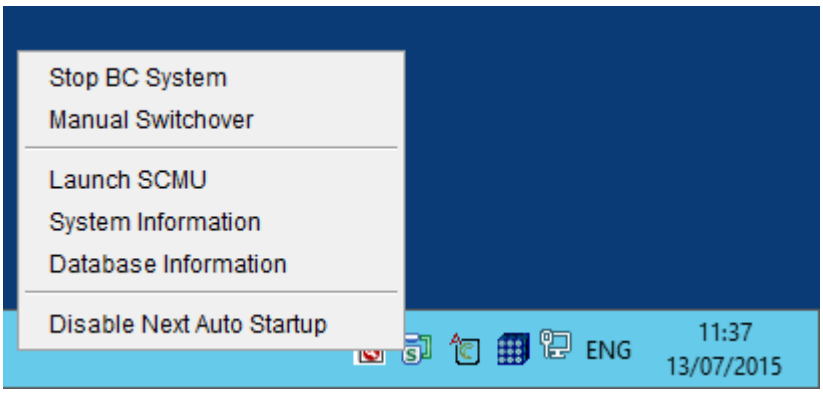


Figure 18: A screenshot of the SMMC system tray with the Manual Switchover option available

Changing server details in Contact Center Manager Administration

About this task

In Contact Center Manager Administration, change the Contact Center Manager Server, Communication Control Toolkit and Contact Center Multimedia details to use the Business Continuity Managed IP address and Managed name details.

The Business Continuity Managed IP address and Managed name details entered here must match those configured in the hosts file.

Procedure

1. Log on to the active server.
2. Log on to the Contact Center Manager Administration application with administrative privileges.
3. On the **Launchpad**, click **Configuration**.
4. From the list of servers in the system tree, right-click on **CC**, and select **Edit Properties**.
5. In the **Server Name** box, type the Business Continuity Managed name of the active server.
6. In the **IP Address** box, ensure this is configured with the Business Continuity Managed IP address of the active server.
7. In the **Display Name** box, type the name of Contact Center Manager Server as you want it to appear in the system tree of Contact Center Administration.
8. Click **Submit**.
9. From the list of servers in the system tree, right-click on CCT, and select **Edit Properties**.
10. In the **Server Name** box, type the Business Continuity Managed name of the active server.

11. In the **IP Address** box, ensure this is configured with the Business Continuity Managed IP address of the active server.
12. In the **Display Name** box, type the name of Communication Control Toolkit as you want it to appear in the system tree of Contact Center Administration.
13. Click **Submit**.
14. From the list of servers in the system tree, right-click on CCMM, and select **Edit Properties**.
15. In the **Server Name** box, type the Business Continuity Managed name of the active server.
16. In the **IP Address** box, ensure this is configured with the Business Continuity Managed IP address of the active server.
17. In the **Display Name** box, type the name of Contact Center Multimedia as you want it to appear in the system tree of Contact Center Administration.
18. Click **Submit**.

Using the Contact Center Manager Administration managed name

Before you begin

- Configure Business Continuity on the active and standby servers.
- Change the server details in CCMA.
- Know the user ID and password to log on to the CCMA.

About this task

Use the Business Continuity managed name of Contact Center Manager Administration to access the CCMA application. When the Contact Center Business Continuity feature is configured and enabled, re-direct all Contact Center Manager Administration client Web browsers to use the managed server name of the server CCMA is installed on.

If you have a Business Continuity campus solution Avaya recommends that you log on to the CCMA Web client using the managed name of the active server. If an active application or server fails, the CCMA client Web browser continues to use the managed name and you can continue working without interruption.

Important:

Do not type the real or Managed IP address in the Address box. Using an IP address results in problems with Scripting, Historical Reporting, Configuration, Contact Center Management, and Access and Partition Management.

Procedure

1. Start Internet Explorer.

2. In the **Address** box, type the URL of the server CCMA is installed on.

   The default URL is https://<*managed name*>; where <*managed name*> is the managed name of the Business Continuity server pair.
3. In the **User ID** box, type your user ID.
4. In the **Password** box, type your password.
5. Click **Login**.

Uninstalling Agent Desktop client software

Before you begin

Ensure that the Agent that uses the Agent Desktop computer is logged off.

About this task

Uninstall the existing Agent Desktop client software from the client computers. In solutions using Business Continuity, you must uninstall the Agent Desktop client software downloaded directly from the original Avaya Contact Center Select server. In Business Continuity solutions you must download the Agent Desktop client software from the Managed IP or Managed name of the Avaya Contact Center Select Business Continuity pair. This ensures Agent Desktop Business Continuity support and future software updates.

Procedure

1. Log on to the Agent Desktop computer.
2. Click **Start** > **Control Panel** > **Add or Remove Programs**.
3. From the list of **Currently installed programs**, select **Avaya Agent Desktop**.
4. Click **Change/Remove**.
5. On the **Avaya Agent Desktop** dialog, select **Remove the application from this computer**.
6. Click **OK**.
7. Follow the on-screen instructions to uninstall Agent Desktop software.
8. Repeat this procedure for all the Agent Desktop client computers.

Configuring the managed name for Agent Desktop

About this task

Configure the Agent Desktop installer on the Avaya Contact Center Select active server to use the Business Continuity managed name.

Procedure

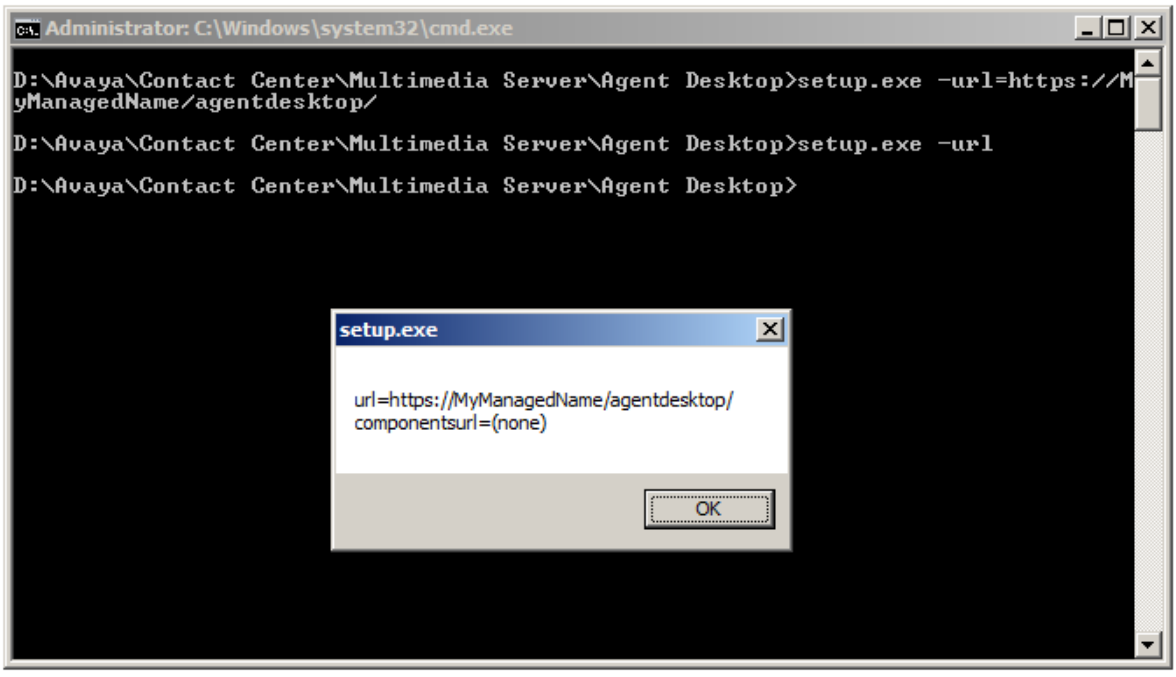
1. Log on to the Avaya Contact Center Select active server as the administrator.
2. Open a command prompt window and navigate to the Agent Desktop folder:

   `<Installed Drive>:\Avaya\Contact Center\Multimedia Server\Agent Desktop\`
3. Enter `setup.exe -url`

   Make a note of the existing URL value.
4. Enter `setup.exe -url=https://ACCS_SERVER_MANAGED_NAME/agentdesktop/`

   Where ACCS_SERVER_MANAGED_NAME is the managed name of your Avaya Contact Center Select Business Continuity pair.
5. Enter `setup.exe -url`
6. Confirm that the Agent Desktop installer now uses your Avaya Contact Center Select Business Continuity pair managed name.

   For example:



Installing Agent Desktop client software

Before you begin

- Ensure that Avaya Contact Center Select Business Continuity is configured.
- Know the Managed IP address or managed name of the Avaya Contact Center Select Business Continuity pair. For more information about the Managed IP address to use, see Configuring Business Continuity on the Active Server on page 84.

About this task

Install Agent Desktop software to handle Avaya Contact Center Select customer contacts.

Procedure

1. Log on to the client computer.
2. In Windows Explorer or Internet Explorer, enter the HTTP address (URL) provided by your Domain Administrator. The URL format is http:/<Avaya Contact Center Select Managed IP address>/agentdesktop. For example, type

   http://10.134.38.124/agentdesktop
3. Click **Launch**.
4. Follow the on-screen instructions to download and install the Agent Desktop software.
5. Repeat this procedure for each client computer.

Verifying Campus Business Continuity switchovers

Before you begin

- Configure Campus Business Continuity on the active and standby Avaya Contact Center Select servers.
- To support Business Continuity resiliency, the Avaya Contact Center Select agents must each have an associated Windows domain user account in the same Windows domain as the active and standby servers. Create Avaya Contact Center Select agents with associated Windows domain accounts. Log these domain-enabled agents in to Agent Desktop. Use these domain-enabled Avaya Contact Center Select agents to verify Business Continuity resiliency.

About this task

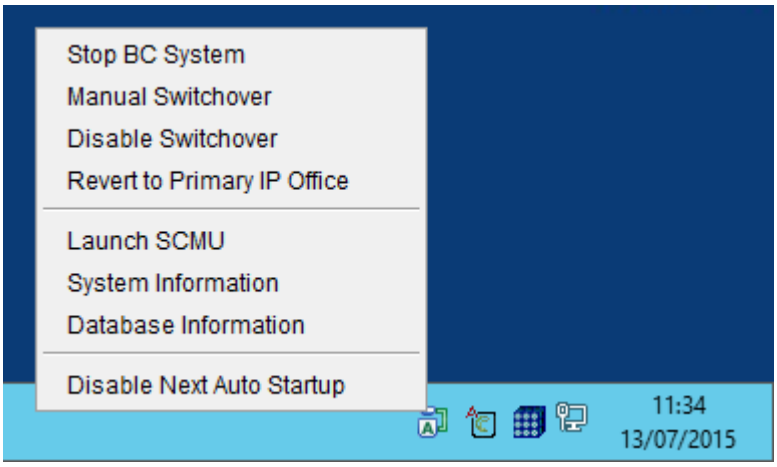
Verify the Campus Business Continuity feature and infrastructure by making a manual switchover from the active Avaya Contact Center Select server to the standby Avaya Contact Center Select server.

Note:

Verify Avaya Contact Center Select Campus Business Continuity before placing the system into production.

Procedure

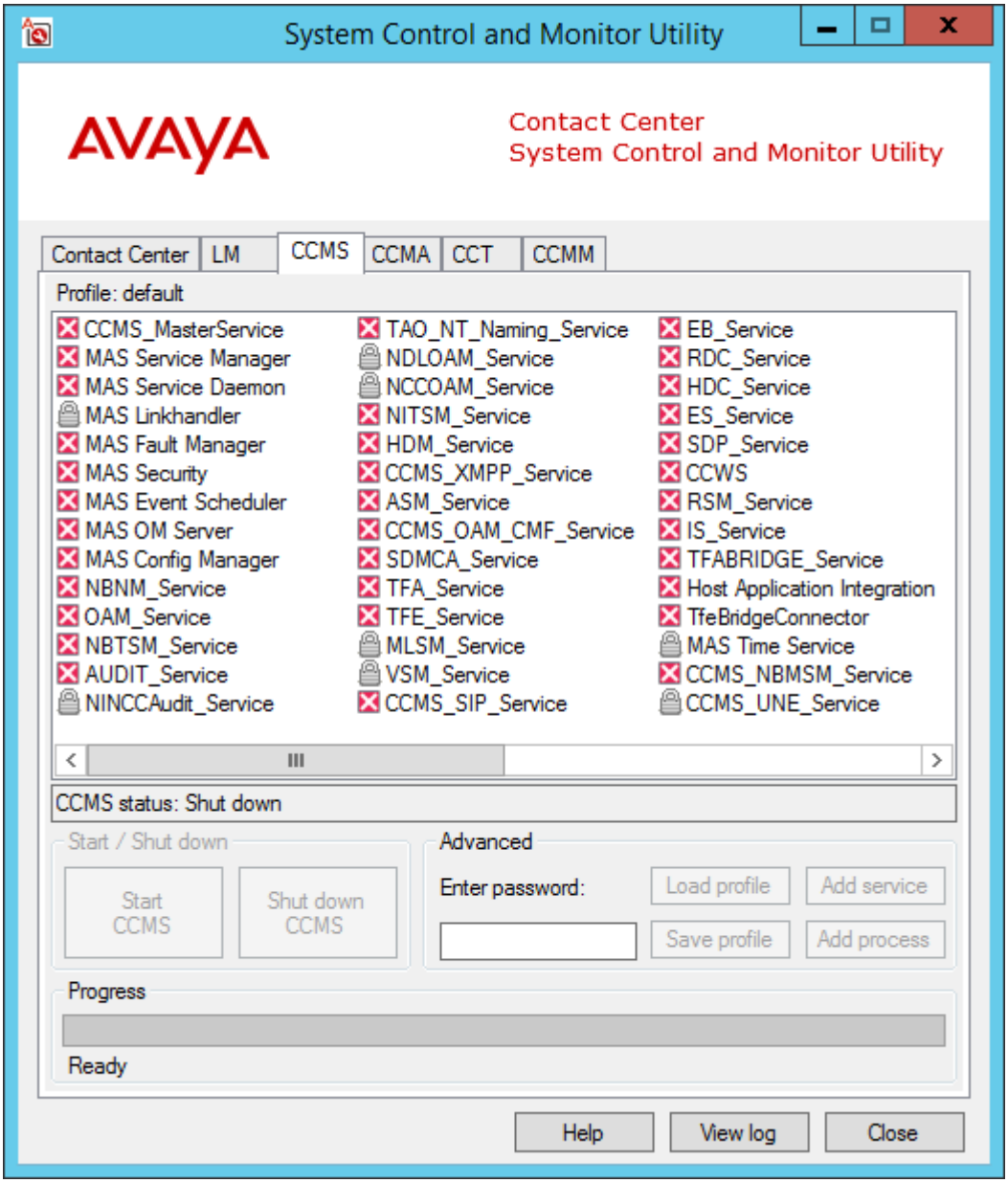
1. Log on to the current active Avaya Contact Center Select (ACCS) server.
2. On the Windows taskbar, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Manual Switchover**.



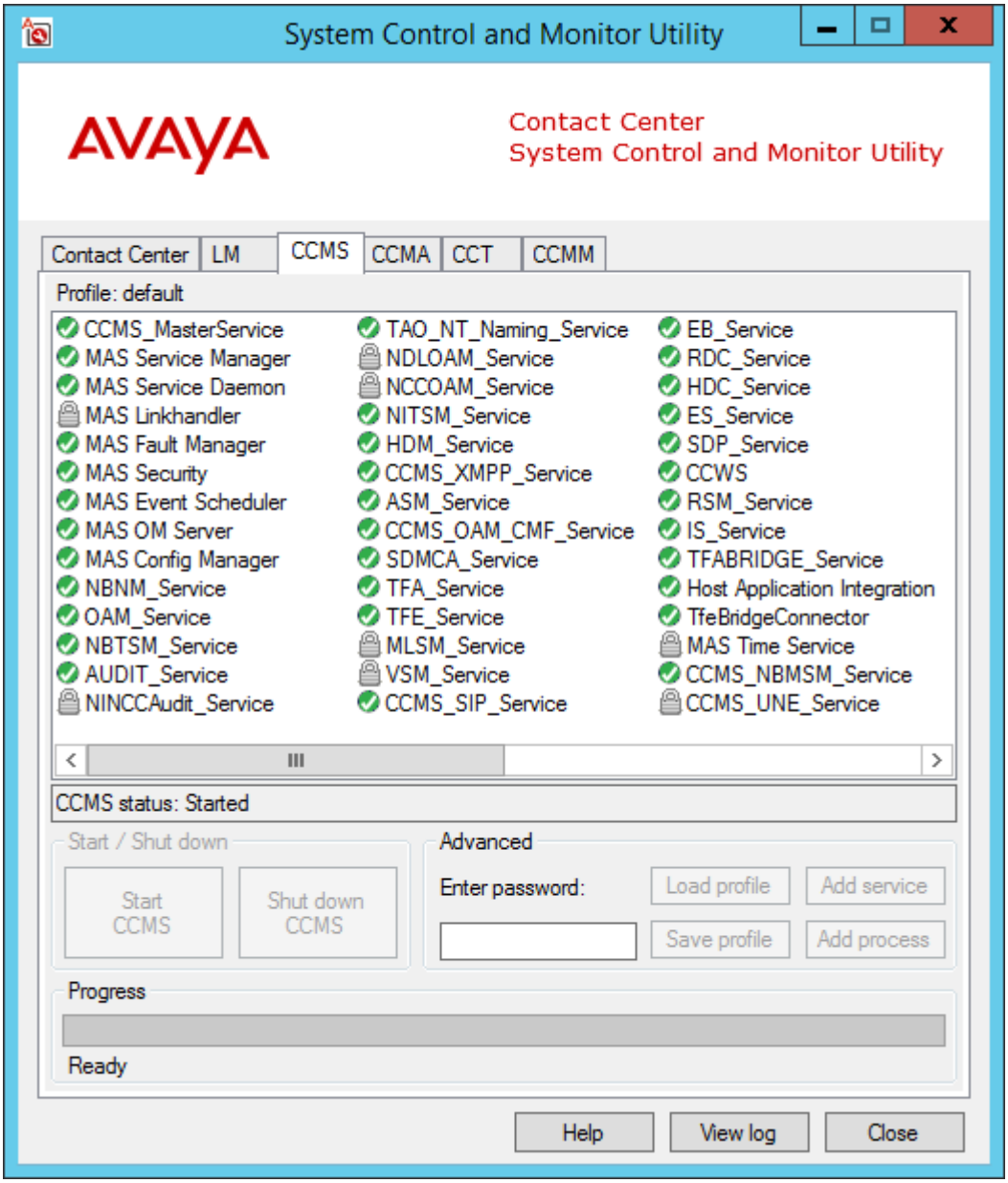
The Campus Business Continuity system begins to transition Customer contact processing from the currently active ACCS server to the current standby server. When the transition is complete, the current standby server becomes the active server.

It typically takes a few minutes to switch over to the standby server. During this time, all active customer contacts are dropped.

3. Using System Control and Monitor Utility (SCMU), verify that the Contact Center services are stopping on the active server. Verify that the Contact Center services on the active server stop running.



4. Using the System Control and Monitor Utility (SCMU), verify that the Contact Center services are starting on the standby server. Verify that the Contact Center services on the standby server start running.



5. When the Contact Center services are running on the standby server, make a test call into the Contact Center. Verify that the call is treated and routed to an agent. Verify that the agent has full call control.
6. If your solution supports multimedia contacts, send a test email to one of the configured mailboxes. Verify that Avaya Contact Center Select receives the email and that it is routed to an agent for processing. Verify that the agent has full multimedia contact control.
7. If you configured Business Continuity email notifications, verify that you received the notification email. For more information, see Configuring email notification on the active server on page 87.

8. After verifying a Campus Business Continuity switchover, the Avaya Contact Center Select system is no longer resilient. The current standby server is not shadowing the current active server. To make the Avaya Contact Center Select system resilient again, reinstate Campus Business Continuity. For more information, see Reinstating Campus Business Continuity after a switchover on page 116.

Reinstating Campus Business Continuity after a switchover

About this task

In a Campus Business Continuity solution, if the active server fails or if a manual switchover is triggered, the standby server starts processing contacts. The initially active server is now stopped, and the Business Continuity - Enable Switchover option is disabled. The standby server becomes the active server and it continues to process contacts. The Business Continuity email notification feature sends an email to the Contact Center Administrator informing them about the switchover. The active server has no corresponding standby server at this point, and the solution is no longer resilient.

When the root cause of the failure has been addressed the contact center administrator can reinstate campus Business Continuity resiliency using the following steps.

Procedure

1. On the currently active running server (previous standby server), run the Database Maintenance utility and back up all database applications to a network share. You do not need to stop the active server to back up the applications.
2. On the currently stopped server (previous active server), stop Business Continuity shadowing.
3. Use the Database Maintenance utility to restore the Contact Center databases from the network share.
4. Ensure that the currently stopped server (previous active server) is configured to use the local Avaya Aura® Media Server. See Configuring the Campus standby Avaya Aura Media Server on page 94.
5. On the Windows taskbar of the active server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Start BC System**.
6. On the Windows taskbar of the active server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Enable Switchover**.
7. On the Windows taskbar of the standby server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Start BC System**
8. If your Business Continuity solution supports multimedia contacts, on the active ACCS server, restart the CCMM Multimedia Contact Manager service.

Verifying IP Office voice platform resilience

Before you begin

- If your Avaya Contact Center Select Business Continuity solution is not using an IP Office resilient system, skip this procedure. If your solution is using an IP Office resilient system, ensure IP Office resilience is configured.

About this task

Verify that when the IP Office Primary Server fails, Avaya Contact Center Select transitions call control from the IP Office Primary Server to the IP Office Secondary Server. If the IP Office Primary Server fails or is stopped, the IP Office Secondary Server continues to process voice calls.

On startup, the active Avaya Contact Center Select (ACCS) server registers with the IP Office Primary Server. If the active ACCS server is not able to communicate and register with the IP Office Primary Server, after a configurable delay, the active ACCS server attempts to register with the IP Office Secondary Server. You can configure this *Registration Switchover Delay* using the ACCS Server Configuration utility.

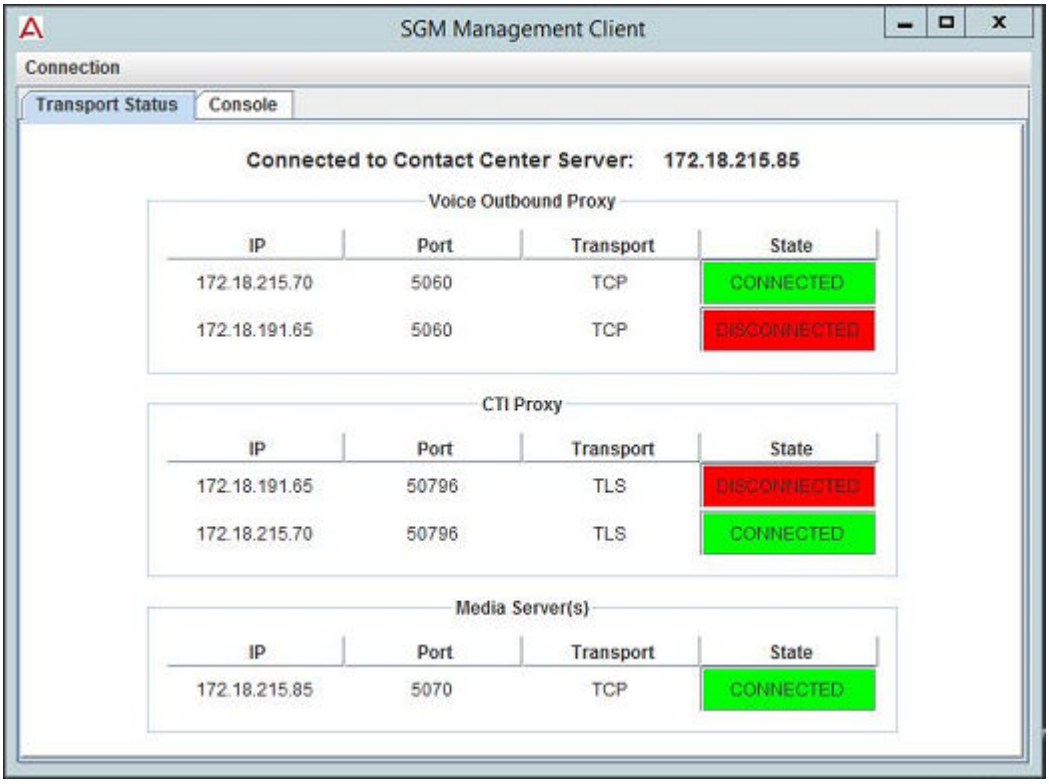
If your Avaya Contact Center Select solution is not using IP Office resiliency, skip this procedure.

Note:

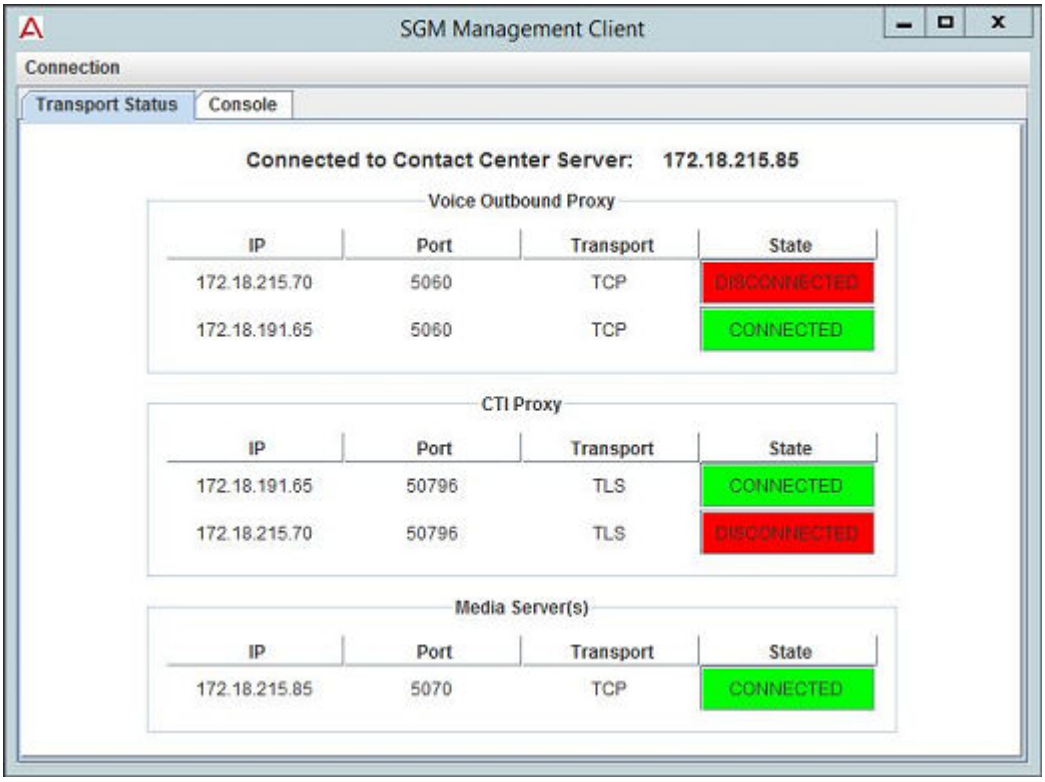
Verify that your IP Office voice platform is resilient before placing the system into production.

Procedure

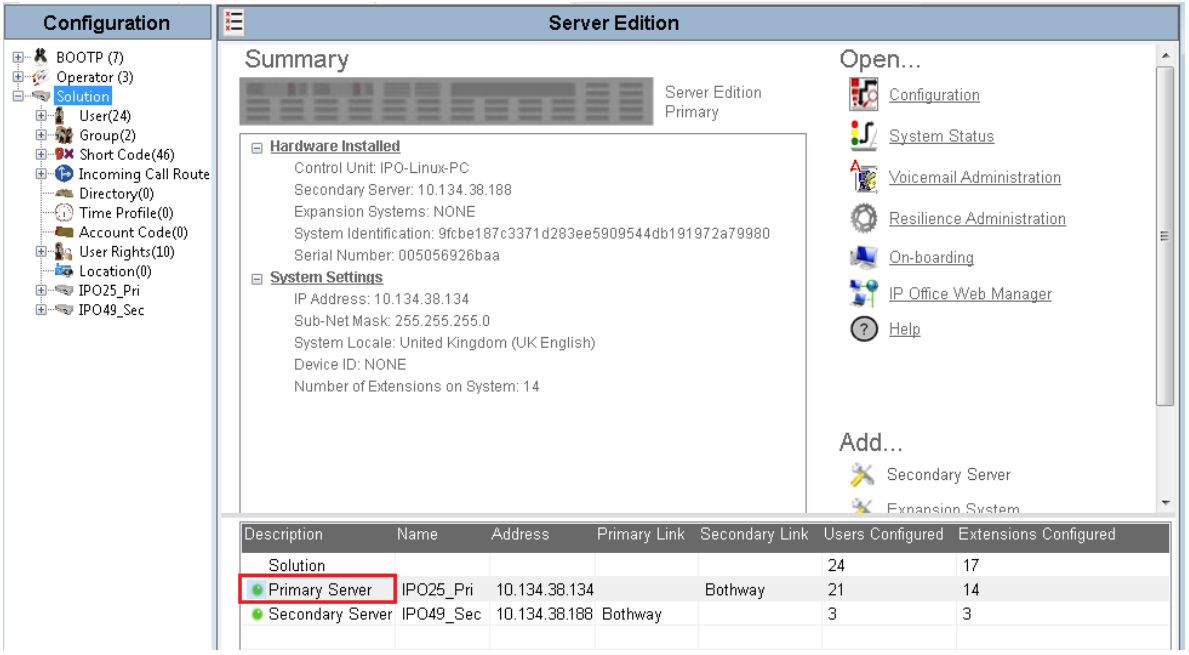
1. Log on to the active ACCS server.
2. On the **Apps** screen, in the **Avaya** section, select **SIP Gateway Management Client**.
3. Verify that the active ACCS server is registered with the IP Office Primary Server.



4. Disconnect the network cable from the IP Office Primary Server.
5. Verify that ACCS agent H.323 phones register with the IP Office Secondary Server.
6. Verify that the IP Office Secondary Server routes customer calls to ACCS and that ACCS agents can process those customer calls. At this time, the IP Office system is no longer resilient. The IP Office Primary Server is offline and the IP Office Secondary Server is processing ACCS contacts. The active ACCS server is now registered with the IP Office Secondary Server.

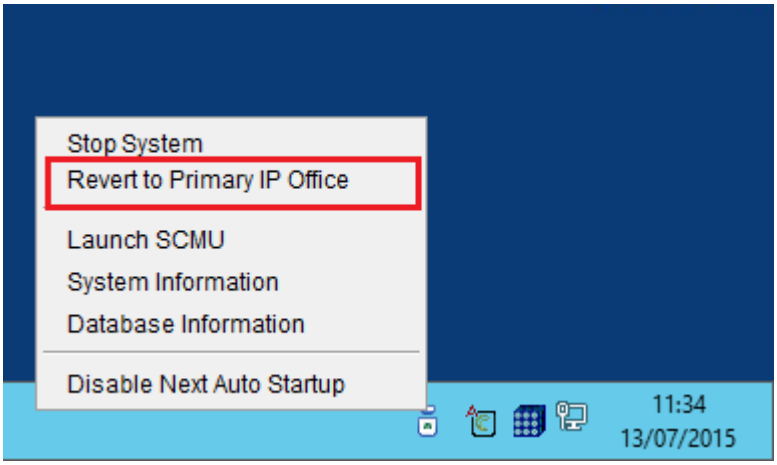


7. Reconnect the network cable to the IP Office Primary Server.
8. Wait for the IP Office Primary Server to start up. Using IP Office Manager, the traffic light icon to the left of the IP Office Primary Server is green when it is ready.

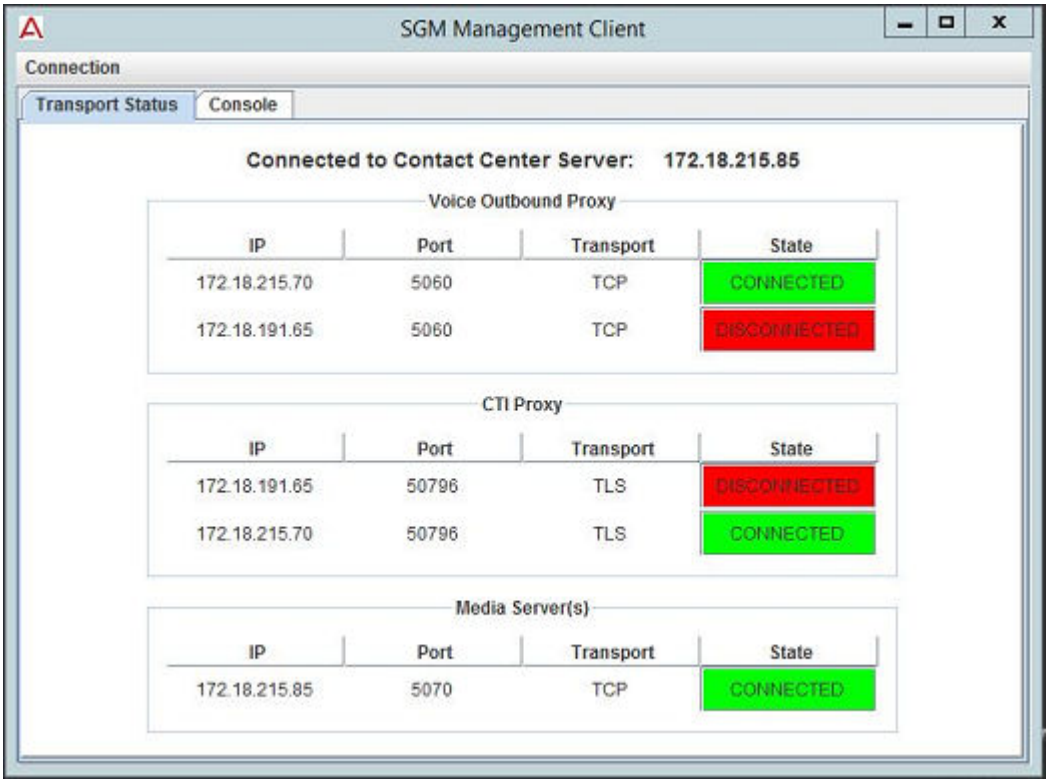


9. Rehome the agent H.323 phones to the IP Office Primary Server.

10. On the ACCS active server, on the Windows taskbar, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Revert to Primary IP Office**.



The ACCS active server registers with the IP Office Primary Server.



11. The IP Office system is now resilient again. The ACCS active server is registered with the IP Office Primary Server.

Chapter 8: Geographic Business Continuity configuration

This section describes how to configure Avaya Contact Center Select (ACCS) Geographic Business Continuity.

The Remote Geographic Node (RGN) ACCS must match the active ACCS:

- If the active ACCS server is a Hardware Appliance, the RGN ACCS server must also be a Hardware Appliance.
- If the active ACCS is a Software Appliance, the RGN ACCS must also be a Software Appliance.
- If the active ACCS is a single-server DVD deployment, the RGN ACCS must also be a single-server DVD deployment. The RGN server must have the exact same hard disk partitions, the same amount of memory and the same CPU type. The RGN server must have the Contact Center software installed on the same partitions as the active server.
- The active and RGN servers must have the same ACCS patch level and the same operating system updates.

Complete all of the procedures in this section in sequential order.

Geographic Business Continuity prerequisites

- Ensure your network and solution hardware meets the requirements for Business Continuity. For more information, see *Avaya Contact Center Select Solution Description*.
- Ensure that your Avaya Contact Center Select solution is using a Windows domain. To support Business Continuity resiliency, the Avaya Contact Center Select agents must each have an associated Windows domain user account in the same Windows domain as the active and RGN servers. Create Avaya Contact Center Select agents with associated Windows domain accounts.
- Obtain Avaya Contact Center Select standby server licenses.
- Ensure the active and Remote Geographic Node servers meet the requirements for Business Continuity. For more information, see *Avaya Contact Center Select Solution Description*.

- Install the Avaya Contact Center Select active and Remote Geographic Node (RGN) servers. For more information about installing Avaya Contact Center Select, see one of the following:
  - *Deploying Avaya Contact Center Select DVD*
  - *Deploying Avaya Contact Center Select Software Appliance*
  - *Deploying Avaya Contact Center Select Hardware Appliance*
- Ensure your IP Office system is configured, enabled, and licensed.

Adding the server to a domain

Before you begin

- Ensure that you have domain administrator privileges, or ask the Domain Administrator to assign you a domain user account for remote access.
- On the server, configure a preferred Domain Name System (DNS) server on the Network Interface Card (NIC).

About this task

Add the server to an existing domain. Ask your System Administrator to add a Domain Name System (DNS) static entry for this server. Each Contact Center server in a domain requires a DNS static entry.

A typical geographic Business Continuity solution with a pair of servers requires two DNS static entries; one DNS static entry for the active server and one DNS static entry for the Remote Geographic Node (RGN) server. Avaya Contact Center Select Business Continuity solutions do not support Dynamic DNS.

Procedure

1. Log on to the Avaya Contact Center Select server.
2. On the **Start** screen, select **Administrative Tools** > **Server Manager**.
3. In the left pane, select **Local Server**.
4. In the right pane, in the **Properties** section, double-click on the **Domain** value.

   The **System Properties** dialog box appears.
5. In the **System Properties** dialog box, click the **Computer Name** tab.
6. Click **Change**.
7. In the **Member of** section, click the **Domain** option.
8. Type the domain name. You must provide the fully qualified domain name, which includes the prefix and suffix.
9. Click **OK**.
10. Type the domain administrator **User name** and **Password**.

11. Click **OK**.
12. Restart the server when you are prompted to do so.
13. Repeat this procedure for the other Avaya Contact Center Select server.

Installing the third-party networking utility

About this task

Install a third-party utility required by Avaya Contact Center Select to support Business Continuity.

Procedure

1. Log on to the active server.
2. Using Windows Explorer, navigate to <installation drive>:\Avaya\Contact Center\Manager Server\CCSMMC\thirdparty\winpcap.
3. Double-click **WinPcap_4_1_3.exe**.
4. On the WinPcap installer dialog, click **Next**.
5. On the WinPcap installer **Setup Wizard** dialog box, click **Next**.
6. On the WinPcap installer **License Agreement** dialog box, click **I Agree**.
7. On the WinPcap installer **Installation options** dialog box, click **Install**.
8. On the WinPcap installer dialog, click **Finish**.
9. Repeat this procedure on the other Avaya Contact Center Select server.

Configuring Avaya Aura® Media Server replication

About this task

Configure the RGN Avaya Contact Center Select Avaya Aura® Media Server to replicate (copy) media files from the Content Store of the active Avaya Contact Center Select Avaya Aura® Media Server.

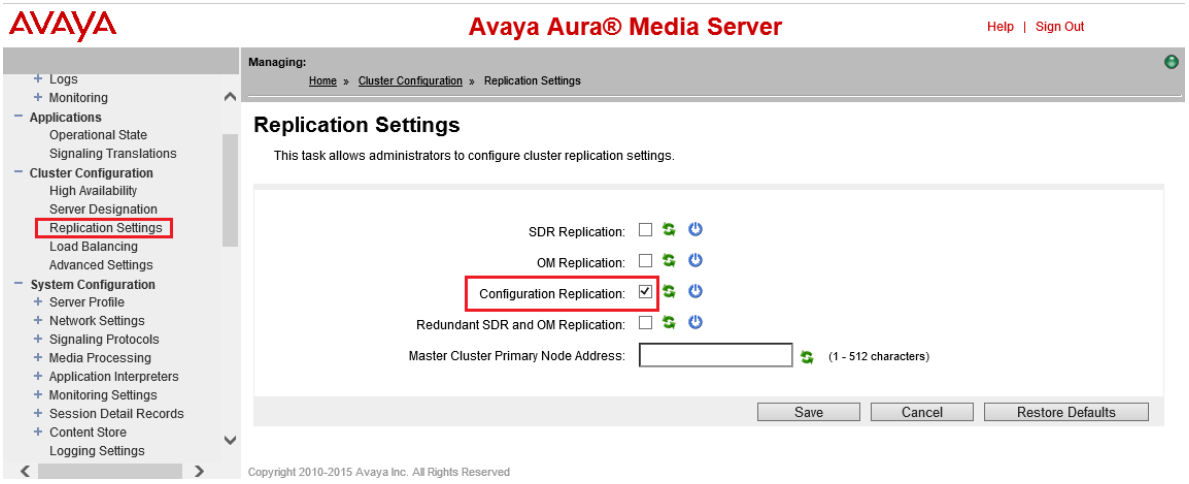
Content Store replication provides media storage replication. If the solution Administrator adds new media files to the Avaya Aura® Media Server of the active Avaya Contact Center Select, these media files are automatically copied to the Avaya Aura® Media Server of the RGN Avaya Contact Center Select system.

Avaya Aura® Media Server uses a custom password protected account to secure Avaya Aura® Media Server Content Store replication. Configure both Avaya Aura® Media Servers with the same replication account username and password details. The Avaya Aura® Media Server replication account is a custom account used only to secure the Avaya Aura® Media Server Content Store during replication, it is not an operating system account.

Procedure

1. On the Avaya Aura® Media Server of the primary Avaya Contact Center Select system, start a Web browser.
2. In the address box, enter https://SERVER_IP_ADDRESS:8443/em. Where SERVER_IP_ADDRESS is the IP address of the Avaya Aura® Media Server of the primary Avaya Contact Center Select system.
3. In the **User ID** box, type the Avaya Aura® Media Server User ID log on account name. The default Element Manager User ID account name is *cust*.
4. In the **Password** box, type the Avaya Aura® Media Server Element Manager password. The default Element Manager password is the cust password for the Avaya Aura® Media Server server. The Avaya Aura® Media Server replication account is a custom account used only to secure the Avaya Aura® Media Server Content Store during replication, it is not an operating system account.
5. Click **Log in**.
6. In the navigation pane, click **Cluster Configuration**.
7. Select **Server Designation**.
8. Under **Local Server**, select **Primary** from the **Role** list.
9. Under **Replication Account**, select the **Enable Replication Account** check box.
10. In the **Username** box, type a username for the replication account. This value is arbitrary, but you must use the same value for both Avaya Aura® Media Server servers.
11. In the **Password** box, type a password for the replication account. This value is arbitrary, but you must use the same value for both Avaya Aura® Media Server servers.
12. In the **Confirm Password** box, retype the password.
13. Click **Save**.
14. On the Avaya Aura® Media Server of the RGN Avaya Contact Center Select system, start a Web browser.
15. In the address box, enter https://SERVER_IP_ADDRESS:8443/em. Where SERVER_IP_ADDRESS is the IP address of the Avaya Aura® Media Server of the RGN Avaya Contact Center Select system.
16. In the **User ID** box, type the Avaya Aura® Media Server User ID log on account name. The default Element Manager User ID account name is *cust*.
17. In the **Password** box, type the Avaya Aura® Media Server Element Manager password. The default Element Manager password is the cust password for the Avaya Aura® Media Server server. The Avaya Aura® Media Server replication account is a custom account used only to secure the Avaya Aura® Media Server Content Store during replication, it is not an operating system account.
18. Click **Log in**.

19. In the navigation pane, click **Cluster Configuration**.
20. Select **Server Designation**.
21. Under **Local Server**, select **Primary** from the **Role** list.
22. Under **Replication Account**, select the **Enable Replication Account** check box.
23. In the **Username** box, type the username for the replication account that you specified on the Avaya Aura® Media Server of the primary Avaya Contact Center Select system.
24. In the **Password** box, type the password for the replication account that you specified on the Avaya Aura® Media Server of the primary Avaya Contact Center Select system.
25. In the **Confirm Password** box, retype the password.
26. Click **Save**.
27. Select **Replication Settings**.



28. Select **Configuration Replication**.
29. In the **Master Cluster Primary Node Address** box, type the IP address of the Avaya Aura® Media Server of the primary Avaya Contact Center Select.
30. Click **Save**.

Configuring ACCS to use IP Office resilience

Before you begin

- If your IP Office solution does not support IP Office resilience, skip this procedure.

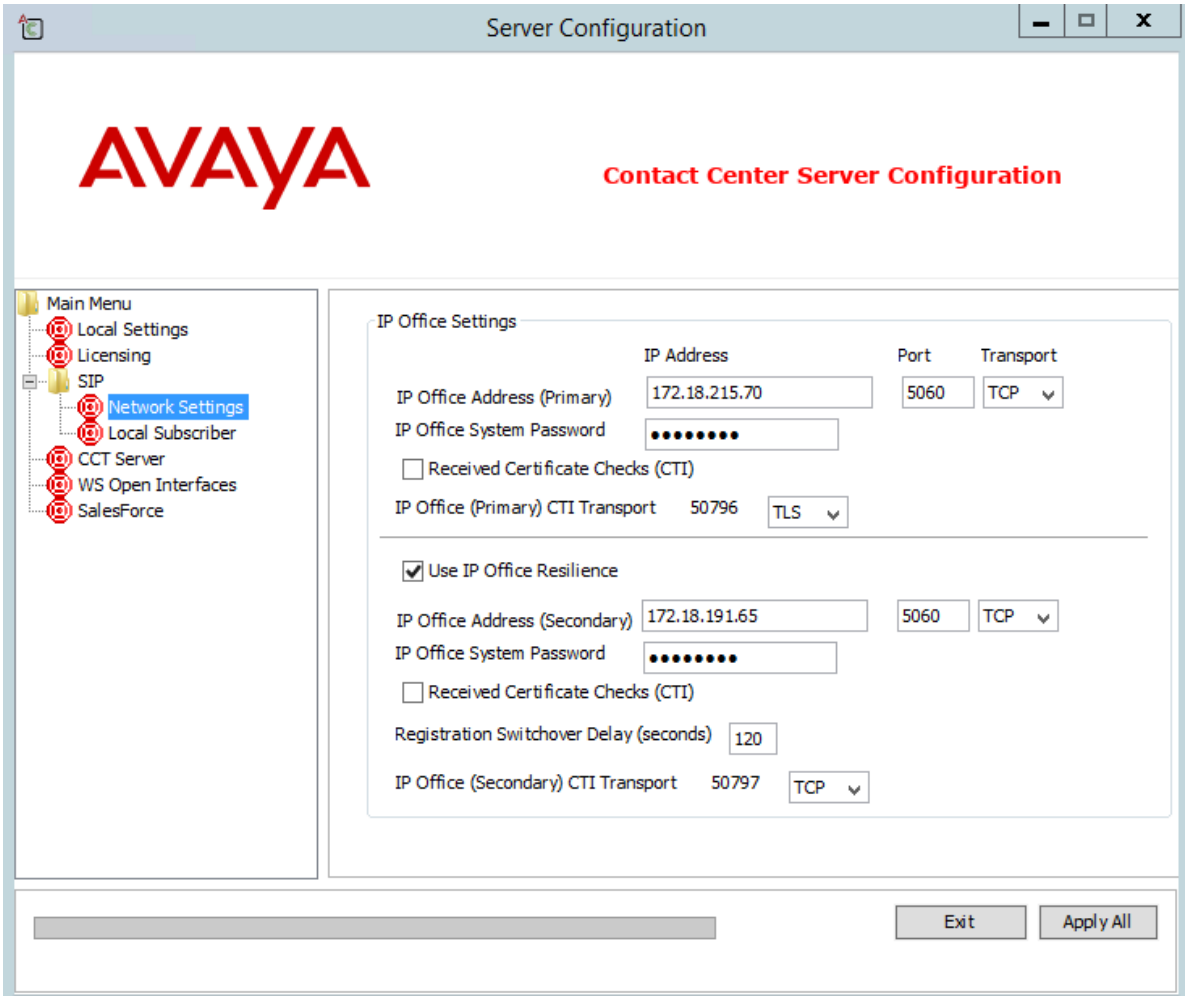
About this task

If your IP Office system has an IP Office Secondary Server and if it is configured to support voice platform resilience, configure Avaya Contact Center Select to use the resilient IP Office system.

If your solution uses TLS communication between Avaya Contact Center Select and IP Office, for more information about configuring TLS security certificates, see *Avaya Contact Center Select Advanced Administration*.

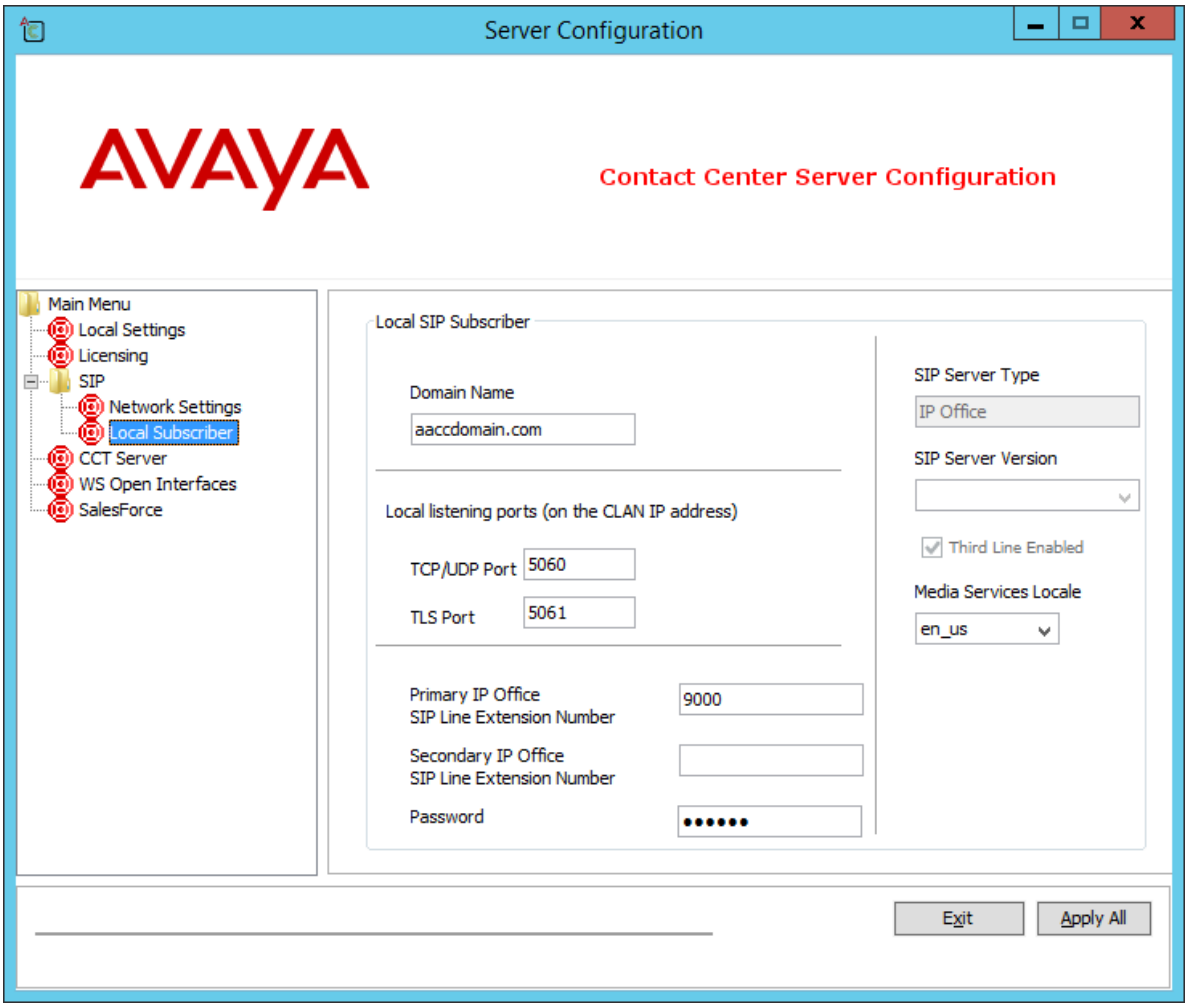
Procedure

1. Log on to the Avaya Contact Center Select active server.
2. On the **Apps** screen, in the **Avaya** section, select **Server Configuration**.
3. In the **Server Configuration** dialog box, under **SIP**, click the **Network Settings** tab.



4. Select **Use IP Office Resilience**.
5. In the **IP Office Address (Secondary)** box, type the IP address of the IP Office Secondary Server.
6. In the Secondary Server **Port** box, type the server listening port. The default port is 5060.
7. From the Secondary Server **Transport** list, select the transport type, **TCP** or **TLS**.

8. In the Secondary Server **IP Office System Password** box, type the system password for your IP Office Secondary Server. Ask your IP Office Administrator for the System Password. If this password changes on the IP Office server, you must update the password in **Server Configuration**.
9. If Avaya Contact Center Select communicates with the IP Office Secondary Server using TLS certification, to enable IP Office Certificate Validation, select **Received Certificate Checks (CTI)**.
10. In the **Registration Switchover Delay (seconds)** box, type the length of time in seconds that the Avaya Contact Center Select server attempts to reconnect to the IP Office Primary Server before attempting to switchover to the IP Office secondary server. The maximum configurable delay is 600 seconds.
11. From the **IP Office (Secondary) CTI Transport** list, select the CTI transport type, **TCP** or **TLS**.
12. In the **Server Configuration** dialog box, under **SIP**, click the **Local Subscriber** tab.



13. In the **Secondary IP Office SIP Line Extension Number** box, type the IP Office SIP User Extension Number used to register Avaya Contact Center Select with the IP Office Secondary Server.
14. In the **Password** box, type the password of the IP Office SIP User Extension Number for the IP Office server.
15. Click **Apply All**.
16. On the **Restart Required** message box, click **Yes**.

Configuring CCMM Server Settings

About this task

Agent Desktop communicates with the Communication Control Toolkit (CCT) component of Avaya Contact Center Select to handle voice contacts. Agent Desktop communicates with the Contact Center Multimedia (CCMM) component of Avaya Contact Center Select to handle multimedia based contacts.

Use the CCMM Administration tool to configure Remote Geographic Node (RGN) CCMM and CCT details.

Important:

Changes to the CCMM Server Settings might require a server restart before they take effect.

After you have configured the new CCMM and CCT settings, you must close down and launch all of the Agent Desktop clients so that they pick up the new server settings.

Procedure

1. Start Internet Explorer.
2. In the **Address** box, type the URL of the Avaya Contact Center Select active server. The default URL is:

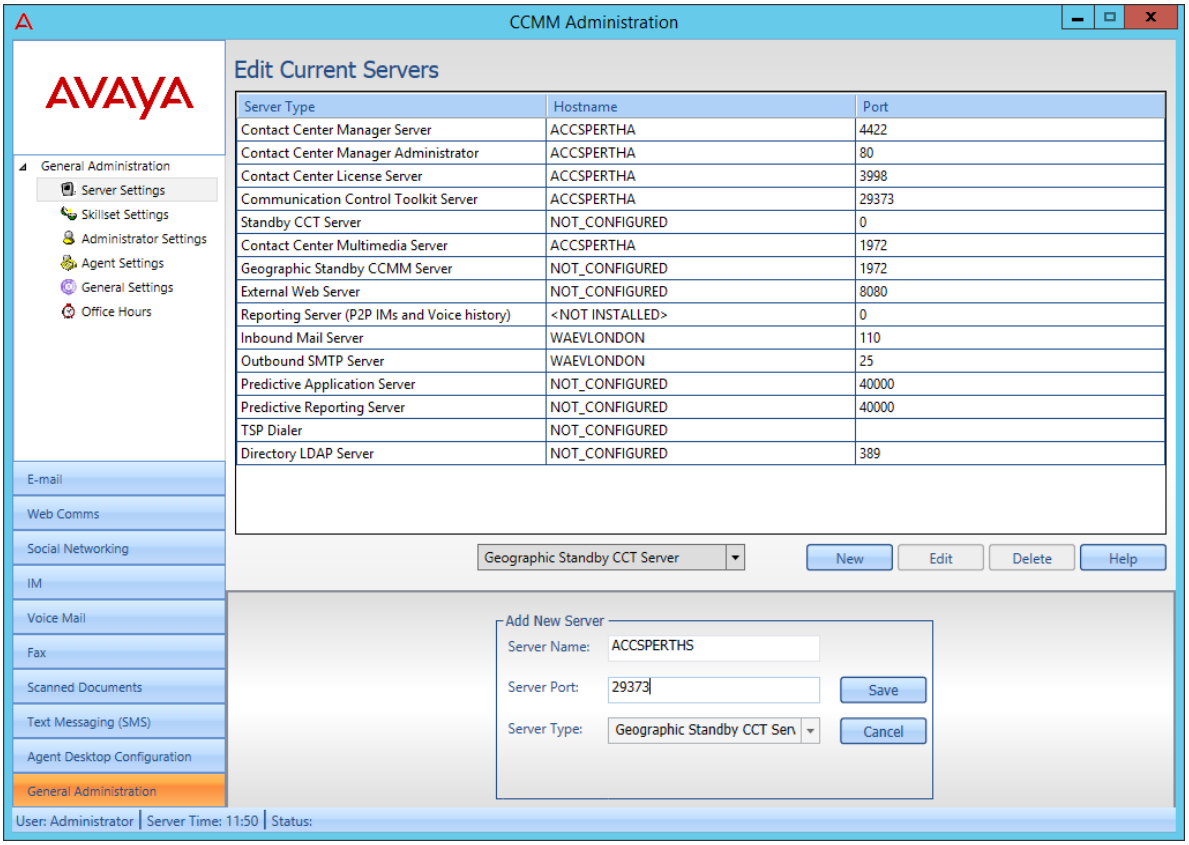
   `http://<server name>`

   where <server name> is the host name of the active Avaya Contact Center Select server.
3. Press **Enter**.
4. In the main Contact Center Manager Administration logon window, in the **User ID** box, type the user name. The default user ID is Administrator.
5. In the **Password** box, type the password. The default user password is Administrator.
6. Click **Log In**.
7. From the **Launchpad**, select **Multimedia**.
8. In the left pane, select the CCMM server to administer.

   The system displays the Multimedia Administration screen in the right pane.

9. Select **Install prerequisite software**.
10. Click **Launch Multimedia Client**.
11. On the **File Download** box, click **Run**.

    The prerequisite software takes some time to install. After the install, the CCMM Administration utility appears.
12. In the left column of the **CCMM Administration** tool, select **General Administration**.
13. Click **Server Settings**.
14. Ensure that **Contact Center Manager Server** is configured with the name of the Avaya Contact Center Select active server.
15. Ensure that **Contact Center License Server** is configured with the name of the Avaya Contact Center Select active server.
16. Ensure that **Contact Center Manager Administration** is configured with the name of the Avaya Contact Center Select active server.
17. Ensure that **Contact Center Multimedia Server** is configured with the name of the Avaya Contact Center Select active server.
18. Ensure that **Communication Control Toolkit Server** is configured with the name of the Avaya Contact Center Select active server.
19. Select the **Geographic Standby CCMM Server** row, and click **Edit**.
20. In the **Edit Server Details** section, in the **Server Name** box, type the name of the Avaya Contact Center Select Remote Geographic Node server.
21. In the **Edit Server Details** section, in the **Server Port** box, type the port number for CCMM on the Avaya Contact Center Select Remote Geographic Node server. The default port number is 1972.
22. Click **Save**.
23. Under **Edit Current Servers**, click **New**.
24. From the drop down list, select **Geographic Standby CCT Server**.
25. In the **Add New Server** section, in the **Server Name** box, type the name of the Avaya Contact Center Select Remote Geographic Node server.
26. In the **Server Port** box, type the port number for CCT on the Avaya Contact Center Select Remote Geographic Node server. The default port number is 29373.



27. Click **Save**.

Verifying services are ready for Business Continuity

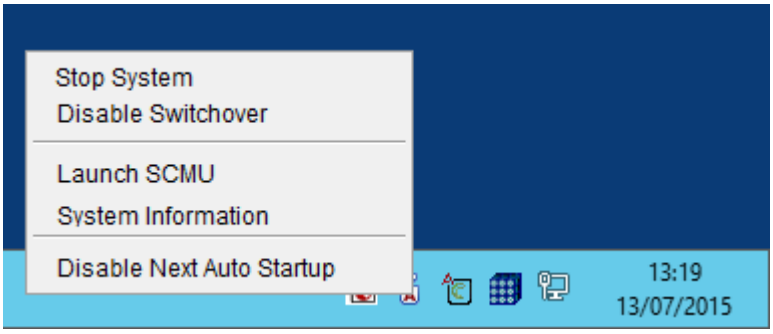
About this task

Verify that all services stop before you configure Business Continuity. This ensures that all resources are available to the active server when it starts.

Perform this procedure using the System Management and Monitoring Component (SMMC) on both Avaya Contact Center Select servers.

Procedure

1. Log on to the active server.
2. On the Windows System Tray, right-click on the System Management and Monitoring Component (SMMC) system tray icon, and select **Stop System**.



3. Repeat this procedure on the other Avaya Contact Center Select server.

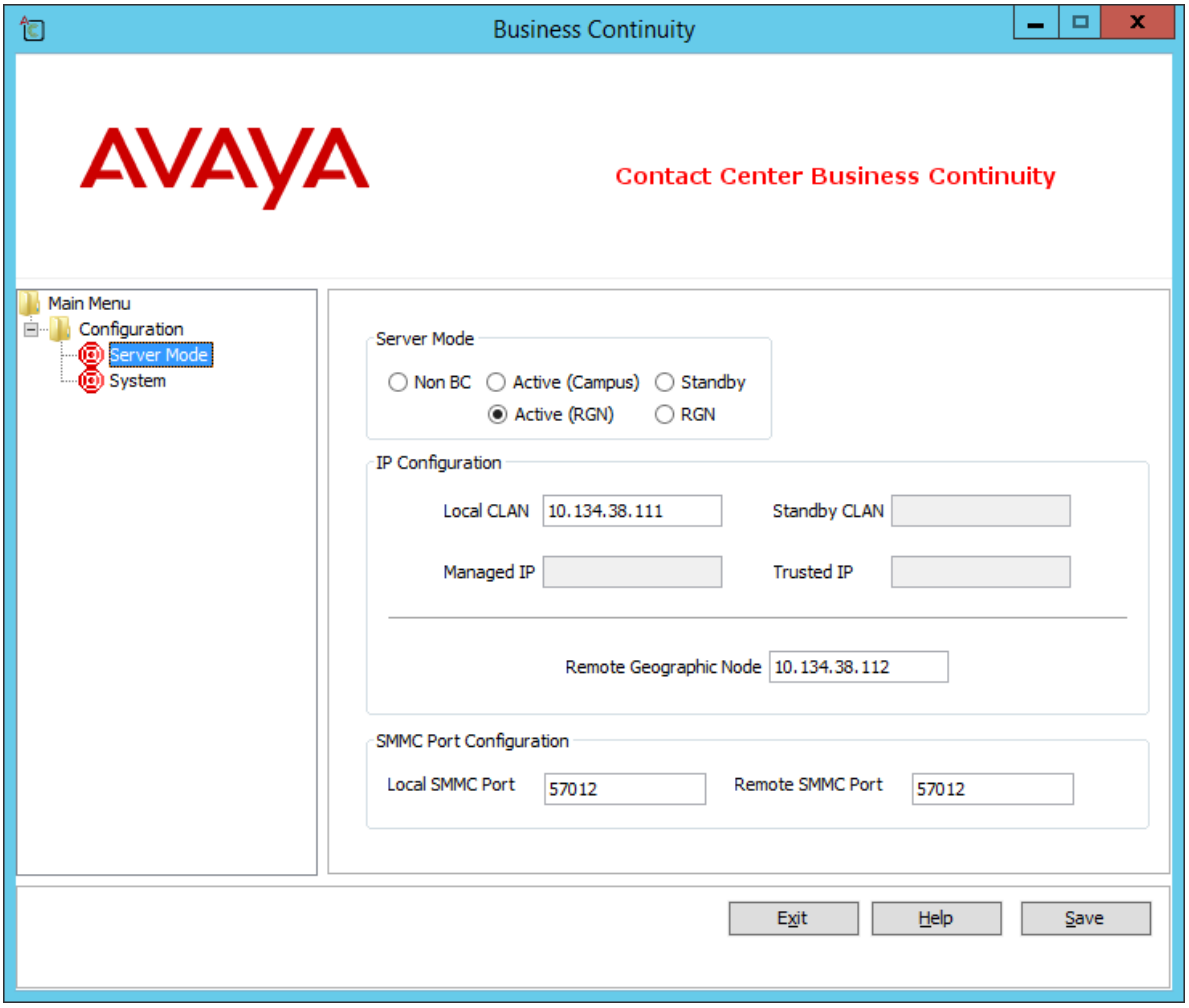
Configuring Business Continuity on the active server

About this task

Configure remote Business Continuity on the active server using the Business Continuity utility. The active server is the server that normally processes contacts.

Procedure

1. Select one server to be the active server and log on.
2. On the **Apps** screen, in the **Avaya** section, select **Business Continuity**.
3. Expand **Configuration**.
4. Double-click **Server Mode**.
5. Select **Active (RGN)**.
6. In the **Local CLAN** box, type the IP address for the server initially configured in active mode.
7. Leave the **Standby CLAN** box empty.
8. In the **Remote Geographic Node** box, type the IP address of the Remote Geographic Node.
9. In the **Local SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the local (active) server. The default port number is 57012.
10. In the **Remote SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the remote (RGN) server. The port number entered here must match the port number set on the remote (RGN) server. The default port number is 57012.



11. Click **Save**.

Backing up the database on the active server

About this task

The active server is configured for Business Continuity. Now the Remote Geographic Node server must be prepared for Business Continuity. Back up the active server to create a snapshot of the database which is then restored to the Remote Geographic Node server. On the active server, all databases must be backed up.

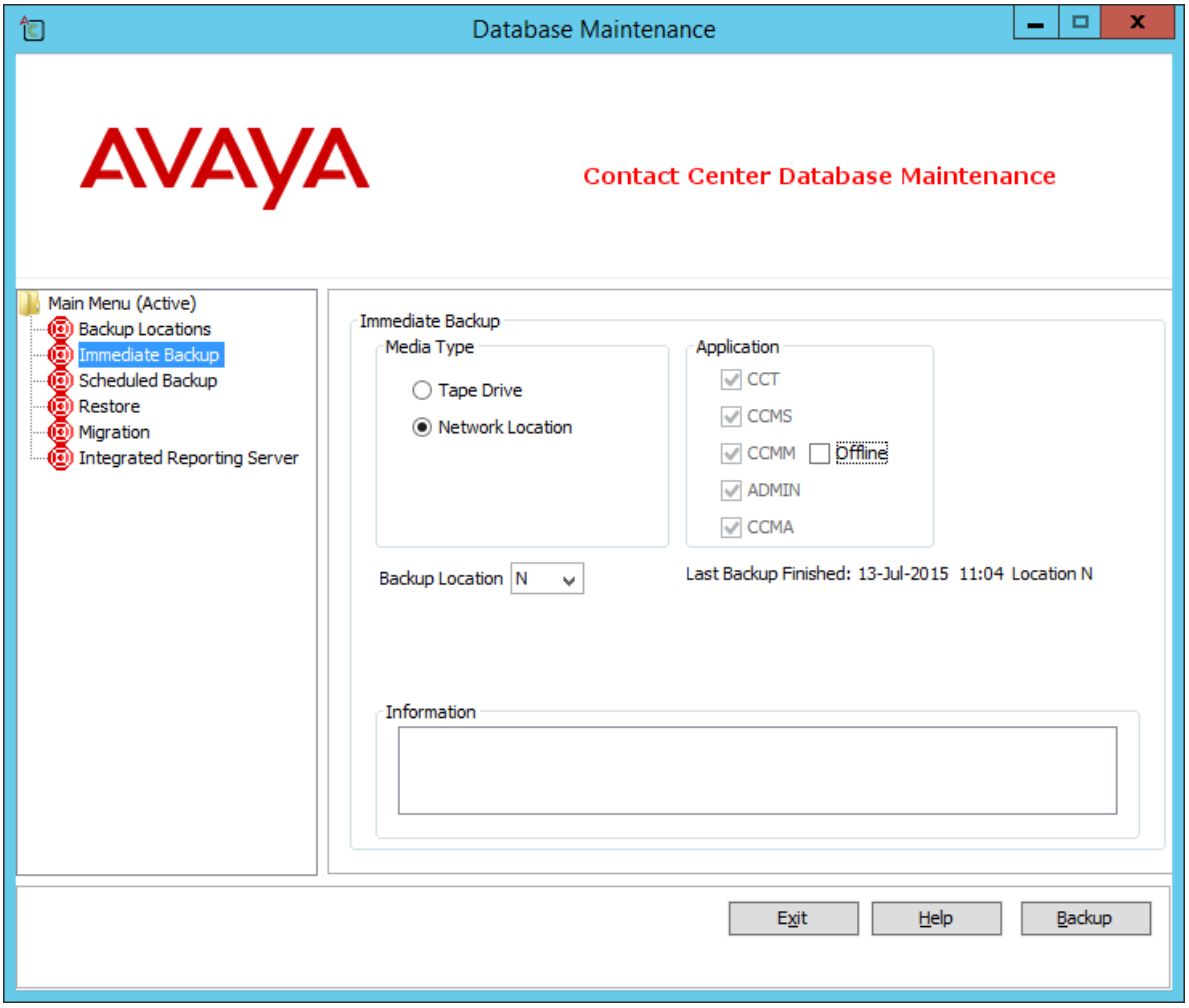
Important:

Do not use a folder on the active or Remote Geographic Node servers as the backup location.

Procedure

1. Log on to the active server.

2. On the **Apps** screen, in the **Avaya** section, select **Database Maintenance**.
3. Click **Backup Locations**.
4. Click **Create**.
5. From the **Driver Letter** list, select the network drive on which you want to store the CCMS, CCT, CCMM, CCMA, and ADMIN databases.
6. In the **UNC Path** box, type the location to store the backup, in the format \\Computer Name \Backup Location. This location must be a shared folder with correct permissions.
7. In the **User Name** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
8. In the **Password** box, type the Windows password.
9. Click **OK**.
10. In the left pane, click **Immediate Backup**.
11. In the **Media Type** section, select **Network Location**.
12. From the **Backup Location** list, select the network drive on which to store the backup.
13. Click **Backup**.



Restoring the database on the Remote Geographic Node server

Before you begin

- Know the location of the backup database.
- For a faster database restore, copy the active database backup to a local network share of the Remote Geographic node server.
- Using the Database maintenance utility, create a backup location on the Remote Geographic node server that references the location of database backup to be restored.
- Stop all Contact Center services using the SCMU utility, if services are running.
- Ensure the patch level on the Remote Geographic Node server is the same as the active server.

Important:

Not all CCT data is stored in the database; therefore the following data must be configured on the Remote Geographic Node server, CCT License, CCT Contact Management Framework, CCT SOA configuration (CCT Web Services), and CCT logging location.

Important:

You must restore all databases on an Avaya Contact Center Select server. Restoring only CCMS and not CCT, CCMM, or ADMIN might leave an inconsistent server and Business Continuity cannot shadow data correctly.

Important:

Restoring the ADMIN database can change configuration of Backup locations on the Remote Geographic Node server if the active server and Remote Geographic Node server backup locations are different. Therefore, after you restore the ADMIN database, close and reopen the Database Maintenance utility.

About this task

Restore the database from the active server to the Remote Geographic Node server to ensure the databases are consistent. The Database Maintenance utility can restore all application databases at once. Restore the data for the CCMS, CCT, CCMM, and ADMIN databases.

You must restore the CCMS, CCT, CCMM, and ADMIN database onto the Remote Geographic Node server.

Procedure

1. Log on to the Remote Geographic Node server.
2. On the **Apps** screen, in the **Avaya** section, select **Database Maintenance**.
3. In the **Database Maintenance** dialog box, in the left pane, click **Restore**.
4. In the right pane, under **Media Type**, select the media type on which the backup is restored.
5. If the backup file is on the network drive, in the **Backup Location** list, select the backup location.
6. Under **Application**, select **CCMS**, **CCT**, **CCMM**, and **ADMIN**.
7. Do not select **CCMA**.
8. Under **Restore contents**, select **Data**.

   Important:

   Do not select **Offline**.
9. Click **Restore**.
10. Use the **Information** field to monitor the progress of the restoration.
11. Click **Exit** to close the Database Maintenance utility.

Variable definitions

Name	Description
Application	The database and applications of Contact Center that you can back up.
Backup Location	The destination of the network disk. The values are configured in the Backup Locations.
Restore contents	The type of content that is stored in the database. Data is in the database. Schema is the data for the database structure, tables and procedures.
Media type	The type of media used for your backup file. You can use a network disk location or a tape drive. If you use a network disk location, you must configure a destination before you can back up the file.

Updating the CCMM dashboard

About this task

Update the CCMM dashboard to allow the Multimedia Administration tool to start from the CCMA Web interface of the RGN server.

Procedure

1. Log on to the RGN server.
2. On the **Apps** screen, in the **Avaya** section, select **Multimedia Dashboard**.
3. In the **Server Availability** section, right-click **Contact Center Manager Administrator** and select **Edit**.
4. In the **User Name** box, type the user name. The default user name is *generaladmin*.
5. In the **Password** box, type the password. The default password is *__ccmm!* (With a double underscore).
6. Click **Login**.
7. In the text box, type the hostname of the RGN server.
8. Click **Save**.

Configuring RGN CCMM General Administration

About this task

Configure the Remote Geographic Node (RGN) Avaya Contact Center Select to use local telephony and multimedia resources.

Important:

Changes to the RGN Avaya Contact Center Select CCMM Settings might require a RGN server restart before they take effect.

Procedure

1. Start Internet Explorer.
2. In the **Address** box, type the URL of the Avaya Contact Center Select RGN server. The default URL is:

   `https://<RGN server name>`

   where <RGN server name> is the host name of the RGN Avaya Contact Center Select server.
3. Press **Enter**.
4. In the main Contact Center Manager Administration logon window, in the **User ID** box, type the user name. The default user ID is Administrator.
5. In the **Password** box, type the password. The default user password is Administrator.
6. Click **Log In**.
7. In the RGN Contact Center Manager Administration, under the **Launchpad**, select **Multimedia**.
8. In the left column, click the RGN Multimedia server.

   The system displays the Multimedia Administration screen in the right pane.
9. Select **Install prerequisite software**.
10. Click **Launch Multimedia Client**.
11. On the **File Download** box, click **Run**.

    The prerequisite software takes some time to install. After the install, the CCMM Administration utility appears.
12. In the left column of the **CCMM Administration** tool, select **General Administration**.
13. Click **Server Settings**.
14. Change the **Contact Center Manager Server** to the name of the Remote Geographic Node Avaya Contact Center Select server.
15. Change the **Contact Center License Server** to the name of the Remote Geographic Node Avaya Contact Center Select server.

16. Change the **Communication Control Toolkit Server** to the name of the Remote Geographic Node Avaya Contact Center Select server.
17. Change the **Standby CCT Server** box to not configured.
18. Change the **Contact Center Multimedia Server** to the name of the Remote Geographic Node Avaya Contact Center Select server.
19. Change the **Geographic Standby CCMM Server** box to not configured.
20. Change the **Geographic Standby CCT Server** box to not configured.
21. In the left column select **E-mail**.
22. Click **General Settings**.
23. Ensure that the Inbound URL is of the form `http://<RGNIPAddress>/inboundattachment`.

    Where *RGIPAddress* is the IP address of the Remote Geographic Node Avaya Contact Center Select server.
24. Ensure that the Outbound URL is of the form `http://<RGNIPAddress>/outboundattachment`.

    Where *RGNIPAddress* is the IP address of the Remote Geographic Node Avaya Contact Center Select server.
25. Click **Save**.

Configuring server details on the Remote Geographic Node

About this task

Configure the Remote Geographic Node server with its own server details.

Important:

Changes to the configuration data might require a server restart.

Procedure

1. Log on to the Remote Geographic Node server.
2. On the **Apps** screen, in the **Avaya** section, select **Server Configuration**.
3. In the **Server Configuration** dialog box, click the **Local Settings** tab.
4. Update the Remote Geographic Node server local settings.
5. In the **Server Configuration** dialog box, click the **Licensing** tab.
6. Update the Remote Geographic Node server licensing details.

7. In the **Server Configuration** dialog box, under **SIP**, click the **Network Settings** tab.
8. Update the Remote Geographic Node server **SIP** > **Network Settings** details.
9. In the **Server Configuration** dialog box, under **SIP**, click the **Local Subscriber** tab.
10. Update the Remote Geographic Node server **SIP** > **Local Subscriber** details.
11. Click **Apply All**.
12. On the **Restart Required** message box, click **Yes**.

Variable definitions

Name	Description
Avaya Server Subnet IP Address	The IP address of the Avaya Contact Center Select server.
IP Office Settings • IP Office Address • IP Office System Password • Port	The networking details for the IP Office voice platform.
Local SIP Subscriber • SIP Line Extension Number • Password	The IP Office SIP User Extension Number used by Avaya Contact Center Select to register for CTI call control and SIP session messaging.
Local SIP Subscriber • Domain Name	Information about the environment of the SIP-enabled contact center and how to identify the server within the network. Associated domain name for the SIP- enabled contact center.
MS Locale	Locale (including language and dialects) of the system environment.
Local Listening Ports	The SIP Communication protocol accepted by the system for incoming calls. TCP/UDP Port default is 5060. TLS Port default is 5061.

Configuring the Remote Geographic Node local resources

About this task

Configure the Remote Geographic Node (RGN) resources to allow the remote site to function as a standalone contact center, if or when the need arises.

When Business Continuity shadowing is enabled, the RGN server shadows some of the configuration data from the active server.

The RGN server does not shadow (replicate) information about the following resources from the active server:

- Media Server and Media Services
- Default DN

On the RGN server, you must configure these resources to use local Avaya Aura® Media Servers and attendants.

Configure a Default DN to catch treated calls that are defaulted by the contact center script and to catch calls not answered by agents. Avaya recommends that you configure a local attendant at the RGN site as the Default DN.

Avaya Contact Center Select uses Avaya Aura® Media Server media processing capabilities to support conferencing, announcements, and dialogs. After restoring the database from the active server to the RGN server, the RGN server configuration has the details of the active server Avaya Aura® Media Server. On the RGN server, in Contact Center Manager Administration, change the Avaya Aura® Media Server details to use the RGN server Avaya Aura® Media Server.

Avaya Contact Center Select uses the media processing capabilities of Avaya Aura® Experience Portal to support external Interactive Voice Response (IVR) dialogs (XDIALOG). If your RGN site uses local Avaya Aura® Experience Portal servers, add these here as Media Servers and configure them to provide external dialog (XDIALOG) services.

Procedure

1. Log on to RGN Contact Center Manager Administration.
2. From the **Launchpad**, select **Configuration**.
3. In the left pane, expand the RGN Contact Center Manager Server on which to configure global settings.
4. Select the **Global Settings** folder.
5. Configure the global settings for your system based on the fields listed in the **Global Settings** window.
6. In the **Default DN** box, type the default DN to use when a script defaults or a treated call is not answered. Avaya recommends that you configure an attendant as the Default DN.
7. Click **Save**.
8. In the left pane, expand the RGN Contact Center Manager Server.
9. Select the **Media Services and Routes** folder.
10. In the **Media Services and Routes** table, select **ACC_APP_ID**.
11. In the **Selected** box, select the active server Avaya Aura® Media Server, and click the left arrow (<).

    The server moves to the **Available** list.
12. Click **Submit**.

13. From the system tree, select the **Media Servers** folder under the RGN Contact Center Manager Server.
14. In the **Media Servers** list, select the row for the active server Avaya Aura® Media Server, and press Delete.
15. On the Confirm Delete dialog, click **Yes**.
16. Select the **Media Servers** folder.
17. In the right pane, in the **Server Name** box, type the name of the RGN server Avaya Aura® Media Server .
18. In the **IP address** box, type the IP address of the RGN server Avaya Aura® Media Server.
19. In the **Port Number** box, type the port number for the RGN server Avaya Aura® Media Server. The port number must match the Avaya Aura® Media Server port number. The default is 5060.
20. Select the **Master Content Store**. Avaya Contact Center Select supports only one Master Content Store.
21. Click any other row in the table to save the changes.
22. In the left pane, expand the RGN Contact Center Manager Server.
23. Select the **Media Services and Routes** folder.
24. On the **Media Services & Routes** table, select **ACC_APP_ID**.
25. From the **Available** list, select the RGN server Avaya Aura® Media Server to associate with the selected conference media service.
26. Click the right arrow (>).

    The server moves to the **Selected** list.
27. Click **Submit**.

Restoring the CCMA database on the Remote Geographic Node server

Before you begin

- Know the location of the backup database.
- For a faster database restore, copy the active database backup to a local network share of the Remote Geographic node server.
- Using the Database maintenance utility, create a backup location on the Remote Geographic node server that references the location of database backup to be restored.
- Stop all Contact Center services using the SCMU utility, if services are running.

About this task

Restore the CCMA database from the active server to the Remote Geographic Node server to ensure the databases are consistent.

Procedure

1. Log on to the Remote Geographic Node server.
2. On the **Apps** screen, in the **Avaya** section, select **Database Maintenance**.
3. In the **Database Maintenance** dialog box, in the left pane, click **Restore**.
4. In the right pane, under **Media Type**, select the media type on which the backup is restored.
5. If the backup file is on the network drive, in the **Backup Location** list, select the backup location.
6. Under **Application**, select **CCMA**.
7. Do not select **CCMS**, **CCT**, **CCMM**, or **ADMIN**.
8. Under **Restore contents**, select **Data**.

   Important:

   Do not select **Offline**.
9. Click **Restore**.
10. Use the **Information** field to monitor the progress of the restoration.
11. Click **Exit** to close the Database Maintenance utility.

Configuring Business Continuity on the Remote Geographic Node server

About this task

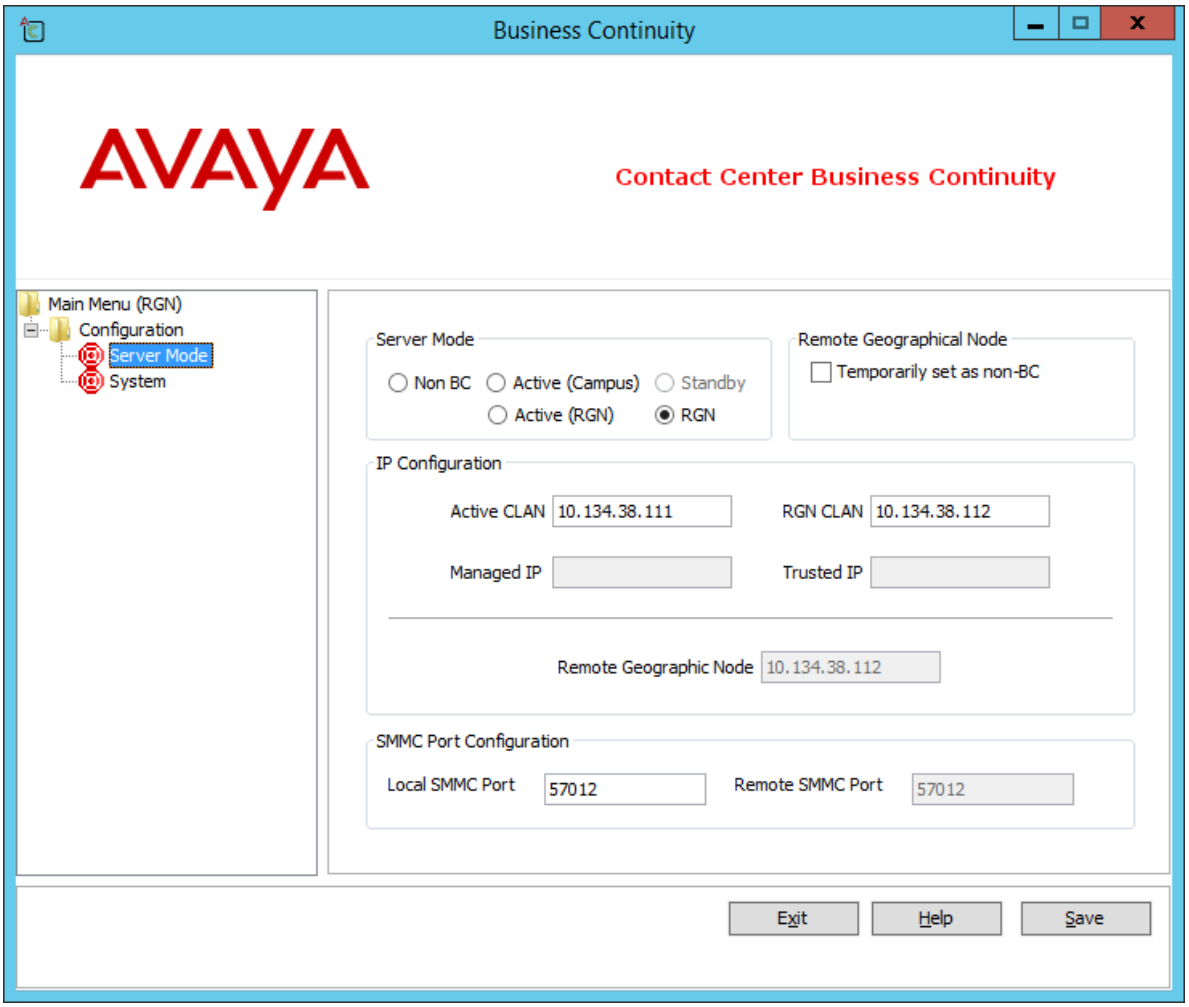
Configure Business Continuity on the Remote Geographic Node server using the Business Continuity utility. The Remote Geographic Node Server shadows the active server.

Procedure

1. Log on to the Remote Geographic Node server.
2. On the **Apps** screen, in the **Avaya** section, select **Business Continuity**.
3. Expand **Configuration**.
4. Double-click **Server Mode**.
5. Under **Server Mode**, select **RGN**.

6. Under **IP Configuration**, in the **Active CLAN** box, type the IP address for the ACCS active server pair.
7. Under **IP Configuration**, in the **RGN CLAN** box, type the IP address for the Remote Geographic Node server.
8. Under **SMMC Port Configuration**, in the **Remote SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the remote (active) server.
9. Under **SMMC Port Configuration**, in the **Local SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the local (RGN) server.
10. Click **Save**.

    Ignore the request to restart ACCS. Do not restart ACCS at this stage in the configuration process.



Variable definitions

Name	Description
Active CLAN	Type the IP address for the ACCS active server.
RGN CLAN	The IP address for the Remote Geographic Node server.
Local SMMC Port	The Network Management port number for System Management and Monitoring Component (SMMC) on the local (RGN) server. The default port number is 57012.
Remote SMMC Port	The Network Management port number for System Management and Monitoring Component (SMMC) on the remote (active) server. The port number entered here must match the port number set on the remote (active) server. The default port number is 57012.

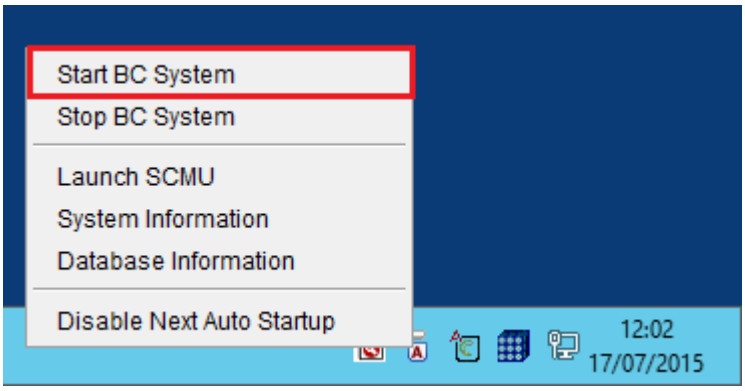
Starting the active server

About this task

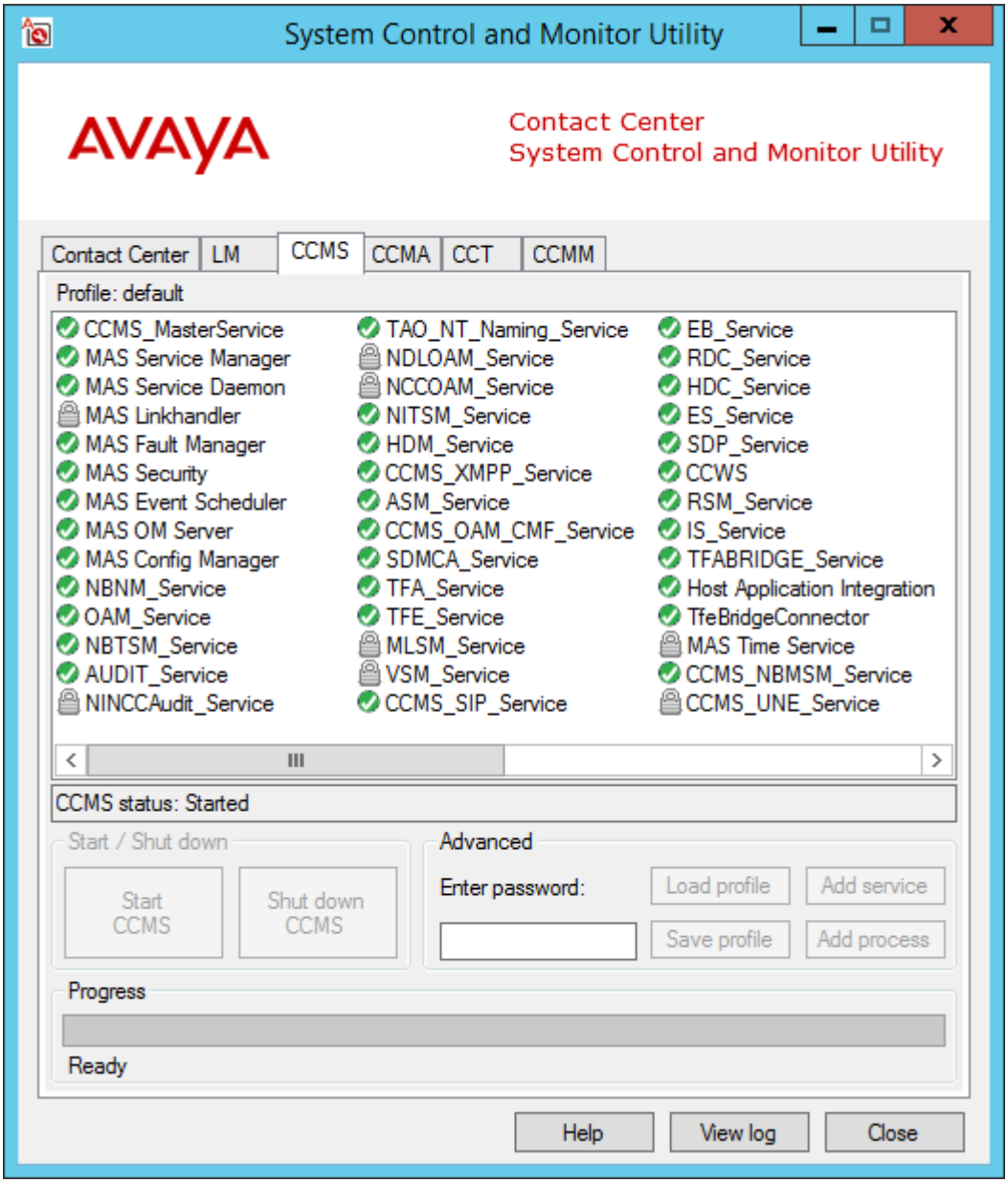
Start the active server using the System Management and Monitoring Component (SMMC) system tray. Starting the active server starts Contact Center services and system processes.

Procedure

1. Log on to the active server.
2. On the Windows taskbar of the active server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Start BC System**.



3. Using the System Control and Monitor Utility (SCMU), verify that the Contact Center services are running.



Starting shadowing on the Remote Geographic Node server

About this task

Start shadowing on the Remote Geographic Node Server using the System Management and Monitoring Component (SMMC) system tray.

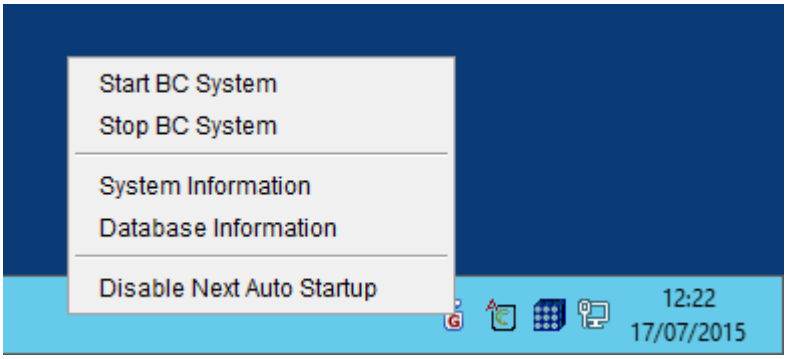
The Remote Geographic Node server shadows the active server, maintaining a near real-time local copy of the Contact Center applications and Administration databases. The Remote Geographic Node server is therefore configured with the most recent data.

Important:

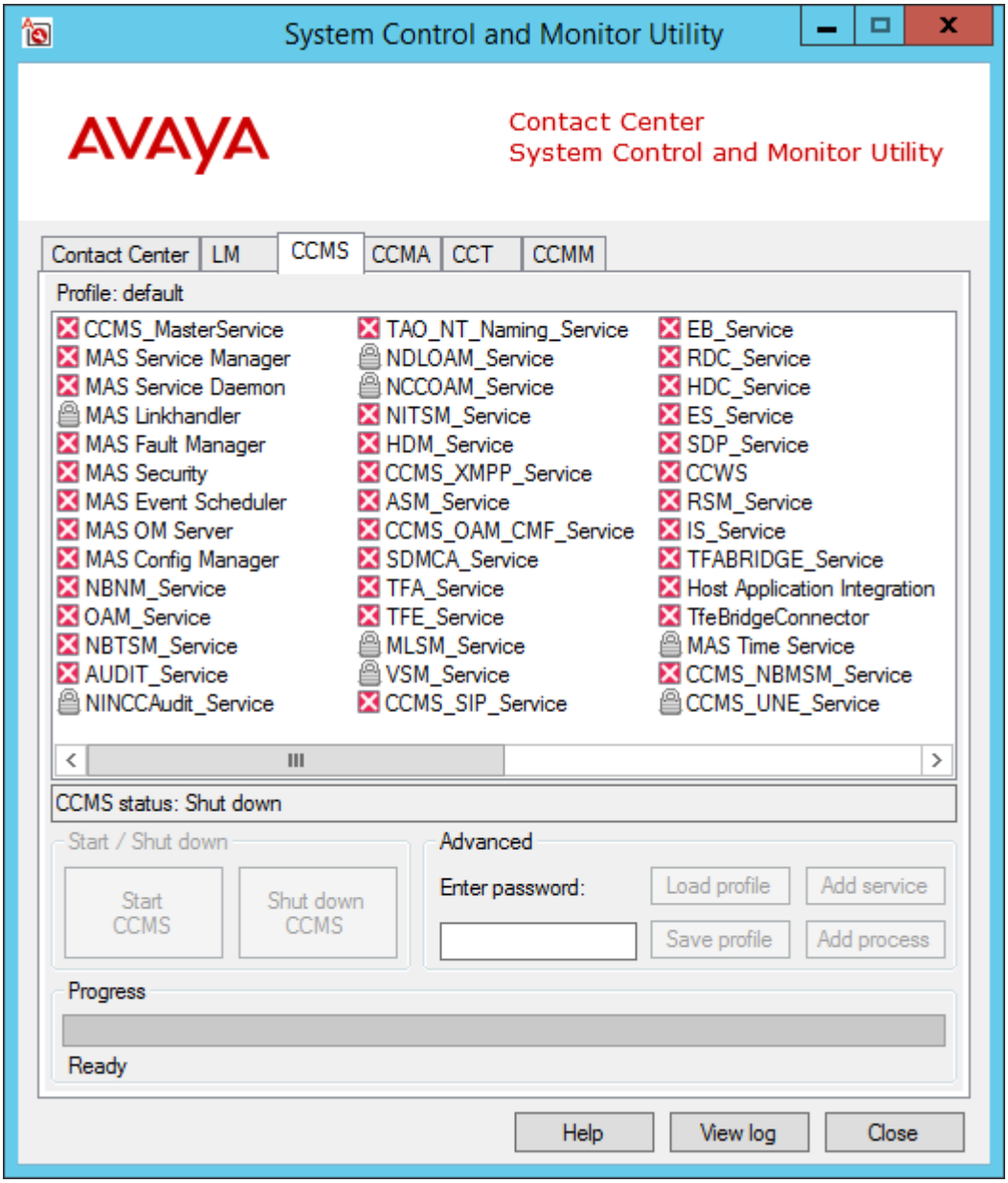
You must backup the active server database, restore it onto the Remote Geographic Node server, and enable shadowing within 24 hours. If the difference in time between the active and Remote Geographic Node server database content is greater than 24 hours then database shadowing does not work. If shadowing is stopped for more than 24 hours then you must backup the active server database and restore it onto the Remote Geographic Node server before re-enabling shadowing. Ensure that the system clock time on the active and Remote Geographic Node servers are synchronized.

Procedure

1. Log on to the Remote Geographic Node server.
2. On the Windows taskbar of the Remote Geographic Node server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Start BC System**.



3. Using the System Control and Monitor Utility (SCMU), check that the Contact Center services are **Shut down**.



Verifying the Avaya Contact Center Select server RGN settings

About this task

Verify the Avaya Contact Center Select server Remote Geographic Node (RGN) settings. The RGN server must be available and manually enabled to take over if the active server fails.

Procedure

1. Log on to the active server.
2. Log on to the CCMA Web client using the RGN server name.
3. On the Launchpad, select **Configuration**.
4. From the server list, select the Avaya Contact Center Select server as the CCMS server.
5. Right-click on the Avaya Contact Center Select - CCMS server, select **Refresh Server**.
6. Ensure the **Remote Geographic Node** section displays the **RGN Server Name** and **RGN Server IP** of the Avaya Contact Center Select server Remote Geographic Node server.

Verifying the Business Continuity RGN is running

About this task

Verify that the Remote Geographic Node (RGN) server is shadowing the active server using the Business Continuity utility. The System dialog box of the Business Continuity utility displays system information about the active and the Remote Geographic Node servers.

The dialog box displays the followings information categories:

- Computer name and operating system version
- Server mode
- Server configuration type
- Port information
- Remote server connection status
- Remote server port information
- License information
- Databases shadowed
- Time of last record shadowed
- Database namespaces
- Local and remote information on system status, shadowing, and network
- CC Application install information
- Database space and journaling information
- Database processes information

Procedure

1. Log on to the active server.
2. On the **Apps** screen, in the **Avaya** section, select **Business Continuity**.
3. In the left pane, expand **Configuration**.

4. Select **System**.
5. Select **Get System Configuration**.

   The most recent system information appears.
6. On to the active server, on the Windows taskbar, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **System Information**.

   The System Information window displays the current status of Business Continuity on the active server.
7. On to the RGN server, on the Windows taskbar, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **System Information**. The System Information window displays the current status of Business Continuity on the RGN server.

   The System Information window displays the current status of Business Continuity on the RGN server.

Relaunching the Agent Desktop clients

About this task

Relaunch the Agent Desktop clients to pick up the RGN server details.

Procedure

1. Log off and close down all Agent Desktop clients.
2. Launch the Agent Desktop clients. During the launch process, Agent Desktop picks up the Avaya Contact Center Select active and RGN server settings. If Agent Desktop cannot communicate with the Avaya Contact Center Select active server, Agent Desktop prompts the agent to reconnect with the active server or connect to the Avaya Contact Center Select RGN server.

Verifying Geographic Business Continuity

Before you begin

- Configure Geographic Business Continuity on the active and Remote Geographic Node Avaya Contact Center Select servers.
- To support Business Continuity resiliency, the Avaya Contact Center Select agents must each have an associated Windows domain user account in the same Windows domain as the active and RGN servers. Create Avaya Contact Center Select agents with associated Windows domain accounts. Log these domain-enabled agents in to Agent Desktop. Use these domain-enabled Avaya Contact Center Select agents to verify Business Continuity resiliency

About this task

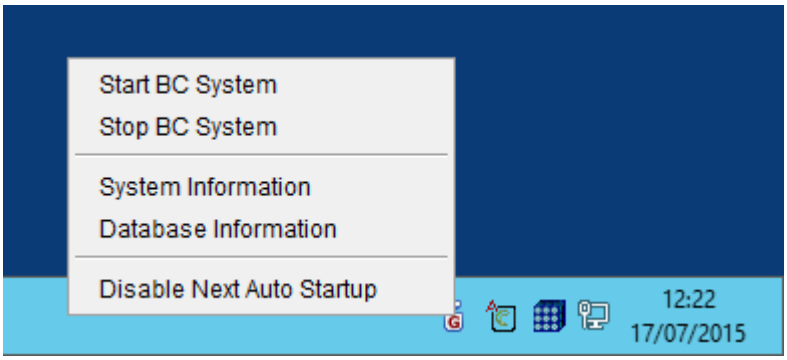
Verify Geographic Business Continuity by temporarily using the Avaya Contact Center Select Remote Geographic Node (RGN) server to process contacts.

Note:

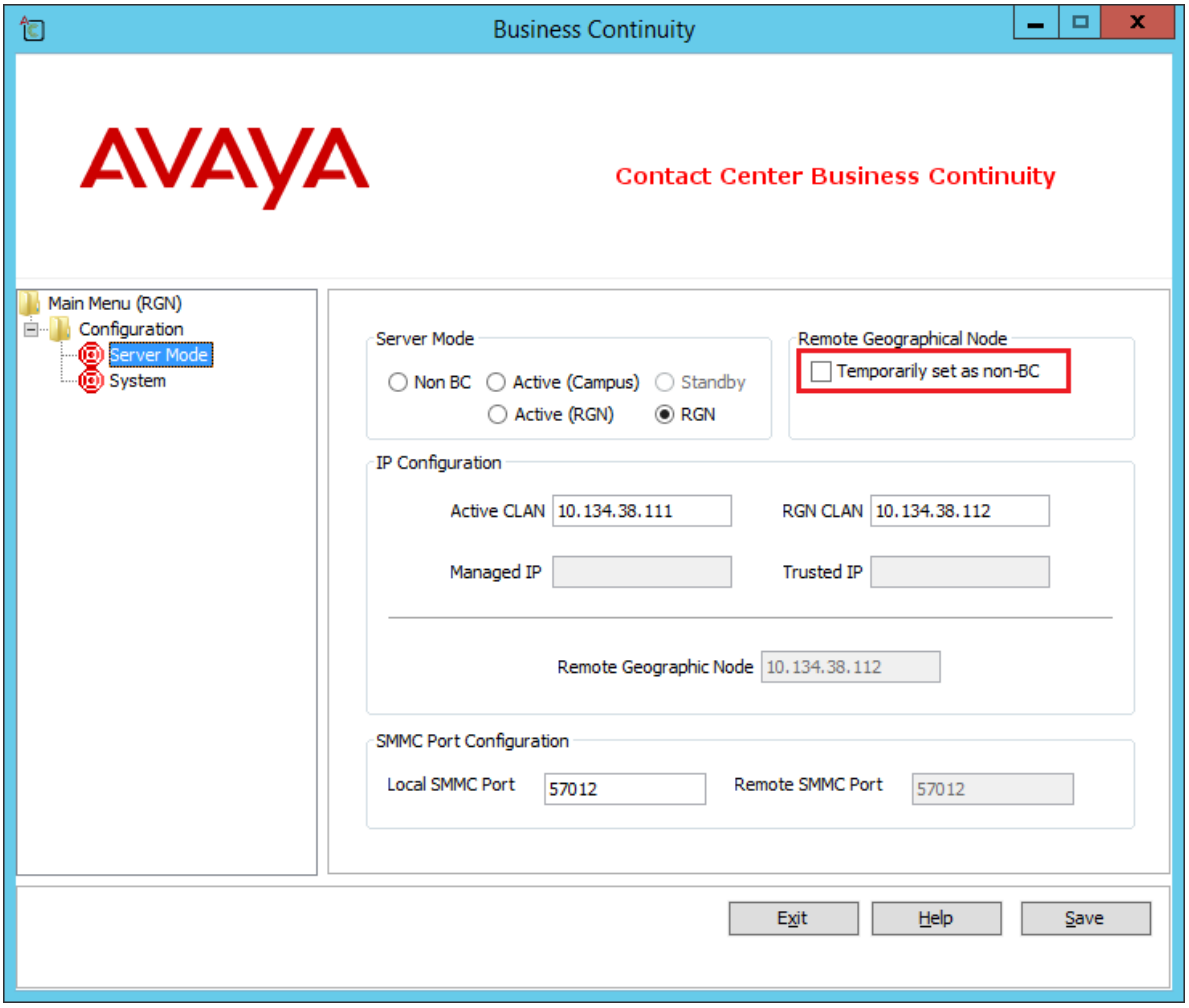
Verify Avaya Contact Center Select Geographic Business Continuity before placing the system into production.

Procedure

1. If you have access to the Avaya Contact Center Select active server, for testing purposes, temporarily power-down the active server. In a real-world disaster recovery scenario, you might not have access to the active server.
2. Log on to the Avaya Contact Center Select (ACCS) RGN server.
3. On the Windows taskbar, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Stop BC System**. This isolates the RGN from the active server.

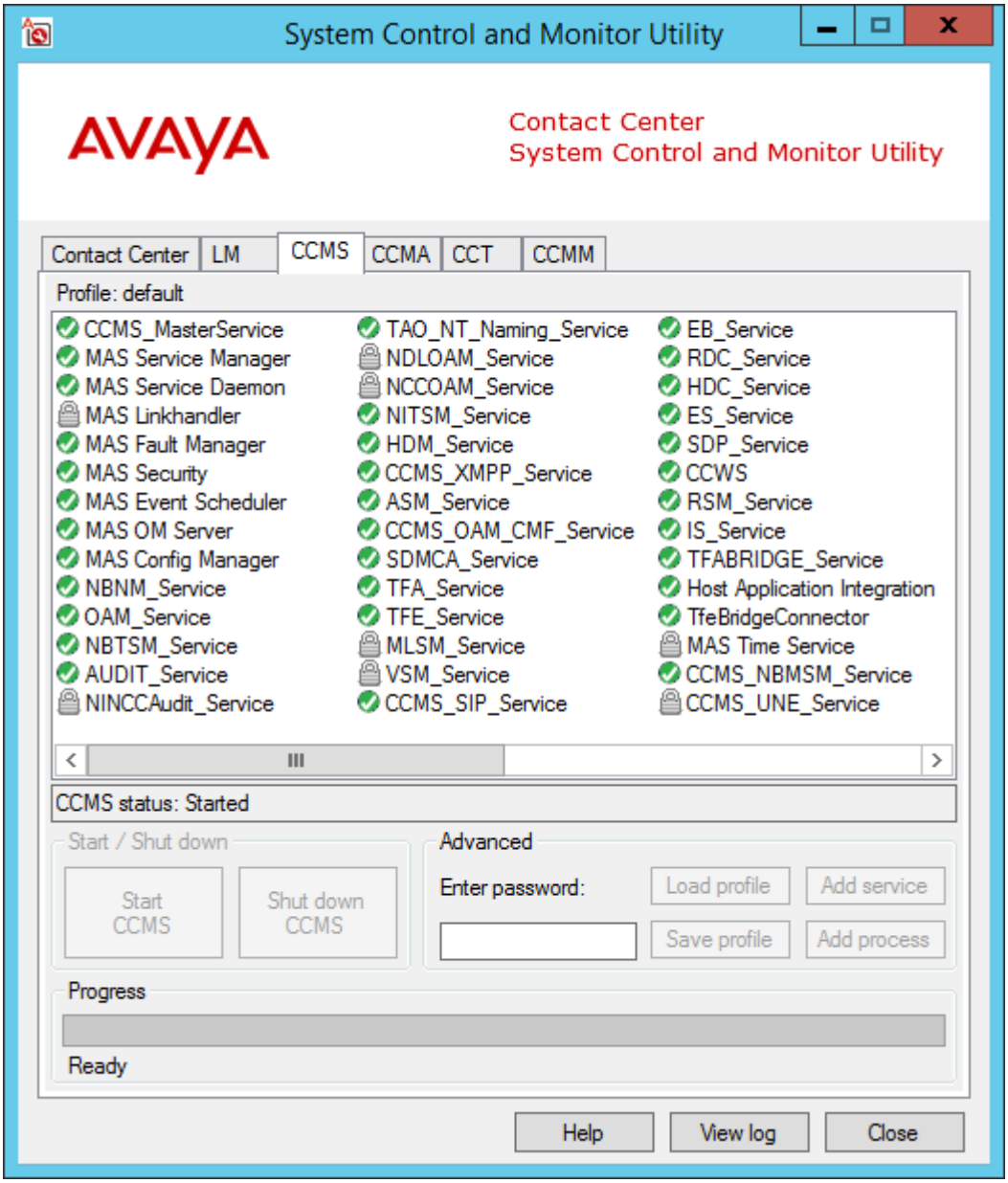


4. On the **Apps** screen, in the **Avaya** section, select **Business Continuity**.
5. Expand **Configuration**.
6. Double-click **Server Mode**.

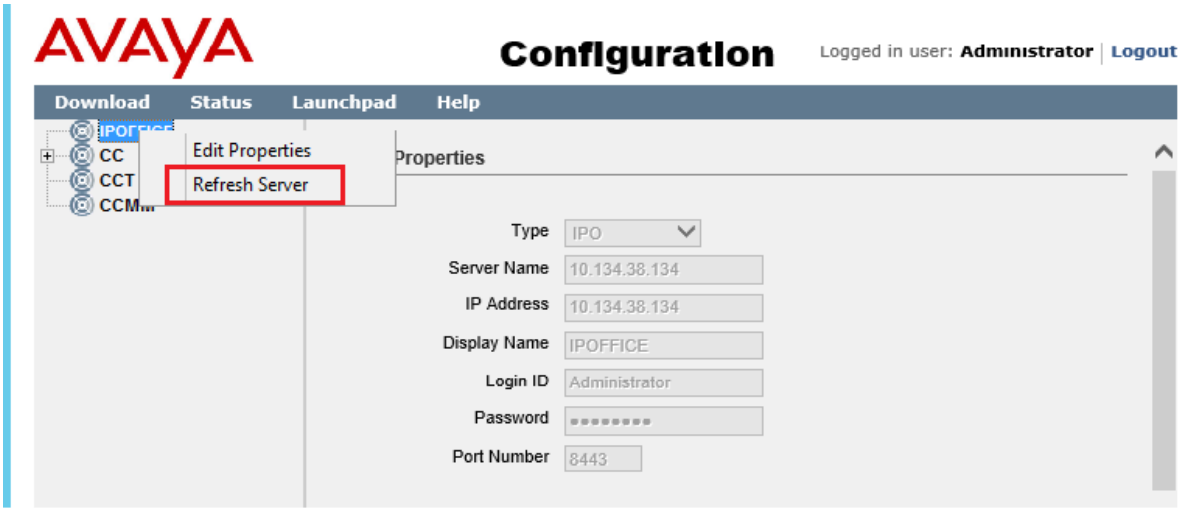


7. Select the **Temporarily set as non-BC** check box.
8. Click **Save**.
9. If a Business Continuity message box appears requesting a server reboot, click **OK** to reboot the server.
10. On the Windows taskbar, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Start System**.

    The Contact Center services on the RGN server begin to start.
11. Using the System Control and Monitor Utility (SCMU), verify that the Contact Center services on the RGN server start running.



12. When the Contact Center services are running on the RGN server, make a test call into the Contact Center. Verify that the call is treated and routed to an agent. Verify that the agent has full call control.
13. On the RGN server, log on to the local RGN CCMA Web interface with Administrator privileges.
14. On the CCMA **Launchpad**, select **Configuration**.
15. In the left pane, right-click on **IPOFFICE**. and select **Refresh Server**.



This updates the IP Office server with the new RGN CCMA IP address and ensures that the Data Synchronization Service with ACCS continues to function.

16. If your solution supports multimedia contacts, send a test email to one of the configured mailboxes. Verify that Avaya Contact Center Select receives the email and that it is routed to an agent for processing. Verify that the agent has full multimedia contact control.
17. If you are using Prompt Management in CCMA, log on to CCMA and in the *Configuration* section, select *Master Content Store* for your local RGN Avaya Aura® Media Server.
18. After verifying Geographic Business Continuity, the Avaya Contact Center Select system is no longer resilient. The current RGN server is not shadowing the current active server. To make the Avaya Contact Center Select system resilient again, reinstate Geographic Business Continuity. For more information, see Reinstating Geographic Business Continuity on page 153.

Reinstating Geographic Business Continuity

About this task

When the root cause of the ACCS active server failure has been addressed, you can reinstate Geographic Business Continuity resiliency using the following steps.

Procedure

1. On the Remote Geographic Node (RGN), use the System Management and Monitoring Component (SMMC) system tray to stop the Business Continuity system. This ensures that the Remote Geographic Node server is not shadowing data from the active server.
2. On the ACCS RGN server, back up all the application databases and the ADMIN database.
3. On the ACCS active server, restore the RGN database backups.

4. On the ACCS RGN server, using the Business Continuity configuration utility, clear the **Temporarily set as non-BC** check box. This puts the RGN server back into RGN mode. If a message box appears prompting you to reboot the server, ignore it.
5. On the active server, open Server Configuration.
6. Verify that all the information under each tab is correct, and click **Apply All**.
7. On the Restart Required message box, click **Yes**.
8. After the active ACCS server has started, log on to CCMA. During the first CCMA log on session, CCMA presents a RGN Information message box requesting confirmation to change CCMS, CCT, and CCMM server names back to the original active server values. Click **Yes** to accept the recommended changes. This CCMA message box is displayed only once.
9. On the active server, log on to the local CCMA Web interface with Administrator privileges. On the CCMA **Launchpad**, select **Configuration**. In the left pane, right-click on **IPOFFICE** and select **Refresh Server**. This updates the IP Office server with the active CCMA IP address and ensures that the Data Synchronization Service with ACCS continues to function.
10. After the active server has started, back up the active server databases and restore them to the RGN server.
11. On the RGN server, open Server Configuration.
12. Verify that all the information under each tab is correct, and click **Apply All**.
13. On the Restart Required message box, click **Yes**.

Verifying IP Office voice platform resilience

Before you begin

- If your Avaya Contact Center Select Business Continuity solution is not using an IP Office resilient system, skip this procedure. If your solution is using an IP Office resilient system, ensure IP Office resilience is configured.

About this task

Verify that when the IP Office Primary Server fails, Avaya Contact Center Select transitions call control from the IP Office Primary Server to the IP Office Secondary Server. If the IP Office Primary Server fails or is stopped, the IP Office Secondary Server continues to process voice calls.

On startup, the active Avaya Contact Center Select (ACCS) server registers with the IP Office Primary Server. If the active ACCS server is not able to communicate and register with the IP Office Primary Server, after a configurable delay, the active ACCS server attempts to register with the IP Office Secondary Server. You can configure this *Registration Switchover Delay* using the ACCS Server Configuration utility.

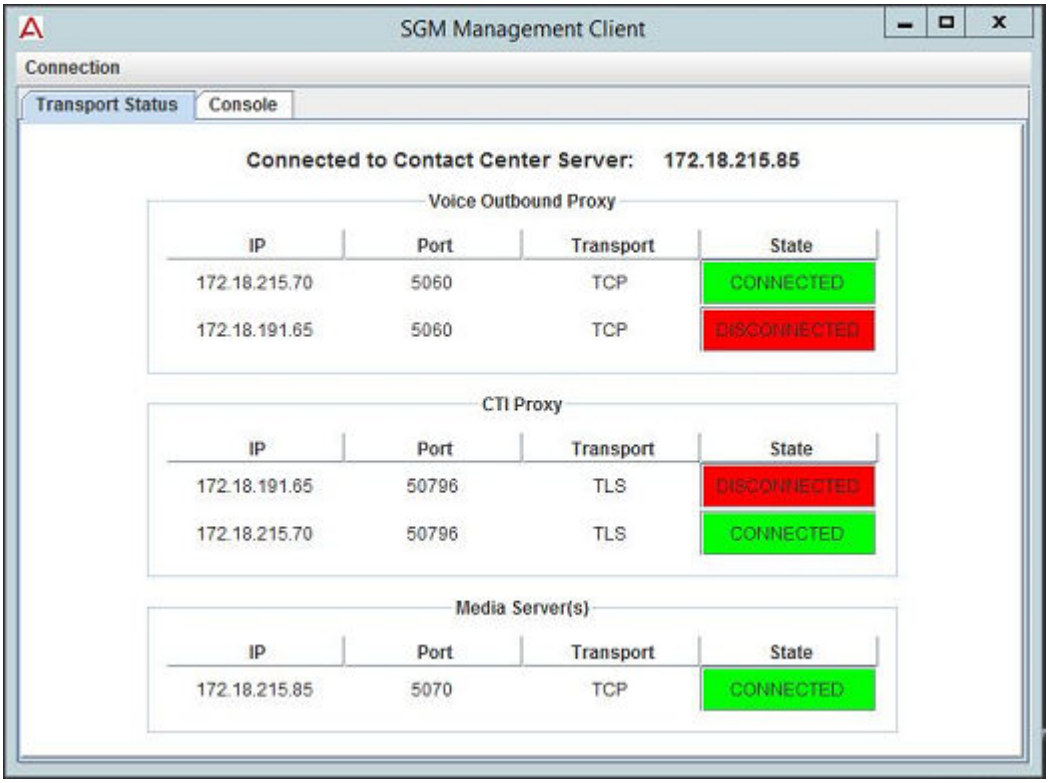
If your Avaya Contact Center Select solution is not using IP Office resiliency, skip this procedure.

Note:

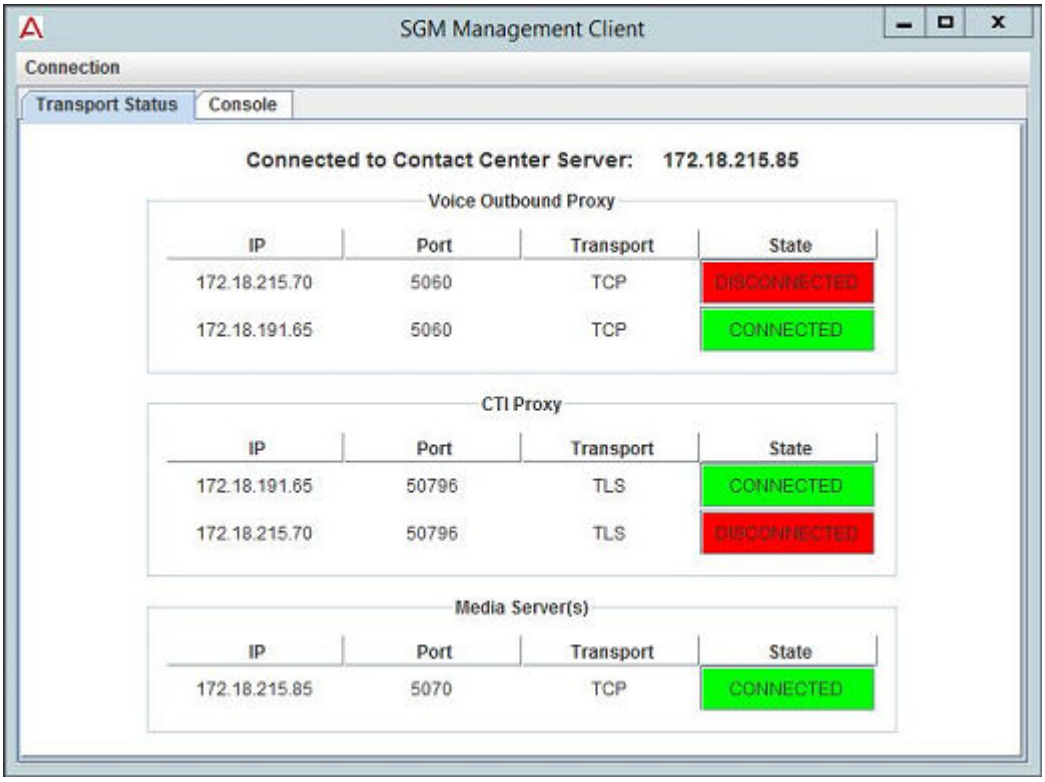
Verify that your IP Office voice platform is resilient before placing the system into production.

Procedure

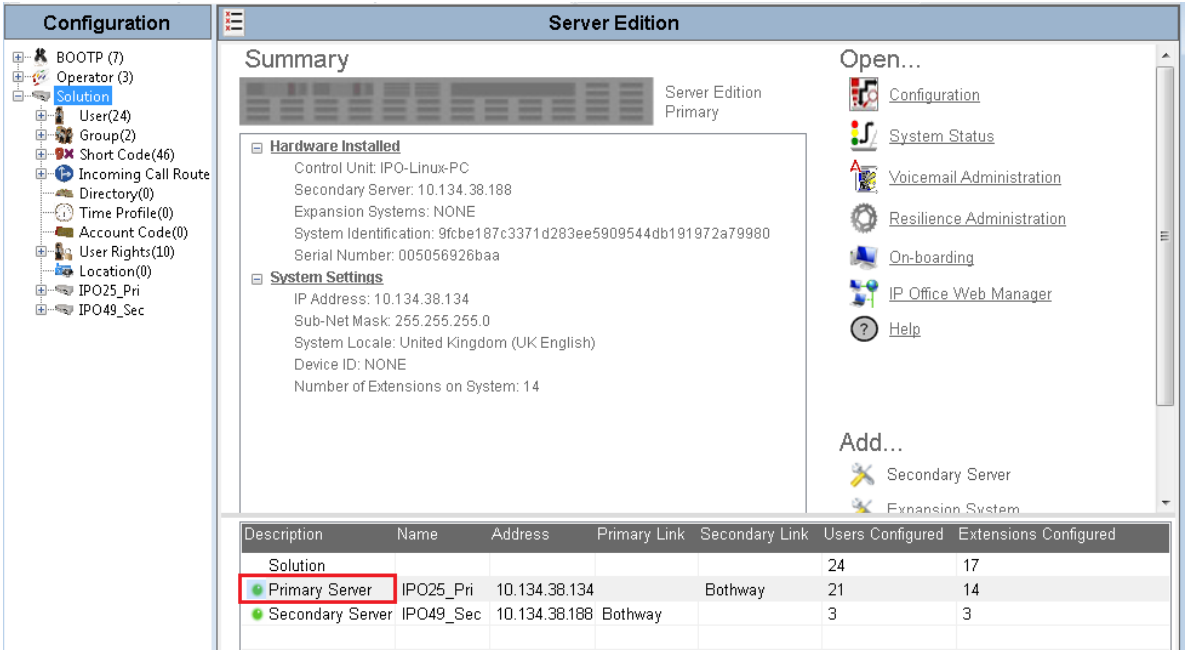
1. Log on to the active ACCS server.
2. On the **Apps** screen, in the **Avaya** section, select **SIP Gateway Management Client**.
3. Verify that the active ACCS server is registered with the IP Office Primary Server.



4. Disconnect the network cable from the IP Office Primary Server.
5. Verify that ACCS agent H.323 phones register with the IP Office Secondary Server.
6. Verify that the IP Office Secondary Server routes customer calls to ACCS and that ACCS agents can process those customer calls. At this time, the IP Office system is no longer resilient. The IP Office Primary Server is offline and the IP Office Secondary Server is processing ACCS contacts. The active ACCS server is now registered with the IP Office Secondary Server.

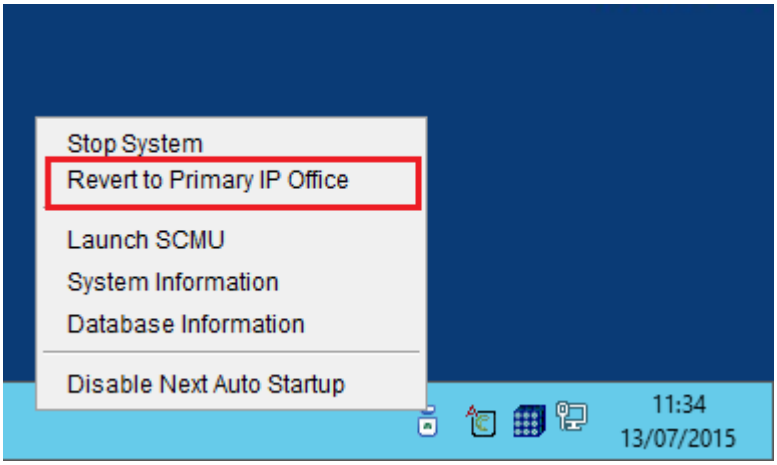


7. Reconnect the network cable to the IP Office Primary Server.
8. Wait for the IP Office Primary Server to start up. Using IP Office Manager, the traffic light icon to the left of the IP Office Primary Server is green when it is ready.

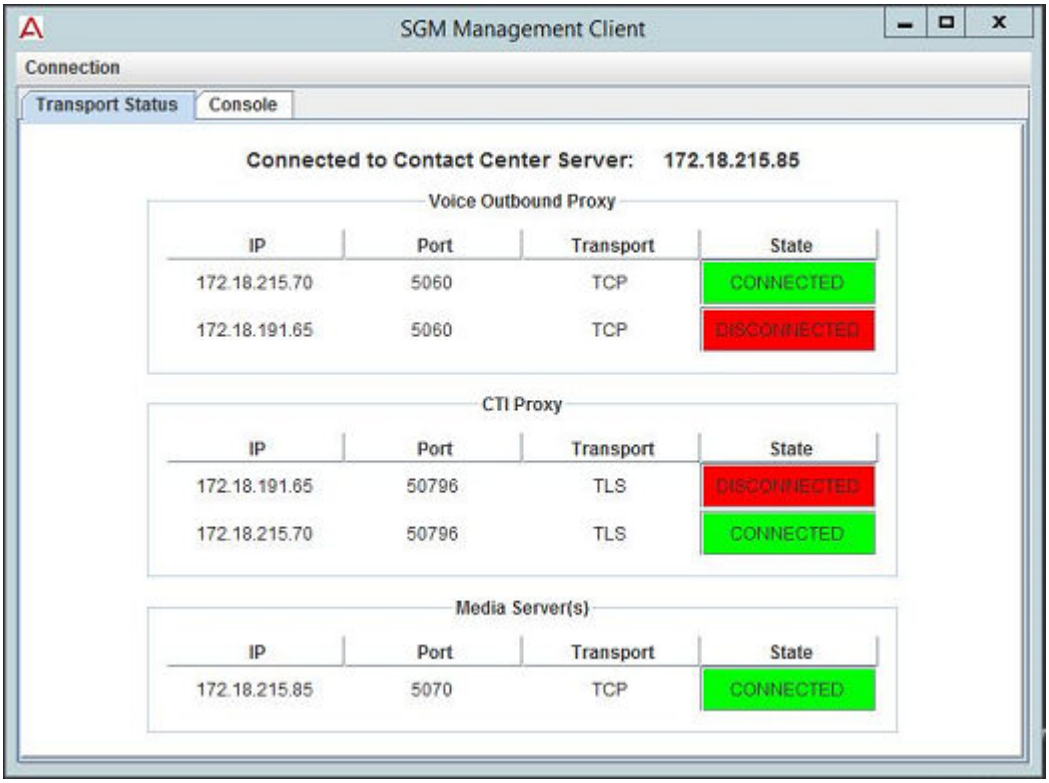


9. Rehome the agent H.323 phones to the IP Office Primary Server.

10. On the ACCS active server, on the Windows taskbar, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Revert to Primary IP Office**.



The ACCS active server registers with the IP Office Primary Server.



11. The IP Office system is now resilient again. The ACCS active server is registered with the IP Office Primary Server.

Configuring the external Web Communications server

Before you begin

- Know the custom interface folder names and paths for the web.xml and .jsp files for the sample Web communications installation.

About this task

If your ACCS solution uses an external Web Communications server, configure the Web Communications server to communicate with the ACCS active server or the ACCS RGN server.

If the ACCS active server is processing contacts, configure the Web Communications server to use the ACCS active server.

If the ACCS RGN server is processing contacts, configure the Web Communications server to use the ACCS RGN server.

You must update for .jsp files with Apache Tomcat. If you use a different servlet engine (for example, JRun or WebLogic) or a different technology (ASP.NET), you must use the standard procedures for your environment.

Procedure

1. Log on to your external Web Communications Web server.
2. Open the config file located at C:\xampp\htdocs\Code\include in Notepad or another text editor.
3. Locate the text string CCMM_MACHINE_NAME and update the ACCS active or the RGN server name after the ’=’ sign.
4. Save and close the file.

Chapter 9: Business Continuity maintenance

This section describes the procedures you use to maintain Avaya Contact Center Select Business Continuity.

Patching Avaya Contact Center Select Business Continuity

Before you begin

- Ensure that you have a standby server license for the server you are patching.
- Ensure both existing Avaya Contact Center Select servers have the same patch level.

About this task

Apply patches to an Avaya Contact Center Select Business Continuity solution to resolve product issues. Both Avaya Contact Center Select servers must be updated to the same patch level.

To install a Contact Center Feature Pack or Service Pack, you must schedule a maintenance cycle and restart the contact center. For more information, read the Feature Pack or Service Pack Readme file.

If shadowing is stopped for more than 24 hours then you must back up the active server database and restore it onto the standby server before re-enabling shadowing. Ensure that the system clock time on the Avaya Contact Center Select servers are synchronized.

Procedure

1. Read the patch Readme file.
2. Use the System Management and Monitoring Component (SMMC) utility to stop the Avaya Contact Center Select active server.

   Note: Stopping the ACCS active server stops the ACCS standby or RGN server.
3. Apply the Avaya Contact Center Select patch to the active server.
4. Apply the Avaya Contact Center Select patch to the standby or RGN server.
5. Start the ACCS active server.

6. When the ACCS active server is running, start the ACCS standby or RGN server.

Starting a Business Continuity active server

About this task

Start the active server using the System Management and Monitoring Component (SMMC) system tray. Starting the active server starts CCMS, CCT, and system processes.

Procedure

1. Log on to the active server.
2. On the Windows taskbar of the active server, right-click on the **System Management and Monitoring Component (SMMC)** system tray, and select **Start BC System**.
3. To verify that the Contact Center services are running using the System Control and Monitor Utility (SCMU). Check that the CCMS and CCT services are running.

Starting shadowing on a Business Continuity standby server

About this task

Start shadowing on the standby server using the System Management and Monitoring Component (SMMC) system tray.

The standby server shadows the active server, maintaining a near real-time local copy of the CCMS, CCT, and Administration databases. The standby server is therefore configured with the most recent data and it can take over from the active server if necessary.

Procedure

1. Log on to the standby server.
2. On Windows taskbar of the standby server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Start BC System**.
3. To verify that the Contact Center services are running using the SCMU, select **Avaya** > **Contact Center** > **Common Utilities** > **System Control and Monitor Utility**. Check that the CCMS and CCT services are not running.

Reviewing shadowing

About this task

Review the server status to confirm that the shadowing is occurring between the servers.

Procedure

1. Log on to the server for which you want to review the switchover status.
2. On the **Apps** screen, in the **Avaya** section, select **Business Continuity**.
3. In the left pane of the Business Continuity window, expand **Configuration**.
4. Select **System**.
5. In the **System Configuration** panel, locate the shadowing entries.
6. Confirm the last record of shadowing is within the last minute of the current time.
7. Click **OK**.

Stopping Business Continuity on a standby server

About this task

Stop shadowing and disable Business Continuity on a standby server using the System Management and Monitoring Component (SMMC) system tray.

Procedure

1. Log on to the standby server.
2. On Windows taskbar of the standby server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Stop BC System**.
3. On the **Apps** screen, in the **Avaya** section, select **Business Continuity**.
4. Expand **Configuration**.
5. Double-click **Server Mode**.
6. Under **Server Mode**, select **Non BC**.
7. Click **OK**.

Stopping Business Continuity on an active server

About this task

Stop shadowing and disable Business Continuity on an active server using the System Management and Monitoring Component (SMMC) system tray.

Procedure

1. Log on to the active server.
2. On Windows taskbar of the active server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Stop BC System**.
3. On the **Apps** screen, in the **Avaya** section, select **Business Continuity**.
4. Expand **Configuration**.
5. Double-click **Server Mode**.
6. Under **Server Mode**, select **Non BC**.
7. Click **OK**.

Disabling Auto Startup on a Business Continuity server after reboot

About this task

Disable your Business Continuity server from automatically starting services after you reboot the server.

This procedure applies to both active and standby servers.

Procedure

1. Log on to the active or standby server.
2. On the Windows taskbar of the server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Disable Next Auto Startup**.

Selecting a startup mode on the standby server after reboot

About this task

Select a startup mode for your standby server. You can choose from the following options:

- **Full BC Startup**. If you choose this option, after a system reboot, SMMC starts all services and starts shadowing the active server.
- **Shadowing Only Startup**. If you choose this option, after a system reboot, SMMC does not start services but starts shadowing the active server.

Procedure

1. Log on to the standby server.

2. On the Windows taskbar of the standby server, right-click on the System Management and Monitoring Component (SMMC) system tray, and click **Select Standby Auto Startup Mode**.
3. Select **Full BC Startup** or **Shadowing Only Startup**.

Re-enabling Business Continuity after stopping services

About this task

This procedure applies only when the Business Continuity state of the active server in the SMMC system tray is running but with switchovers disabled. This state occurs when you stop a critical service on the active server using System Control and Monitor Utility (SCMU).

Re-enable Business Continuity to ensure all services are started and your active Business Continuity server is in running state.

Procedure

1. Log on to the active server.
2. On the Windows taskbar of the server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Re-enable BC System**.

   All services are now started and the active Business Continuity server is in running state.

Chapter 10: Troubleshooting

This section describes the procedures you use to troubleshoot Avaya Contact Center Select Business Continuity.

Troubleshoot Avaya Contact Center Select Business Continuity to resolve errors that occur when the active server does not switch over as expected or when the standby server fails to shadow the active server.

Troubleshooting Business Continuity

About this task

Troubleshoot Business Continuity resiliency for a pair of Avaya Contact Center Select servers in a campus solution.

In a campus Business Continuity solution, a CCMS or CCT service failure, hardware, network, or database failure can initiate a switchover but only in the following situations:

- The active server is in the active mode.
- The active server is running. All the critical CCMS and CCT services are monitored and running.
- The active server has Enable Switchover enabled.
- The active and standby servers can communicate with the trusted server.
- The active server database and standby server database are synchronized. The standby server database is shadowing the active server database, and is up to date.

If the Contact Center Administrator uses the Windows Service Control Manager (SCM) to stop a monitored service on an active server, a switchover occurs. If the Contact Center Administrator uses the System Control and Monitor Utility (SCMU) to stop a monitored service on an active server, a switchover does not occur. If a critical service is down or restarts on the active server, a switchover does not occur.

Business Continuity utility

Configure Business Continuity resiliency for CCMS and CCT using the Business Continuity (BC) utility in the Database Utilities. The Business Continuity utility is used to configure which server is the active and which is the standby server. The BC utility also configures the Managed IP of the active server.

SMMC system tray

The Contact Center System Management and Monitoring Component (SMMC) system tray gives quick access to action items in your Business Continuity environment. The SMMC system tray has the following main menu options and action items:

- Start BC System
- Stop BC System
- Disable Switchover
- Enable Switchover
- Launch SCMU
- System Information
- Database Information
- Disable Auto Startup
- Re-enable BC System

To access the SMMC system tray menu, right-click the SMMC icon on the Windows taskbar.

Business Continuity utility and SMMC system tray

To commission Business Continuity, use the Business Continuity utility to configure Business Continuity IP addresses and to configure which server is the active server and which is the standby server. Then use the System Management and Monitoring Component (SMMC) system tray to start database shadowing and Business Continuity functionality.

To troubleshoot Business Continuity, use the System Management and Monitoring Component (SMMC) utility, Windows Events logs, and the System Control and Monitor Utility (SCMU) to diagnose Business Continuity issues. Then use the Business Continuity utility in to resolve the diagnosed issues.

Procedure

1. Log on to the active server.
2. On the Windows System Tray, right-click on the System Management and Monitoring Component (SMMC) system tray icon, and select **System Information**.
3. Examine the **System Information** dialog to determine the cause of Business Continuity related issues.
4. On the Windows System Tray, right-click on the System Management and Monitoring Component (SMMC) system tray icon, and select **Database Information**.
5. Examine the **Database Information** dialog to determine the cause of Business Continuity related issues.
6. Repeat these steps on the standby or Remote Geographic Node (RGN) server.

Procedure job aid

The following examples are from a functional pair of campus Business Continuity Avaya Contact Center Select servers.

Use the System Management and Monitoring Component (SMMC) utility to diagnose Business Continuity issues. Use the Business Continuity (BC) Utility in the Database Utilities to resolve the diagnosed issues.

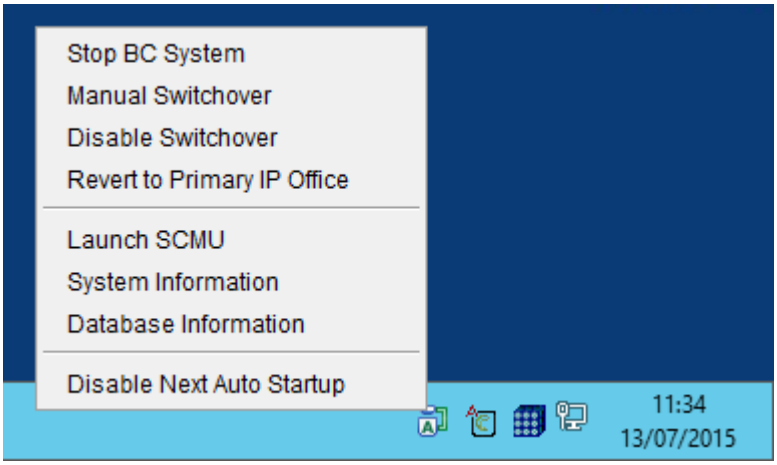


Figure 19: Example of using SMMC on a functional active server

In a Business Continuity solution, the SMMC system tray icon displays “A” to indicate that the server is configured as a Business Continuity active server. You can use SMMC on active server to perform a Manual Switchover to the standby server.

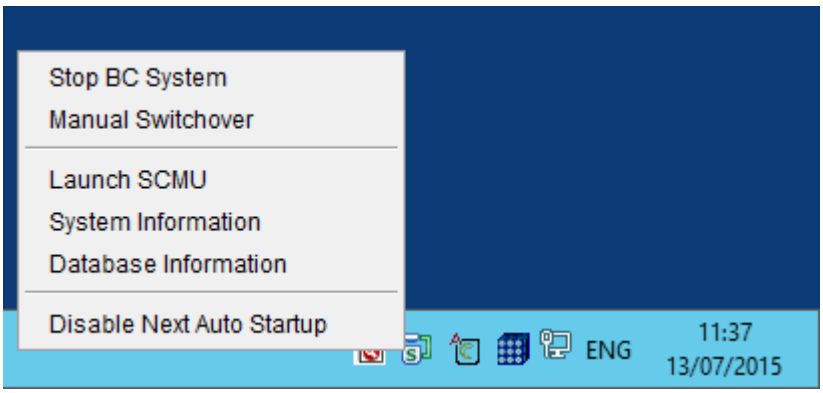


Figure 20: Example of using SMMC on a functional standby server

In a Business Continuity solution, the SMMC system tray icon displays “S” to indicate that the server is configured as a Business Continuity standby server. The standby server has different SMMC system tray menu options to the active server.

You can use SMMC system tray to display system and database information, and to diagnose Business Continuity related issues.

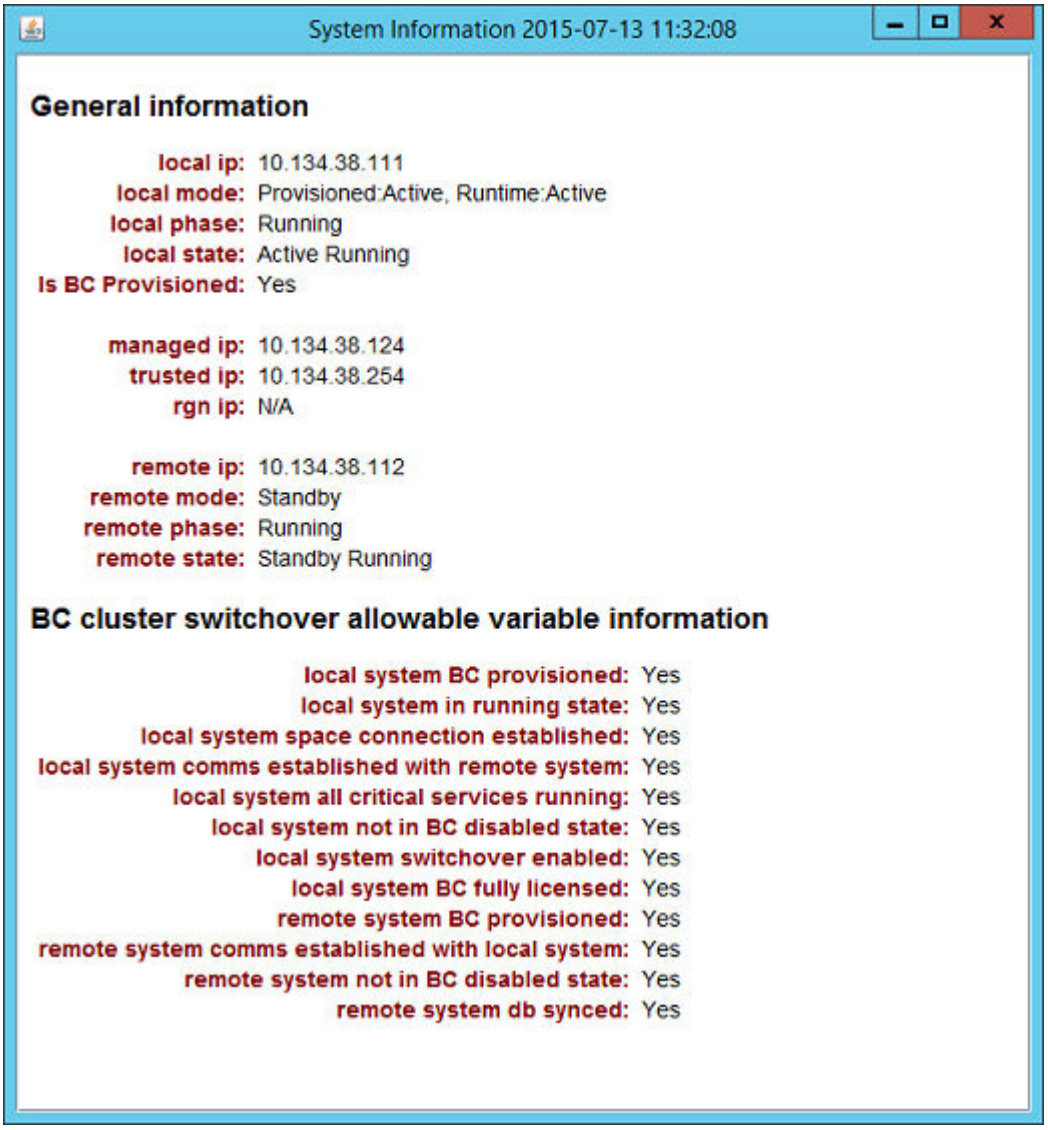


Figure 21: Example of a functional Business Continuity active server System Information dialog

Examine the System Information dialogs on the active server and standby server dialogs to ensure they mirror each other. The Trusted IP address and Managed IP address must be the same on both servers. Examine the “General Information” section to ensure that your Business Continuity solution is configured correctly, and to determine why Business Continuity last stopped. When in Stopped state, System Information displays a “Local last known stop reason”.

On the active server, examine “local system switchover enabled” to confirm that switchover is supported and enabled.

On the active server, examine “local system all critical services running” to confirm that all the necessary services are running. If any critical service is not running, use the System Control and Monitor Utility (SCMU) to investigate further.

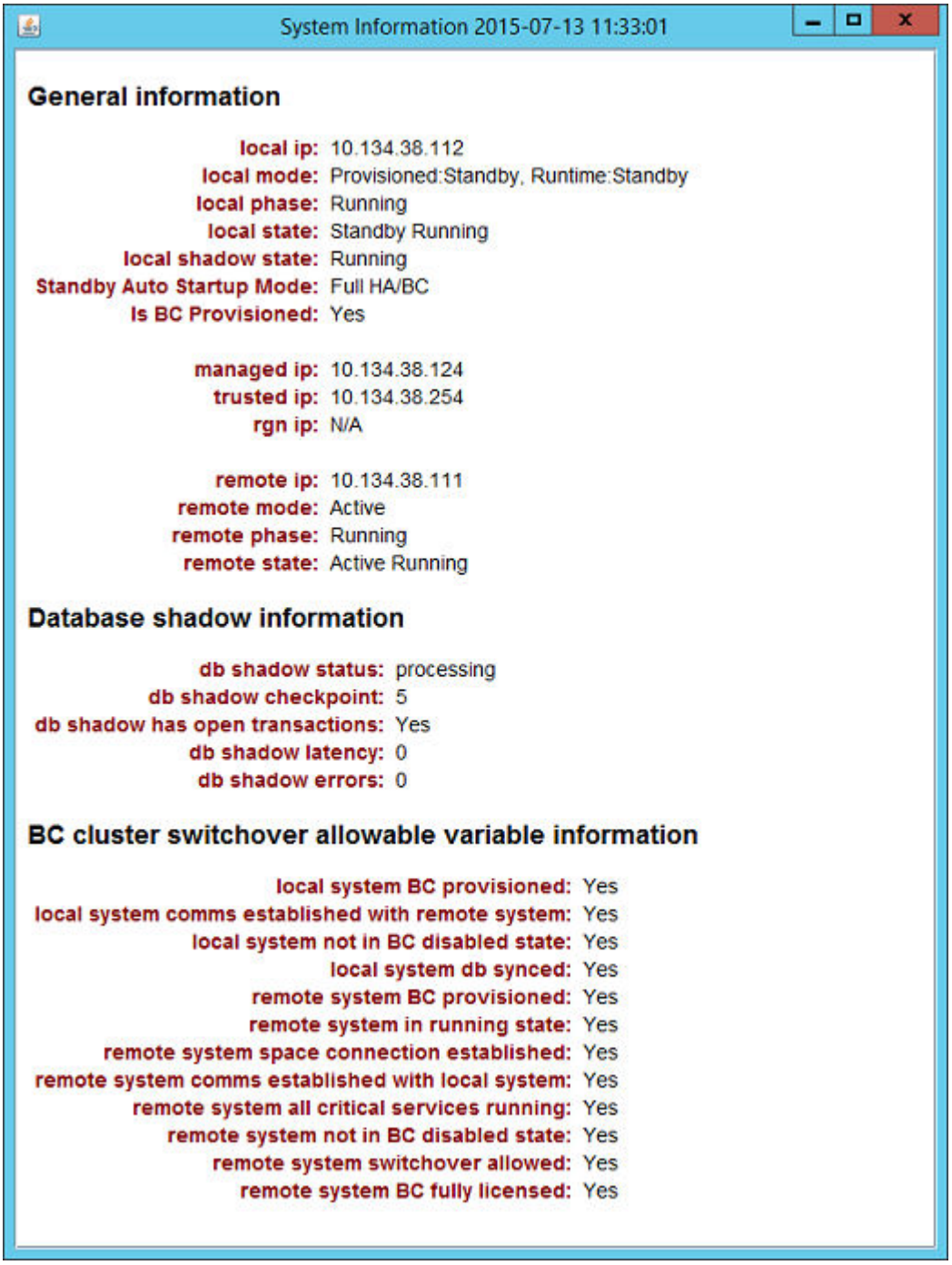


Figure 22: Example of a functional Business Continuity standby server System Information dialog

The standby server system information dialog displays Database Shadowing information. Examine the “Database shadow information” section to determine if the network in your Business Continuity solution is causing shadowing issues.

Examine “**local system comms established with remote system**” to confirm that the SMMC on the standby server can communicate with the SMMC on the active server, and vice versa.

Troubleshooting when shadowing fails to start

About this task

You must backup the active server database, restore it onto the standby server, and enable shadowing within 24 hours. If the difference in time between the active and standby server database content is greater than 24 hours then database shadowing does not work. If shadowing is stopped for more than 24 hours then you must backup the active server database and restore it onto the standby server before re-enabling shadowing. Ensure that the system clock time on the active and standby servers are synchronized.

Procedure

1. Use the Database Maintenance utility to make a new backup of the active server database.
2. Use the Database Maintenance utility to restore the database to the standby server.
3. Re-commission Business Continuity on the standby server.
4. Use the Business Continuity utility to enable shadowing.

Troubleshooting when SMMC fails to start

About this task

The Contact Center System Management and Monitoring Component (SMMC) system tray gives quick access to action items in your Business Continuity environment.

To access the SMMC system tray menu, right-click the SMMC icon on the Windows taskbar. The SMMC system tray is a graphical interface for the underlying SMMC system. If the SMMC system fails or stops, the SMMC system tray can display a “No connection to SMMC” message. You can use the SMMC system tray menu to restart the SMMC system.

Procedure

1. Log on to the server.
2. On the Windows System Tray, right-click the System Management and Monitoring Component (SMMC) system tray icon, and select **Start SMMC**.

Troubleshooting when services fail to start

About this task

The active and standby servers use a Trusted IP address to verify network connectivity. If the active server cannot communicate with the standby server it attempts to communicate with the Trusted IP address. If the active server cannot communicate with the Trusted IP address on startup then no Contact Center services start on that server.

Avaya recommends that you use the IP address of some part of your IT infrastructure that is always available to respond to a ping request, as the Trusted IP address.

Procedure

Verify the active and standby servers can communicate with the Trusted IP address.

Troubleshooting shadowing failures

About this task

Troubleshoot when the standby server does not shadow the active server. The standby set of Avaya Contact Center Select applications monitors and shadows the active applications in the system and does not process calls.

Procedure

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 the Cache service is running on the standby server.
3. Verify that you have installed a standby server license to enable Business Continuity.
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 Business Continuity 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. Verify that both the active and standby servers can ping the Trusted IP address.
9. Examine the Windows Event Viewer on the active and standby servers for Business Continuity, network, or Contact Center-related error messages.

Troubleshooting switchover failure

About this task

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.

Procedure

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 Business Continuity.
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 Business Continuity 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. Verify that both the active and standby servers can ping the Trusted IP address.
10. Examine the Windows Event Viewer on the active and standby servers for Business Continuity, network, or Contact Center related error messages.

Glossary

Active server	The Avaya Contact Center Select server in the solution that processes customer contacts and records statistical information.
Business Continuity	Business Continuity is the name of an Avaya Contact Center Select (ACCS) licensed feature. ACCS solutions that support Business Continuity have two ACCS servers. One server, called the active server, processes customer contacts. The other ACCS server (Standby or Remote Geographic Node) shadows the active server. If the active server fails, the other ACCS server takes over contact processing. This feature therefore provides ACCS redundancy, data resiliency, and disaster recovery.
Campus	A single network subnet, physical location, and Windows domain that contains the Avaya Contact Center Select active and standby servers.
IP Office Resilience	Resilience is the name of an IP Office solution feature. In solutions with an IP Office Primary Server and an IP Office Secondary Server, you can enable the IP Office Resilience feature. The IP Office solution can use the IP Office Secondary Server for redundancy or for shared resource resilience. If the IP Office Primary Server fails or is stopped for maintenance, the IP Office Secondary Server automatically continues to process voice calls.
Managed IP address	A Managed IP address is a virtual IP address that is attached to a Network Interface Controller (NIC) on the currently active server of a solution. In the solution, the server hosting the Managed IP address can change, but the Managed IP address remains constant. This allows client applications that connect to the solution using the Managed IP address to continue functioning irrespective of which solution server is currently active.
Remote Geographic Node	The standby server located in a different network subnet or remote geographic location outside of the campus location.
Standby server	The standby server shadows the active server. If the active server fails or is stopped for maintenance, the standby server can take over and process customer contacts.

Switchover	If the active server fails or is stopped for maintenance, the standby server in the ACCS solution starts up and begins to process customer contacts. This managed transition from the active server to the standby server is called a switchover. In a Campus Business Continuity solution, the switchover is automatic. In a Geographic Business Continuity solution, the switchover requires manual intervention.
Voice platform	The phone switch, typically used by a business to service internal phone needs. A phone switch usually offers more advanced features than are generally available on the public network. Also known as a private automatic branch exchange (PABX) private branch exchange (PBX). In Avaya Contact Center Select solutions, the voice platform is IP Office.

Index

P

R

S

T

U

V

W