Avaya Contact Center – Extended Capacity Solution Description

Release 10.0.2
Issue 2
March 2023

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

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 as indicated in the order, Documentation, or as authorized by Avaya in writing. 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.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

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

Third Party Components

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

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

Service Provider

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

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction

Purpose

This document provides a technical description of Avaya Contact Center – Extended Capacity. It describes the product features, interoperability, performance specifications, security, and licensing requirements.

This document is intended for implementation engineers and support personnel.

Required skills and knowledge

Ensure that you have the following administrative skills and knowledge:

- Red Hat® Enterprise Linux® or Oracle Linux.
- Avaya Aura® Call Center Elite. For general information about the Call Center Elite solution, see *Avaya Aura® Call Center Elite Overview and Specification*.
- Avaya Call Management System. For more information about administering Avaya Call Management System, see *Administering Avaya Call Management System*.
- Avaya Aura® Application Enablement Services. For more information about administering Application Enablement Services, see *Administering Avaya Aura® Application Enablement Services*.
- Avaya Experience Portal. For more information about administering Avaya Experience Portal, see *Administering Avaya Experience Portal*.
- Avaya Workplace Client. For more information about administering Avaya Workplace Client, see *Planning for and Administering Avaya Workplace Client for Android, iOS, Mac, and Windows*.
- The Avaya Agent for Desktop application. For general information about Avaya Agent for Desktop, see *Using Avaya Agent for Desktop*.
- SIP endpoints, such as 9600 series IP deskphones and Avaya J100 Series IP Phones. For more information about 9600 series IP deskphones, see *9600 Series IP Deskphones Overview and Specifications*. For more information about Avaya J100 Series IP Phones, see *Avaya J100 Series SIP IP Phones Overview and Specifications*.

New in this release

Avaya Contact Center – Extended Capacity Release 10.0.2 includes the following features and enhancements:

Support for call work codes

Avaya Contact Center – Extended Capacity supports call work codes. With this feature, agents can enter up to 16 digits to record customer-related information associated with a call. A work code specifies customer-specific event. The type of code depends on the call center usage.

Support for displaying of Collected Digits

Avaya Contact Center – Extended Capacity supports displaying of the collected digits information associated with a call to the agents. Up to 16 digits can be provided for display which can represent the caller-related information, such as an account number.

Support for post-call survey

Avaya Contact Center – Extended Capacity supports the post-call treatment by directing the calls to Avaya Experience Portal. When the agent completes the call before the caller, the contact center routes the call to the VDN extension specified for the VDN return destination.

The system administrator can configure which type of calls that the contact center can route to the post-call survey.

Support for malicious call trace

Avaya Contact Center – Extended Capacity supports malicious call trace. With this feature, agents can report malicious calls. The contact center tracks the calls and sends a report to Call Management System.

Support for multiple service observers

Avaya Contact Center – Extended Capacity supports two service observers to monitor the same agent login ID or endpoint extension. When one of the service observers stops monitoring the call, the other supervisor continues to observe calls.

Support for Service Observe Warning Tone (SOWT)

Avaya Contact Center – Extended Capacity includes an option to play a warning tone when an observer monitors an ongoing call.

The system administrator can configure SOWT for each agent profile in Contact Center Administration.

Support for service observing disconnect tones

Avaya Contact Center – Extended Capacity supports the service observing disconnect tones. The contact center plays various disconnect tones to indicate who ended the call first. There are an agent disconnect tone and a caller disconnect tone.

Support for new agent profile configuration parameters

Avaya Contact Center – Extended Capacity provides additional agent profile fields to configure parameters for call redirection, AUX work mode, and disconnect tones.

Dialed number and agent ID length changes

Avaya Contact Center – Extended Capacity supports a maximum length of 16 digits for dialed numbers and agent IDs configured for local, private, and reserved call types. The administrator can configure call types in the dial plan.

Support for the endpoints Group ID

Avaya Contact Center – Extended Capacity supports the Group ID configuration for endpoints. With the Group ID, an administrator can indicate which Network Location parameters the endpoint will use.

Restricted licensing modes

Avaya Contact Center – Extended Capacity supports the License Error and License Restricted modes when it detects that the license has expired. Avaya Contact Center – Extended Capacity enters License Error mode for 60 days. The Configuration Server web portal notifies the administrator that the contact center is in License Error mode.

Avaya Contact Center – Extended Capacity enters the License Restricted mode if the administrator does not install a license after deploying the contact center or if the contact center is in License Error mode for more than 60 days.

Support for redirecting network calls

Avaya Contact Center – Extended Capacity supports Network Call Redirection (NCR) for incoming trunk calls on its VDNs. When it receives a trunk call on a VDN, Avaya Contact Center – Extended Capacity requests the service provider to redirect the call and releases Routing Core Server resources from the resulting redirected call.

Support for a set vector step to manage music-on-hold

Avaya Contact Center – Extended Capacity supports the Music on Hold source configuration using a SET vector step. The contact center plays the Music on Hold when the caller is on hold. The administrator can configure Music on Hold for each agent profile, skill, or SET vector step in Contact Center Administration.

Support for the G.729 and G.729B codecs

Avaya Contact Center – Extended Capacity supports the G.729 and G.729B codecs for media handling between the Routing Core Server and agent endpoints.

Support for RTCP

Avaya Contact Center – Extended Capacity supports Real-time Transport Control Protocol (RTCP) to monitor transmission statistics and service quality and synchronize multiple streams. The system administrator can configure time interval and quality of service parameters for transmitting RTCP messages.

Support for SRTP and SRTCP

Avaya Contact Center – Extended Capacity supports Secure RTP (SRTP) and Secure RTCP (SRTCP) protocols for media transmission. The SRTP and SRTCP profiles provide transmission encryption of media data and message authentication.

Support for Avaya Workplace Client

Avaya Contact Center – Extended Capacity supports Avaya Workplace Client. Avaya Workplace Client is a soft phone application that provides access to Unified Communications (UC) and Over the Top (OTT) services.

Support for disaster recovery for geo-redundant HA deployment without Layer 2 networking

Avaya Contact Center – Extended Capacity supports disaster recovery for geo-redundant HA deployment without Layer 2 networking. The solution does not ensure call and state preservation in case of contact center failure.

Support for remote login through SBCE

With this feature, system administrators can configure Avaya Session Border Controller for Enterprise (SBCE) to enable contact center agents to log in remotely without using VPN.

Chapter 2: Avaya Contact Center – Extended Capacity solution overview

Avaya Contact Center – Extended Capacity is a single-server solution for large contact centers supporting up to 30,000 concurrent agents. The solution provides most of the Avaya Aura® Call Center Elite functionality, including advanced agent features. The system administrator can migrate from Call Center Elite to Avaya Contact Center – Extended Capacity without purchasing additional peripherals, such as agent endpoints and contact center applications.

In the Avaya Contact Center – Extended Capacity solution, the Routing Core Configuration Server (Configuration Server) provides the administration capabilities of Avaya Aura® System Manager. The administrator can configure most contact center services from the Configuration Server web portal.

The administrator can integrate Avaya Contact Center – Extended Capacity with performance management applications, such as Avaya Call Management System and Avaya Experience Platform™ Workforce Engagement. The administrator can also integrate the contact center with Computer Telephony Interface (CTI) applications using Application Enablement Services.

Avaya Contact Center – Extended Capacity uses various routing algorithms to increase agent productivity and maximize resource utilization. The routing algorithms and options are similar to the Avaya Aura® Call Center Elite solution. Additionally, the solution supports Enterprise Behavioral Pairing and provides AI routing.

Component overview

The Avaya Contact Center – Extended Capacity solution provides maximum efficiency through a combination of multiple services on a single Routing Core Server. The server contains all core Automatic Call Distribution (ACD) components that provide call routing, agent management functionality, and contact center connectivity. The solution supports High Availability so that if one server within the availability group fails, another server can continue operation.

The software that operates outside the Routing Core Server includes the following groups:

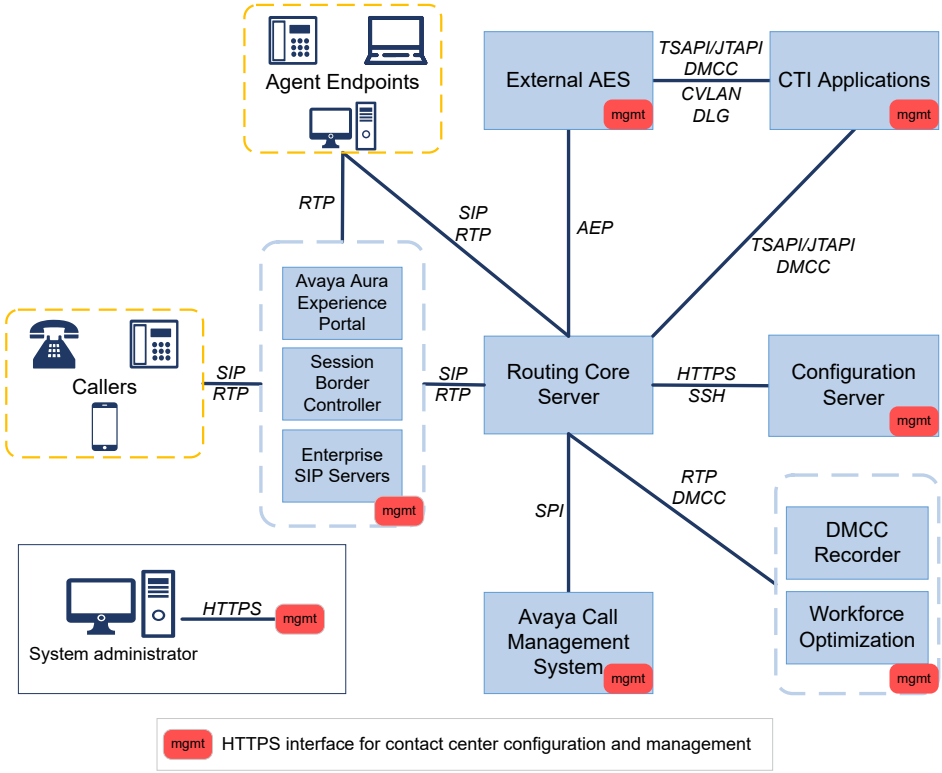
- The software essential to the contact center configuration: the Configuration Server.
- The software essential for the contact center reporting: Call Management System.
- The optional software that the system administrator needs to install separately for additional functionality. For example, the Session Border Controller software.

- The software maintained by Avaya Services for enabling the solution service in the contact center environment. For example, the billing software.

Most of the solution components have an HTTPS interface, through which an administrator can manage and configure the contact center.

Topology

The following diagram provides an overview of the contact center architecture and components:



Component	Description
Routing Core Server	Provides ACD functionality.
Configuration Server	Manages the contact center system, security, and maintenance configuration and operation.
Call Management System	Provides real-time and historical reports on contact center entities, such as agents and skills. It also provides an administrative interface for supervisors to manage the agent skills.
DMCC Recorder	Records calls using Device, Media, and Call Control (DMCC) APIs.
Workforce Optimization	Enhances contact center productivity through agent scheduling and quality management.

Table continues…

Component	Description
External Application Enablement Services	Provides CTI via TSAPI/JTAPI, DMCC, CVLAN, and DLG. Avaya Contact Center – Extended Capacity supports external AE Services for migration from Avaya Aura® Call Center Elite. The contact center also supports internal AE Services within the Routing Core Server.
CTI applications	Monitor and control endpoints, agents, and calls through Application Enablement Services.
Avaya Experience Portal	Manages all voice self-service and Integrated Voice Response (IVR) applications.
Session Border Controller	Provides network security and interoperability between networks.
Enterprise SIP servers	Manage other Unified Communications (UC) and Call Center (CC) systems with SIP interfaces, such as Avaya Aura®.

Routing Core Server components

The contact center software that provides the ACD functionality runs within the Routing Core Server. Each server has a set of unique IP addresses and a single shared memory segment for Docker containers within the server.

The following table describes the Routing Core Server components:

Component	Description
Linux operating system	Manages software and hardware. Avaya Contact Center – Extended Capacity requires Red Hat® Enterprise Linux® (RHEL) or Oracle Linux operating system. The system administrator must install the required operating system with minimal configuration.
Docker	Manages container operations.
High Availability Sync service	Copies shared memory updates into a shared memory segment of a standby server over a network socket.
ACD Core	Manages call flows, call queues, agent selection not based on Enterprise Behavioral Pairing, contact and call information.
Telephony Feature Server (TFS)	Manages Avaya Advanced SIP Telephony (AST) procedures. Provides all telephony features, such as call transferring, conferencing, and Redirection on No Answer. Manages button presses and LED indication.
Media Server	Provides media functionality.
Avaya Contact Center – Extended Capacity Session Manager	Handles all SIP messages that go through the TFS. Avaya Contact Center – Extended Capacity Session Manager also handles endpoint registration and authentication.
Internal Application Enablement Services	Provides CTI capabilities.

Configuration Server overview

The Configuration Server provides a management platform with the following functionality:

- Collects log files from all contact center servers
- Provides secure authentication to the contact center
- Manages the database for all the configuration information
- Provides a web interface for configuring contact center servers
- Manages Avaya Contact Center – Extended Capacity license files
- Manages local and client certificates through certificate authorities

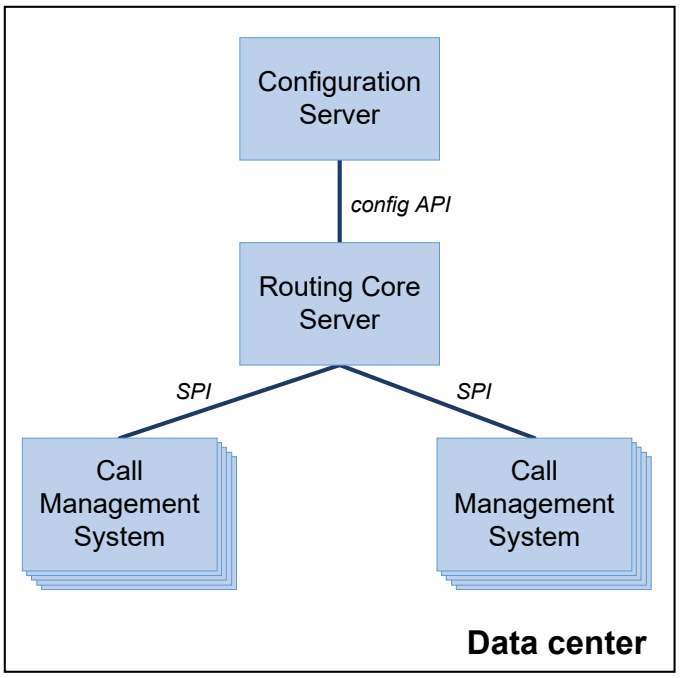
Contact center deployment environments

The system administrator can deploy Avaya Contact Center – Extended Capacity in the Simplex, local High Availability (local HA), or geo-redundant High Availability (geo-redundant HA) without Layer 2 networking environments.

Simplex deployment

In the Simplex deployment, the contact center operates in one data center that contains one Configuration Server and one Routing Core Server. The contact center does not provide server High Availability and cannot operate in case of server failure or maintenance procedures. Avaya recommends that you use Simplex deployment only in a lab environment.

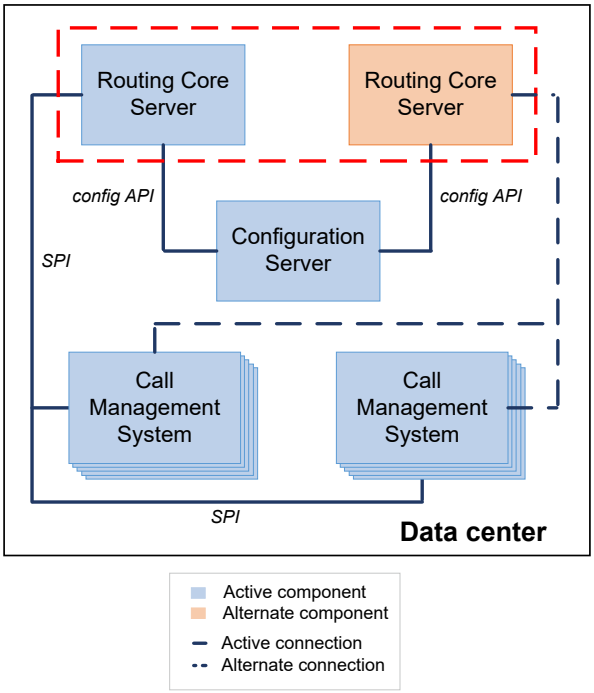
The following diagram provides an overview of the Simplex deployment architecture:



Local HA deployment

In the local HA deployment, the contact center operates in one data center that contains one Configuration Server and two Routing Core Servers.

The following diagram provides an overview of the local HA deployment architecture:

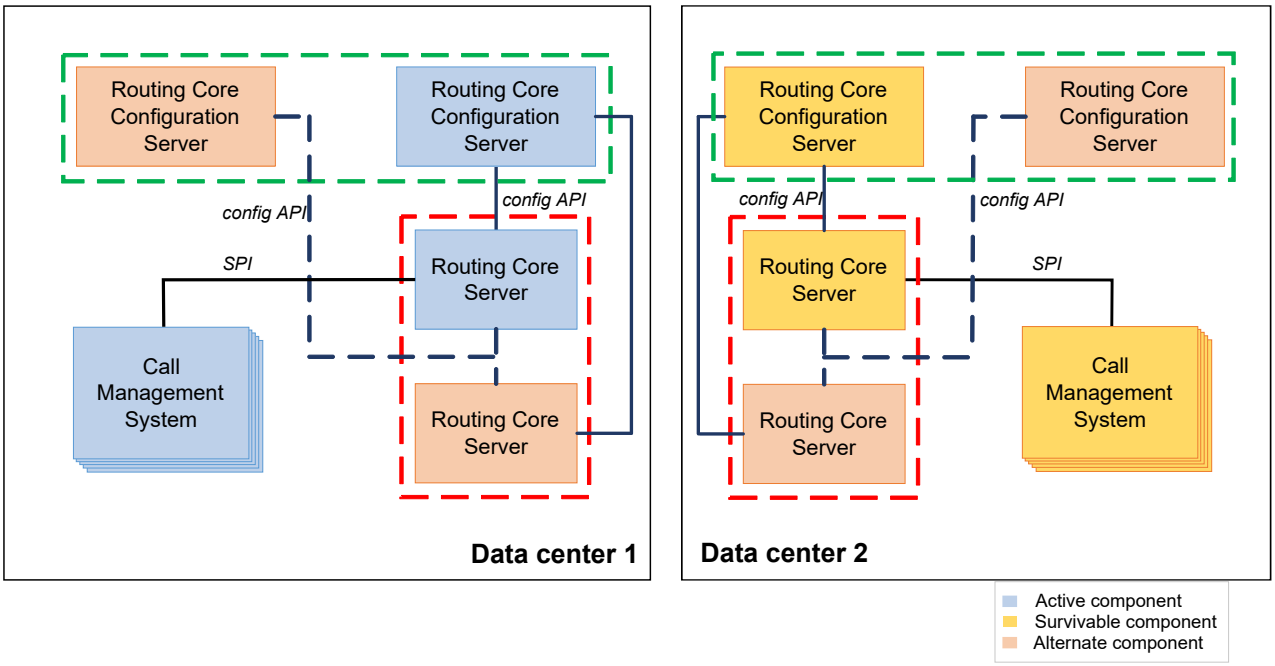


Geo-redundant HA deployment without Layer 2 networking

The contact center operates in two geographically separate data centers. Each data center contains two Configuration Server and two Routing Core Server instances.

Without Layer 2 networking, each data center contains an independent set of contact center servers and supports disaster recovery. In case of the primary data center failure, the Avaya Contact Center – Extended Capacity recovers contact center operations in the secondary data center and does not preserve active calls and agent states. The contact center supports high availability for Configuration Server and Routing Core Server instances within each data center.

The following diagrams provide an overview of the geo-redundant HA deployment architecture without layer 2 networking:


Routing Core Configuration Server
Routing Core Configuration Server
config API
config API
SPI
Routing Core Server
Call Management System
Routing Core Server
Data center 1
Routing Core Configuration Server
Routing Core Configuration Server
config API
config API
Routing Core Server
SPI
Call Management System
Routing Core Server
Data center 2
Active component
Survivable component
Alternate component

Chapter 3: Interoperability

Product compatibility

The following table specifies the compatibility of Avaya Contact Center – Extended Capacity with other Avaya products:

Avaya product	Release
9600 series IP deskphones - SIP	7.1 Agent Greeting support - 7.1.12
Avaya J100 Series IP Phones - SIP	4.0.x Agent Greeting support - 4.0.8
Avaya Workplace Client	3.26
Avaya Agent for Desktop	2.0.6
External Application Enablement Services	10
Avaya Call Management System	20.x
Avaya Aura®	10
Avaya Aura® Messaging	7.2
Avaya Messaging	11.0
Avaya Experience Portal	8.1.1
Callback Assist	5.0.1
Survey Assist	4.2
Avaya Session Border Controller for Enterprise	10.1
Avaya Experience Platform™ Workforce Engagement	15.2.2

For more information about the listed Avaya products and their requirements, see the corresponding product documentation at https://support.avaya.com/. For customization and implementation of third-party products, contact Avaya support personnel.

9600 series IP deskphones and Avaya J100 Series IP Phones model support

Avaya Contact Center – Extended Capacity supports the following SIP endpoint models:

Endpoint series	Supported SIP endpoint models
9600 series IP deskphones	• Avaya 9601 IP Deskphone • Avaya 9608 IP Deskphone • Avaya 9611G IP Deskphone • Avaya 9621G IP Deskphone • Avaya 9641G IP Deskphone • Avaya 9641GS IP Deskphone
Avaya J100 Series IP Phones	• Avaya J169 IP Phone • Avaya J179 IP Phone • Avaya J189 IP Phone

Chapter 4: Performance specifications

Maximum overall capacities

The following tables describe the maximum capacities for Avaya Contact Center – Extended Capacity components:

Routing Core Server capacities

Feature	Maximum value
Simultaneously registered endpoints	34,000
Simultaneously logged-in agents	30,000
Simultaneously logged-in supervisors	3,000
Concurrent calls	45,000
Calls in queue	45,000
External SIP servers	400
Maximum sustained call rate	85/sec
Media channels	150,000
Media mixers active	3,000
Agent and endpoint login rate	10/sec

Call Management System capacities

The Call Management System capacities depend on the Call Management System version used in the contact center.

Feature	Maximum value
Supported Call Management System links	4
Measured trunks	100,000
Number of agent and skill pairs	1,000,000
VDNs	30,000
Skills	15,000
Vectors	32,000
Simultaneous real-time reports	3,000

Configuration Server capacities

Feature	Maximum value
SAML and LDAP supported servers	2
Controlled Routing Core Server instances	4
Simultaneously logged-in administrators	100

Hardware requirements

Routing Core Server hardware requirements

For the Routing Core Server, Avaya recommends using Dell EMC PowerEdge R940 or an equivalent server with the following specifications:

Hardware	Minimum requirements
CPU	112 hyper-threaded, 2.1 GHz cores
Memory	1 TB
Storage	8 TB
Network	10 Gbps or 100 Gbps for larger configurations

Configuration Server hardware requirements

For the Configuration Server, Avaya recommends using a virtual machine with the following specifications:

Hardware	Minimum requirements
CPU	12 vCPUs, 2.1 GHz cores
Memory	20 GB
Storage	500 GB
Network	1 Gbps

Alternatively, the system administrator can use Dell EMC PowerEdge R640 or an equivalent server with the same or greater capacities of the Configuration Server on a virtual machine.

To ensure High Availability, Avaya recommends using dual power supplies and bonded network interface cards. The administrator must also configure RAID storage.

RAID configuration	Minimum requirements
RAID 1	240 GB X 2 disks. You must install the operating system on these disks.
RAID 5+1 (1 disk as hot spare)	1.6 TB X 8 disks

You must configure VMWare and the virtual machines on the RAID 1 and RAID 5 data stores respectively.

Software requirements

Avaya Contact Center – Extended Capacity server software requires one of the following operating systems:

- Red Hat® Enterprise Linux® (RHEL) versions 8.6
- Oracle Linux version 7.9

Disk partitioning requirements

When the administrator installs the operating system, Avaya recommends configuring the following disk partitioning for contact center servers:

Routing Core Server

Disk partition	Minimum storage requirements for 1 TB of disk space	Recommended increase for each extra 1 TB of disk space	Recommended storage requirements for 10 TB of disk space
`/boot`, `/boot/efi`, `swap`	Default	–	Default
`/`	100 GB	Minimal	200 GB
`/home`	150 GB	Up to 10%	800 GB
`/var`, including `/var/lib`	500 GB	Up to 50%	4.5 TB
`/var/log`	250 GB	Up to 50%	4.5 TB

Configuration Server

Disk partition	Minimum storage requirements for 500 GB of disk space	Recommended increase for each extra 500 GB of disk space	Recommended storage requirements for 5 TB of disk space
`/boot`, `/boot/efi`, `swap`	Default	–	Default
`/`	100 GB	Minimal	200 GB
`/home`	150 GB	Up to 10%	800 GB
`/var`, including `/var/lib`	150 GB	Up to 50%	2 TB
`/var/log`	100 GB	Up to 50%	2 TB

If contact center servers have more storage space available, Avaya recommends allocating most of the remaining free space to the `/var` and `/var/log` directories.

Chapter 5: Basic configuration

Dial plan overview

The system administrator can define a prefix and the total length for each call type that the contact center processes to route a call appropriately.

Avaya Contact Center – Extended Capacity supports the following predefined call types:

- deny: Defines numbers that the contact center blocks.
- public: Defines numbers outside the enterprise.
- local: Defines numbers inside the contact center.
- private: Defines private network calls inside the enterprise.
- emergency: Defines numbers for emergency calling.
- external-prefix: Defines the prefix a user dials for calls outside the enterprise.
- reserved: Defines numbers for DMCC.

The administrator can also configure custom call types on the Configuration Server web portal.

Avaya Contact Center – Extended Capacity supports 24-digit dialing, short and long number dialing, flexible phone number formats, and flexible extension number lengths for call appearance. The contact center also supports dialing for extensions that are in the same location as the server and for extensions that are spread across several locations. Avaya Contact Center – Extended Capacity supports dial prefixes that agents can dial before an extension. Dial prefixes prevent conflicts between extensions and numbers used for dialing within an agent profile.

For more information about configuring dial plan analysis and call types, see the dial plan configuration section in *Administering Avaya Contact Center – Extended Capacity*.

Number adaptation overview

The system administrator can create adaptations for all phone numbers of incoming and outgoing calls from the dial plan of a local SIP network to the dial plan configured on the Configuration Server, and vice versa. The administrator can configure number adaptations for all incoming and outgoing calls so that the contact center routes the calls correctly. For example, the administrator can configure number adaptations for handling an international call.

For more information about number adaptation configuration, see the number adaptation configuration section in *Administering Avaya Contact Center – Extended Capacity*.

SIP server overview

Avaya Contact Center – Extended Capacity is a SIP server that can connect to external SIP servers, such as Session Border Controller, or other communication systems. SIP servers handle call traffic in the contact center network. The system administrator must specify external SIP servers on the Configuration Server web portal for connecting to the contact center.

A SIP server can do the following:

- Set up a connection between multiple endpoints.
- Transmit media parameters and specifications for the communication session for each endpoint using the SDP protocol.
- Modify media parameters and specifications during a session. For example, a SIP server can update the related media parameters when the agent puts a call on hold.
- Update endpoint parameters. For example, a SIP server can update the related media parameters when the agent transfers a call to another agent or endpoint.
- Terminate a session.

For more information about SIP server configuration, see the SIP server configuration section in *Administering Avaya Contact Center – Extended Capacity*.

Media handling

Avaya Contact Center – Extended Capacity provides a media service for call conferencing, call recording, and service observing. The solution currently supports the G.711 (mu-law), G.729, and G.729B codecs.

The system administrator can manage media sources for playing announcements, queue music, and Music on Hold. For more information about configuring media sources, see the announcement configuration section in *Administering Avaya Contact Center – Extended Capacity*.

Related links

Music on Hold on page 40
Call recording on page 41
Service observing on page 49

Permission sets

A permission set is a collection of settings that allows agents and supervisors to access or prevents them from accessing various features, such as Service Observing, VDN of Origin Announcement, and Direct Agent Calling. The system administrator can restrict contact center users from making any calls or to make calls only of a specific type. The administrator can also assign permission sets to a particular agent login ID, endpoint extension, VDN, or vector.

For more information about configuring permission sets, see the permission set configuration section in *Administering Avaya Contact Center – Extended Capacity*.

Related links

Direct Agent Calling on page 42
VDN of Origin Announcement on page 44
Service observing on page 49

Service Hours table overview

In Avaya Contact Center – Extended Capacity, vectors use Service Hours tables to determine call treatment during working and non-working hours. The system administrator can add up to 999 Service Hours tables to adjust call routing to the shift schedule of the contact center. The administrator can configure service hours for each day of the week.

Service Hours tables simplify vector configuration by reducing the number of steps in a vector. With a Service Hours table, the administrator can add only one vector step to determine if the contact center receives the call within the specified service hours and routes the call appropriately. The administrator does not need to add several steps for call routing based on the time of day when the call arrives.

For more information about Service Hours table configuration, see the service hours table configuration section in *Administering Avaya Contact Center – Extended Capacity*.

Holiday table overview

Vectors use Holiday tables to determine how the contact center handles calls during the configured holiday period. The system administrator can control call routing during holidays to ensure that the contact center processes all calls accordingly when the contact center closes or the staff reduces on non-working days. Holiday tables simplify vector configuration by reducing the number of steps in a vector. The administrator can configure up to 999 Holiday tables.

For more information about Holiday tables configuration, see the holiday table configuration section in *Administering Avaya Contact Center – Extended Capacity*.

Agent profiles and time zones

In Avaya Contact Center – Extended Capacity, an agent profile determines what features are applicable for endpoints associated with this location. The system administrator can configure an agent profile for a specific endpoint or agent login ID and specify settings for call routing and contact center features.

The administrator can associate a specific time zone with an agent profile for the contact center to route calls only within service hours of the contact center. The default time zone is America/New York.

For more information about configuring agent profiles, see the agent profile overview section in *Administering Avaya Contact Center – Extended Capacity*.

Network locations

A network location is a specific set of network settings that the contact center applies to endpoints based on the endpoint IP address. If the administrator does not assign an agent profile to an endpoint or agent login ID, Avaya Contact Center – Extended Capacity uses the endpoint IP address to map this endpoint to the corresponding network location. Each network location has an associated agent profile. When the endpoint IP address does not match any configured network location, the contact center uses the default network location.

For more information about configuring network locations, see the network location configuration section in *Administering Avaya Contact Center – Extended Capacity*.

Chapter 6: Call vectoring

Call vectoring is a management mechanism for call routing and treatment.

A call vector is a series of command steps that the contact center uses to route calls and determine the treatment for each call. Avaya Contact Center – Extended Capacity can route calls to destinations within or outside the network, ACD agents, or other vectors.

The contact center primarily directs incoming calls to an administered vector directory number (VDN). A VDN can represent a call type or a service category. The VDN then directs the call to a vector for call routing and treatment.

The system administrator can use vector steps to manage the following call-related functions:

- Call treatment based on the dial plan configuration and service hours
- Call routing to more than one skill if the agent cannot answer a call
- Collection of caller information
- Moving from one vector step to another step or vector
- Redirecting callers to voicemail when the agent is unavailable
- Provisioning music, announcements, and contact center tones

Vector directory numbers

A vector directory number (VDN) is an extension number that connects an incoming call to a specific vector. This number is an extension that is not assigned to a device. The system administrator can map each VDN only to one call vector.

A VDN represents a call type or a service category, for example, billing or customer service. Multiple VDNs can point to the same vector or to different vectors depending on the call treatment.

The administrator can specify a VDN return destination for the post-call treatment. VDN return destination is a VDN extension to which the contact center routes the call for the post-call survey when an agent completes the call before the caller.

For more information about configuring VDNs, see the VDN configuration section in *Administering Avaya Contact Center – Extended Capacity*.

VDN variables

Contact centers use multiple vectors with the same basic call flow but unique settings, such as announcements, route-to destinations, holiday tables, and conditions. With VDN variables, system administrators can create a generic call flow vector. VDN variables reduce the number of vectors, ensure common flows and ease of administration. The system administrator can use VDN variables as indirect references to announcement extensions and other sources.

For more information about VDN variable configuration, see the VDN configuration section in *Administering Avaya Contact Center – Extended Capacity*.

Vector overview

A vector is a series of command steps that the contact center uses to handle incoming calls. The system administrator can configure vectors to customize call routing and call treatment.

The Routing Core Server reads steps, follows step commands, and stops vector processing after the last step.

The solution provides the following types of vector processing:

- Sequential: The contact center processes vector steps sequentially.
- Unconditional branching: The contact center moves vector processing from the current vector step to either a preceding or a succeeding vector step or to a different vector without checking a condition.
- Conditional branching: The contact center moves vector processing from the current vector step to either a preceding or a succeeding vector step or to another vector based on the specified condition.

For more information about vector configuration, see the vector configuration section in *Administering Avaya Contact Center – Extended Capacity*.

Vector variables

With Avaya Contact Center – Extended Capacity, system administrators can create vector variables to:

- Improve the efficiency of vector configuration
- Provide management and application control
- Create vectors that better serve contact center operations

Different types of variables are available for certain call processing purposes. The system administrator can define vector variables on the Configuration Server web portal. Depending on the variable type, variables can use either call-specific data or values that are identical for all calls. The administrator can use one variable in multiple vectors.

For more information about vector variable types and configuration, see the vector variable configuration section in *Administering Avaya Contact Center – Extended Capacity*.

Vector step description

The following table lists Avaya Contact Center – Extended Capacity call vectoring steps:

Vector step	Description
#	To add comments to vectors.
adjunct	To request a routing destination from an adjunct connected to Application Enablement Services.
announcement	To play an announcement to the caller.
busy	To play a busy tone to the caller.
check	To queue a call based on the specified conditions.
collect	To prompt the caller to enter digits.
consider	To determine the best service for a call.
disconnect	To disconnect a call after playing an optional announcement.
goto	To move vector processing to another step or a vector.
messaging	To prompt the caller to leave a message at a specified extension.
queue-to	To connect or queue a call to a skill.
return	To return vector processing to the step following the **goto** step after processing steps in a different vector.
route-to	To connect a call to the configured destination or the destination that the caller enters.
serv-obsrv	To activate Service Observing for remote supervisors.
set	To perform mathematical and digit string operations during vector processing and store digits in the shared memory.
stop	To stop vector processing.
wait-time	To initiate feedback to the caller and to delay processing of the next vector step.

step

The **#** (hash) step adds comments to vectors. The system administrator can include comments within vectors for easier maintenance and troubleshooting. The contact center does not analyze this vector step and continues vector processing with the next step.

The administrator can type up to 71 Unicode characters in the **#** step. The contact center counts two or more consecutive **#** steps as one step.

ADJUNCT step

The **adjunct** step requests a call routing destination from an adjunct connected to Application Enablement Services. Avaya Contact Center – Extended Capacity provides the caller information in the Adjunct Route Request message. An ASAI adjunct typically uses the dialed number, caller or billing number, or digits obtained by the **collect** step to access the caller information and to determine call routing destination.

An adjunct specified in the **adjunct** step can route a call to an internal or external number, a VDN, or a specific agent. The adjunct can also set call queuing priority.

The step that follows the **adjunct** step determines the time during which the contact center waits for the ASAI adjunct to reply with a routing destination. The system administrator must always include a **wait-time** or **announcement** step after an **adjunct** step. If the administrator does not add a **wait-time** or **announcement** step, the contact center skips the **adjunct** step.

The system administrator can include more than one **adjunct** step in a vector for Avaya Contact Center – Extended Capacity to simultaneously process multiple route requests and to distribute incoming call load more efficiently.

When the contact center routes a call, the caller can hear normal call tones and feedback. However, if the contact center routes the call to an extension with no available call appearances and coverage path, the caller can hear a busy tone.

ANNOUNCEMENT step

The system administrator can use the **announcement** step to play a recorded announcement to the caller. When an agent becomes available, Avaya Contact Center – Extended Capacity interrupts the announcement. Any audio, for example, queue music or a ringback tone, continues until the contact center plays the announcement.

If the specified announcement is not available, the contact center skips the **announcement** step. When an **announcement** step follows an **adjunct** step, Avaya Contact Center – Extended Capacity interrupts the announcement as soon as the adjunct application receives a response to the Adjunct Route Request message.

BUSY step

The **busy** step ends vector processing after playing a busy tone. If the caller does not end the call after hearing a busy tone, the contact center plays the busy tone for 45 seconds and then ends the call. If Avaya Contact Center – Extended Capacity does not queue a call or an agent does not answer a call, the contact center plays the busy tone.

CHECK step

The system administrator can add the **check** step to check the status of skill queues. The contact center adds the call to the specified skill queue if the queue meets the conditions that the administrator specifies in the **check** step. The system administrator can use one of the following options with the **check** step:

- best: Checks the expected wait time of the best skill identified by a series of preceding **consider** steps. The value range is 1 through 9,999 seconds. If the expected wait time in

the skill queue is less than the specified value, the contact center adds the call to the skill queue with the priority level specified in the corresponding **consider** step.

- skill: Checks the status of a skill queue against a specific condition at the specified priority level.

The system administrator can queue a call to up to three skills simultaneously. A call remains queued until vector processing ends with a **disconnect**, **busy**, or **route-to** step.

CHECK SKILL step conditions

The system administrator can check the skill queue against one of the following conditions:

- Number of available agents is greater than the threshold value.
- Number of calls queued for a specified priority level or higher is less than the threshold value.
- The expected wait time is less than the threshold value.
- The oldest call waiting in a queue at the specified priority level or higher is waiting less than the threshold value.
- The current average speed of answer is less than the threshold value.
- Number of logged-in agents is greater than the threshold value.
- The expected wait time for subsequent calls in the queue is less than the threshold value after the contact center queues the current call.

The system administrator can also put a call in the queue without checking any condition.

COLLECT step

The **collect** step collects up to 16 digits that the caller enters on their phone. The system administrator can then assign the collected digits to a COLLECT variable.

The administrator can use an announcement to prompt the caller to enter the digits. If the caller enters incorrect digits, the administrator can use an announcement to prompt the caller to enter an asterisk (*). When the caller enters an asterisk, Avaya Contact Center – Extended Capacity deletes the digits collected from the current **collect** step and collects the digits again.

The system administrator must specify the maximum number of digits that the contact center can accept from a caller. If the caller enters fewer digits than the administered limit, the administrator can configure an announcement to prompt the caller to enter a pound sign (#) that indicates the end of the digit string. If the caller fails to enter the pound sign, the contact center skips the **collect** step.

CONSIDER step

The **consider** step retrieves the Expected Wait Time (EWT) data from skill queues. The contact center compares the data to determine the skill queue with a quicker response time.

The system administrator must configure a series of **consider** steps in a vector for the contact center to determine the best service. A **consider** step that tests the preferred skill must be the first in the series. The series ends if the administrator adds a **queue-to best** or a **check best** step to queue the call.

DISCONNECT step

The **disconnect** step ends the call treatment and removes the call from vector processing. The system administrator can use this step in case of a failure, if all agents are logged out or in Aux work mode, or the number of calls in the queue has reached a threshold value. The contact center usually disconnects the call after playing an announcement to the caller that asks them to call at a later time.

The administrator must specify an announcement extension, a vector variable or a VDN variable in the **disconnect** step for the contact center to play the announcement before disconnecting a call.

GOTO step

The system administrator can use the **goto** step for moving vector processing to a preceding or subsequent step in the vector or to another vector. The administrator must specify the vector and vector step for the contact center to redirect vector processing. The **goto** step does not remove a call from the queue.

MESSAGING step

The **messaging** step prompts the caller to leave a voice message for the extension specified in a VDN or vector variable, the active or latest VDN extension. The system administrator can specify the voicemail server which handles the caller message. If the specified extension is valid, Avaya Contact Center – Extended Capacity connects the call to the voicemail server, plays a ringback tone to the caller, and ends vector processing.

QUEUE-TO step

The **queue-to** step queues calls to a skill if all agents with the assigned skill are busy. The system administrator can also assign a queuing priority level to the call. When the call enters a queue, the **queue-to** step does not provide audible feedback to the caller. Other vector steps can provide wait treatment for calls in the queue.

The system administrator can also use the best option in the **queue-to** step to queue a call to the skill identified by a series of **consider** steps.

Avaya Contact Center – Extended Capacity can queue a call to up to three skills. A call remains in the queue until a **disconnect**, **busy**, or **route-to** step terminates vector processing.

RETURN step

The **goto vector** step directs a call to a specific step within another vector. The contact center processes subsequent steps in another vector until the call goes through the **return** step.

When a call processes the **goto vector** step, Avaya Contact Center – Extended Capacity retains the step position. When the contact center processes a **return** step in another vector, vector processing returns to the step subsequent to the **goto vector** step in the original vector.

ROUTE-TO step

The **route-to** step routes calls either to a set of collected digits or to a number that the system administrator configures within the vector step. The **route-to digits** step routes a call to a set of digits collected from an adjunct or the caller.

The system administrator can use the **route-to number** step to route a call to a specific destination. The total length of the routing destination string must be within the 16-character limit. The variable must always be the last entry, and the administrator cannot append digits to the string.

The system administrator must also indicate whether Avaya Contact Center – Extended Capacity routes a call to the coverage path for the specified destination if the agent is unavailable.

SERV-OBSRV step

With the **serv-obsrv** step, remote supervisors can observe calls on a device that is not directly associated with Avaya Contact Center – Extended Capacity. The system administrator can also configure the contact center to require the supervisor to enter a security code after dialing a VDN extension for Service Observing from a remote device.

With the **serv-obsrv** step, remote supervisors can monitor calls either to an extension obtained by the **collect** step or to an endpoint extension, an agent, or a VDN. The system administrator must also specify the Permission Sets (COR) of the observed agent, endpoint, or VDN, and the supervisor observe mode.

Related links

Remote service observing on page 52

SET step

With the **set** step, system administrators can manage values using mathematical and digit string operations. The administrator can use the **set** step to do the following:

- Perform numeric and digit string operations
- Store new digits in the shared memory
- Assign agent login IDs to ASAIUUI variables for the post-call survey
- Music On Hold

The administrator can forward the **set** step result with the shared UUI, send it over ASAI, or use it to route calls with the **route-to digits** step.

STOP step

The **stop** step pauses the processing of any subsequent vector steps. After the contact center processes the **stop** step, queued calls remain in the queue and Avaya Contact Center – Extended Capacity continues applying wait treatment until the agent becomes available.

WAIT-TIME step

The **wait-time** step delays the call with optional audible feedback and keeps the caller waiting for the time specified in the step. The system administrator can specify the wait time in seconds, minutes, or hours. The administrator can also indicate the audio that the caller can hear when in the queue. The administrator can specify one of the following:

- Music: The contact center plays audio configured for the current VDN extension. If the VDN extension does not have an associated audio source, the caller can hear the music configured for music source on Global config. If no music source is specified for the office location, the contact center plays the audio configured in the global settings on the Configuration Server web portal.
- Ringback: The contact center plays a ringback tone.
- Silence: The contact center does not play any audio.
- Audio extension defined in a variable: The contact center plays audio configured in a vector or a VDN variable.

The caller can hear optional audible feedback until the wait treatment changes or an agent becomes available.

Chapter 7: Call routing

Avaya Contact Center – Extended Capacity supports call routing for distributing incoming calls to individual agents or queues. The solution provides the following types of call routing:

- Expert Agent Distribution (EAD)
- Uniform Call Distribution (UCD)
- Enterprise Behavioral Pairing (EBP)

System administrators can configure up to 15,000 skills for contact centers. Each agent can have a maximum of 120 assigned skills.

To improve the caller experience, Avaya Contact Center – Extended Capacity can switch between routing algorithms.

Expert Agent Distribution routing

Expert Agent Distribution (EAD) algorithm routes calls to the most suitable agent based on the agent area and level of expertise. The system administrator can assign agents with a level of expertise from 1 through 16. Level 1 indicates that an agent has the highest qualification to address a query. When multiple agents are available, the contact center routes a call to the agent with the highest skill level.

Avaya Contact Center – Extended Capacity uses the following EAD methods:

- Most Idle Agent (MIA): If agents have the same skill level, the contact center routes a call to the agent who has the longest idle time since the last call.
- Least Occupied Agent (LOA): If agents have the same skill level, the contact center routes a call to the agent who has the longest idle time since login.

Avaya Contact Center – Extended Capacity provides an estimation of wait time to the caller based on the skill group occupancy and queue size. Different skills can have different wait times.

Uniform Call Distribution routing

In Uniform Call Distribution (UCD) routing, all contact center agents have the same skill level. Avaya Contact Center – Extended Capacity uses the following UCD methods:

- Most Idle Agent (MIA): When multiple agents are available, the contact center routes a call to the agent who has the longest idle time since the last call.

- Least Occupied Agent (LOA): When multiple agents are available, the contact center routes a call to the agent who has the longest idle time since login.

Avaya Contact Center – Extended Capacity provides an estimation of wait time to the caller based on the queue size. The contact center allocates approximately the same wait time for all callers.

Enterprise Behavioral Pairing routing

The Enterprise Behavioral Pairing (EBP) routing uses artificial intelligence to identify patterns of human interaction from current and prior calls to contact center. Based on the EBP data, the contact center chooses the agent that can be most helpful to the caller when routing the call.

Avaya Contact Center – Extended Capacity mainly applies the EBP routing in the two following scenarios

- When agents are available and can answer the incoming call immediately, the EBP uses data from previous calls to find the best match among available agents for the call.
- When no agents are available to answer the call, the EBP considers data from previous calls and the call-specific data, such as expected wait time (EWT), to route the call to the most suitable agent.

The EBP algorithm gathers the information from the current call and updates the EBP data after the call is complete. The EBP routing improves further interactions of callers who have similar requests with Avaya Contact Center – Extended Capacity.

Chapter 8: Feature overview

In addition to basic call features, such as call transferring and emergency calling, Avaya Contact Center – Extended Capacity supports advanced features that improve contact center efficiency. With the advanced contact center functionality, the system administrator can do the following:

- Control agents and calls using CTI applications
- Collect and monitor call data with Avaya Call Management System (CMS)
- Administer contact center announcements
- Store agent-specific greetings
- Configure agent work modes

Basic call features

Auto Dial

With the Auto Dial feature, the system administrator can assign specific extensions and labels to buttons on the endpoint for quick access. When the agent presses the **Auto Dial** button, the contact center automatically calls the assigned extension. For example, the administrator can assign `1234` to the **Auto Dial** button on the endpoint and label the button as `Human Resources`. When the agent presses this button, the contact center routes the call to the Human Resources department.

Contact center agents can later edit button labels on their endpoints. On 9600 series IP deskphones, agents can update the auto dial number if the administrator did not configure it for the **Auto Dial** button. For the list of supported 9600 series IP deskphones, see *Installing and Maintaining Avaya 9601/9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones SIP*.

For more information about configuring Auto Dial, see the endpoint configuration section in *Administering Avaya Contact Center – Extended Capacity*.

Coverage to voicemail

The system administrator can configure a coverage path to voicemail for contact center supervisors. The administrator can also configure coverage path to voicemail for agents when they receive direct agent calls. The contact center redirects calls to the configured coverage path so that the caller can leave a voice message when the supervisor or agent is logged out or cannot answer the call. When the caller leaves a voice message, the Message Waiting Indicator LED on the endpoint lights up. When the supervisor or agent presses the **Voice Mail** button, the endpoint

retrieves the voice message from the voicemail server. The Message Waiting Indicator LED turns off after the supervisor or agent listens to all voice messages.

For more information about configuring coverage paths, see the coverage path configuration section in *Administering Avaya Contact Center – Extended Capacity*.

Call Transfer

Contact center users can transfer calls to other destinations, such as a supervisor, agent, or VDN. If a supervisor is observing the call, the contact center does not disconnect them from a transferred call. Avaya Contact Center – Extended Capacity supports the following types of call transfer:

- Attended transfer: Before transferring a call, the agent puts the caller on hold and calls a transfer target to check if they are available for calls.
- Semi-attended transfer: The agent puts the caller on hold and calls a transfer target. The agent can hear a ringback tone and transfers the first call before the transfer target becomes available.
- Unattended transfer: The agent enters the transfer destination and does not stay on the call to ensure the transfer succeeds.
- Transfer by call join: The agent sets up a three-party conference call with a transfer target and disconnects from the call when the caller and the transfer target start talking.

When the agent puts the call on hold as part of call transfer, the caller can hear music. When the call with the transfer target is completed, Avaya Contact Center – Extended Capacity displays the caller information to the transfer target. The agent can cancel the transfer before completing the call.

The contact center reserves one call appearance for a consultation call with a transfer target. If all call appearances are busy, the contact center cannot transfer a call.

For more information about configuring call appearances, see the endpoint configuration section in *Administering Avaya Contact Center – Extended Capacity*.

Call Conference

Avaya Contact Center – Extended Capacity supports up to six participants on a conference call. When agents press the **Conference** button on the endpoint, they can add another participant to a conference call, for example, an agent or supervisor. The agent can enter the following caller details to add a participant to a conference call:

- Agent login ID
- Endpoint extension
- VDN extension

When the agent presses the **Conference** feature button, the contact center puts the other party on hold until the conference call is established or the agent cancels the conference call request.

When the agent puts a conference call on hold, active participants can continue the conference and do not hear music or other wait treatment tones. If the agent disconnects from a conference, other conference participants can continue the call.

Call Hold

The contact center puts a call on hold in the following cases:

- An agent is transferring the current call to another agent.
- An agent is adding other participants to the call to set up a conference call.
- An agent presses the **Hold** button on the endpoint.
- An agent selects another call appearance on an active call.

If the system administrator configures Music on Hold, the contact center plays music for the call participant on hold.

When agents press the **Hold** button, they can select another call appearance to make or receive calls. The number of configured **Call Appearance** buttons on the endpoint determines the number of calls that an agent can put on hold. If all call appearances are on hold, the agent cannot make or receive calls.

If the agent selects another call appearance on an active call, the contact center automatically puts the current call on hold. One call appearance always stays active unless the agent presses the **Hold** button on the active call appearance.

When the agent puts a call on hold, the LED on the endpoint for the corresponding call appearance starts flashing. To take the call on the call appearance off hold, the agent must press the corresponding **Call Appearance** button.

For more information about configuring call appearances, see the endpoint configuration in *Administering Avaya Contact Center – Extended Capacity*.

Music on Hold

The system administrator can configure media sources for Music on Hold. When the contact center agent or supervisor puts a call on hold, the caller can hear music when waiting on the line. If a conference call is put on hold, other conference participants do not hear the music and can continue the call.

The system administrator can configure the contact center to play different media sources for Music on Hold and queue music. The administrator can configure Music on Hold for each agent profile or for the entire contact center (Agent, Station, Skill, Vector).

For more information about administering Music on Hold, see the global configuration section in *Administering Avaya Contact Center – Extended Capacity*.

Emergency calling

The system administrator can configure a dial plan so that the contact center can route emergency calls without a dialed prefix. The administrator can set a priority level 1 through 10 for each configured dialed string, where level 1 indicates the highest priority. For example, the administrator can set a priority level 1 for the 911 emergency number in North America. If a region has more than one emergency service, the administrator can configure all emergency service numbers without a dialed prefix in the dial plan.

Avaya Contact Center – Extended Capacity can identify and route emergency calls separately from other calls. The system administrator can configure the dial plan for emergency calls so that the caller does not need to dial a prefix. The contact center requires a separate emergency call

routing adjunct to identify the caller location and to route emergency calls to the closest Public Safety Answering Point (PSAP).

The administrator can use an external adjunct to provide on-site notifications to locate a caller within the organization. The contact center passes the location of the caller to the closest PSAP and notifies the organization security desk or switchboard about the emergency call and location of the caller.

For more information about configuring dial plans and office and network locations, see the dial plan configuration, office location configuration, and network location configuration sections in *Administering Avaya Contact Center – Extended Capacity*.

Malicious call trace

Avaya Contact Center – Extended Capacity supports tracking of malicious calls. If an agent using a SIP endpoint determines the call to be malicious, the agent can press the Malicious Call Trace (MCT) feature button on the SIP endpoint to activate call tracing. Routing Core Server identifies the call source, records malicious call data, and notifies the contact center about an active malicious call. After the malicious call ends, Routing Core Server deactivates the MCT feature, and the contact center sends the malicious call report to Call Management System.

For more information about the MCT feature button configuration, refer to the endpoint documentation.

Contact center features

Active VDN name display

With Expert Agent Distribution (EAD) routing methods, Avaya Contact Center – Extended Capacity processes all incoming calls using VDNs, which direct the call to a vector for further call processing and treatment. Based on vector programming, calls can go through multiple VDNs or stay within the original VDN that received the call. If calls go through multiple VDNs, the contact center assigns one of the VDNs as the active VDN for the call. When the agent receives an incoming call, the agent endpoint displays the caller identification and the name of the last VDN that the contact center sets as active during vector processing.

For more information about configuring VDNs, see the VDN configuration section in *Administering Avaya Contact Center – Extended Capacity*.

Related links

Expert Agent Distribution routing on page 36

Call recording

Avaya Contact Center – Extended Capacity supports call recording with DMCC and TSAPI APIs from the internal Application Enablement Services server. The AE Services server enables CTI applications to monitor telephony services on TFS.

AE Services uses DMCC interfaces to capture media for call recording with the Multiple Registration method. The AE Services server registers all extensions that CTI applications record when CTI applications connect to AE Services. The system administrator can register several endpoints on a single extension for each recorder. When a call arrives at the monitored extension, CTI applications start call recording. When the call is complete, the AE Services server forwards media over Real-time Transport Protocol (RTP) streams to CTI applications.

AE Services uses TSAPI interfaces to capture media for call recording with the Single Step Conference method. The administrator can register several endpoint extensions on the AE Services server for each CTI application. When a call arrives at the monitored extension, the CTI application requests the TFS server to monitor the call using TSAPI APIs for capturing media. When the call is complete, the AE Services server forwards media over RTP to the CTI application.

For more information about setting up DMCC and TSAPI APIs, see the service administration section in *Administering Application Enablement Services for Avaya Contact Center – Extended Capacity*.

Direct Agent Calling

A direct agent call (DAC) is a special type of ACD call that the contact center routes directly to an agent. Avaya Contact Center – Extended Capacity does not connect a direct agent call to an agent if the agent is on another call. A direct agent call is put into the skill queue configured for direct agent calls, and the contact center assigns the call a higher priority than other calls in the skill queue. Avaya Contact Center – Extended Capacity notifies the agent with a ring tone if a direct agent call is in the queue.

The contact center treats a call as a direct agent call when the agent has the permission set configured for direct agent calls. Otherwise, the call is treated as a regular ACD call.

If the agent does not answer a direct agent call, the administrator can configure the contact center to send the call to voicemail. If the system administrator does not configure a coverage path for voicemail, the contact center uses Redirection on No Answer (RONA). If the administrator does not enable RONA for the agent, the call continues until the caller ends the call or the ring timer expires.

For more information about configuring direct agent calls, RONA, and permission sets, see the agent configuration, skill configuration, and permission set configuration sections in *Administering Avaya Contact Center – Extended Capacity*.

Related links

Coverage to voicemail on page 38
Redirection on No Answer on page 43

Forced Agent Logout by Clock Time

With the Forced Agent Logout by Clock Time feature, contact center administrators can configure the contact center to log out agents when their shift ends. The logout time depends on the agent profile assigned to the agent. Avaya Contact Center – Extended Capacity logs out an agent regardless of the agent work mode. If the agent is on an ACD or direct agent call, the contact center logs out the agent when they end the call.

The agent can log in again if the maximum number of logged-in agents for the shift is not reached. If the system administrator does not configure Forced Agent Logout by Clock Time for an agent, the agent stays logged in at the end of their shift.

For more information about configuring forced agent logout time, see the agent configuration section in *Administering Avaya Contact Center – Extended Capacity*.

Post-call survey

Avaya Contact Center – Extended Capacity provides the capability to direct the call to Avaya Experience Portal for the post-call treatment. When the agent completes the call before the caller, the contact center routes the call to the VDN extension specified for the VDN return destination. The system administrator can configure the type of calls that the contact center routes to the post-call survey. Based on the call origin, the contact center can route internal, external, or both types of calls to the VDN return destination. For more information about configuring the VDN return destination, see the VDN overview section in *Administering Avaya Contact Center – Extended Capacity*.

The contact center sends the agent login ID of the last agent that handles the call to Avaya Experience Portal over Shared UUI for the post-call treatment. The administrator can define AGENT and ASAIUUI vector variables to store the agent login ID. The administrator can assign the agent login ID stored in an AGENT variable to an ASAIUUI vector variable using the **`set`** vector step. For more information about configuring vectors and vector variables, see the vector and vector variable overview sections in *Administering Avaya Contact Center – Extended Capacity*.

Related links

Shared User-to-User Information on page 44

Network Call Redirection

Avaya Contact Center – Extended Capacity supports Network Call Redirection (NCR) for incoming trunk calls on its VDNs. When it receives a trunk call on a VDN, Avaya Contact Center – Extended Capacity requests the service provider to redirect the call and releases Routing Core Server resources from the resulting redirected call. Avaya Contact Center – Extended Capacity performs NCR in the following conditions:

1. The incoming call is from a trunk user to one of the VDNs.
2. The VDN that receives the call does not have VDN Return Destination (VRD) configured.
3. The vector uses the **`route-to <destination>`** function to redirect the call to an external number, which is neither a station, agent, VDN, nor announcement.

If the service provider accepts the request, Routing Core Server uses the route-to function to successfully route the incoming trunk call and exit the call handling process. Routing Core Server redirects incoming trunk calls in a maximum of 150 milliseconds.

If the service provider denies the request, Routing Core Server retains the trunk call at its VDN.

Redirection on No Answer

Redirection on No Answer (RONA) prevents an unanswered call from ringing indefinitely. If an agent cannot answer the call or a server fails, RONA prevents the call from getting lost. The

contact center redirects an ACD call to the skill that the call was originally queued to or to the specified RONA VDN for alternative call handling. The contact center routes the direct agent call to the agent coverage path. If no coverage path is assigned to the agent, the contact center routes a direct agent call to the specified RONA VDN. When RONA is activated, Avaya Contact Center – Extended Capacity changes the agent work mode to Aux work to block routing calls to the agent.

If the agent does not answer the call and the agent endpoint has Auto Answer configured, the contact center processes the call and cannot redirect the call to another VDN or agent coverage path.

For more information about configuring RONA parameters, see the skill configuration section in *Administering Avaya Contact Center – Extended Capacity*.

Redirection on IP failure

Redirection on IP failure (ROIF) verifies the connection between the contact center and the agent endpoint and redirects the call in case of an IP failure. If an agent cannot answer an ACD call after the administered number of rings, the contact center queues the call to the original skill or redirects the call to the specified ROIF VDN. If an agent cannot answer a direct agent call, the contact center redirects the call to the agent coverage path, specified ROIF VDN, or to the original skill queue with the highest priority.

For more information about configuring ROIF parameters, see the skill configuration section in *Administering Avaya Contact Center – Extended Capacity*.

Shared User-to-User Information

The contact center uses the Shared User-to-User Information (Shared UUI) to provide caller-related information, such as Universal Call ID and VDN Name, on the agent endpoint. In Avaya Contact Center – Extended Capacity, the Shared UUI supports the transmission of Adjunct Switch Application Interface (ASAI) UUI and Universal Call ID (UCID) from Avaya Experience Portal to agent endpoints.

The system administrator can configure a **ASAI UUI Info** feature button on agent endpoints. When the agent presses the **ASAI UUI Info** button during the call, the endpoint displays ASAI UUI and UCID information for the current call.

ASAI UUI contains the caller information, such as a destination number. The UCID is a unique call ID that distinguishes a call from all other calls that the contact center processes simultaneously. Avaya Contact Center – Extended Capacity generates a UCID for every call within the contact center. When the agent transfers a call to a new party or makes a conference call, the contact center sends the ASAI UUI and UCID information with Shared UUI to the new party endpoint using SIP signaling.

For more information about configuring the ASAI and UCID settings, see the CTI link configuration and global configuration sections in *Administering Avaya Contact Center – Extended Capacity*.

VDN of Origin Announcement

VDN of Origin Announcement (VOA) provides agents with a short message about the requested service based on the VDN that processes the call. VOA helps agents to respond appropriately to caller requests.

When the contact center routes an incoming call to a VDN with an assigned VOA, the VDN routes the call to a vector that places the call in the queue. When the agent answers a call, they hear the VOA message, and the contact center connects the caller to the agent after the message ends.

The agent cannot hear the caller when Avaya Contact Center – Extended Capacity plays the VOA message. The caller can hear a ringback tone when the agent is listening to the VOA. The **Call Appearance** button for an incoming call flashes when the contact center plays a VOA message.

For more information about configuring VDN of Origin Announcement, see the announcement configuration, VDN configuration, and permission set configuration sections *Administering Avaya Contact Center – Extended Capacity*.

Wait treatment

The system administrator can configure the contact center to provide the caller with an expected wait time announcement. Avaya Contact Center – Extended Capacity estimates the wait time based on average call duration and the number of calls in the queue. When the caller is in a waiting queue, the contact center can periodically announce the updated expected wait time.

The estimation of expected wait time can vary based on the routing algorithm that the contact center uses. When the caller is waiting in the queue, Avaya Contact Center – Extended Capacity can switch between routing algorithms. The transition to another routing algorithm does not affect the expected wait time.

For more information about configuring announcements, see the announcement configuration section in *Administering Avaya Contact Center – Extended Capacity*.

Related links

Call routing on page 36

Agent and supervisor features

Agent Greeting

With Agent Greeting, agents can record their personal greeting messages on endpoints. An agent can store up to 6 greetings on one endpoint with a maximum recording time of 10 seconds each. The endpoint automatically plays the greeting message to the caller when the agent answers a call. An agent can also press the **Agent Greeting** feature button on their endpoint to play the greeting message.

Agent login

An agent can log in to the contact center using one of the following:

- **Agent Login** feature button on the agent endpoint. To log in, the agent enters an agent login ID and the associated password.
- CTI desktop application. To log in, the agent enters an agent login ID, endpoint extension, and one of the assigned skills. Agents can also specify their work mode when logging in to the contact center.

When the agent logs in successfully, the endpoint or the CTI application displays the current agent work mode and the list of skills assigned to this agent. By default, the agent enters Aux work mode with the default reason code after logging in.

Related links

Agent work modes on page 47

Agent login with the Agent Login feature button

An agent can log in to the contact center using the **Agent Login** feature button on the agent endpoint that the system administrator can configure on the Configuration Server web portal. When the agent presses the button, Avaya Contact Center – Extended Capacity prompts the agent to enter an agent login ID and the associated password.

When the agent logs in successfully, the endpoint displays the current agent work mode and the list of skills assigned to this agent. By default, the agent enters Aux work mode with the default reason code after logging in. The administrator can configure the contact center to allow the agent to log in with a different work mode.

For more information about configuring feature buttons, see the endpoint configuration section in *Administering Avaya Contact Center – Extended Capacity*.

Agent login with a CTI desktop application

An agent can log in to the contact center using a CTI application, such as Coral Agent Desktop. To log in to Avaya Contact Center – Extended Capacity with a CTI desktop application, the agent must enter the following:

- Agent login ID
- Endpoint extension
- One of the skills assigned to the agent

Agents can also specify their work mode when logging in to the contact center.

If the agent enters valid login credentials, the agent endpoint displays the current agent work mode and a list of skills. If the agent does not enter the agent work mode at login, the contact center logs the agent in with Aux work mode and the default reason code.

Agent logout

An agent can log out of the contact center using one of the following:

- The **Agent Login** feature button on the agent endpoint. The button label changes to **Agent Logout** when the agent logs in. If the system administrator configures logout reason codes on the Configuration Server web portal, Avaya Contact Center – Extended Capacity prompts the agent to enter a reason code for logging out. A logged-in agent can start logging out during an active call. The contact center logs the agent out after the call ends.
- A CTI desktop application. CTI application sends a logout request to Avaya Contact Center – Extended Capacity. The request must contain the agent login ID, one of the agent skills, and the endpoint extension. The logout request can also contain a logout reason code if the administrator configured reason codes for the contact center.

For more information about configuring reason codes, see the reason code configuration and agent profile overview sections in *Administering Avaya Contact Center – Extended Capacity*.

Related links

Reason codes on page 49

Agent work modes

Agent work mode reflects the current status of an agent. In the Avaya Contact Center – Extended Capacity solution, contact center agents can enter Auxiliary Work (Aux work) and After Call Work (ACW) modes.

An agent enters Aux work mode for non-ACD activities, such as taking a break or making an outgoing call. If the system administrator configures reason codes for Aux work mode, the contact center prompts the agent to enter a reason code for changing their work mode to Aux work mode. Avaya Contact Center – Extended Capacity puts the agent in ACW mode after the agent completes the call for call-related activities or for taking a break before the next call. Agents in Aux work and ACW modes cannot receive ACD calls. When the agent is available to receive ACD calls, they can switch to Auto-In or Manual-In mode.

If the agent presses the feature button for a specific mode during an active call, the contact center puts the agent into the requested mode after the current call ends. When the agent is not on a call and presses the **Auto-In** or **Manual-In** feature button, Avaya Contact Center – Extended Capacity immediately changes agent work mode.

CTI applications that monitor the agent endpoint can also send the request to change agent work mode through the AE Services server. CTI desktop applications can have alternate agent work mode names. For more information about CTI application work modes, see the corresponding CTI application documentation.

The administrator can configure a forced entry of call work codes for a particular skill. An agent must enter call work codes (CWCs) during an ACD call or after the call ends. An agent cannot enter Manual-In or Auto-In mode until the agent enters CWCs.

For more information about configuring feature buttons, Aux work, and ACW mode parameters, see the agent and endpoint configuration sections in *Administering Avaya Contact Center – Extended Capacity*.

Related links

Reason codes on page 49

Auto-In work mode

When an agent is in Auto-In mode, the contact center makes the agent available to receive the next ACD call immediately after the current ACD call ends. The agent does not need to press a button to receive the next ACD call. Using this mode increases the number of calls that the agent can answer during a certain time interval. Agents can use this mode when they have few or no call-related activities after ending an ACD call.

The system administrator can set the timed After Call Work interval for Auto-In mode. If the administrator configures this interval for a skill, Avaya Contact Center – Extended Capacity puts the agent in ACW mode for a configured time after the current call ends. When the time-out elapses, the agent automatically becomes available for ACD calls. If the agent presses the **After Call Work** feature button during an active call, the contact center disables the ACW time-out for the current call and puts the agent in ACW mode after the call ends.

For more information about configuring feature buttons and timed ACW intervals, see the endpoint and skill configuration sections in *Administering Avaya Contact Center – Extended Capacity*.

Manual-In work mode

When an agent is in Manual-In mode, Avaya Contact Center – Extended Capacity automatically puts the agent in ACW mode after the current call ends for completing call-related activities. Agents can use this mode to perform call-related tasks after finishing an ACD call. In ACW mode, the agent is unavailable for ACD calls. To receive an ACD call after processing the previous call, the agent must press the **Manual-In** feature button on the agent endpoint.

Call work codes

With call work codes (CWCs), agents can enter up to 16 digits to record customer-related information associated with a call. A work code specifies customer-specific events. The type of call work code depends on the call center usage, for example, a call work code can be an account number or a social security number.

Account administrators can configure forced call work codes for a skill. With forced call work codes enabled, an agent must enter the call work code before changing the work mode from ACW to Manual-In. Additionally, an agent can enter a call work code during the active call.

Auto Answer with zip tones

The system administrator can configure Auto Answer for a specific agent login ID or an endpoint extension even when the agent is not logged in. The following options are available for configuring Auto Answer:

Option	Agent login ID	Endpoint extension
None	Auto Answer is not configured. The agent answers each new call manually.	Auto Answer is not configured. The agent answers each new call manually.
All	The contact center automatically answers all calls when the agent or endpoint is idle.	The contact center automatically answers all calls when the agent or endpoint is idle.
ACD	The contact center automatically answers all ACD and direct agent calls when the agent is idle.	The contact center automatically answers all ACD and direct agent calls when the agent is idle.
Station	The contact center uses the Auto Answer settings configured for the endpoint extension.	This option does not apply to endpoint extensions.

The Auto Answer settings configured for an agent override the Auto Answer settings for the agent endpoint extension. If the administrator sets the Auto Answer setting for the agent to **Station**, the contact center uses the Auto Answer settings configured for the endpoint extension.

The system administrator can enable zip tones. When the contact center automatically answers an incoming call, the agent can hear a 440 Hz zip tone for a second. If the administrator configures VDN of Origin Announcement (VOA), the contact center plays zip tone first and then the announcement.

Avaya recommends that agents use a headset or take the endpoint off hook to hear a zip tone.

For more information about configuring Auto Answer and zip tones, see the agent configuration and global configuration sections in *Administering Avaya Contact Center – Extended Capacity*.

Reason codes

With reason codes, supervisors can monitor agent activity. Agents can enter a numeric 1-digit or a 2-digit code that describes the reason for entering Aux work mode or for logging out of the contact center. The system administrator can configure up to 99 Aux work reason codes and 9 Logout reason codes. When an agent does not enter a reason code, Avaya Contact Center – Extended Capacity stores a default code of zero.

The system administrator can configure reason codes for a specific agent profile or a particular agent. If the administrator configures reason codes for an agent, they precede agent profile reason code settings.

The administrator can also specify reason codes for the situations when the contact center forces an agent into Aux work mode or logs an agent out due to a network failure. For example, the administrator can specify a reason code for the situation when the agent does not answer an ACD call and automatically enters Aux work mode.

The administrator can configure feature buttons on endpoints for specific Aux work reason codes so that if the agent presses a configured button, the endpoint automatically sends the reason for entering Aux work mode to Avaya Contact Center – Extended Capacity.

For more information about configuring reason codes, see the reason code configuration section in *Administering Avaya Contact Center – Extended Capacity*.

Service observing

With Service Observing, supervisors can monitor calls to endpoint extensions, agents, or VDNs. To enable service observing, the system administrator must configure a permission set for observed agents, endpoint and VDN extensions.

The administrator can specify the Listen Only or Coach mode for each **Service Observe** button on the supervisor endpoint. These modes determine whether the supervisor can switch to the Listen and Talk or Coach mode when observing the call.

Supervisors can monitor calls in one of the following modes:

- Listen Only: The supervisor can listen to the call. In this mode, the supervisor can switch to Listen and Talk or Coach mode if the administrator configures these modes for the supervisor endpoint.
- Listen and Talk: The supervisor can talk during the call. In this mode, the supervisor can switch to Listen Only or Coach mode if the administrator configures these modes for the supervisor endpoint.
- Next Call Listen Only: The contact center adds the supervisor to the next call in the queue in Listen Only mode. In this mode, the supervisor can switch to Listen and Talk or Couch mode if the administrator configures these modes for the supervisor endpoint.
- Next Call Listen and Talk: The contact center adds the supervisor to the next call in the queue in Listen and Talk mode. In this mode, the supervisor can switch to Listen Only or Coach mode if the administrator configures these modes for the supervisor endpoint.

- By Location Listen Only: The supervisor can observe calls in a particular contact center location in Listen Only mode. The supervisor must enter the VDN extension and agent profile to observe.
- By Location Listen and Talk: The supervisor can observe calls in a particular agent profile in Listen and Talk mode. The supervisor must enter the VDN extension and agent profile to observe.
- Coach: The supervisor can coach a logged-in agent on a call. In this mode, the caller does not hear the supervisor. The supervisor can switch to Listen and Talk or Listen Only mode if the administrator configures these modes for the supervisor endpoint.

If the call is put on hold, Avaya Contact Center – Extended Capacity puts the supervisor in the wait state until the call is active again.

For more information about configuring service observing, see the VDN configuration and permission set configuration sections in *Administering Avaya Contact Center – Extended Capacity*.

Multiple service observing

Avaya Contact Center – Extended Capacity supports two service observers to monitor the same agent login ID or endpoint extension. If one of the service observers stops monitoring the call, the other supervisor continues to observe calls. Only one of the observers on the call can coach an agent.

Multiple service observers cannot monitor the same VDN extension. When a supervisor observes the VDN extension on a call, the second supervisor observes the agent login ID or endpoint extension. If another supervisor attempts to monitor calls on the VDN extension, Avaya Contact Center – Extended Capacity assigns the monitoring role to the supervisor who starts observing first. The second supervisor can monitor the next call on the VDN extension.

The contact center assigns the highest priority to supervisors who start observing calls first. If the total number of service observers on a call is greater than two due to call transferring, call conferencing, or direct agent calling, the contact center retains only two supervisors with the highest priority.

The multiple service observing feature includes the following capabilities:

- In a single call, one service observer can monitor a VDN extension and the second service observer can monitor the agent.
- In a single call, two service observers can monitor an agent, while nobody monitors the VDN extension.
- Two supervisors can activate service observing to observe the same call.
- Two supervisors can observe the same call from a remote device.
- Two supervisors can use the **Activate Service Observing** CTI event from AES applications to observe the same call.
- Two supervisors can use a combination of local, remote, and CTI-based service observing mechanisms to observe the same call.
- Avaya Contact Center – Extended Capacity retains both service observers observing two separate calls, when these two calls are conferenced together.

Service Observing by endpoint extension

Supervisors can monitor all incoming internal, ACD, and direct agent calls to endpoint extensions. To observe calls, the supervisor presses the **Service Observe** feature button and enters an endpoint extension on their endpoint. When the supervisor enters an endpoint extension that is already observed, Avaya Contact Center – Extended Capacity puts the supervisor in the wait state. The contact center rejects the observing session if the specified endpoint is unregistered.

The system administrator must configure a permission set to enable Service Observing for calls coming to the specified endpoint.

Service Observing by agent login ID

Supervisors can monitor all incoming internal, ACD, and direct agent calls to agent login IDs. To observe calls, the supervisor presses the **Service Observe** feature button and enters an agent login ID on their endpoint. When the supervisor enters an agent login ID that is already observed, Avaya Contact Center – Extended Capacity puts the supervisor in the wait state. The contact center rejects the observing session if an agent with the specified login ID is not logged in.

The system administrator must configure a permission set to enable Service Observing for calls coming to the specified agent.

Service Observing by VDN extension

To monitor a VDN, supervisors must press the **Service Observe** feature button and enter a VDN extension on their endpoint. Avaya Contact Center – Extended Capacity connects the supervisor to the next call that enters call processing on the specified VDN. The contact center can connect only one supervisor to a VDN extension at a time. The observer can hear all call prompts, announcements, music, and other wait treatment tones that the agent and caller hear. The system administrator can configure the VDN to not play treatment tones to the supervisor and to start service observing when the agent answers the call.

Avaya Contact Center – Extended Capacity keeps the service observing session until the supervisor disconnects from the VDN extension. If the supervisor stays on the VDN extension when the caller ends the call, the contact center connects the supervisor to the next call on the same VDN. The supervisor is in Listen Only mode until the agent is available for the next call.

The system administrator must configure a permission set to enable Service Observing for calls coming to the specified VDN.

Service observing warning tones

The system administrator can configure the contact center to play a warning tone when an observer monitors an ongoing call. The tone lets an agent and a caller know that the call is under observation. If the warning tone is enabled, the contact center plays a tone when the observer starts observing a call. Subsequently, the tone plays periodically until the observation ends. The warning tone is used for agent observation, extension observation (if the agent ID differs from the station extension), and VDN observation.

If there are multiple observers, the tone plays for all of them. If one of the observers finishes call monitoring, the tone continues to play for the caller and the remaining observer.

For more information about enabling warning tones, see the agent profile section in *Administering Avaya Contact Center – Extended Capacity*.

The warning tone has a 440 Hz sound that plays at the following intervals: an initial two-second tone when the observation starts and a half-a-second tone for every 12 seconds until the observation ends.

Service observing disconnect tones

The system administrator can configure the contact center to play disconnect tones when agents or callers end an inbound ACD or direct agent call. The contact center plays different disconnect tones to indicate who ended the call first, so there is an agent disconnect tone and a caller disconnect tone. When a caller ends the call first, both agents and supervisors hear the caller disconnect tone. When an agent ends the call first, and the caller is the last active party on the call, the supervisor hears an agent disconnect tone.

For more information on enabling disconnect tones, see the agent profile configuration fields section in *Administering Avaya Contact Center – Extended Capacity*.

The contact center provides the following disconnect tones in the US:

Tone	Definition
Agent disconnect tone	A sound sequence of a 50-ms silence, followed by a 100-ms tone of 480 Hz at -17 dB. The contact center plays the sequence three times.
Caller disconnect tone	A sound sequence of a 50-ms silence, followed by a 100-ms tone of 480 Hz at -17 dB. The contact center plays the sequence two times.

Remote service observing

In Avaya Contact Center – Extended Capacity, supervisors can observe calls remotely from a device that is not directly associated with the contact center. The system administrator can associate a VDN extension that the supervisor enters to observe calls with a vector that activates remote Service Observing. The administrator must configure a permission set to enable Service Observing for the VDN extension that the supervisor enters to observe calls. The administrator can configure the contact center to require the supervisor to enter a security code after dialing a VDN extension.

When Avaya Contact Center – Extended Capacity activates Service Observing, the supervisor can hear a confirmation tone. If Service Observing mode is Listen Only or Listen and Talk, the contact center immediately adds the supervisor to the call. If Service Observing mode is Next Call Listen Only or Next Call Listen and Talk, Avaya Contact Center – Extended Capacity keeps the supervisor in the wait state until the next call. The administrator can also specify an agent profile when configuring Service Observing vectors to observe calls for a specific contact center office. When the supervisor joins the call remotely, the supervisor cannot switch to another observing mode or monitor calls in Coach mode.

If the supervisor observes the call for an agent login ID or endpoint extension, Avaya Contact Center – Extended Capacity puts the supervisor in the wait state when the call is put on hold. When the agent creates a consultation or conference call, the supervisor remains on the call. The contact center disconnects the supervisor from the call if the agent transfers the call.

If the supervisor observes the call for a VDN extension, the supervisor continues to observe the call when the agent puts the call on hold or transfers the call. Supervisors cannot observe conference or consultation calls.

To use the remote Service Observing feature on Avaya Agent for Desktop, the system administrator must set the **DMTF Type** setting to **rtp-payload**. For more information about configuring Avaya Agent for Desktop, see the post-installation configuration section in *Deploying and configuring Avaya Agent for Desktop*.

VuStats

With VuStats, agents and supervisors can view statistics for agents and skills. Agents can monitor their performance and supervisors can use the statistics to manage skills.

The statistics reflect the information collected during an administered time interval. When the system administrator configures the **VuStats** button, the administrator can set up to 50 data formats to display on the agent or supervisor endpoints.

The administrator can configure the contact center to show the VuStats information for a configured time interval or until the agent clears it. The administrator can also specify an update interval, after which Avaya Contact Center – Extended Capacity updates the VuStats information.

When an agent logs in or presses the configured **VuStats** button, the agent endpoint downloads agent and contact center statistics.

The endpoint administrator can set the CC-Info timer to automatically finish the VuStats session. If the agent is logged in and the CC-Info timer expires, the agent endpoint continues displaying the VuStats information until the agent logs out. Avaya Contact Center – Extended Capacity refreshes the VuStats session when the agent logs in or presses the **VuStats** button again.

For more information about configuring VuStats settings, see the endpoint configuration and VuStats configuration sections in *Administering Avaya Contact Center – Extended Capacity*.

VuStats interactions

Interaction	Description
The endpoint displays call prompts.	When the agent presses the **VuStats** button, the agent endpoint stops displaying the caller information and displays VuStats data.
The agent changes skills.	The agent endpoint stops displaying VuStats data when the agent changes skills.
The system administrator removes a skill from the agent configuration.	When the system administrator removes a skill from the agent configuration, the Configuration Server continues to associate the skill with the **VuStats** button. The agent endpoint continues to receive the VuStats information for the skill.
The agent logs in.	If the VuStats session is active on the endpoint before an agent or supervisor logs in, Avaya Contact Center – Extended Capacity updates the VuStats information.
The CC-Info timer expires.	If the CC-Info timer expires when the agent is logged in, the agent endpoint continues displaying the VuStats information until the agent logs out.

Remote login using Avaya SBCE

The system administrators can configure Avaya Session Border Controller for Enterprise (SBCE) to enable contact center agents to log in remotely without using VPN. Avaya SBCE authenticates SIP users to the contact center and secures communication through proxy and device provisioning.

To ensure secure communication, the administrator must configure Avaya SBCE to use recommended values of TLS and SRTP.

Reporting features

Automatic Call Distribution Integration

In the Avaya Contact Center – Extended Capacity solution, the Avaya Call Management System supports the Communication Manager Automatic Call Distribution (ACD) and the Routing Core ACD.

Reporting

The Avaya Call Management System provides real-time, historical, and integrated reporting to track all the activities in the contact center. Using the CMS data, you can make business decisions based on the entities such as agents, split/skills, vectors, vector directory numbers, and trunks.

CMS reports are available using CMS Supervisor for Voice only contact centers. Reporting is available through Aceyus for all other contact centers.

CMS stores all the Automatic Call Distribution (ACD) data received from an ACD in real-time and historical databases. Real-time databases include tables for the current and previous intra-hour interval data. The storage interval can be 15, 30, or 60 minutes. Historical databases include tables for the intra-hour, daily, weekly, and monthly data.

Automatic Call Distribution administration

The Avaya Call Management System provides an administrative interface to the supported Automatic Call Distribution (ACD)s. You can use CMS Supervisor to view or change the parameters related to the ACDs, call vectoring, and Expert Agent Selection (EAS) on an ACD system. An administrator can also run reports that analyze the operation of the contact centers.

For example, an administrator can:

- Add or remove agents from splits or skills.
- Move extensions between splits or skills.
- Change split or skill assignments.
- Change trunk group to split.
- Change trunk group to VDN.

- Change VDN-to-vector assignments.
- Start an agent trace.
- List the agents being traced.
- Create, copy, and edit call vectors.

Data backup

The Avaya Call Management System uses the following methods to support data backup, migrations, and restores:

- Tape
- USB storage device, non-tape backup
- NFS mounted file system, non-tape backup
- IBM Spectrum Protect (formerly Tivoli Storage Manager)
- Veritas NetBackup (formerly Symantec NetBackup)

Enterprise Login

There are two login methods available with Avaya Call Management System:

- Local Login
- Enterprise Login

Local Login:

- Users use the administered CMS user ID and password to log in to CMS.
- LDAP Password authentication is available for Local Login by optionally administering individual users for password authentication through Microsoft Active Directory.

Enterprise Login:

- Microsoft Azure is used for login authentication.
- Only available for use with CMS Web Client.
- Multifactor authentication (MFA) is enforced if Microsoft Azure is configured for MFA.
- The LDAP package is not required.
- The user must have a login ID configured on CMS.
- CMS administration is required to enable CMS to be recognized by Microsoft Azure.

Login authentication through a personal certificate is also available. Login authentication through a personal certificate is a requirement of the Joint Interoperability Test Command (JITC) certification. For Federal and Department of Defense (DoD) employees, personal certificates are encoded and provided by Common Access Card (CAC).

The CMS implementation does not limit support to requiring certificates to be on CACs. Personal certificates can be in a regular certificate store, such as Microsoft Certificate Store.

Avaya Call Management System Connectors

The following add-on connectors are installed on CMS that support integration into other solution components, such as POM, BRE, Verint for WFO, and Aceyus for Reporting.

The connectors that provide these integrations are:

- BP-RTA - Agent state data to Verint WFO to support adherence.
- Blue Pumpkin Historical - Agent, skill, VDN, and login-logout data sent to Verint WFO to support Forecasting and Scheduling and Agent Scorecards. The data sent is in the form of ASCII text delimited files. The connectors are scheduled to run after each CMS interval, every 15 minutes, or once a day, depending on the specific connector and receiving application.
- RT_Socket – Used to send CMS real-time data for splits/skills, VDNs, agents, to Aceyus, POM, and BRE.
- ECH Handler - External Call History (ECH) is the external version of call detail records of CMS. The ECH Handler add-on converts the binary ECH data files into ASCII data files and then SFTP them to the Aceyus for further reporting.

Chapter 9: High Availability and Disaster Recovery overview

The Avaya Contact Center – Extended Capacity solution provides High Availability (HA) and supports the active/alternate HA model. Active servers host virtual IP (VIP) addresses and manage contact center activity. The solution provides alternate servers to ensure high availability. The level of the contact center high availability depends on the solution deployment environment. The system administrator can deploy the contact center in the Simplex, local HA, or geo-redundant HA environment.

Avaya Contact Center – Extended Capacity supports geographic data resiliency and disaster recovery. The administrator can configure the contact center without Layer 2 networking. In case of failure, the contact center assumes that the primary data center is not recoverable and restores the data and services to survivable components in the secondary data center. Contact center deployment with disaster recovery networking does not preserve the state of agents and active calls.

Related links

Contact center deployment environments on page 15

Virtual IP address

Each server in the Avaya Contact Center – Extended Capacity solution has a static IP address. Active servers also have VIP addresses assigned to their network interfaces and process contact center activity. All other components and clients connect to active servers using a VIP address. If an active component fails, an alternate component assigns a VIP address to its network interface and becomes active. When a component stops being active, it stops hosting a VIP address.

Call Management System High Availability

Avaya Contact Center – Extended Capacity supports Call Management System (CMS) High Availability. The system administrator can deploy two or more CMS servers in the contact center. The solution can support up to ten highly available CMS servers. The number of servers depends on the agent and supervisor capacity. All CMS servers are active, which ensures reliability and backup of ACD call data across servers.

All CMS servers collect data independently from Avaya Contact Center – Extended Capacity and provide full CMS capabilities. If one server fails or loses connection to the contact center, other servers can handle the entire CMS activity load.

Avaya recommends using one Call Management System as a primary server for administrative tasks. `Admin-Sync` pushes administrative data from the primary CMS to all CMS servers every 24 hours. You can configure this schedule as required.

Contact center users must also use the primary CMS server for logging in and call reporting. If the server fails, contact center users must connect to an alternate CMS server to manage reports. After the connection to the primary CMS server is restored, the administrator can copy data from the previously active CMS to provide the missing data to the primary server.

All Avaya Contact Center – Extended Capacity deployment models support CMS High Availability. For more information about CMS High Availability, see *Using Avaya Call Management System High Availability and Admin-Sync*.

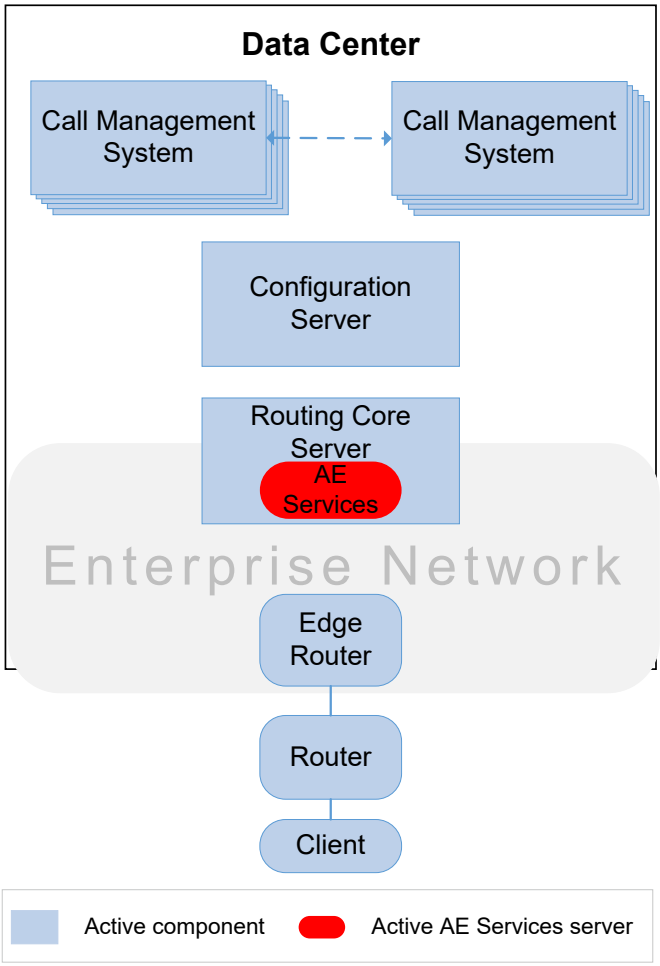
Related links

Contact center deployment environments on page 15

High Availability in the Simplex deployment

In the Simplex deployment, the contact center operates in one data center that contains a Routing Core Server and a Configuration Server. The contact center does not provide server High Availability and cannot operate in case of server failure or maintenance procedures. Avaya recommends that you do not use Simplex deployment in a production environment. The system administrator can connect the contact center to two or more CMS servers for call reporting and configure CMS High Availability.

The following diagram provides an overview of the contact center topology in the Simplex configuration:



Related links

Contact center deployment environments on page 15
Call Management System High Availability on page 57

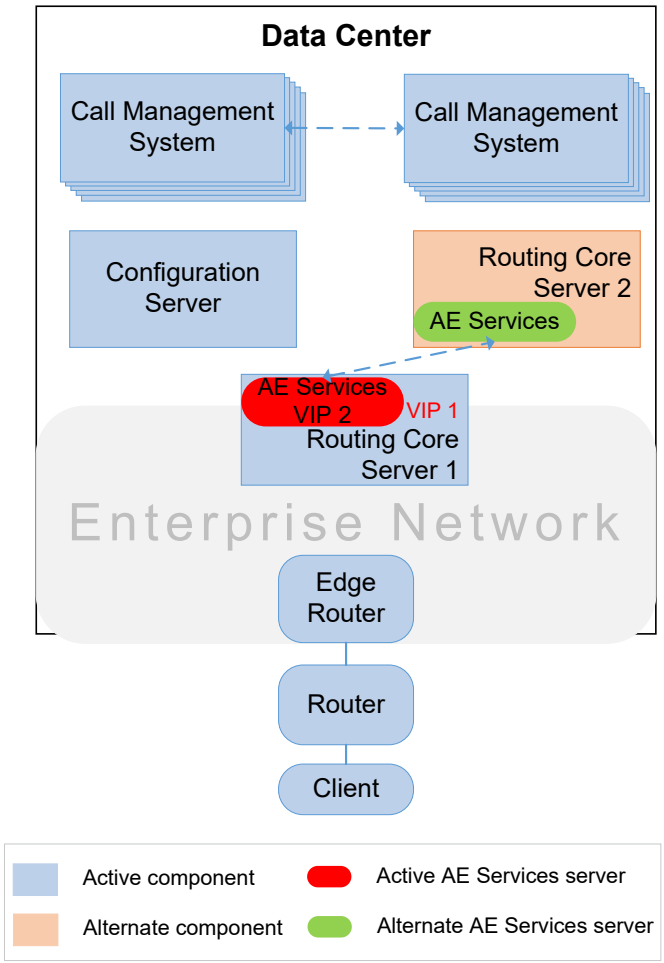
High Availability in the local HA deployment

In the local HA deployment, the contact center operates in one data center. Avaya Contact Center – Extended Capacity components are resilient to the failure of the network or another server.

The data center contains two Routing Core Servers and one Configuration Server. The Configuration Server and one Routing Core Server are active and the other Routing Core Server is in alternate mode.

The local HA model ensures High Availability of the Routing Core Server, Application Enablement Services, and Call Management System servers.

The following diagram provides an overview of the contact center topology in the local HA deployment:



Related links

Contact center deployment environments on page 15
Call Management System High Availability on page 57

Routing Core Server in the local HA deployment

In the local HA deployment, the contact center operates in one data center that contains two Rotuing Servers. One Routing Core Server is active and holds the VIP address. The other server is in alternate mode.

When the active server fails, it stops hosting the VIP address and the alternate Routing Core Server becomes active. Avaya Contact Center – Extended Capacity connects the Configuration Server to the currently active Routing Core Server.

AE Services in the local HA deployment

AE Services server operates within the Routing Core Server. Each AE Services server has a static IP address. In the local HA deployment, Avaya Contact Center – Extended Capacity provides one active/alternate AE Services server pair. The active AE Services server operates within the active Routing Core Server and has a VIP address assigned to its interface.

CTI connection failure

AE Services preserves the DMCC service status information. When a failure of the active AE Services server occurs, the alternate server takes over the VIP address and the DMCC service replicates the status information to the new active server. Avaya recommends that the system administrator restores DMCC sessions on CTI applications that use the DMCC service and verify that all monitors and registrations are active after a failover. When CTI applications reestablish the sessions, the DMCC service sends event messages to the applications for any resources that could not recover.

In case of failover, CTI applications that use TSAPI and CVLAN services reestablish socket connections, monitors, and registrations. TSAPI applications also reinitiate route registrations.

AEP connection failure

Each AE Services server connects to its own AE Services Interface (AESi) using an AEP connection. If the AEP connection fails, TSAPI, JTAPI, and DMCC applications receive a notification about the link failure. After the AEP connection is reestablished with another AE Services server or another AESi, CTI applications that use TSAPI, JTAPI, and DMCC services receive a notification that the link is up and refresh CTI sessions with the preserved service status.

For more information about AE Services High Availability, see the High Availability section in *Administering Application Enablement Services for Avaya Contact Center – Extended Capacity*.

Disaster Recovery in the geo-redundant HA environment

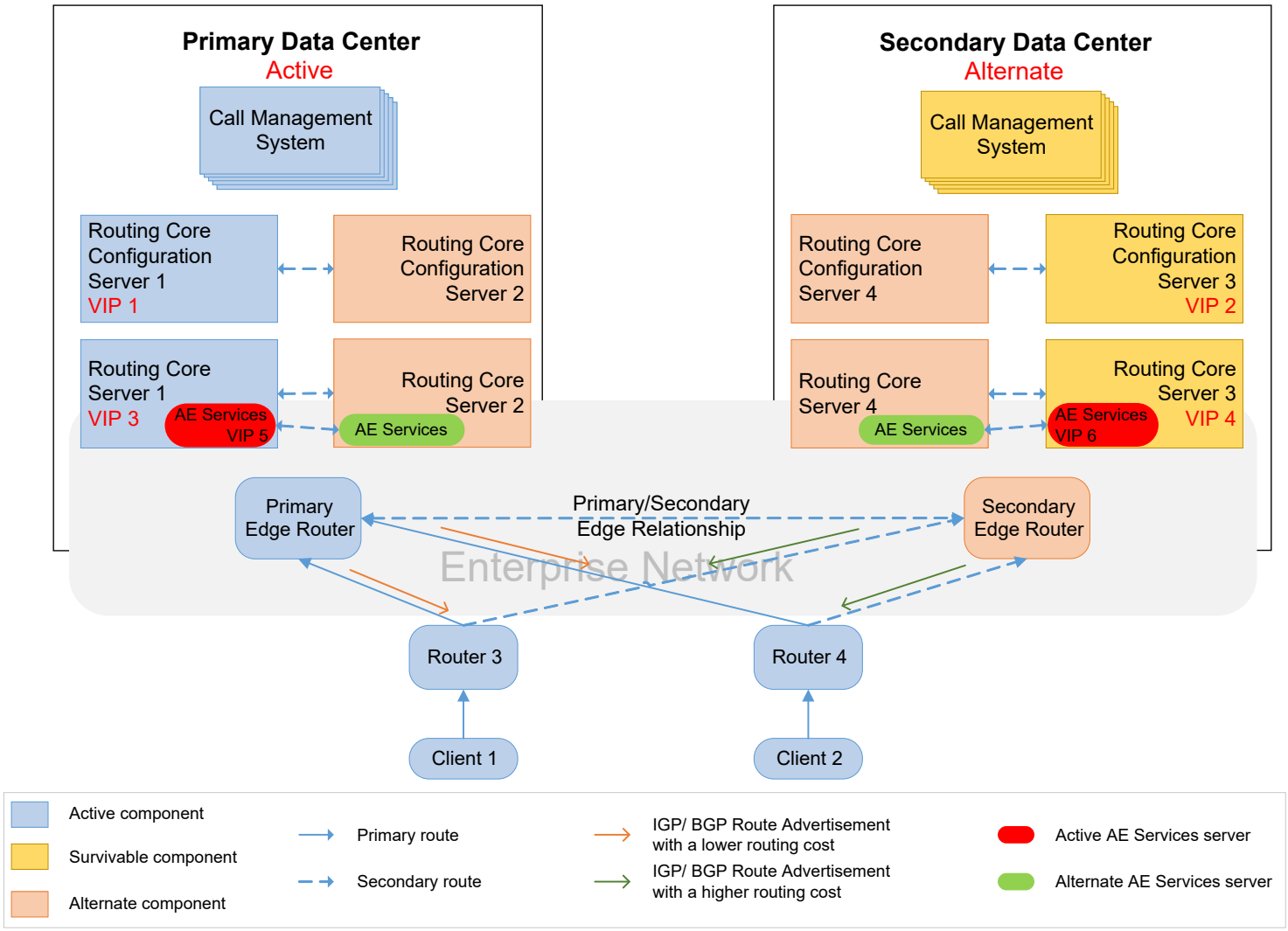
Avaya Contact Center – Extended Capacity supports disaster recovery for geo-redundant HA deployment without Layer 2 networking. The solution does not ensure call and state preservation in case of data center failure.

Each data center contains two Configuration Server and Routing Core Server instances. One Configuration Server and one Routing Core Server in the primary data center are active. The corresponding servers in the secondary data center are in survivable state.

Each data center contains one alternate Routing Core Server and Configuration Server. The Configuration Server and Routing Core Server pairs in the data centers have independent virtual IP addresses so that if an active server in a data center fails, the alternate server can take over the VIP and continue operation.

In case of the data center failure, the contact center assumes the primary data center to be unrecoverable and restores the data and contact center services on survivable servers in the secondary data center. If the data center failure occurs, the contact center drops all calls and logs out all agents. After survivable components become active, the contact center can start processing calls again.

The following diagram provides an overview of the contact center topology with disaster recovery in the geo-redundant HA deployment:



Chapter 10: Licensing requirements

Overview

The Avaya Contact Center – Extended Capacity solution provides a subscription license for a fixed number of logged-in users. The licensed number of users must correspond to the operational capacity of the organization.

Avaya Contact Center – Extended Capacity provides the concurrent user license, which means that only the specified number of agents can access and use the solution simultaneously, regardless to the named user. When more users try to log in, the contact center denies them access until a license becomes available.

Avaya provides a Web-based License Manager to manage Avaya Contact Center – Extended Capacity license. To track and manage licenses, WebLM requires a license file from Product Licensing and Delivery System (PLDS). For more information about PLDS, see https://plds.avaya.com.

License modes

Avaya Contact Center – Extended Capacity uses the following license modes:

Mode	Description
License Normal mode	The contact center has access to the WebLM server and shares the latest license information.

Table continues…

Mode	Description
License Error mode	Avaya Contact Center – Extended Capacity enters License Error mode under one of the following conditions: • The contact center cannot connect to the WebLM server for more than two days. • The WebLM server cannot find the license. • Invalid license installed on the WebLM server. • Expired license installed on the WebLM server. Avaya Contact Center – Extended Capacity enters License Error mode for 60 days. The Configuration Server web portal notifies the administrator that the contact center is in License Error mode. The contact center raises an alarm once every day until the system administrator resolved all license violations and the contact center goes back to License Normal mode. The Configuration Server web portal displays a License Error mode page after the login page, notifying the administrator about the upcoming license expiration 30 days before the license expires. If the contact center is in License Error mode for more than 60 days, Avaya Contact Center – Extended Capacity enters License Restricted mode.
License Restricted mode	Avaya Contact Center – Extended Capacity is in License Restricted mode if the administrator does not install a license after deploying the contact center or if the contact center is in License Error mode for more than 60 days. The Configuration Server web portal notifies the administrator that the contact center is in License Restricted mode. Avaya Contact Center – Extended Capacity raises an alarm until the system administrator resolves all license violations. In License Restricted mode, Avaya is authorized to stop processing call at any time. Avaya limits the contact center capacity to 5 concurrent agents. If more than 5 agents try to log in, Avaya Contact Center – Extended Capacity logs off all agents and allows a maximum of 5 agents to log in again.

Chapter 11: Security Overview

For Avaya Contact Center – Extended Capacity, the implementation personnel is responsible for setting the security configuration on the contact center network and for configuring the security features.

The solution provides the following security features:

- AE Services security: To manage user access. For more information about AE Services security features, see the security section in *Administering Application Enablement Services for Avaya Contact Center – Extended Capacity*.
- Data privacy and protection: To store the caller data using security encryption and hashing mechanisms.
- Permission sets: To secure access to certain contact center features, such as Service Observing and Direct Agent Calling. The system administrator can also lock agent endpoints when no one uses the endpoint by assigning a permission set that restricts outbound calls.
- Recorded announcements: To indicate that Avaya Contact Center – Extended Capacity is monitoring and recording the call.
- Remote Service Observing: To prevent unauthorized users from observing calls from remote devices.
- Security certificates: To establish a secure Transport Layer Security (TLS) connection between contact center components and authenticate the client and server.

Data privacy and protection

Avaya Contact Center – Extended Capacity stores caller information in log files. Using announcements, the administrator must notify the caller that the contact center collects the caller data and records the call. By continuing the call, the caller agrees to personal data processing. The contact center also stores agent information, such as agent names and phone numbers, in the internal database and log files. When installing an operating system during the deployment, the administrator must enable disk encryption to protect the caller and agent data. For more information about data privacy, see the data privacy and security section in *Maintaining Avaya Contact Center – Extended Capacity*.

The system administrator can also configure the log retention period on Application Enablement Services to store data for the specified time. By default, the log retention period is 30 days. For more information, see the log file management section in *Administering Application Enablement Services for Avaya Contact Center – Extended Capacity*.

Media security

Avaya Contact Center – Extended Capacity supports Real-time Transport Protocol (RTP) for transmitting media to and from the data center. Along with RTP, the contact center uses Real-time Transport Control Protocol (RTCP) to monitor transmission statistics and service quality and synchronize multiple streams. The system administrator can configure time interval and quality of service parameters for transmitting RTCP messages.

If you require secure connections, the administrator can configure the contact center to use Secure RTP (SRTP) and Secure RTCP (SRTCP) protocols for media transmission. The SRTP and SRTCP profiles provide transmission encryption of media data and message authentication. For more information about configuring RTCP and SRTP transmission settings, see the network configuration section in *Administering Avaya Contact Center – Extended Capacity*.

Signaling security

Avaya Contact Center – Extended Capacity supports TLS encryption for secure signaling transport. The TLS encryption secures the transmission of the SIP and HTTP messages with contact center endpoints and between the solution components in the same data center.

Certificate management

All server components of Avaya Contact Center – Extended Capacity require identity and trusted Certificate Authority (CA) root certificates for establishing a secure TLS connection, client and server authentication. The trusted CA signs the identity certificates. The system administrator must import all certificates into the contact center truststore.

The administrator must install the certificates for the contact center components that use a TLS connection, including the Routing Core Server, Configuration Server, Application Enablement Services interface, and the Call Management System interface. Data centers in the same High Availability group and contact center endpoints also use a TLS connection and require the trusted CA root certificate.

Avaya Contact Center – Extended Capacity supports certificate revocation. CAs keep track of SSL certificates. After the CA revokes an SSL certificate, the CA retrieves the certificate serial number and adds it to the certificate revocation list.

For more information about certificate installation and revocation, see the certificate installation section in *Deploying Avaya Contact Center – Extended Capacity*.

Chapter 12: Resources

Documentation

Title	Use this document to	Audience
Overview		
Avaya Contact Center – Extended Capacity Solution Description	Understand high-level product functionality, performance specifications, security, and licensing.	Customers and sales, services, and support personnel
Implementing		
Deploying Avaya Contact Center – Extended Capacity	Install and configure Avaya Contact Center – Extended Capacity.	Implementation personnel
Migrating to Avaya Contact Center – Extended Capacity	Migrate from Avaya Aura® Call Center Elite to Avaya Contact Center – Extended Capacity.	Implementation personnel
Administering		
Administering Avaya Contact Center – Extended Capacity	Administer and manage Avaya Contact Center – Extended Capacity.	Implementation personnel
Administering Application Enablement Services for Avaya Contact Center – Extended Capacity	Administer and manage Application Enablement Services for integration with Avaya Contact Center – Extended Capacity.	Implementation personnel
Maintaining		
Maintaining Avaya Contact Center – Extended Capacity	Perform basic maintenance procedures and troubleshoot Avaya Contact Center – Extended Capacity services.	• System administrators • Customers and sales, services, and support personnel

Finding documents on the Avaya Support website

Procedure

1. Go to https://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 the appropriate release number.

   The **Choose Release** field is not available if there is only one release for the product.
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 only displays the documents for the selected category.
7. Click **Enter**.

Avaya Documentation Center navigation

For some programs, the latest customer documentation is now available on the Avaya Documentation Center website at https://documentation.avaya.com.

Important:

For documents that are not available on Avaya Documentation Center, click **More Sites** > **Support** on the top menu to open https://support.avaya.com.

Using the Avaya Documentation Center, you can:

- Search for keywords.

  To filter by product, click **Filters** and select a product.
- Search for documents.

  From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.
- Sort documents on the search results page.
- Click **Languages** ( ) to change the display language and view localized documents.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection using **My Docs** ( ).

  Navigate to the **Manage Content** > **My Docs** menu, and do any of the following:

  - Create, rename, and delete a collection.
  - Add topics from various documents to a collection.
  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collection that others have shared with you.
- Add yourself as a watcher using the **Watch** icon ( ).

Navigate to the **Manage Content** > **Watchlist** menu, and do the following:

- Enable **Include in email notification** to receive email alerts.
- Unwatch selected content, all content in a document, or all content on the Watch list page.

As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the website.

- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.
- Send feedback on a section and rate the content.

Note:

Some functionality is only available when you log in to the website. The available functionality depends on your role.

Support

Go to the Avaya Support website at https://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.

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs
- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya user ID and password.

   The system displays the Avaya Support page.
3. Click **Support by Product** > **Product-specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.

5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Index

G

H

I

L

M

N

P

Q

R

S

T

U

V

W

Z