Avaya IP Office™ Platform Feature Description

Release 9.1.2
Issue 01.08
September 2015

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.

For full support, please see the complete document, *Avaya Support Notices for Hardware Documentation*, document number 03–600759.

For full support, please see the complete document, *Avaya Support Notices for Software Documentation*, document number 03–600758.

To locate this document on our website, simply go to http://www.avaya.com/support and search for the document number in the search box.

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on 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: http://support.avaya.com or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

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

Hosted Service

THE FOLLOWING APPLIES IF YOU PURCHASE A 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, HTTP://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. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA’S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO 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. 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 Designated Processor that hosts 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)

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: http://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: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

Purpose

This document contains IP Office high-level feature descriptions and provides details about feature characteristics, capabilities, capacities and interactions.

Intended audience

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

Related resources

Documentation

See the following related documents at the Avaya Support website at support.avaya.com and at the IP Office Knowledge Base at marketingtools.avaya.com/knowledgebase.

Document number	Title	Use this document to:	Audience
Overview			
16-604278	*Avaya IP Office™ Platform Documentation Catalog*	See a list of all the documents related to the solution.	Everyone
None	*Avaya IP Office™ Platform Solution Description*	Understand the solution at a high-level.	Everyone
Reference			
	Avaya IP Office™ Platform Short Code and Button Action Reference	Understand short codes and buttons action details.	Administrators

Table continues…

Document number	Title	Use this document to:	Audience
	Avaya IP Office™ Platform Security Guidelines	Understand Avaya IP Office™ Platform security details.	Implementation engineers Administrators

Finding documents on the Avaya Support website

About this task

Use this procedure to find product documentation on the Avaya Support website.

Procedure

1. Use a browser to navigate to the Avaya Support website at http://support.avaya.com/.
2. At the top of the screen, enter your username and password and click **Login**.
3. Put your cursor over **Support by Product**.
4. Click **Documents**.
5. In the **Enter your Product Here** search box, type the product name and then select the product from the drop-down list.
6. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.
7. Use the **Content Type** filter on the left to select the type of document you are looking for, or click **Select All** to see a list of all available documents.

   For example, if you are looking for user guides, select **User Guides** in the **Content Type** filter. Only documents in the selected category will appear in the list of documents.
8. Click **Enter**.

Training

Avaya training and credentials are designed to ensure our Business Partners have the capabilities and skills to successfully sell, implement, and support Avaya solutions and exceed customer expectations. The following credentials are available:

- Avaya Certified Sales Specialist (APSS)
- Avaya Implementation Professional Specialist (AIPS)
- Avaya Certified Support Specialist (ACSS)

Credential maps are available on the Avaya Learning website at www.avaya-learning.com.

The following courses are also available on the Avaya Learning website. After logging in to the website, enter the course code or the course title in the **Search** field and click **Go** to search for the course.

Course code	Course title
10S00005E	Knowledge Collection Access: SMB Implementation Only AIPS – Avaya IP Office (AIPS – 4000) Curriculum and Online Test
5S00004E	Knowledge Collection Access: SMB Support Only ACSS – SME Communications (ACSS – 3000) Curriculum
0S00010E	Knowledge Collection Access: SMB Implementation and Support AIPS – Avaya IP Office (AIPS – 4000) Curriculum and Online Test plus ACSS – 3000 Curriculum
2S00012W	APSS – Small and MidMarket Communications – IP Office™ Platform 9.1 and 9.1 Select – Overview
2S00013W	APSS – Small and MidMarket Communications – IP Office™ Platform 9.1 and 9.1 Select – Core Components
2S00014W	APSS – Selling IP Office™ Platform 9.1 and 9.1 Select
2S00010A	APSS – Selling IP Office Assessment

Included in all Knowledge Collection Access offers above is a separate area called IP Office Supplemental Knowledge. This floor in the Virtual Campus contains self-directed learning objects, which cover IP Office delta information. This material can be consumed by technicians experienced in IP Office.

Viewing Avaya Mentor videos

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

About this task

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

Procedure

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

Note:

Videos are not available for all products.

Additional resources

You can find information at the following additional resource websites.

Avaya

http://www.avaya.com is the official Avaya website. The front page also provides access to individual Avaya websites for different countries.

Avaya Sales & Partner Portal

http://sales.avaya.com is the official website for all Avaya Business Partners. The site requires registration for a user name and password. Once accessed, the portal can be customized for specific products and information types that you wish to see and be notified about by email.

Avaya IP Office Knowledge Base

http://marketingtools.avaya.com/knowledgebase provides access to an online, regularly updated version of the IP Office Knowledge Base.

Avaya maintenance, lifecycle and warranty information

Avaya support services complement standard Avaya maintenance, lifecycle and warranty policies that are posted on http://support.avaya.com. For more information, send email to support@avaya.com.

International Avaya User Group

http://www.iaug.org is the official discussion forum for Avaya product users.

Non-Avaya websites

There are several web forums that discuss IP Office. Refer to these websites for information about how IP Office is used. Some of these forums require you to register as a member. These are not official Avaya-sponsored forums and Avaya does not monitor or sanction the information provided.

- Tek-Tips: http://www.tek-tips.com
- CZ Technologies IP Office Info: http://ipofficeinfo.com
- PBX Tech: http://www.pbxtech.info/forumdisplay.php?f=8

Chapter 2: Avaya IP Office™ Platform overview

The Avaya IP Office™ Platform is a cost-effective telephony system that supports a mobile, distributed workforce with voice and video on virtually any device. IP Office is an integrated, modular communications solution that scales up to 2500 extensions and 150 sites in a multisite network with resiliency. Match a deployment model to infrastructure needs from simple appliances to virtualized software in a data center with options in between. Improve customer experience and contact center agent efficiency with powerful, affordable multichannel functionality for voice, email and web chat. The solution combines collaboration software plus multichannel contact centers, networking, security and video.

IP Office provides a hybrid PBX with both Time Division Multiplexing (TDM) and IP telephony with trunk support, used in either mode or both concurrently. IP Office has data capabilities built-in, providing IP routing, switching and firewall protection, between LAN and WAN (LAN2).

In addition to basic telephony services and voicemail, IP Office offers both hard phone and soft phone options. Soft phone applications are designed to provide flexibility for remote workers and to allow workers to access telephony services, such as making and receiving calls, voicemail, and call forwarding from their computer or mobile device.

IP Office editions

IP Office also offers advanced features such as audio and video conferencing and voice over IP to meet the evolving needs of small, medium, and large enterprises.

IP Office is available in many deployment models based on the size of the enterprise and the features required using one or all the following elements:

- Virtualized IP Office software running in a virtual machine
- Dedicated server
- IP Office 500 version 2 (IP500 V2) control unit

Edition	Platform	Business size (users)	Addresses business needs
Basic Edition	IP500 V2	<25	Simple telephony and messaging

Table continues…

Edition	Platform	Business size (users)	Addresses business needs
Essential Edition	IP500 V2	20–99	Basic Edition capabilities plus IP telephony with essential mobility
Preferred Edition	IP500 V2	21–250	Essential Edition capabilities plus unified communications with preferred mobility
Server Edition	Linux Server, IP500 V2 and Linux Expansion	100 — 2000	Essential Edition capabilities plus unified communications with preferred mobility
Server Edition Select	Linux Server, IP500 V2 and Linux Expansion	100 — 3000	Essential Edition capabilities plus unified communications with preferred mobility

IP Office Essential and Preferred editions are also referred to as IP Office Standard Mode. Each edition builds upon the next to offer additional functionality: Essential requires Basic and Preferred requires Essential.

New in this release

IP Office™ Platform 9.1 contains the following new features and capabilities:

- IP Office Select
- Branch enhancements
- Key features and enhancements
- Unified Communications enhancements
- IP Office Web Manager and IP Office Managerenhancements
- Security updates
- Customer feature requests

Note:

Features are available worldwide unless otherwise specified. Not all features are supported on all platforms and phones. See descriptions for details.

IP Office Select

IP Office Server Edition is now available in a “Select” offer that combines higher scalability, enhanced resiliency and sophisticated applications, including:

- Premium Server Edition offer, increasing the addressable market with 3000 users, 100% Unified Communication (UC) across 150 sites
- Extensive resiliency options
- Continued low total cost of ownership and simplicity for mid-market

- Non-Select Server Edition also available

Note:

All systems within the solution must be licensed the same: either Select or non-Select. Select is not supported on Basic, Essential or Preferred editions. Server Edition Select licenses are required to activate new capacities and functionality. For more information on capacity, see *Deploying Avaya IP Office™ Platform Server Edition* .

Resiliency improvements: New and improved functionality includes:

- VMware high availability
- Integration with LDAP and Active Directory

User capacity and scalability improvements: Select and non-select systems now support a maximum of 3000 users (server model capacity limitations apply). All 3000 users can be on a single server and non-Select systems can support up to 2000 users with 1500 user on a single server depending on the server model deployed.

Server model	Non-Select users	Select users
Dell R620/OVA	1500	3000
HP DL360	1500	1500
Dell R220 or HP DL120	750	750
IP500 V2	384	384

Increased expansion nodes: Nodes increased to 150, up from 32. Users can be distributed across a maximum of 150 nodes: 1 node on the primary server, 1 on the secondary server and 148 on the expansion systems (Linux and IP500 V2). (Non-Select systems using IP500 V2 continue to support up to 32 nodes.) The number of expansion systems supported depends on the server model deployed.

Server model	Non-Select expansions	Select expansions
Dell R620/OVA	30	148
HP DL360	30	30
Dell R220 or HP DL120	30	30

Increased Voicemail Pro capacity:

- Increased to 250 ports, up from 150, depending on the server model deployed.

Server model	Non-Select Voicemail Pro ports	Select Voicemail Pro ports
Dell R620/OVA	150	250
HP DL360	150	150
Dell R220 or HP DL120	75	75

- Recording channel capacities increased, depending on the server model deployed.

Server model	Non-Select Voicemail Pro recording channels	Select Voicemail Pro recording channels
Dell R620/OVA	85	170
HP DL360	85	85
Dell R220 or HP DL120	42	42
IP500 V2	42	42

- With the option of having two active Voicemail Pro servers, the maximum number of ports increases to 500. Supports up to 2 active Voicemail Pro systems: 1 on the primary server and 1 on the secondary server. Each expansion system can be configured to use one or the other. Both support a maximum of 250 channels, depending on the server model deployed. Users on the primary server use the voicemail on the primary server, and users on the secondary server use the voicemail on the secondary server. Expansion systems can be configured to use either server. Each Voicemail Pro is a master and provides backup for the other. There is no load balancing. Hot desking is supported.

Hunt group capacity and processing improvement:

- Increased to 500 hunt groups, up from 300. The number of hunt groups members increase as follows:

Hunt group capacity	Non-Select	Select
Maximum hunt groups	300	500
Maximum hunt group size	750	1250
Total hunt group members	3000	5000

- Hunt groups can now be defined on any node.
- Efficient use of resources by defining dual Voicemail Pro support on the secondary server.
- Define local processing on the expansion server or resilience on another expansion server.

Increased conference port capacity: Increased to 512 ports, up from 256, depending on the server model deployed. The number in brackets in the following table is the maximum supported conference size.

Server model	Non-Select	Select
Dell R620/OVA	256 (1 x 256)	512 (2 x 256)
HP DL360	256 (1 x 256)	256 (1 x 256)
Dell R220 or HP DL120	128 (1 x 128)	128 (1 x 128)
IP500 V2	128 (2 x 64)	128 (2 x 64)

Increased SIP trunk session capacity: Increased to 1024 sessions per node, up from 512, depending on the server model deployed.

Server model	Non-Select	Select
Dell R620/OVA	512 (direct media) 256 (indirect media)	1024 (direct media) 512 (indirect media)

Table continues…

Server model	Non-Select	Select
HP DL360	512 (direct media) 256 (indirect media)	512 (direct media) 256 (indirect media)
Dell R220 or HP DL120	256 (direct media) 128 (indirect media)	256 (direct media) 128 (indirect media)
IP500 V2	128 (direct media) 120 (indirect media)	128 (direct media) 120 (indirect media)

Increased small community network (SCN) channel capacity: Increased to 500 channels per trunk, up from 250.

SCN channel capacity	Non-Select		Select	
	Linux	IP500 V2	Linux	IP500 V2
Maximum SCN trunks	32	32	150	32
Maximum channels per SCN trunk	250	250 (Direct) 120 (Indirect)	500	250 (Direct) 120 (Indirect)

Increased SoftConsole capacity: Increased to 50, up from 32.

Active SoftConsole platform	Non-Select	Select
Primary server	32	50
Linux server expansion	10	10
IP500 V2 expansion	4	4

Increased Busy Hour Call Completion (BHCC) capacity: Increased to 20000, up from 18000, depending on the server model deployed and the number of active Avaya one-X® Portal users.

Active users	Non-Select				Select			
	R620/OVA	DL360	R220	IP500 V2	R620/OVA	DL360	R220	IP500 V2
No Avaya one-X® Portal active users	18000	18000	7200	7200	20000	18000	7200	7200
With Avaya one-X® Portal active users	9000	9000	7200	7200	10000	9000	7200	7200

Expansion system SCN links: Select systems can link expansion systems with an SCN trunk using WebSocket or and existing SCN connection. Supports extra routing resilience, direct expansion, and one expansion can act as a fallback to another for both phones and hunt groups.

Location resilience: Select systems can provide the ability for a group of extensions to fallback to a given node in the SCN. The fallback system for a group of extensions is defined at the location level. Supports 96x1, 96x0 and 16xx phones. Location-based fallback overrides the system configuration. H.323 phones (not SIP phones) that are not part of a location with a fallback system set will still follow the system fallback configuration. (A system can only be chosen from the nodes with a defined SCN line.) The following new resilience constructs are supported:

- Primary and or secondary phones fallback to one or more expansion systems.
- Expansion system phones fallback to another expansion system.
- Hosted where phones can fallback to local CPE.
- Can make a subset of H.323 phones resilient, previously an all-or-nothing option.

IP Office Branch enhancements

As with non-Branch IP Office deployments, the feature set can range from basic telephony to rich Unified Communications.

In a Branch deployment, IP Office includes support for:

- Standalone branch offices
- Avaya Aura® and CS1000 distributed branch offices
- Avaya Aura® centralized branch offices
- Avaya Aura® mixed branch offices

IP Office Branch supports the following scalability and user capacity:

- Number of users per branch: 5 to 50 (recommended), 384 (maximum)
- Number of locations: 10 to 2,000 branches

Avaya Aura® System Manager and Central Management enhancements:

- Administrative support for the UCM V2 and Application Server when IP Office is deployed as a branch, which includes the support for backup, restore and upgrade of the UCM and IP Office Application Server
- The ability to administer, create, edit and delete Voicemail Pro call flows and system preferences
- The integration of the IP Office Web Manager to enable user management and the management of end point templates
- The ability to backup and restore multiple versions of an IP Office configuration on a remote server
- Download a system configuration onto an administrator's local machine

Avaya Aura® centralized applications, services and solution enhancements:

- Support for new endpoints within the branch, for example E129
- Support access to centralized applications or services within the core data center, for example Experience Portal (IVR)
- Deliver high degree of collaboration through seamless interoperability, for example branch/ branch/HQ Video

Key features and enhancements

The following new features have been added based on input directly from Avaya business partners and customers:

- Automatic Fallback Recovery: After a fallback event, if the new setting **System | Telephony | Phone Failback** is set to **Automatic**, and the phone's primary gatekeeper has been up for more than 10 minutes, the system causes idle phones to perform a failback recovery to the original system.

- New Unified Communications Module (UCM V2) next generation processor for Voicemail Pro and one-X Portal, requires Preferred license
- Answer Supervision Analog/ATM4 trunks
- Enable SIP third-party endpoints to be members of page groups
- Location-based time zones
- FSK Message Wait Indicator (MWI) support to analog extensions
- Speed dial/Directory to override barring
- Set MWI on SIP extension from short codes or CTI
- DECT R4 resiliency
- India toll bypass restriction enhancement to Restrict Network Interconnect for the India locale (default)
- Localization and locale settings for Phillipines, Czech Republic, Korea and Japan
- SIP service provider trunk enhancements
- New diagnostics
- Automated on-boarding and SSL/VPN related enhancements
- Expanded communications accessibility support
- MWI for another mailbox on a programmable button
- Make authorization codes generally available
- Call forwarding for hunt groups
- Add override restriction/barring option for each entry
- Support enhancements:
  - Voice quality monitoring
  - SNMP full qualified domain name (FQDN)
  - Free text descriptions in Manager ARS and trunk configuration areas
- SIP Line user interface simplification and line silence suppression
- IP DECT line resiliency
- NoCallerid alarm can now be suppressed
- Call barring can be overridden for numbers entered in the external directory
- Toll Bypass Prevention default added for preventing India toll bypass
- Web Collaboration added to user configuration
- Analog Trunk VAD setting added for answer and disconnect supervision
- Third-party voice quality monitoring enabled to send RTCP data to a third-party QoS monitoring application
- Enable remote working with SIP phones using Avaya Session Border Controller for Enterprise

- Enable to disable system-wide outcalling on Voicemail Pro
- Authorization code enhancements:
  - Authorization codes are now enabled by default
  - SMDR field 19 shows not applicable regardless of whether an authorization code is used
  - Authorization codes can no longer be associated with user rights. instead, they are associated with users
- SIP Registrar Enable setting changes can now be merged without a system reboot
- New alarms:
  - Log stamped
  - CPU warning/critical
  - Memory use warning/critical

Unified Communications enhancements

100% Unified Communications for up to 3000 users, up from 750. This increased functionality supports a 1:1 ratio between users and power users. It requires a standalone Avaya one-X® Portal for IP Office on the application server (reduced numbers occur if deployed on the primary server).

UC configuration	Non-Select			Select		
	R620/OVA	DL360	R220	R620/OVA	DL360	R220
Primary	750	750	375	1250	750	375
Standalone	750	750	750	3000	1500	750

Note:

Maximums include all one-X Portal client types of any mix, including plug-ins. HTTP or HTTPS. Not more than 50% can be Microsoft Windows Communicator clients.

The new version of Unified Communications is cloud-ready for optimization to gain higher margins, scale and security. The client interfaces support the latest versions of Microsoft Windows, Exchange, Lync, iOS, and Android.

Web collaboration: A new web collaboration feature leverages the Avaya Aura Conferencing solution on the Preferred, Server and IP Office Select editions. With Server Edition and IP Office Select Edition, web collaboration is part of the base software distribution and runs co-resident with the one-X Portal application on the primary server. It can also run on a standalone one-X server for additional scale. With Preferred Edition, web collaboration runs on an external Application Server. Web Collaboration is enabled via new Web Collaboration user license for each moderator/host. Prerequisites for Preferred Edition are one Office Worker, Teleworker, or Power User license for each moderator/host. Server Edition and IP Office Select require one Office Worker or Power User license for each moderator/host. Network bandwidth requirements are between 104 kbps and 251 kbps per user. Browser support includes Internet Explorer 8+, Firefox, Chrome, and Safari. Capacities for each server are:

Platform	User capacity
R620 standalone	512

Table continues…

Platform	User capacity
R210/R220	128
R620 primary server	128
R210/R220 primary server	32

Mobility enhancements: The one-X Mobile Preferred mobility clients for iOS and Android have been enhanced to provide better security, better user experience and more features. IP Office 9.1 delivers several enhancements to deliver Hosted IP Office. The mobility applications have been updated to enable secure communication protocols with the IP Office PBX and the one-X Portal Application Server:

- Certificate validation ON by default
- SRTP support
- Password change

Other enhancements include better user experience, feature consistency and device and operating system support.

Desktop integration enhancements:

- Remote installation and automatic configuration
- Scalability enhancements
- Secure communication with the one-X Portal server
- Simultaneous mode support for clients
- User experience enhancements
- Accessiblity enhancements

one-X Portal enhancements:

- Conference scheduling (requires a Power User license)
- Web conference integration
- Hunt group queue gadgets
- Scalability
- Improved security

IP Office Video softphone update: Licensing available for Mac and existing customers can use older versions on their devices with the IP Office 9.1 release.

SoftConsole enhancements: In addition to increased capacity. SoftConsole clients used by Receptionists now provides instant messaging support as well as interworking and better security in a cloud environment.

Avaya Communicator: (Previously known as Avaya Flare Communicator) Supports Windows and iPad operating systems. All Avaya Flare Experience users must use the new Avaya Communicator client for this release.

IP Office Manager enhancements

- Net4 support allows more memory and multi-threading for Standard and Server Editions.
- New PC minimum platform specifications:

Element	Standard Edition Manager	Server Edition Manager	Select Server Edition Manager
CPU	Core i3	Core i5	Core i5
RAM	4 GB	6 GB	8 GB
Operating system	32/64 bit	32/64 bit	64 bit

Web Manager enhancements

- Improved user interface
- Section 508 of the Rehabilitation Act accessibility support
- Embedded file management
- A new Web Control option allows you to increase the primary HDD partition size from the default 100 GB.
- In **Platform View**, you can now see services running on the system and view optional services such as **Contact Recorder** (not new, but moved), **Web Collaboration** and **Web License Manager**.
- Voicemail Pro preferences management
- UCM management
- Web management coverage increased for “day 2” administration including:
  - Short codes, alternate route selection (ARS), incoming call routes (ICR)
  - Time profiles
  - System directory
  - Locations
  - IP routes
  - SNMP
  - Voicemail Pro settings and call flow management
  - Embedded file manager
  - Certificate management
- LDAP configuration integration including user synchronization from LDAP directories (for Select only)
- Background configuration synchronization to help performance
- Automatic security database synchronization
- IP500 V2 dashboard with a summary of the system and a pictorial view
- Single screen wizard for backup, restore and upgrade
- Improved browser support:
  - Internet Explorer 10.0, 11.0 (8.0 and 9.0 are no longer supported)
  - Firefox latest version
  - Chrome for Windows/iPad, Samsung Galaxy tablet (Adroid)
  - Safari for iPad

DECT R4 improvements

Security changes: For new systems and systems with defaulted security settings, the security service user used for the provisioning connection between the IP Office and the DECT master base station is disabled by default. The service user must be enabled and their password changed. The same user name and password must be matched in the DECT system's configuration.

Master base station mirroring: It is now possible to configure two base stations to act as mirrored master base stations. One becomes the active master base station whilst the other becomes a standby master base station. If for any reason the active master base station becomes unavailable, the IP Office switches to using the standby master base station to continue DECT operation.

Switch resilience: The IP Office controlling the DECT system can be configured to allow that control to be automatically passed to another IP Office when it is not available. The SCN line between the two systems can be configured to allow DECT backup for resiliency scenarios in the same was as existing resilience for H.323 IP phones. If for any reason the primary IP Office system becomes unavailable, DECT control and users are switched to the backup IP Office system.

Calling party name in the call log: Previously, the calling party's name and number were shown for alerting and connected calls and only the number appeared in the call log display. Now for 3720, 3725, 3740 and 3749 phones, the call log shows the calling party's name.

CTI Auto-Answer with IP Office applications: Previously, when using an application such as one-X Portal for IP Office to make and answer calls, the user also had to answer and drop connections using the phone. Now for 3720, 3725, 3740 and 3749 phones, the CTI application can automatically connect and end the call. Some limitations apply.

IP DECT Line Addition no longer requires a reboot: Adding or deleting the DECT line in the IP Office configuration no longer requires an IP Office system reboot. Note however that changes to an existing DECT line may require a reboot.

Virtualization enhancements

- VMware OVA mirrors native performance capacities for the Dell R620 server with reductions in vCPU and vRAM usage.
- Support for VMware high availability.
- Latest vSphere and hardware version support:
  - vSphere 5.1 and 5.5
  - ESXi 5.5 and hardware version 8
  - Now supports more than 8 vCPUs
  - Requires ESXi 5.0+
  - Upgrade of existing OVA will not update ESXi or the hardware version.

Security enhancements

This release includes the following security enhancements:

- Better defaults and default behaviors
- More secure interfaces and fewer insecure interfaces
- Improved certificates/PKI
- SRTP
- New Linux security right

- Syslog-TLS
- Authentication improvements
- Basic Linux firewall

Previously unsecure interfaces now secure: The following previously unsecure interfaces now have secure options:

- SoftConsole
- Voicemail Pro
- SSA
- SysMonitor
- IP Office Line (SCN trunk)
- Linux HTTPS backup service with quota support
- Syslog

Operating system and application hardening:

Operating system	Enhancement
one-X Tomcat	• Disabled auto-completion on login page. • Removed HTTP trace method. • Removed version information from ports and services. • Not run with root privileges.
Linux	• Not run with root privileges. • Basic Linux firewall with forwarding between interfaces disabled. • Traffic for web management ports 7070 and 7071 rate limited to prevent Denial of Service attacks. • All ports used by the applications are open, other ports are blocked. • Rejects are logged in order to discover any attack and identify the possible issues. • SSL VPN and NAPT interfaces allowed by the firewall. • New right added for Linux security role.
All operating systems: Certificate PKI improvements	• Primary and application servers now have a certificate authority (CA). • Better distribution of server ID certificates. • More useful Linux certificate support.
All operating systems: PKI trust domains	• Everything kept at default where applicable for consistency. • Use the primary server CA to generate an ID certificate for all nodes. • Use a third-party CA and purchase ID certificates for all nodes. • Variations and other options are possible. For more information see *Avaya IP Office™ Platform Security Guidelines*.

Table continues…

Operating system	Enhancement
All operating systems: ID certificate distribution	• For a Linux server, the automatically created or imported ID certificate is automatically distributed to all local applications. • Imported using IP Office Manager, Web Manager, or SCEP, including the application server. • ID certificates can now support intermediate CAs to ensure third-party PKI schemes need minimum client administration.

New access mechanisms

The solution now includes new management access mechanisms to support hosted and 150 nodes.

Solution Management Application (SMA) and Central Access: IP Office Manager and Web Manager use the Solution Management Application (SMA) to access the system configuration. SMA resides on the primary or secondary server. Settings are available for remote access and Server Edition Central Access. Central Access communicates with the primary or secondary server rather than to each node individually. Avaya requires Central Access for a hosted environment and recommends it for non-hosted environments with more than 32 nodes.

Remote access: IP Office Manager uses remote access whenever the manager is remote from the system and needs to use the public address or SSL/VPN for communication. This feature can be combined with Central Access and is required for hosted, SSL/VPN, and other remote access methods.

Use Proxy: A new setting routes all management messages through the SCN WebSocket trunk to allow SMA to communicate with all systems through the SCN WebSocket trunk. This feature can be combined with Central Access to allow the manager to communicate using this method. Avaya requires this access method for hosted environments and does not recommend it for non-hosted environments.

Contact Center application support changes

The following Contact Center applications' conference and voicemail channels reflect the new Server Edition Select capacities when the applications are connected:

- IP Office Contact Center
- Avaya Contact Center Select (Requires additional Preferred support. Additionally, requires a per-system ACCS license.)

Note:

CCR is no longer supported in this release.

Increased Contact Center application conference channels: The following conference channel capacities are supported:

Platform	Non-Select	Select	Avaya Contact Center Select	IP Office Contact Center	Notes
DL120 R210	128	128	414	414	All Linux servers will indicate the

Table continues…

Platform	Non-Select	Select	Avaya Contact Center Select	IP Office Contact Center	Notes
					elevated IPOCC quantities.
DL360	256	256	825	825	
R620	256	512	825	825	
OVA	256	512	825	825	Dependent on vCPU and vRAM assigned.
IP500 V2	128	128	128	128	

Increased Contact Center application Voicemail Pro channels: The following Voicemail Pro channel capacities are supported:

Platform	Non-Select	Select	Avaya Contact Center Select	IP Office Contact Center	Notes
DL120 R210	75	75	175	175	All Linux servers indicate the elevated IPOCC quantities.
DL360	150	150	350	350	
R620	150	250	350	350	
OVA	150	250	350	350	Dependent on vCPU and vRAM assigned.
IP500 V2	40	40	40	40	

Increased Contact Center application Voicemail Pro server quantities: The following Voicemail Pro server quantities are supported:

Platform	Non-Select	Select	Avaya Contact Center Select	IP Office Contact Center
DL120 R210	1	2	1/2	1/2
DL360	1	2	1/2	1/2
R620	1	2	1/2	1/2
OVA	1	2	1/2	1/2
IP500 V2	1	1	1	1

Secondary server required for secondary Voicemail Pro server.

Discontinued platform and application support

This release is supported on the IP500 V2 and the IP Office Server Edition only.

The following items are longer supported:

- IP500 control unit
- IP400 control units including expansion modules and plug-in modules on the Legacy Carrier Cards.
- IP400 DS16 and 30 expansion modules
- Analog Trunk 16 expansion module
- Customer Call Reporter (CCR)
- Advanced Edition
- IP Office Video Softphone on Windows for new installations (Avaya recommends using Avaya Communicator). Older versions of the Mac Softphone and Windows softphone will not be distributed by Avaya, however customers can still use them after upgrading.

Chapter 3: Features

Call handling features

IP Office provides a comprehensive set of telephony features to enable fast and efficient responses to phone calls. Features such as Caller ID Display and Call Tagging allow users to see who is calling and who they are calling before they pick the call up. Client information can be displayed on a user's PC.

Wireless handsets and twinning offer employees mobility around the office. For those employees working away from the office, comprehensive and easy to use call forwarding features, Softphone and a remote access service allow them to stay in contact and access centralized resources at all times.

Users can handle incoming calls efficiently using either direct dialling (DDI/DID) or dedicated operators. For out of hours calls, IP Office provides voicemail and optional Auto-Attendant services. TDM-specific and TDM phone-specific features are not supported on Linux.

Basic call handling

Automatic Callback

A user can set an automatic callback two ways:

- When calling an extension that is busy, request a call when the extension becomes free.
- When calling an extension that only rings, request a call when the extension is next used.

Depending on the type of phone a user has, request a call back when free by dialing a short code if an internal busy tone is heard, selecting an option from an interactive menu or pressing a programmed DSS/BLF key. A user can also activate a callback when free from Phone Manager. A user can also set a callback when free or a callback when next used using a short code without attempting a call.

This feature is available across both multisite and small community networks.

Distinctive ringing

The system uses various ringing sequences to indicate call types. For example, internal and external calls can have different rings, called distinctive ringing.

On analog phones, the distinctive ringing sequences are adjustable. On digital and IP phones, distinctive ringing is fixed as follows:

- Internal call: Repeated single-ring
- External call: Repeated double-ring
- Ringback call: Single ring followed by two short rings

Ringing sequences work with the following call types:

- Calls returning from park
- Calls returning from hold
- Transferring calls
- Call back when free calls
- Voicemail ringback calls

This feature is available across both multisite and small community networks.

Call screening

Users can screen for important calls and decide to answer a call or let it go to voice mail.

Users can screen incoming calls while the phone is in an idle state and listen to incoming calls transferred to voicemail. When an incoming call arrives at a phone and is directed to and answered by the voicemail system, the user automatically hears the caller on his or her phone speaker, but the caller cannot hear the user. Users can decide whether to answer the call or drop from the call and let the voicemail system continue to handle the call. A user cannot screen a call while he or she is on another call.

Forwarding

Users can forward calls to another extension or external number including mobile devices.

Users can forward calls in a number of ways and if the call is not answered at the forward destination it will go to voicemail if enabled for the user and call supervision is available. Once the numbers have been entered, the user can toggle the forwarding to be active or not as required without having to reenter the numbers.

If the user is a member of a hunt group, some types of hunt group calls can also forward unconditionally. Users can select if forwarding is applied to external calls only, or all calls. Call forwarding is processed after do not disturb and follow-me conditions are tested.

Coverage to Operator

Administrators can configure an operator or a group of operators to provide coverage for external calls that would otherwise go to voicemail.

Unanswered calls are routed to an operator or a group of operators. For example, local government offices prefer to provide a personal service rather than voicemail.

Follow Me

Follow Me enables all the features that a user has set on their phone to follow them to another phone. Forwarding only forwards calls only, not phone settings.

When users are away from their desk at another work area, they can forward call settings from their main phone for calls that follow the user including Forward On Busy or No Answer.

User can set Follow Me either from their primary phone (Follow Me To) or from the phone where they want calls to be received (Follow Me From). Several people can have their phones forwarded to a one destination and if the phone has a display it will indicate who the call is for.

Forward Hunt Group

Users can forward a hunt group to forward calls for a group. For example, in a sales or support environments where a number of people may be out of the office using mobile phones, this feature allows them to participate in the hunt group as if they are in the office.

Calls for a hunt group that the user belongs to can also follow forward unconditional. The hunt group must be set for either sequential or rotary ring type and if the call is not answered at the forward destination it will follow the hunt group call handling instead of going to voicemail.

Forward On Busy

If enabled, this forward occurs when a user is busy and another call is routed to them, but the system does not forward calls for a hunt group that they may be a member of.

Users are considered to be busy when they are on a call, but depending on call waiting settings and key and lamp features, this may not be the case.

Forward On No Answer

If a call rings for a user but the user doesn’t answer it within the configured answer time, the system forwards the call that has been indicating call waiting if enabled.

Forward Unconditional

The system forwards all calls for the user to a number, but if a call is not answered within the configured answer time, the system sends the call to voicemail if enabled.

Unconditional Forward To Voicemail

Users can divert all calls to voicemail even when a user's voicemail is not activated.

Hold

Users can place calls on hold with optional hold music. A held call is presented back to the extension after a time out, set by the system administrator, so that held calls cannot be forgotten.

Toggle Calls

The system cycles each call that the user has on hold to their extension, presenting them one at a time to the user.

Hold Call Waiting

Combine hold and answer to hold an existing call and answer a waiting call through a one button press.

Park

As an alternative to placing calls on hold, users can park calls to be picked by another user.

Park is available on the user's phone, Avaya one-X® Portal for IP Office, Phone Manager and SoftConsole.

The system parks a call using a park slot number which can be announced over a paging system. The designated user can go to any phone and take the call by dialing the park slot number.

Phone Manager has 4 predefined Park buttons. On digital phones with DSS/BLF keys, it is possible to program park keys to indicate when there is a call in a particular park slot and allow calls to be parked or retrieved.

Administrators can determine how long a call remains parked before it is presented to the extension that originally parked the call.

Personalized ringing

Users can change the sound or tone of a phone’s ring.

On many digital phones, users can personalize the ringer sound. Changing the ringer sound does not alter the ring sequence used for distinctive ringing. This feature is local to the phone and not supported on all types of phones.

Tones

The system generates the correct tones for the geography. These tones are generated for all extension types: analog, digital and IP.

Supported tones are:

- Normal, alternate, and secondary
- Busy
- Unobtainable
- Re-order
- Conferencing

Transfer

Users can transfer a call in progress to either an internal extension or an external public number. The system places the caller on hold while it performs the transfer.

If the transferring user hangs up before the destination user answers, the system automatically transfers the call, called an unsupervised or blind transfer. Alternatively, a user can wait for the destination to be answered and announce the transfer before hanging up to complete the transfer, called a supervised transfer.

Unless restricted by the administrator, the system does not differentiate between internal or external call transfers.

Advanced call handling

Absence text

Users can set absence text on their phone to inform other internal users of their current status and likely availability.

Absence text is also available for users of standard analog phones, but it can only be displayed on selected display phones, Phone Manager and SoftConsole. Most supported feature phones give the option of adding text.

When a user has an absence text message set, call processing is not affected to the user and they still have the choice of using features like do not disturb and forwarding. Telephones that support the interactive setting of absence text also display it on the users own phone for the benefit of people who come to their desk. There are 10 predefined strings and 1 custom string for absence text:

1. On vacation until
2. Will be back
3. At lunch until
4. Meeting until
5. Please call
6. Don't disturb until
7. With visitors until
8. With customer until
9. Back soon
10. Back tomorrow
11. Custom

All message text include the option to add a time, for example, message 4 plus `10:00` displays **Meeting until 10:00**. Text strings are localized to the system language.

This feature is available across both multisite and small community networks.

Call recording

Users can record a call and save the recording to the a voicemail mailbox, a group mailbox or the voice recording library.

When a caller provides detailed information like an address or phone number, the caller hears a warning message or tone that the call is being recorded in some countries. Where call recording is required for quality assurance, administrators can configure IP Office to automatically record a percentage of calls for later review.

Any call on any phone type can be recorded. Where notification of recording needs to be played, the system ignores voicemail port licensing if an insufficient number of voicemail channels have been licensed.

Note:

On IP phones, a VCM channel is used for the duration of the recording.

Call tagging

Call tagging displays a text message to provide additional information about the call on a user's phone or Phone Manager when a call is presented to it.

Users tag calls when transferring calls from Phone Manager or Soft Console to provide caller information they are not able to announce the call.

Users can add a tag to a call automatically using CTI and Voicemail Pro based on the incoming call route.

Note:

On some phones, displaying the tag may mean that it is not possible to display the usual call source and target information.

Call waiting

Users may not want callers to receive busy tone if they are on another call. Instead, callers hear a normal ring tone. Users hear an alert that there is a call waiting.

Users can decide to finish or hold the current call and answer the one that is waiting. The amount of information that is available about the call that is waiting depends on the type of phone the user has, or if they are using Avaya one-X® Portal for IP Office or Phone Manager.

Because the call waiting tone can be disruptive, for example during conference calls. Users can turn the feature on or off and even suspend it for a single call.

Coaching intrusion

Designated users can join an existing conversation on internal or external calls. This features also allows a user to interrupt a call to without the caller hearing the conversation.

Administrators and supervisors designate users with the Can Intrude setting. Users can join calls on any extension on the system, however, administrators can also designate users with the Cannot be Intruded setting, which prevents others from intruding on their calls.

On Essential and Preferred Edition systems, Silent Intrusion or Whisper Page can be effective in a scenario where a user intrudes into a call to whisper that a very important customer is waiting. The user hears the whisper while talking to the caller but the caller will not be able to hear the whisper.

Used in call center scenarios and with other applications between employees. Supports the interruption or inclusion of a supervisor on a live call to talk to an agent without the far-end caller listening to the conversation. This is useful when the agent needs coaching support/training or when the supervisor needs to intrude to give instructions to an agent. The caller may still talk to the agent, but the caller will not hear what the supervisor is saying. The agent will be able to hear both the caller and the supervisor.

The feature enables users on a call to “intrude” and listen depending on the configuration of the end users if Coaching Intrusion or Whisper Page is used. Coaching Intrusion and Whisper Page cannot be done on and idle user. It may be done for internal calls or with external calls. This feature is enable through the IP Office Managerfor each user. Only authorized users can use the coach/ whisper feature. The default setting is off.

Conferencing

Users can place calls on hold and a create a conference using either the telephone or desktop applications. Additional conference members may be added, however a single conference may not have more than 64 members (with IP500 V2 only and more on Server Edition).

For ad-hoc conferencing, the system requires as many digital trunks/VoIP channels as external participants (as well as Preferred Edition for Meet-Me conferences). The system supports 128 conferencing channels on the IP500 V2, allowing multiple conferences of any size from 3 to 64 parties. The system support 42 3-party conferences, 2 64-party conferences or any combination in between. Meet-Me capabilities require Preferred Edition for direct dial into a conference bridge with PIN code security. In an SCN network, only one centralized Preferred Edition license is required to host Meet-Me conferences at any of the sites. Conference IDs are also shared across the SCN sites.

The following conference channel capacities are available:

Table 1: Conferencing channel capacities

Platform	Non-Select	Select	Avaya Contact Center Select	IP Office Contact Center
HP DL120 Dell R210	128	128	414	414
HP DL360	256	256	825	825
Dell R620	256	512	825	825
OVA	256	512	825	825
IP500V2	128	128	128	128

To initiate a conference, users dial the direct number allocated to the conference bridge, type in the PIN (require Preferred Edition and Voicemail Pro) if required. For ad-hoc conferences with a few participants, users can easily set up immediate conferences by calling all parties and bringing them to the conference bridge. With Avaya one-X® Portal for IP Office, the originator of the conference can keep control: the Caller ID number (and the associated name if recognized) of each participant is displayed. If required, they can selectively hang-up a specific participant. The system plays a single beep on entry and a double beep on exit. The owner of the conference may use their extension number as the conference ID. The owner of the conference has control of the conference with the ability to mute and drop calls of participants. All participants will hear the system Music on

Hold (MOH) until the owner joins, and will hear MOH when the owner drops. Note that any internal party has the option to view and drop participants (not just the conference originator).

Users can record a personalized greeting for a conference (requires Preferred Edition and Voicemail Pro).

Users can record the conference using Avaya one-X® Portal for IP Office, digital or IP display phone or a short code (requires Preferred Edition and Voicemail Pro). To prevent unauthorized access to the conference bridge, PIN codes, Caller ID number screening as well as time and date profiles can be set-up using Voicemail Pro. One user can manage the conferencing bridge facility from any location.

Conferencing has the following restrictions:

- Only two calls connecting through analog trunks are permitted in any single conference.
- Each external caller requires a digital trunk/VoIP channel (for example 1 T1 allows 23/24 external parties, 1 E1 allows 30 parties and a fully licensed VCM-64 allows 64 parties).
- There are no limits on the mix of internal and external calls in conference, but if all internal participants disconnect from the conference bridge, the external participants can be disconnected automatically by the system for added security (configurable system setting).
- System features such as call intrusion, call recording and silent monitoring all use conference resources, as does automatic recording if enabled. When any of these features are active the number of slots available for conference parties is reduced. For example, a conference call between 3 parties and being recorded will use 4 conference slots.

Related Links

Meet-Me conferencing on page 87
Video collaboration on page 88
Collaboration Agent on page 89

Dial On Pickup

By taking the phone off hook, users can automatically dial a specified extension.

Use this feature in unmanned reception areas or for door entry systems to allow visitors to easily gain assistance. This feature is also known as “Hotline”.

Do Not Disturb

Users can temporarily stop incoming calls ringing at a their phones.

This feature prevents users from receiving hunt group calls and gives direct callers either voicemail, if enabled, or a busy signal. Users can enable and disable Do Not Disturb (DND) from their phone, Avaya one-X® Portal for IP Office or Phone Manager.

Users can allow some calls to bypass the DND setting and ring the phone. For example a manager can add their assistant’s extension number to the DND exceptions list. Users can manage the exceptions list with Avaya one-X® Portal for IP Office and Phone Manager. Both internal and external numbers can be on the exception list.

Emergency 911 call

(North America only) When an emergency call is connected, the system provides calling party information to an external line interface unit. The external unit carries out a number to text translation and forwards this to the emergency services bureau so that the originating location of the call is clearly identified.

Hunt Group Enable/Disable

User can temporarily join or leave individual hunt groups, for example, to assist during call peaks.

Supervisors or administrators don't usually take calls but at times of high call traffic they can join a group to take calls and when the peak is over, leave the group to resume their regular tasks. Administrators configure users as members of hunt groups. A user can not arbitrarily join a hunt group that they have not been identified as a member of.

Inclusion

Selected users can intrude on calls that are already in progress.

When the intruding user joins a call, all parties hear a tone. The speech path is enabled between the intruding party and the called user; the other party is forced onto hold and will not hear the conversation. On completion of the intrusion, the called party speech path is reconnected to the original connected party. Administrators enable or disable Inclusion on a per user basis through the Manager.

Off Hook Station

Off-Hook Station is designed for users who want their analog phone to operate like digital or IP feature phone, to isolate the user's phone idle state from the Hook state. This is a useful feature when using Avaya one-X® Mobile, Phone Manager or SoftConsole to control the phone state when using a headset on an analog phone and with call control and dialing from Avaya one-X® Mobile, or SoftConsole.

Pickup

Users can answer a call presented to another extension.

Call pickup scenarios include:

- Pick up any call ringing on another extension.
- Pick up a hunt group call ringing on another extension, where the user must be a member of that hunt group.
- Pick up a ringing call at a specified extension.
- Pick up any call ringing on another extension that is a member of the hunt group specified.

This feature is available across both multisite and small community networks.

Reclaim Call

Users can recover, or reclaim, the last call at their phone that is ringing or is connected elsewhere.

If users miss a call that goes to voicemail or call coverage, they can get the call back while it is still being presented or connected through the system. This is a version of the Acquire Call feature that only applies to the last call at an extension.

Relay On/Off/Pulse

The system has 2 independent switch outputs for controlling external equipment such as door entry systems.

Control switches using allocated handsets to open, close or pulse switches as required. Users can also control switches with Receptionist, SoftConsole and Voicemail Pro.

Restrict Network Interconnect

The Restrict Network Interconnect feature

India Toll Bypass Prevention

Indian telecom regulation states that the VoIP call should not be mixed with PSTN call if the call origination location and call targeting location are in different toll areas.

The India Toll Bypass Prevention feature ensures that the system is compliant with this regulation and allow calls to and from IP phones to connect to local PSTN public trunks only if the IP phone's location is the same as the system location. The feature is enabled by default for the India locale and disabled by default for all other locales. This feature is available for Branch and SCN deployments on IP500 V2 in Essential, Preferred and Select editions. No additional licenses are required.

Voice quality monitoring

Call administration features

Coverage to Operator

Administrators can configure an operator or a group of operators to provide coverage for external calls that would otherwise go to voicemail.

Unanswered calls are routed to an operator or a group of operators. For example, local government offices prefer to provide a personal service rather than voicemail.

Dial Emergency

Dial Emergency is a short code and permits specific numbers to be dialed regardless of call barring or a logged out phone.

Dial plan

IP Office has a very flexible numbering scheme for extensions, hunt groups and feature commands. While the system has default numbering for feature codes and extensions, they can all be redefined. Default extensions and hunt groups have 3 digit numbers starting at 200 but these can be changed from 2 to 9 digits through the IP Office Manager. There is a default set of feature access short codes, but these can be changed to whatever the end user requires, within limits. This is useful for example if IP Office is replacing a system where DND was accessed by dialing *21, it is possible to change the short code to mimic the code of the replaced system.

In certain countries IP Office can support a secondary dial tone when an access digit is dialed, though this limits some functionality like Alternate Route Selection (ARS). IP Office can also be configured to work without line access digits, by analyzing digits as they are dialed and determining if they are for an internal number or should be sent out on a line - this is valuable in SOHO installations where users will not necessarily be used to dialing an access digit for an outside line.

Direct Inward Dialing

Direct Inward Dialing (DID/DDI) relies on the local phone exchange passing all or part of the dialed number to IP Office.

Call routing software routes the call to an individual phone or a group of phones. Use this feature to reduce the workload on a receptionist by giving staff members or departments individual numbers for direct calls. Typically, the extension or group number is the same as the digits supplied from the network, but IP Office can convert the number to another number as needed within limits.

In North America, T1 circuits are required for DID.

Maximum call length

Maximum call length allows the system to control the maximum duration of any call based on the dialed number. Use this feature to control calls to cellular networks or data calls made over the public network to ISPs.

Paging

Supervisors and administrators can broadcast audio messages to digital and IP phones with loudspeakers without having to install a separate paging system. Paging can be to individual phones or groups of phones.

Implementation engineers can configure analog extension ports to an external overhead paging system, usually through an adapter, so that a port can be included in a paging group to permit mixed phone and overhead paging.

Some digital and IP phones can answer a page by pressing a key while the page is going on, this terminates the page and turns it into a normal call.

Relay On/Off/Pulse

The system has 2 independent switch outputs for controlling external equipment such as door entry systems.

Control switches using allocated handsets to open, close or pulse switches as required. Users can also control switches with Receptionist, SoftConsole and Voicemail Pro.

Transferable dial out privilege

Administrators and supervisors can grant outside line access to restricted phones, for example phones in public areas or conference rooms, to control external calls.

A privileged user, such as a supervisor, can transfer an outside line (secondary dial tone) to a user that does not have external dial out privileges.

Contact Center features

Account codes

Through the call records, supervisors and administrators can group calls by account code for the purpose of call costing and tracking. Supervisors and administrators can also restrict outgoing calls by requiring users to enter valid account codes.

The system stores a list of valid account code numbers. When making a call or during the call, a user can enter the account code they want associated with that call. The system checks the account code against the list of valid codes and requests the user to reenter the code if it is not valid. For incoming calls, the Caller ID can be used to match it with an account code from the list of valid codes and report the account code with the call for billing.

Supervisors and administrators can designate users to use a forced account code requiring them to enter a valid account code before making external calls. Using short codes it is possible to identify certain numbers or call types as requiring a valid account code before permitting the call to proceed, for example long distance or international numbers. Analog phone users can only enter account codes before making a call or in response to an audible system prompt to enter a code when making the call.

Account codes can also be entered through the Avaya one-X™ Portal for IP Office and Phone Manager. A system wide setting determines whether Phone Manager will display a list of account codes from which the user can select the code required or will hide the account code list.

In all the cases above, the account code entered is included with the call details in the IP Office's call record output. (SMDR).

Acquire Call

The Acquire Call feature allows users to take over a call connected to another extension. This feature is also known as Call Steal.

Administrators can set Acquire Call as a short code or assign it to a button on a digital or IP phone with programmable buttons. This feature is affected by intrusion control settings: the user acquiring a call must be set to be able to intrude and the user whose call is being acquired must be set so it can be intruded.

Acquire Call works in two ways:

Without a number Allows a user to reclaim a call that was ringing on their phone but has now gone elsewhere, for example to voicemail or a Forward No Answer destination. The Intrude settings are not checked. The user can reclaim the call even if it has been answered. If the last call to ring this user is no longer ringing or connected on the system, the feature will fail.

With a number Where the number is the phone number of a user who currently has the call to be acquired. If the user has a call ringing or waiting Acquire Call will act like the Call Pickup Extension short code and the user executing Acquire Call will be connected to the oldest ringing/waiting call. If the user has a connected call with no call waiting and the Intrude settings of the two users allow it, the call will be connected to the user executing the Acquire Call and the other user will be disconnected. If the user does not have a call the feature will fail.

Hold music

Administrators can access up to 32 sources for music on hold. On Linux systems up to four USB sources are supported.

A music source can be a locally stored single WAV file (default) or a local directory of WAV files. You can configure playback to start every time from the beginning of the file or directory, or to start from where it left off the last time.

Alternate music sources can be located on Server Edition Primary, Secondary, and expansion systems. Server Edition also supports centralized music on hold, where the Primary Server streams music to the Secondary Server and all expansion servers.

Agent login

Contact center agents must log in before they can make or receive calls.

Administrators and supervisors can set a login idle period to determine how long an extension can be idle before the user is automatically logged out, ensuring that an extension is not left logged in with calls going unanswered.

Monitor calls

Users can monitor another user's call by listening in.

This feature is not available by default; implementation engineers must enable it during system configuration. This feature includes an option to have a tone indicate when monitoring is in use. The user is only able to listen; they cannot speak during the conversation.

Outbound calling

Depending on the type of business, calls need to be treated in a specific way, such as recorded against a project or client through the use of account codes.

A business may have several sites linked through a private network but certain users, like customer service agents, may need to be able to call colleagues in other offices when the network is busy, while other users wait for a line to come free. Least cost routes can automatically translate the internal number to a direct dial call over the public network while other users wait.

Authorization codes

Authorization codes allow a user to go to another extension on the system and make calls using their personal toll restrictions; this may grant the user greater or fewer privileges than the normal owner of the extension they use.

Authorization codes are independent of account codes, so the user has to enter both if the required by the system configuration. All entered codes are logged in SMDR.

Call barring

Supervisors and administrators can prevent or allow calls to certain numbers such as international numbers or premium rate numbers for individual users or on a system-wide basis.

The system supports call barring at many levels. Short codes can be used at the system or individual user level to block the external routing of specific numbers or types of numbers. Typically the barring short codes are set to return busy tone, however they could route the call to an alternate number or to a Voicemail service that returns a 'barred dialing message'.

Users can allocate short codes to a user rights template. The users can then apply the template to the users whose calls need restriction. Administrators can also bar the forwarding of calls to external numbers on a per user basis.

Idle line preference

Idle line preference allows the user to select a specific external line for companies that prefer to work in key system mode.

Going off hook selects the first idle line appearance and the user connects to an outside line.

Override call barring

Override Barring can allow numbers dialed from the directory, using redial, call log, button programming, short codes, and numbers manually entered to external numbers present in the public directory (System Directory, LDAP, HTTP) even though a barred short code has been matched against dialed digits.

Private Call

Users can set Private Call status using short codes or a programmed button.

Private calls cannot be recorded, intruded on, bridged into or monitored.

Inbound calling

Hunt groups

A hunt group is a collection of users, typically users handling similar types of calls, for example a sales department. An incoming caller wishing to speak to someone in a group can call one number and the call can be answered by any number of extensions that are members of the hunt group.

There are four ways a hunt group can process calls:

Sequential	One extension at a time sequentially, always starting at the top of the list.
Collective	All extensions in the hunt group simultaneously.
Rotary	Start with the extension in the list immediately following the extension that answered the last hunt group call.
Longest Waiting	Start with the extension that has been free for the longest time period.

Announcements

Use voicemail in conjunction with hunt groups to:

- Record all group related messages.
- Play an announcement when the hunt group is in Night Service or Out of Service mode.

- Play announcements while a call is held in a queue.

A broadcast option is available for internal voicemail. This feature changes the voicemail box operation so that the message notification will only be turned off for each hunt group member when they retrieve their own copy of the message. Hunt group announcements are separated from hunt group queuing and can be used when queuing is off. Hunt group announcements are supported by Embedded Voicemail and Voicemail Pro. Administrators and supervisors can set times for the first announcement, second announcement, and between repeated announcements.

Hunt groups in a small community network can include members located on other systems within the network.

Assign Call On Agent Answer

Supervisors can set the Assign Call On Agent Answer hunt group option to enable CTI applications to correctly report the details for the call that is alerting and ensures that the call at the head of the queue is always answered first.

Night Service and Out of Service modes

Outside normal operation a hunt group can be put into two special modes: Night Service and Out of Service.

Night Service mode

Users can switch in or out of Night Service mode by dialing the appropriate short code. Calls are presented to a Night Service group. This can be controlled automatically by setting a time profile which defines the hours of operation of the main group or manually using a phone feature code. During Night Service mode, the original hunt group is temporarily disabled. You can design callers to the hunt group to do any of the following actions:

- Pass to a Night Service Fallback group passing calls to a manned extension or external number.
- Be played the Out of Hours greeting if set in voicemail.
- Receive a busy tone.

Out of Service mode

Users control Out of Service mode manually from a phone. While in this mode, calls are presented to the Out of Service group. Night service fallback using a time profile is not applied to a hunt group set to Out of Service.

Overflow groups

Supervisors can designate an overflow group to take calls if all extensions in the hunt group are busy or not answered.

Supervisors can also set overflow time to stipulate how long a call will queue before passing to the Overflow Group. Overflow time can be set for individual calls and for all calls in the group. The system can change the status of users who do not answer a hunt group call presented to them. The user status can be set to Busy Wrap-up, Busy Not Available or Logged Out. The change of status can be set per user and per hunt group.

Queuing

Queuing allows calls to a hunt group to be held in a queue when all extensions in the group extension List are busy. When an extension becomes free the queued call is then presented. The definition of queued calls now includes ringing calls and calls waiting to be presented for ringing. The queue limit can be set to control the maximum number of calls to wait against a hunt group.

While queuing, if Voicemail is operational, the caller will be played the announcements for this hunt group.

Queue threshold alert

Supervisors and administrators can set an alert to occur at a selected analog extension port when the number of calls queued against a hunt group exceeds a threshold.

Typically the alert is a loud ringer or other alerting device. The alert does not present a call.

Incoming call routing

Intelligent call routing makes routing decisions based on any or all of the following criteria:

- Digits from the exchange such as DDI/DID or ISDN MSN
- Calling phone number or Caller ID or part of the number received such as an area code
- ISDN sub-address
- ISDN/PRI service type such as Voice Call or Data Call

For example, a DDI/DID call to a sales group can be handled differently depending on which part of the country the call is originating from.

Each incoming Call Route supports a secondary destination Night Service that can provide alternative routing for an incoming call based on time of day and day of week criteria, as well as calendar-based routing for specific dates.

Calls that cannot be routed to the configured destination are rerouted to a user-defined Fall Back destination. This can be particularly useful where calls are normally answered by an auto-attendant and a network fault occurs.

Where multiple call routes are set up to the same destination, a priority level can be associated with the call. The priority level determines a call's queue position in place of simple arrival time.

Note:

calls already ringing a free extension are not considered queuing and are not affected by a high priority call joining a queue (unless the option Assign Call On Agent Answer is selected for that hunt group).

Supervisors can configure a Priority Promotion Timer to increase the priority of calls which have been in the queue for more than a defined time and add and optional tag to calls on the Incoming Call Route, which can be displayed on the alerting phone.

Time profiles

Time profiles set the operational times for service. For example, a time profile could be set up to make Internet access available to staff only during lunch times.

Using time profiles it is also possible to define an alternative service to operate outside the operational hours of the main service. This option may be used to take advantage of alternative tariffs at off peak periods. Switching to this fallback service can also be controlled manually by dialing a secure short code from a handset. This can be particularly useful in allowing quick restoration of service in the event of an ISP failure. This feature also applies to days of the week or specific calendar dates.

IP telephony features

Auto-create extensions

Implementation engineers can configure IP Office to create extension entries for new IP phones added onto the local area network.

In cases where the local area network is not secure this facility can be disabled, but simplifies installation.

Direct media path

Direct media path allows the speech path between two IP extensions (after call setup) to be routed directly to each other. This allows the system to free up voice compression resources after establishing the end to end connection, allowing the resources to be used in the most efficient way.

Early media and PRACK support

IP Office supports in-band announcements such as:

- Branding from discount or bulk long distance providers
- Progress indications when extraordinary wait times are inherent in the call scenario, for example when trying to locate a cell phone
- Country-specific ring back and other progress tones
- Conferencing in the IP domain before call answer, for example, in call recording scenarios or for automatic dialers' conferencing in agents

Implementation engineers can configure SIP trunks to support early media by adding the **100rel to Supported** header in the **INVITE** parameter.

Fast start

Implementation engineers can configure fast start on an IP extension to reduce the protocol overhead allowing an audio path to be established more quickly.

Fax transport

IP Office supports Avaya proprietary and T.38 fax transport protocols.

Avaya proprietary fax transport protocol

Fx calls route over VoIP trunks between IP Office systems on an IP network using a proprietary Avaya transport protocol.

T.38 fax transport protocol

IP Office supports the T.38 protocol for fax messages transmission between IP Office and SIP trunks and SIP extensions.

Note:

T.38 protocol is not supported on Server Edition systems. G.711 fax transport is used.

Platforms	IP500 V2 with a VCM32 or VCM64 module
Trunk types	SIP
Extensions	SIP
Transport layers	UDPTL with optional redundancy error correction
Versions	0–3
Call types	Voice calls with transition to fax relay on detection of fax tones and calls which are negotiated as fax-only.
Fax fallback	SIP Trunks and SIP Extensions can now configure the Fax Transport Support to T38 Fallback so that outgoing fax calls use T.38 fax, but when the called destination doesn't support T.38 and rejects the call, a re-invite is sent for fax transport over G.711. Incoming audio calls that detect fax tones also initiate fax transport using T.38 Fallback. This allows IP Office to support additional deployments where T.38 fax may not be universally available.

Inbound call directory name display

Administrators can select either the CLID or directory name as the default display for inbound calls.

Out of band DTMF

Implementation engineers can configure out of band DTMF on IP extensions to signal to the other end of a connection the digits to be regenerated by a local DTMF generator on behalf of the sending IP extension. This is useful when navigating external voicemail systems and auto-attendant systems.

PAI and privacy headers

PAI and privacy header defaults allow callers and calling parties to have anonymity while still providing necessary billing and traceability information, and emergency 911 information to the network. This feature satisfies the functionality with implementation guidelines outlined in the SIPconnect 1.1 Technical Recommendation.

Silence suppression

Silence suppression makes the best use of available bandwidth, such as the connection over which the caller is listening, not speaking. Silence suppression works by sending descriptions of the background noise, rather than the actual noise itself, during gaps in conversation, thereby reducing the number and frequency of voice packets sent on the network. Background noise is very important during a phone call. Without noise the call will feel very unnatural and give a perception of poor quality. Ensure that silence suppression configuration matches at both ends of the SCN trunk for correct operation and also for improved sound quality.

SIP features

SIP endpoints are supported on IP Office audio (voice) and T.38 fax communication using SIP terminal adapters. Users can use standards-compliant IP phones using the open SIP standard, offering a choice of endpoints including special purpose devices such as conference phones, hotel phones and terminal adapters.

IP Office supports Avaya 1100 and 1200 series phones using the SIP protocol. The phone user interface can vary when used on BCM with UNIStim. For example, with SIP, the 1100 and 1200 series IP phones only support a single call appearance although multiple calls are supported by the 1100 and 1200 series phones.

Note:

These phones are only supported on IP500 V2 control units.

In pure SIP systems, IP Office expands the feature set beyond the SIP standard offering features on SIP endpoints delivering features consistently between SIP and Avaya digital and IP endpoints.

Note:

In order to use a non-Avaya SIP endpoint with IP Office, obtain a Third-party IP Endpoint license from Avaya. This license supports endpoints based on the H.323 standard and is required for generic SIP endpoints on IP Office. Avaya IP Office SIP phones use the IP Endpoint license.

PSTN toll bypass

Toll bypass allows each system to leverage the trunk connections of the other system in the network to avoid international and long distance charges.

Standard call features

- Basic Call Completion
- Handling of busy called party
- DTMF and ring-back tone
- Hold and Retrieve
- Transfer
- Call Waiting presentation
- Called Number display
- Calling number and name display
- Abandoned call
- Single call appearance

Advanced call features

SIP endpoints support a number of extended features according to the SIP service samples, also referred to as "Sipping-19". Features include:

- Calling line identification
- Hold/Consultation Hold
- Attended/Unattended Transfer
- Message waiting
- Do not disturb
- Conference Add
- From in Clear when privacy is requested
- User agent header (configurable) included to identify call in SIP trunks for troubleshooting
- Busy lamp keys with speed-dial, status indication, and pickup
- Self-labeling feature keys for softkey support including a Special feature key. The supported features are also available pressing a feature key plus the appropriate feature code. The feature codes are identical to the features codes from BCM

Feature activation key features

A large number of additional features are supported on IP Office using feature activation keys. These features include but are not limited to:

- Call forward: Unconditional/Busy/no Answer
- Follow me
- Park/Unpark
- Music on Hold
- Meet me conferencing
- Conference join
- Ring back when free
- Multiple call appearances

  Note:

  Does not include bridged appearances or outside-line appearances.

CTI features

SIP endpoints support the following CTI-based features using the TAPI interface:

- Outgoing call (without remote activation of speakerphone/headset)
- Hang up
- Hold
- Attended/Unattended transfer
- Conferencing
- Voicemail collect
- Set forwarding/DND (IP Office based)
- Park/Ride (IP Office based)

Note:

Avaya Phone Manager and Phone Manager Pro and SoftConsole are currently not supported in combination with SIP endpoints.

Video conferencing

Video conferencing is supported in the following configurations:

- Local system
- Small community network
- Video-ready SIP trunk such as Avaya Aura®

All video communication is end-to-end; IP Office does not natively manage or perform video conferencing.

The softphone application handles video conferencing. IP Office video conference supports the following features using feature access codes:

- Make calls to all phones and trunk lines as audio only
- Receive audio calls
- Call forwarding
- Forward to voicemail recording audio streams, not video.
- Application sharing
- Accept several video calls in parallel to leverage the Multi-Conference Unit (MCU) functionality, for example, the Avaya 1040 system

Video requires high network bandwidth, depending on codec video quality it can be up to 1 Mbit/sec. IP Office supports with H.263 and H.264 codecs. During planning, a network assessment identifies the bandwidth requirements. Refer to product details for video requirements. Typical bandwidth requirements for HD video are:

- 1010: 1 Mbps for 720p/30fps
- 1040:
    - 768 Kbps for 720p 30fps
    - 1.1 Mbps for 720p 60fps
    - 1.7 Mbps for 1080p 30fps

Voice compression

IP Office supports a wide range of voice compression standards including G.711, G.729a and G. 722. The method of compression can be either automatically established on a call-by-call basis or configured on an individual extension basis.

Voice compression

G.722 is supported on the following types of SIP phones:

- 9600 series
- 96x1 series
- B179 conference phones
- 1100/1200 IP phones
- Third-party SIP phones

Note:

G.722 is not supported for 5600 and 1600 series phones.

IP Office Branch telephony

Telephony services

The Branch solution provides telephony services to centralized users and IP Office users.

IP Office users obtain telephony services from the local IP Office. The Branch solution supports all hard and softIP Office endpoints. For a list of IP Office endpoints, see “Phones” in *IP500/IP500 V2 Installation* (15-601042).

Centralized users register to the Avaya Aura® Session Manager and obtain telephony services from the Avaya Aura® Communication Manager Feature Server or Evolution Server in the enterprise core. Centralized users can use one of the following supported centralized endpoints:

- 9620 SIP 2.6
- 9630 SIP 2.6
- 9640 SIP 2.6
- 9650 SIP 2.6
- 9601 SIP 6.2.2
- 9608 SIP 6.2.2
- 9611G SIP 6.2.2
- 9621G SIP 6.2.2
- 9641G SIP 6.2.2
- Avaya one-X® Communicator SIP 6.2 (audio only)

  Note:

  The 9600 series SIP phones and Avaya one-X® Communicator SIP are supported only as Centralized phones for use by Centralized users. They are not supported as IP Office phones for use by IP Office users.

- The 1100 and 1200 series phones are supported as IP Office users or as Centralized users.
- E.129 series phones are supported as IP Office users but are not supported as Centralized users.
- B.179 series phones are supported as IP Office users or as Centralized users.

Survivability for centralized users

If WAN connectivity to the Avaya Aura® Session Manager is lost or if all deployed Avaya Aura® Session Manager servers are down, centralized users automatically get basic telephony services from the local IP Office with survivability or rainy day mode. The telephony features provided by the IP Office in rainy day mode are limited compared to the features that are normally provided to the centralized phone.

The following features are available on 9600 Series centralized SIP phones registered to IP Office in rainy day mode.

- Make or receive calls to or from other endpoints in the branch and to or from any type of local PSTN trunk
- Caller ID
- Multiple call appearances but not bridged appearances
- Call hold and consultative hold
- Music on hold
- Attended call transfer
- Unattended call transfer
- Three-party ad-hoc conferencing done locally on the phone, as well as capability to dial into Meet-Me conferencing on the IP Office up to 64-party conference
- Centralized voice mail coverage and access over PSTN, but no Message Waiting Indication (MWI)
- Automated Attendant
- Survivability mode indication on the phone screen
- Local telephone features: redial, mute, audio selection (speaker / headset / handset), Call Logs, Volume Control, local contacts, speed-dials, auto dials
- Station Message Detail Recording (SMDR) records stored on the IP Office for retrieval after WAN recovery
- Hunt groups

  IP Office can be configured with Centralized hunt groups for which IP Office processing is in effect only in the Rainy day mode. The IP Office administrator must configure the hunt groups on the IP Office consistent with the configuration on the central Avaya Aura® Communication Manager for the Sunny day mode.
- Call Management

  IP Office can be configured with short codes using the Barred feature to restrict in the Rainy day mode what calls the Centralized user can make. The IP Office administrator must configure this consistent with the Class of Restriction (CoR) configured on Communication Manager, which is applied to the same user in the Sunny day mode.
- Send call to mobile phone

  IP Office can be configured with Mobile Twinning to send calls for the Centralized user in the Rainy day mode to a mobile number. The IP Office administrator must configure this on the IP Office consistent with the EC500 configuration on the central Communication Manager for the same Centralized user.
- Call forwarding

  Local Call Forwarding on the phone in the Rainy day mode can be configured. The Call Forwarding set on Communication Manager in the Sunny day mode has no impact on the local behavior of the phone or on the IP Office behavior in the Rainy day mode. Also, the local Call Forwarding set on the phone works only in the Rainy day mode after failback.

- Authorization codes

  IP Officecan be configured to support authorization codes that Centralized users can use in the Rainy day mode. The IP Office administrator must configure authorization codes consistent with the authorization codes configured on Communication Manager, which are available to the same Centralized users in the Sunny day mode. Centralized SIP phone users in Sunny day will hear 3 beeps to indicate that an authorization code is required. In the Rainy day mode, the Centralized SIP phone users will hear 1 beep that repeats approximately every 5 seconds.

Messaging features

Messaging enables users to manage all of their messages, both emails and voicemails, in one place. Since the main messaging platform is typically email, IP Office enables users to manage voicemails through the email system in order to keep all messages synchronized through one user interface. IP Office offers two voicemail options: Embedded Voicemail and Voicemail Pro.

Voicemail in general provides a phone answering machine with a personalized greeting on every employee's desk and allows callers to leave spoken messages when the user cannot answer a phone call. Voicemail messages are retrieved either locally or remotely via any phone (users are prompted for a PIN if they are using any phone other than their allocated extension or a trusted location e.g. mobile phone).

The voicemail server is multilingual and can offer different prompts depending on the user's preferred language, independently of the default system setup. Similarly, external callers can hear prompts in their own language depending on their incoming call route (for example, based on caller ID).

Voicemail options available are:

- IP Office Essential Edition Embedded Voicemail enables some basic messaging through the ability to forward voicemail messages to the user's email inbox.
- IP Office Preferred Edition
  - Voicemail Pro - for single site use but use in an SCN from remote users
  - Distributed Voicemail Pro - for multisite use in an SCN
  - Centralized Modular Messaging - for use with Avaya Aura® Communication Manager

IP Office Preferred Edition is available for Windows and Linux OS. Preferred Edition on Linux provides the same functionality as described further in this chapter, with the following exceptions:

- Web Voicemail is provided by the user productivity application which comes with Office Worker, Teleworker and Power User licenses.
- VPNM
- IVR related actions (Database and VB Scripting)

- Voice Recording Library Authentication (VRLA)

Related Links

Messaging feature comparison on page 53

Messaging feature comparison

The following table summarizes the operational and functional differences between the messaging applications IP Office supports on the IP500 V2 control unit.

Capacities

Capacity	Voicemail Pro	Embedded Voicemail
Number of mailboxes	No Limit - Limited only by IP Office configuration.	Limited only by IP Office configuration.
Concurrent calls (ports)	Up to 40 dependent on license	6 simultaneous calls
Recording time	PC dependent (Requires 1 MB per minute)	2 ports: Up to 15 hours 4 ports: Up to 20 hours 6 ports: Up to 25 hours

Features

Feature	Voicemail Pro	Embedded Voicemail
Runs as a service	Yes	No
Multilingual support	Yes	Yes
Voicemail for individual users	Yes	Yes
Voicemail for virtual users	Yes	Yes
Voicemail for hunt groups	Yes	Yes
Group broadcast	Yes	No
Unified Messaging Service (UMS)	Option	No
Integration with Microsoft Exchange Server	Option	No
Capable to interact with Blackberry solution	Option[1]	No
Resilience and Backup	Option	No
Small Community Network operation	Yes	No
Centralized voicemail services	Yes	No

Table continues…

[1] Requires UMS (enabled through the Power User, Office Worker and the Teleworker licenses) and MS Exchange Server 2007/2010 with a mobility solution (for example a Blackberry) - not provided by Avaya.

Feature	Voicemail Pro	Embedded Voicemail
Distributed voicemail servers in an SCN	Yes	No
Voicemail Ringback	Internal and external	Yes
Voicemail Help TUI	Yes	No
Message Waiting Indication	Yes	Yes
Visual Voice (interactive menu on phone display)	Yes	Yes
Integration with Phone Manager Pro	Yes	No
Personalized greetings	Yes	Yes
Extended personal greetings	Yes[2]	No
Continuous Loop Greeting	Yes	No
Forward to email	Yes	Yes
Copy to email	Yes	Yes
Listen to email (Text-To-Speech)	Yes[2]	No
Send email notification	Yes	Yes
Save message	Yes	Yes
Delete message	Yes	Yes
Forward Message to another mailbox	Yes	Yes
Forward to multiple mailboxes	Yes	Yes
Forward with a header message	Yes	Yes
Repeat message	Yes	Yes
Rewind message	Yes	Yes
Fast forward message	Yes	Yes
Pause message	Yes	No
Skip message	Yes	Yes
Oldest message first/newest message first Message Playback Option	Yes	No
Set message priority	Yes[2]	No
Set automatic message deletion time frame	Yes	No
Alphanumeric Data Collection	Yes[2]	No
Callers Caller ID, time and date announced	Yes	Yes

Table continues…

[2] Intuity mode only.

Feature	Voicemail Pro	Embedded Voicemail
Call Back Sender (if Caller ID available)	Yes	Yes
Remote Access to Mailbox	Yes	Yes
User Definable PIN Code	Yes	Yes
Known Caller ID PIN Code By-Pass	Yes	Yes
Breakout to Reception	Internal and external.	Internal and external.

In queue announcements

Feature	Voicemail Pro	Embedded Voicemail
Queue Entry Announcement	Yes	Yes
Queue Update Announcement	Yes	Yes
Queue Position Announcement	Yes	No
Time in Queue Announcement	Yes	No
Time in System Announcement	Yes	No
Estimated Time to Answer (ETA)	Yes	No
Exit Queue to alternative answer point	Yes	No

Auto-Attendant/Audiotex

Feature	Voicemail Pro	Embedded Voicemail
Multi-Level Tree Structure	Yes	Yes
Message Announcements	Yes	No
Whisper Announce	Yes	No
Alarm Calls	Yes	No
Assisted Transfers	Yes	No
Dial by Name	Yes	Yes
Direct Dial by Number	Yes	Yes

Other features

Feature	Voicemail Pro	Embedded Voicemail
Call Recording	Yes	No
Tamper proofed/verified Call Recording	Yes	No
Test Conditions	Yes	No
Personal Numbering	Yes	No
Speaking Clock	Yes	No

Table continues…

Feature	Voicemail Pro	Embedded Voicemail
Campaign Manager	Yes	No
Voicemail Pro Manager	Yes	No
Customized voicemail	Yes	No
Intuity TUI emulation mode	Yes	No
Forward Emails to external systems (VPIM)	Yes	Yes
Third-party database Access (IVR)	Yes	No
Text-To-Speech within call flows	Yes	No
Support for Visual Basic Scripts	Yes	No

Related Links

Messaging features on page 52

IP Office Branch messaging

Messaging

The IP Office Branch solution supports IP Office voice mail systems and centralized voice mail systems.

The following centralized voice mail systems are supported:

- Avaya Aura® Messaging
- Avaya Modular Messaging
- Avaya CallPilot®: Only supported in distributed branch environments connected to CS 1000.

The following IP Office voice mail systems are supported:

- Embedded Voicemail: Default IP Office voice mail system
- Voicemail Pro: Available with IP Office Preferred and Advanced editions

For information about the configuration requirements of each voice mail system, see *Reference Configuration for Avaya IP Office in a Branch Environment* (15–604253).

In a stand-alone branch environment, the enterprise branch can only use an IP Office voice mail system.

In a distributed branch environment, the enterprise branch can choose an IP Office voice mail system or a centralized voice mail system for users. If the distributed environment is connected to CS 1000, users can also use Avaya CallPilot® as their voice mail system.

In a mixed or centralized branch environment, the enterprise branch can only use a centralized voice mail system.

Related Links

Messaging features on page 52

Mobility features

Hot desking

Hot desking allows users nonexclusive use of the a single extension.

Users log with their own identity so they can receive calls and can access their voicemail and other facilities. For example, sales personnel who visit the office infrequently can be provided with telephony and voicemail services without being permanently assigned a physical extension. When finished, they simply log out to make the extension available to others or if users log in at another phone, they are automatically logged out of the original extension.

Remote access features

IP Office's integral firewall, service quotas and timebands all apply to remote access calls. Remote access security can be supplemented by CHAP (encrypted passwords) to verify the end users, or PAP which does not support encryption. Timebands can control the hours within which the remote access service is available.

A trusted location can be set for dial in. These are locations that the system will allow either data access, for example, a user dialing in from home, or access to voicemail without a voicemail code for a user collecting their voicemail messages from a mobile. The trusted location is also the location the voicemail server will call to inform the user of a new message.

Conversely a specified location can be set which restricts remote access from only that location, this specified location can also be a designated dial back number thereby minimizing the threat of unauthorized remote access.

IP Office can also incorporate remote access dial back services so that if a user always remotely accesses the office from a single location, for example, their home, then after login verification, the system disconnects their call and dials them back. In addition to the added level of security dial back provides, it can also be an excellent method of consolidating remote access charges onto the central office phone bill.

In addition to remote access from phone adaptors, all ATM4 trunk cards (including the IP500 V2 Combination Card ATM) support switching of the first analog trunk to an integral V.32 modem for remote access.

Remote hot desking

Users can make and receive calls from any office as if using the phone on their own desk. Users have access to the centralized system and personal directory as well as their call logs (available on digital, analog and IP phones).

When a user logs in to a remote IP Office system, all their user settings are transferred to that system.

- The user's incoming calls are rerouted across the SCN.
- The user's outgoing calls use the settings of the remote IP Office.
- However some settings may become unusable or may operate differently. For example, if the user uses a time profile for some features, those feature will only work if a time profile of the same name also exists on the remote IP Office.

IP Office supports remote hot desking between IP Office systems within an SCN. The system on which the user configured is termed their “home” IP Office, all other systems are “remote” IP Offices. No additional licenses are required to support remote hot desking other than the Voice Networking license on each IP500 V2 within the SCN. A single number provides improved mobility and easy access to familiar features. For example consultants, managers, and lawyers can use their phone services at different offices on different days.

In some scenarios a hot desking user logged in at a remote system will want to dial a number using the system short codes of another system. This can be done using either short codes with the Break Out feature or a programmable button set to Break Out. This feature can be used by any user within the SCN but is of significant use to remote hot deskers.

Note:

Remote hot desking is not supported for use with contact center. Features handled by the phone itself are not affected by hot desking, for example, call log and phone speed dials)

Remote Worker

Remote Worker allows the connection of remote 9600 Series IP phones with the H.323 FW which resides behind a NAT router to IP Office. The configuration does not require any VPN concentrator equipment with IP Office.

With the Remote Worker feature enabled, remote 9600 H.323 IP Phones can connect to IP Office even if it is located behind a NAT router. The sets are authenticated on IP Office in the same way as sets in the private network. The IP Office determines that a set is located outside the private network and relays the VoIP RTP traffic to ensure it transverses the NAT router.

Note:

The H.323 signaling and the media traffic is not encrypted however the proprietary binary format adds a basic level of encryption.

To reach the IP Office from the remote private network remote H.323 IP phone needs to be configured to the public IP address of the NAT router hosting IP Office. Configurable ports need to be forwarded to IP Office. IP Office requires a valid public IP address configured for the feature to function. The public IP address can be statically configured or dynamically discovered via a STUN server.

Administrators enable Remote Worker using IP Office Manager. To use the Remote Worker feature, the Essential Edition license is required which provides 4 remote worker seats. Additional remote worker capability is available with the Teleworker User package and a Preferred Edition license.

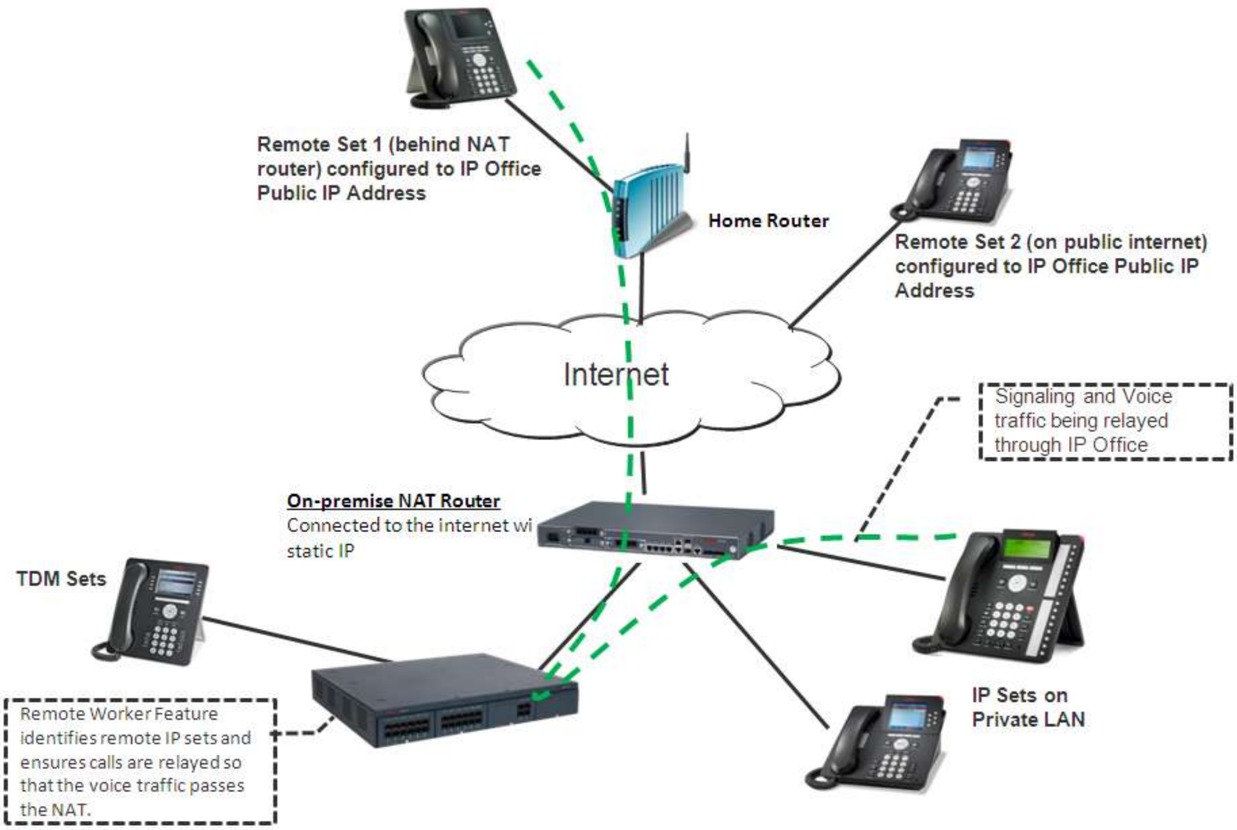


Figure 1: Remote Worker interactions

Telecommuter mode

Users can make and receive calls and the retrieve voicemails from an external phone number as if they were in the office, with the server providing the call control.

The typical scenario is the remote worker that occasionally works from home or from a hotel room. This feature also provides billing convenience and potential cost savings for remote workers and mobile work force as all the calls are established by IP Office. There is no need to check bills or to pay for expensive hotel calls.

Twinning

Twinning allows a primary extension and a secondary number (extension or external) to operate together as a single phone.

Twinning allows calls to a user main extension number to alert at both that extension and a secondary extension. This feature is aimed primarily at users who have both a desk phone and a wireless extension. Calls from the secondary twinned extension are presented as if from the user's main extension. Presentation of call waiting and busy is based on whether either of the twinned extensions is in use.

When a call is presented to the primary phone the secondary will ring. If the primary phone does not ring, for example in Do Not Disturb, the secondary phone will not ring.

This is typically used in scenarios like workshops or warehouses where team supervisors may have a desk with a fixed phone but also have a wireless extension (e.g. DECT). When a call is made from either twinned phone, the call will appear to have come from the primary phone. Other users of the system need not know that the supervisor has two different phones. The supervisor’s Coverage Timer and No Answer Time are started for the call and if the call is not answered within that time, the call will be delivered to available coverage buttons and then voicemail.

The following features are supported with twinning:

- Follow Me To
- Follow Me Here
- Forwarding
- Do Not Disturb (including exceptions)
- Context less hunt group actions: Membership/Service Status/Fallback Group configuration
- Voicemail On/Off/Access
- Call Log (Central Call Log for T3 and 1600 phones only)
- Redial (Central Call Log for T3 and 1600 phones only)
- Personal Directory Entries (for T3 and 1600 phones only)

Mobility features include:

- Mobile (external) Twinning
- Mobile Call Control
- Mobility Callback
- Avaya one-X Mobile Client Support

VPN Phone

VPN Phone is a full-featured IP telephony solution that provides secure communication over public ISP networks to IP Office at the company headquarters. VPN phones provide full telephony features available at the user's desktop to a remote location like a home-office. There is no restriction on VPN phone usage.

VPN Phone is a software-only feature on the standard 5610/5620/5621 or 4610/21 IP phones. In combination with one of these phones and the most popular VPN gateway products, the software extends enterprise telephony to remote locations. VPN functionality is supported on 9600 IP phones and does not require additional software.

VPN Phone works in the following situations:

- Virtual Office workers
- Remote workers
- Remote call center
- Business continuity support
- Very small locations that require a single phone only
- Temporary installations such as conferences, off-site meetings, and trade shows

VPN Phone has been tested with a number of VPN-gateways from major vendors like Cisco or Juniper as well as with smaller VPN-access devices from companies like Adtran, Kentrox, Netgear, and SonicWall. Refer to the support pages (support.avaya.com) for a list of available application notes on VPN-gateways tested with each line of phones.

Networking features

Alternate Route Selection

If a primary trunk is unavailable, then Alternate Route Selection (ARS) provides automatic fallback to an available trunk, for example, analog trunk fallback if a T1 or SIP trunk fails, or use PSTN for SCN fallback.

By configuring ARS, the system can route calls through the optimum carrier. You can also use time profiles to take advantage of less expensive rates or better quality at specific times of day.

Multiple carriers are supported. For example, local calls are to go through one carrier between specific hours and international calls through an alternative carrier. Carrier selection using two-stage call set up through in-band DTMF is possible. It is possible to assign specific routes on a per user basis to only allow expensive routes to be used by critical staff.

Auto Connect

If a service is idle, that is no one is using the internet, Auto Connect allows the system to periodically connect to a service. This is ideal for mail polling to retrieve email from an internet service provider. An Auto Connect Time Profile controls the time period during which automatic calls are made, for example not at weekends or during the middle of the night.

Callback

Three types of call back are supported:

Link Control Protocol (LCP)	After authentication the incoming call is dropped and an outgoing call is made to a predefined number to reestablish the link.
Microsoft Callback Control Protocol (CP)	After authentication from both ends, the incoming call is dropped and an outgoing call to a predefined number made to reestablish the link.
Extended Callback Control Protocol (CBCP)	Similar to Callback CP however, the Microsoft application at the remote end will prompt for a phone number. An outgoing call will then be made to that number to reestablish the link.

Firewall

IP Office integrated firewall provides packet filtering of the most common IP protocols including File Transfer Protocol (FTP) and Internet browsing (HTTP). Each protocol passing through the firewall can be restricted/allowed access in four different ways:

Drop	No sessions using this protocol will be allowed through the firewall.
In	An incoming session can get through the firewall to allow traffic in both directions.
Out	An outgoing session can get through the firewall to allow traffic in both directions.
Bothway	An incoming or outgoing sessions can get through the firewall to allow traffic in both directions.

In cases where a protocol is not supported by default, the firewall can be customized to control packets based on their content.

IP Office allows the configuration of as many firewalls as needed through IP Office Manager. This permits different security regulations to be applied to individual dial-in users and data services.

Internet Access

IP Office provides shared, secure, high-speed access to the internet via exchange lines (Central Office), digital leased lines or IP VPN services.

IP Office handles internet security with an integrated firewall removing the need for a standalone firewall. System administrators can configure the firewall to accommodate a variety of situations and to control who can access external resources and when.

The firewall isolates private networks from the internet, ensuring that the network remains beyond the reach of hackers, while allowing service quotas to be set against a remote access service to ensure authorized users can gain access. Service Quotas place a time limit on outgoing calls to a particular IP Service so limiting costs.

Each service can be configured with an alternative fall back, for example, to connect to an ISP during working hours and at other times take advantage of varying call charges from an alternative ISP. Or, set up one service to connect during peak times and another to act as fallback during the cheaper period.

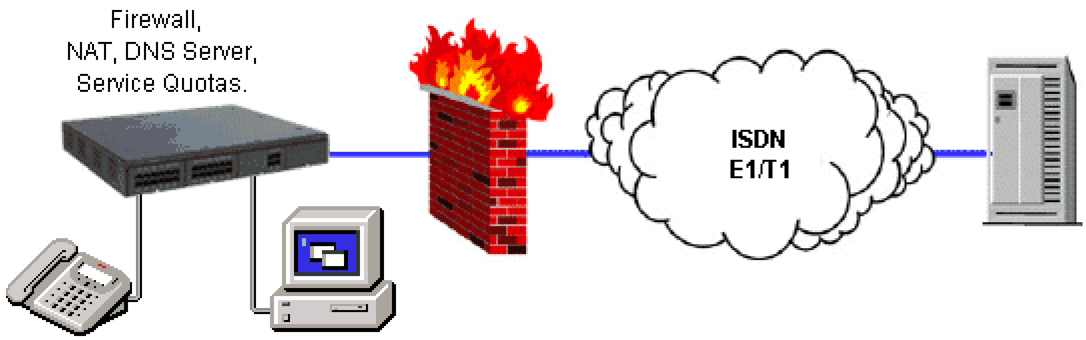


Figure 2: Internet access

Network Numbering Schemes

IP Office provides flexible network numbering options. The system can manipulate dialed digits adding or removing digits and access codes to fit into any numbering scheme. Two types of numbering schemes are commonly deployed: linked numbering and node numbering.

In linked numbering schemes each site within the network has a unique range of extension numbers and users simply dial the extension number of the called party. Often, linked numbering schemes are used in very small networks (less than 5 sites) with less than 500 extensions.

With node numbering schemes, each site is given a node ID and this is prefixed by the user when dialing extensions at other sites. In this way extension numbers can be replicated across sites while still appearing unique across the network. Node numbering schemes are common in larger networks.

Linked numbering schemes and node numbering schemes are sometimes both used within the same network with node numbering used at the large offices and linked numbering employed at clusters of satellite offices.

Service Quotas

IP Office can be configured to limit the maximum number of minutes that a service, such as Internet Access, is available for each user. This is the sum total of calls made and does not include periods of inactivity. Once the quota has been used the service is no longer available. The quota can be either automatically refreshed daily, weekly or monthly or manually refreshed by dialing a secure feature code on a handset.

Time Profiles

Time Profiles can be used to define when a Service, Hunt Group, Least Cost Route, Conference Bridge or a user's dial-in facility are operational. For example, a time profile can be used to route hunt group calls to a manned extension or voicemail outside of office hours, or be used to apply different Least Cost Routes at varying times of day to take advantage of cheaper call rates. Multiple Time Entries can be created so that a Time Profile can be used to define specific hours in the day e.g. 09:00-12:00 and 13:00-17:00. Outside of a Time Profile, voice calls would be re-routed according to the configuration but any currently connected calls at the time the Time Profile changes would not get cut off as the change only affects the routing. Data calls will get cut off as the time profile goes out of service but a new data call will start immediately if specified. Time Profiles can also be based on specific calendar dates to make allowance for public holidays or other events.

Multisite networking

When connecting IP Office systems together over IP or packet-based networks, Small Community Networks (SCNs) enhance feature transparency. These networks can support up to a maximum of 1000 users across 32 sites.

IP Office supports the following features in an SCN environment:

Basic call setup (voice)	Supported by H.323 and SIP on IP trunks
Call Hold (local)	Supported by H.323 and SIP on IP trunks
Call Transfer (local)	Supported by H.323 and SIP on IP trunks
Called/Calling Name	Supported by H.323 and SIP on IP trunks
Called/Calling Number	Supported by H.323 and SIP on IP trunks
Busy Lamp Field (BLF)	
Camp-on	
Call Back When Free	
Paging	
Pickup	

Location based time zones	Different times zones for group of extensions based on locations. For 96xx, 16xx, 11xx/12xx, D100, and E129 phones
Centralized Personal Directory	For 1400, 1600, 9600 and T3 phones and Avaya one-X® Portal for IP Office
Centralized System Directory	For 1400, 1600, 9600 and T3 phones and Avaya one-X® Portal for IP Office
Centralized Call Log	For 1400, 1600, 9600 and T3 phones and Avaya one-X® Portal for IP Office
Centralized Voicemail	Preferred Edition. Support for mailboxes, call recording, dial by name and auto attendants. Remote queuing on remote systems is also supported.
Distributed/Backup Voice Messaging	
Internal Directory	
Absence Text	
Anti-Tromboning	
Distributed Hunt Groups	Hunt groups can include users located on other IP Office systems within the network.
Remote Hot Desking	Users can hot desk between IP Office systems within the network. The system on which the user configured is termed their home IP Office; all other systems are remote IP Office systems.
Breakout Dialing	This feature allows the user to select an IP Office system in the network from a displayed list and then dial a subsequent number as if dialing locally on the chosen system. This feature is triggered either by a programmable button or short code.

Resiliency

As an example, in an SCN configuration of System A and System B where the centralized voicemail is connected to System B, and a number of IP phones are connected to either System A or System B. If System B fails then:

- System A will automatically take over from System B and support IP phones, hunt groups, and DHCP if required.
- Voicemail Pro will reregister to System A.
- For users in an SCN, when they hot desk to another IP Office system, they retain their licensed profile setting as configured on their home system.

- All System B users' personal contacts and call logs will continue to be available (96x1, 9600, and 1600 phones).

For multisite networks, VCM modules are required in all systems being connected. The IP lines may be configured in a start or a meshed configuration. One of the advantages of a meshed configuration is that it removes the risk of a single point of failure within the network. Also the names and numbers (groups, line, services, etc.) on the separate IP Office systems should be unique to reduce potential maintenance confusion.

EachIP Office system broadcasts UDP messages on Port 50795. These broadcasts typically recur every 30 seconds but BLF updates are potentially more frequent. There are no updates if there is no activity and the overall level of traffic is very low - typically less than 1 kbps per system.

Multisite networking is supported between IP Office systems with differing software levels but network features will be based on the lowest level of software within the network. This option is intended to allow the phased upgrading of sites within a multisite network and it is still recommended that all systems within a network are upgraded to the same level where possible.

If larger networks are required Q.SIG can be used to link multiple SCNs together. Functionality between the communities is governed by the Q.SIG feature set.

Voice networking licenses

On IP500 V2 systems, multisite networking (with SCN) requires one or more additional licenses. Server Edition Expansion (V2) systems do not require voice networking licenses.

Q.SIG, H.323 and SCN capabilities are not enabled by default on IP500 V2. An additional license is required to enable this functionality with 4 simultaneous networking channels (no channel limit for Q.SIG). Additional channels can then be licensed in increments of 4. A Voice Networking license is still required to enable TDM Q.SIG, even though there is no limit to the number of TDM Q.SIG calls that can be made or received once licensed.

Networking services

Dial-Up Circuit Support

Where the amount of traffic does not justify the cost of a dedicated leased line, the system can provide data connectivity via ISDN dial-up circuits using its E1/T1 or Basic Rate trunks. Where data speeds greater than a single channel are required (64K/56K), additional channels can be added to the call as and when they are needed.

DHCP Server

IP Office can manage your IP Network for you through its integral DHCP Server. IP Office can be configured to hold a pool of IP addresses for users on the Local Area Network. When a user powers up their PC, the system will allocate them an IP address for the duration of their session. The DHCP server also provides the user's PC with the address of the Domain Name Service (DNS) server and the Windows Name Service (WINS) server. Alternatively, for customers who have a separate DHCP Server, IP Office can be configured to obtain its address from that DHCP server or be set with its own static IP address. IP500 V2 has two independent DHCP servers, each one dedicated to Layer 3 switched LANs.

Domain Name Service (DNS) Proxy

Domain Name Service servers provide the translation of names such as www.avaya.com to the domain's IP address required to establish a connection. IP Office provides this service to PCs on the network by proxy.

LAN/WAN Services

The IP500 V2 supports a firewalled 2 port Layer 3 Ethernet Switch.

When computers on the LAN communicate they do not care where the destination is, they just send messages with the address of the destination. These messages are likely to be received at all other computers on the same network but only one - the target destination - will act on the message. Where the destination is on another network, the router is needed to be the "gateway" to the rest of the world and find the optimum route to send the message on to the destination. The router alleviates the need to establish and hold a call for the duration of a communication session (when messages or IP packets are being sent between source and destination) by automatically establishing a connection only when data is to be passed. Routers may be connected together using WAN (Wide Area Network) links that could be point-to-point leased lines, managed IP networks, Frame Relay networks or exchange lines (Central Office). The IP Office system supports all of these types of network connections.

IP Office has an integral router with support for bandwidth on demand that allows the negotiation of extra bandwidth dynamically over time. Where connection is over ISDN, IP Office initiates extra data connections between sites only when there is data to be sent or sufficient data to warrant additional channels. It then drops the extra channels when they are no longer needed. The calls are made automatically, without the users being aware of when calls begin or end. The rules for making calls, how long to keep calls up etc, are configurable within IP Office.

It is possible to have several different routing destinations or paths active at any time linking the office to other offices and the Internet simultaneously.

LAN to LAN Routing

All businesses now have a need for data routing whether it's a requirement to share resources such as email servers, file servers and internet gateways, or seamlessly transport data between sites or network to and from their customers and suppliers. This is why each IP Office platform offers IP routing as standard.

Embedding a router within IP Office removes the costs, complexity and additional points of failure of external WAN multiplexers by allowing data and voice traffic to converge and share the network resources of IP Office. These network resources can range from dial up ISDN connections, point-to-point leased circuits, managed IP networks or Frame Relay as IP Office supports all these types of network connections.

Integral 10/100 Mbit Layer 3 Ethernet Switch

Layer 3 switching is particularly useful in situations where it is desirable to have a 'trusted' and 'unsecured' network, where the 'unsecured' network is uncontrolled and carries public traffic on it.

It is possible to set up a firewall between two LAN segments using the IP Office layer 3 switch. IP500 V2 supports a two-port Layer 3 Ethernet switch with the firewall between them. Both of these switched ports have their own IP addresses (LAN1 and LAN2) and in order for traffic to pass from one port to the other, a route is configured in the system's routing tables.

Leased Line Support

IP Office is capable of connecting to leased line services.

IP Office WAN services are supported over E1/T1 PRI trunks and BRI trunks. E1/T1 trunks can be configured to operate in a fractional mode for 'point to multi-point' applications i.e. a single 2M interface could be treated as 3 x 512K and 8 x 64K going to 11 different locations. When using T1 as a Leased Line it is possible to use the same circuit for switched circuit services. Not all types of leased line are available in all territories, check for availability.

Remote Access Server

IP Office provides Remote Access Server (RAS) functionality allowing external users to dial in to the local area network from modems, phone adaptors and routers.

Several of the previously described features and services can be applied to the dial-in users to create RAS capabilities. Dial-in users can be authenticated using either PAP or CHAP. Once authenticated the DHCP server can automatically assign the user an IP address to use while connected to the LAN. Individual time profiles and firewalls can be applied to the user restricting what they have access to and when they have access. For further security and accounting ease, IP Office can automatically call a user back. This keeps the cost of the phone call on the company phone bill removing the need to process individual expense claims.

SSL/VPN Remote Access

SSL/VPN remote access provides Avaya and Avaya partners with reliable remote access that enhances service delivery while reducing the cost associated with truck rolls. The solution enables partners of any size to create an infrastructure that automates management and maintenance of IP Office systems.

IP Office software includes an embedded SSL/VPN client. On the server side (should the partner decide to host the server side), the partner will need to install a server (VM) and install the Avaya VPN Gateway (AVG) software. The Partner will establish the SSL/VPN Gateway configuration on the IP Office so that the IP Office can trigger a secure tunnel back to the Gateway.

A username/password is setup during the configuration step for security purposes. A second level of security is also provided with a server-side certificate authentication. A radius server will then validate the username/password upon connection request initiated from the IP Office. Once the credentials are validated, the secure remote access is established.

At a minimum, the partner needs to ensure that a broadband connection is available at the customer site. A partner deciding to host the server side can purchase (scale as you go) the SSL/VPN licenses based on how many simultaneous connections are required. The AVG software is installed on a VM server software (the partner can choose the server of their choice) and set up a radius server for username/password authentication. The same VM server can also act as a radius server or the partner can use a separate radius server or reuse an existing radius server based on their IT department's recommendations and security policy.

Partners wanting to host the server side gateway should refer to the Avaya enterprise portal for more detailed information about the Avaya VPN gateway solution (see https://enterpriseportal.avaya.com/ptlWeb/gs/products/P0623/AllCollateral).

SSL/VPN remote access provides the following functionality:

- Secure remote access at broadband speeds for enhanced support
- Simple configuration and deployment
- Scaling to accommodate future growth requirements
- Networking expertise not required at the customer site (No IT admin required at the customer site)
- No requirement to open holes in the firewall (Firewall-agnostic as the connection is initiated from the customers' site to the Gateway)
- Connection can be “Always-ON” or can be initiated via Dial-Up or Phone.
- Facilitation of remote configuration, management, monitoring, diagnostics, and upgrades.

Phone features

Alerting/ring tone for covered calls

Users can choose how the covered call will alert and set the alert noise to low in open floor plan offices.

Users can set the alert signal (ring tone) for incoming calls for covered phones to the following values:

- Ring (default)
- Abbreviated ring
- No ring

Buttons, keys and lamps

IP Office supports up to 10 buttons on each phone and 10 phones with the same line appearance.

The key and lamp features require a phone with buttons and indicators and on certain Avaya digital and IP phones. Key and lamp operation is not supported on analog phones. You can set a ring delay on each appearance button to allow time for the target number to answer before another extension rings, or set a visual alert only — without a ring.

Programmable buttons

Digital and IP phones have dedicated function buttons for mute, volume, hold, conference and transfer. On many digital and IP phones administrator users can program keys and buttons with a range of selected special functions.

These buttons are used for calling other extensions on the system or for other options such as speed dialing numbers and do not disturb. Many features use an indicator to show whether a feature is enabled. Implementation engineers can program buttons as part of the system configuration, although some phones allow users to program buttons and functions where given administration rights.

For more information see *Avaya IP Office™ Platform Short Code and Button Action Reference*.

Appearance buttons

Many Avaya digital and IP phones have programmable buttons. These buttons can be assigned to appearance functions that allow the handling of calls.

Use the programmable buttons available on Avaya digital and IP phones to represent individual calls. Answer, originate and join calls by pressing the appropriate appearance buttons. The appearance buttons on the phone indicate calls connected and calls waiting. This allows the user to handle multiple calls from a single phone.

Line appearance buttons

Line appearance indicate users making and answering calls on a specific external trunk.

Line appearance buttons show the use of a trunk line on the system and tracks the activity on the line. Only external calls can be answered or made on line appearances. Line appearances can be used with Analog, E1 PRI, T1 PRI and BRI trunks PSTN trunks. They cannot be used with E1R2, Q.SIG and IP trunks.

Call appearance buttons

Call appearance buttons allow a user to make, answer and switch between multiple calls by pressing the appropriate call appearance button for each call.

On digital and IP phones that have programmable buttons, you can be set them as call appearance buttons using IP Office Manager. The number of call appearance buttons set for a user determines the number of simultaneous calls they can make and answer. When call appearance buttons are used, a minimum of three call appearance buttons is recommended where possible, although some phones are restricted to two call appearance buttons by the number or design of their programmable buttons. Where possible, the status of the calls (ringing, connected or held) is indicated by the button indicator.

Note:

Note that the use of call appearance buttons overrides call waiting features. It is only when all call appearances are in use that subsequent callers receive either busy tone, voicemail or follow a forward on busy action.

Bridged appearance buttons

Bridged appearance buttons allow the user to have an appearance button that matches another user's call appearance button.

A bridged appearance button allows a user to answer and make calls on behalf of another user. An audible indication of calls is presented to the bridged user where programmed. The button provides a visual indication of when the other user has calls presented, held or connected. A user can join and exchange calls using the paired call appearance and bridged appearance buttons.

For example, when one user’s call appearance button shows a ringing call, the bridged appearance button on another user’s phone also shows the ringing call and that user can use it to answer the call. Similarly, if a user uses the bridged appearance button to make a call, the call activity shows on the matching call appearance button. The user can join or takeover the call using their call appearance button.

Bridged appearance buttons allow paired “manager/secretary” style operation between two users, and are only supported for users who have call appearance buttons.

Call coverage buttons

Call coverage buttons allow unanswered calls to alert at other user extensions and be answered there before being forwarded or going to voicemail.

Call coverage buttons allow users to answer a colleague's unanswered call before it goes to voicemail. When a user has an unanswered call ringing, after a configurable delay, the call will also start alerting on any call coverage buttons associated with the user on other extensions. Another user can answer the call by pressing the call coverage button. If the call goes unanswered, the call is forwarded or goes to voicemail.

You can adjust the time a call rings before alerting on associated call coverage buttons.

Busy lamp field indicators

Busy lamp field (BLF) indicators show when a button or associated feature is active.

Digital and IP phones have programmable buttons which can be assigned to various features. When those buttons include some form of BLF indicator, the button can also be used to indicate when the feature is active. For example, a button associated with another user will indicate when that user is active on a call. A button associated with a group will indicate when the group has calls waiting to be answered.

The directory entries in and the speed dial icons within the Phone Manager and SoftConsole applications also act as BLFs. When the icons are associated with internal users, the icons will change to indicate the current status of the users.

Avaya one-X® Portal for IP Office shows these conditions:

Text or icon	State	Description
`available`	Available	You are available and can be called.

Table continues…

Text or icon	State	Description
	Busy	You have a call in progress.
	Do not disturb	You have enabled do not disturb on the phone system. Calls to you are redirected to voicemail if available. Otherwise, the callers receive a busy tone. The exception is calls from numbers that you have added to your list of do not disturb exceptions.
	Logged out	You have not logged into the extension on the phone system. Calls to you are redirected to voicemail if available. Otherwise, the callers receive a busy tone. You cannot make calls. However you can still use to alter your configuration settings.
	Ringing	The phone is ringing and you have an incoming call.
`unknown`	Unknown	Your presence on the phone system is unknown. The presence cannot be determined as the phone number is not an extension on the system.

External call lamps

Users can determine if covered calls are internal or external based on the indicator flash pattern.

Users can select the lamp flash pattern for external calls on bridged and call coverage appearance buttons.

Message waiting lamps

IP Office uses message waiting indication (MWI) to set a lamp or other indication on phones when a new message has been left for the user, either in a personal voice mailbox or in a group mailbox or call back message. After the system plays the message, it turns the lamp off.

All digital and IP phones have in-built message waiting lamps. Avaya one-X® Portal for IP Office provides message waiting indication on screen.

For analog phones, IP Office provides a variety of analog message waiting indication (MWI) methods:

- 51 V stepped
- 81 V
- 101 V
- Line reversal

The system administrator or installer selects the MWI method using IP Office Manager during configuration to match the properties of the analog phones.

Note:

101V signaling is only available on IP500 phone cards and expansion modules.

Call history

IP Office keeps a record of calls made and received, including unanswered calls. Details are store for both users (maximum 30 entries) and hunt groups (maximum 10 entries). The method of operation varies according to the phone type but in all cases the call records can be used for return calls.

Call history can display data for all calls, missed calls, inbound calls and outbound calls. Entries in the call history can be used for return calls, sorted and added to the local directory or speed dials. Call log data is retained even after power down and a system reset. A centralized call log is supported in the SCN when using hotdesking maintaining consistency between desktop phones and user productivity applications. Call log entries can be added to the personal directory.

Caller ID

If the service provider supplies a caller ID, IP Office can pass it to the answering phone or application and is includes it in any call log or history supported by the phone or application. If the caller ID matches a number in the directory, IP Office displays the matching directory name.

If IP Office Phone Manager or TAPI service links to a database, IP Office performs an automatic query on the supplied Caller ID and displays the caller's record to the user before the call is answered.

For outgoing calls, IP Office can insert a system wide caller ID or set a flag to have caller ID withheld. For users with a direct dial number routed to their extension, IP Office uses that number as their caller ID for outgoing calls. Alternatively, IP Office can use short codes to specify the caller ID that should be sent with outgoing calls.

Note:

Sending and receiving the caller ID is subject to the service provider supporting that service. The service provider may also restrict which numbers can be used for outgoing caller ID.

Centralized Personal Directory

The Personal Directory is a list of up to 100 numbers and associated names stored centrally in the system for a specific user. A directory entry can be used to label an incoming call on a caller display telephone or on a PC application. The directory also gives a system wide list of frequently used numbers for speed dialing.

For example “Mr. Smith” can be displayed when a known Caller ID is received. A user can also select **Mr. Smith** in the Directory List in Phone Manager, or on a display phone to speed dial this number. All entries may be added, deleted or modified by Manager, , a telephone, or an external service. The personal directory data is sent/updated whenever the user is logged in a SCN.

Language

Avaya digital and IP phone menus and displays are available in many languages and usually the system default setting will be applicable to all phones, however it is possible to have language set on an extension by extension basis, this will also change the language of menus for IP Office Voicemail.

On Hook Dialing

Avaya digital and IP telephones allow the user to make calls by just dialing the number on the keypad, without having to lift the handset or pressing a speaker button. Usually the call progress can be monitored using the speaker in the phone On phones that support hands free usage, the conversation can be had without having to lift the handset.

Self-Administration

The IP Office administrator may give select users the ability to change some of the phone settings themselves. The range of changes that the user can make depends on the phone.

Visual voice

Users can access and control voice messages through the digital or IP phone display. Visual Voice works on Preferred or Essential Edition, and can only be used with large display LCD sets only from the 1400, 1600, 2400, 5400, 4600, 5600, 9500, 9600 and T3 Series. (1403, 1603, 1603SW, 2402, 5402, 4601, 4602SW, 5601, 5602SW do not support Visual Voice).

On phones that have a display but do not support visual voice, mailbox access using voice prompts and direct to voicemail transfer during a call is supported (does not include T3 and T3 IP phones).

Visual voice allows users to perform the following tasks:

- Access new, old and saved messages for personal and hunt group mailboxes
- Next and previous message
- Fast forward and rewind
- Pause message
- Save, delete and copy a message to other users of the system
- Change default greeting
- Change password
- Change email settings (Preferred Edition only)

Chapter 4: Applications

User applications

Avaya one-X® Mobile

Avaya one-X® Mobile is an application that mobile users use to connect to IP Office.

Avaya one-X® Mobile works in call-back telephony mode. For example, when a user initiates a call from the client, IP Office initiates a call to the caller's mobile device and then dials the destination. This mode offers cost savings to users in countries where incoming voice calls are free or for users who have a cheaper unlimited voice plan as compared with a data plan.

The one-X Mobile Preferred mobility client also works in Voice over IP (VoIP) mode. In the VoIP mode, the client makes calls over Wi-Fi/3G/4G data networks. The client, using its underlying SIP stack, registers with IP Office over the data network and functions as an office extension.

Users in countries where incoming calls are charged will see a significant cost savings in the VoIP mode especially when on Wi-Fi networks. The availability of both call-back and VoIP modes on the mobility client will enable users to toggle between the modes based on their network connections. This will empower end-users to make a choice of the appropriate mode based on their voice and data plan as well as the availability and quality of their data connection (WiFi/3G/4G). For example,

- The user can choose the call-back mode when he or she doesn't have Wi-Fi access and the 3G data connection is not providing good quality for voice.
- The user can choose the VoIP mode when he or she has access to a mobile hotspot where a Wi-Fi data connection is available or when the 3G or 4G data connection is good.

One one-X Mobile Preferred mobility client supports VoIP mode on both iOS and Android devices. VoIP mode is available with the Power User profile. Users with Mobile Worker profiles can only use call-back mode. VoIP mode does not require an IP endpoint license. The following features are available:

- Ring-tone selection
- High bandwidth or narrowband codec selection based on the network connection available
- Bluetooth headset audio control on VoIP calls
- Conference screen
- Contact phone number selection
- Voicemail priority indicator

- Swipe support for instant messaging on home screen
- Group action support
- Emoticons
- CLID lookup in contacts for calls
- Send voicemail as WAV in email
- Enable or disable mobile twinning (simultaneous ring)
- Enable or disable DND (send all calls)
- Call log combined with voicemails in the event history
- Call monitoring to see and interact with all calls
- VoIP mode dial plan
- Transfer calls as a third-party call controller (3PCC)

Avaya one-X® Portal for IP Office

Avaya one-X® Portal for IP Office provides users control of their telephone from a networked PC. Use this application with any extension; analog, digital or any IP telephone, wired or wireless, that is available as part of the Office Worker, Power User or Teleworker user licenses.

Avaya one-X® Portal for IP Office is a server-based application that the user accesses via web browser.

For Telecommuter mode, One-X applications require answer supervision and disconnect detection for proper functioning. As a result, the one-X applications will not work with trunks that do not support answer supervision and disconnect detection.

Note:

one-X applications function on trunk types such as PRI, BRI, and SIP, however, they will not function on E1R2, T1 RBS and analog loop start trunks.

System administrators can control if Avaya one-X® Portal for IP Office can be accessed over a secure protocol only, recommended for hosted deployments to provide "secure only" access. The other option is to allow users to access the client over a secure and unsecure protocol (HTTP/HTTPS). The client application forces users to change their passwords and voicemail passcodes to meet the complexity settings configured by the administrator.

Through gadgets, Avaya one-X® Portal for IP Office provides the following features:

- Call information
- Call and conference control
- Presence and instant messaging notifications, monitoring and archiving
- Contact import and export
- XMPP groups displayed in the **System Directory** tab

- Dial to user's own bridge and invite other users to join
- Conference call and other meeting scheduling including port reservations, email support and automatic report creation — available within the Outlook interface
- One-click web conferencing hosting and single sign-on joining web conferences as a participant

Avaya Communicator

Avaya Communicator is a collaboration software client that delivers an innovative interface for real time communications for Windows and on the iPad. It enables users to handle phone calls, instant messages, conferencing, web collaboration, presence, enterprise contacts and e-mail, all from a single interface. Avaya Communicator delivers the intuitive graphic design of spotlights, media menu, notification bar, and contact cards.

Avaya Communicator for IP Office communicates with both IP Office and Avaya one-X® Portal to provide communication and collaboration features. Telephony features such as make/receive calls, hold/unhold, mute/unmute, DTMF, MWI etc. are provided by IP500 V2 and UC features such as IM, presence, and enterprise contacts are provided by the Avaya one-X® Portal server.

If Avaya one-X® Portal server is unavailable, either due to licensing restriction or connectivity issues, the Avaya Communicator client will work in a telephony-only mode providing only telephony features. Interoperability with Avaya Session Border Controller for Enterprise allows the Flare Communicator client to be used by users with the Remote Worker profile and register with IP Office without requiring a VPN connection.

Avaya Communicator provides the following features:

- Add participants using dial-pad or drag and drop
- Mute and unmute all or a subset of participants
- Lock and unlock the conference
- Place conference in lecture mode
- Enable and disable entry and exit tones
- Drop all or some participants from the conference
- End the conference
- Enable and disable continuation to allow the conference continue after the moderator drops
- Promote participants to moderator
- Create ad-hoc conferences by merging P2P calls
- Authorization and account codes (Windows only)
- Hold timeout reminder (Windows only)
- Compact user experience
- TSL/SRTP support

- Contact filtering
- Web conferencing integration
- Unsupervised transfer
- Auto-answer
- Simultaneous mode
- Password change
- Account codes
- Auto configuration (iOS only)
- Bluetooth and headset device support and selection (iOS only)
- Interoperability with Scopia (Radvision XT5000)

Note:

Avaya Communicator does not support recording and active speaker indicator.

Related Links

Avaya Communicator for iPad on page 78
Avaya Communicator for Windows on page 79

Avaya Communicator for iPad

Avaya Communicator for iPad integrates voice, video, presence, instant messaging, directories into one unified interface over Wi-Fi or 3G cellular and VPN connections.

Avaya Communicator is a software-only solution that can be easily downloaded from the Apple iTunes Store supporting iPad2, iPad3, iPad4, iPad Mini (with and without retina display), iPad Air both Wi-Fi and 3G models and the following iOS versions: 6.1.x, 7.0.x, 7.1.x, and 8.0.x.

Note:

Avaya Communicator is not supported on iOS 6.0.x.

With Avaya Communicator, IP Office users can use iPad devices for:

- Easy access to the real-time communications tools they rely on every day (phone, presence, IM, etc.)
- Blending real-time communications and business processes, such as mobile sales
- Taking advantage of Wi-Fi and 3G connectivity for cost-saving VoIP
- Secure signaling over TLS and secure media exchange over SRTP in cloud environments
- As a web conferencing moderator, the ability to share white board and documents
- Changing passwords
- Auto-answer support
- Unsupervised transfers

- Auto configuration services using a configuration profile hosted on a web server by email address or URL
- Bluetooth and headset device support and selection
- System directory search
- Add/delete members from a team (XMPP Group)
- Search the system directory and add to a team or personal contact
- Radvision XT5000 support for point-to-point video calls

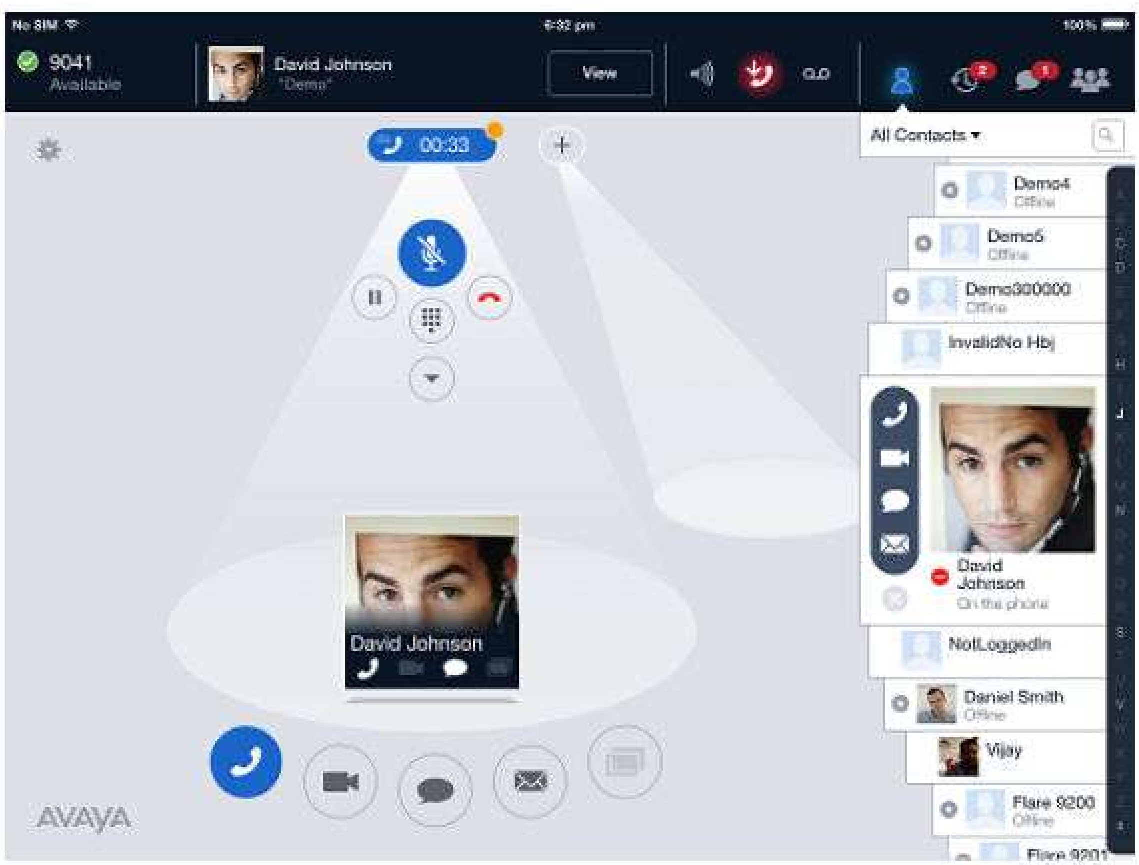


Figure 3: Avaya Communicator for iPad

Related Links

Avaya Communicator on page 77

Avaya Communicator for Windows

Avaya Communicator for Windows integrates voice, presence, instant messaging and directories into one unified offering for Windows laptops and desktops over a LAN connection.

Avaya Communicator provides the following features:

- Compact mode occupying less screen real estate

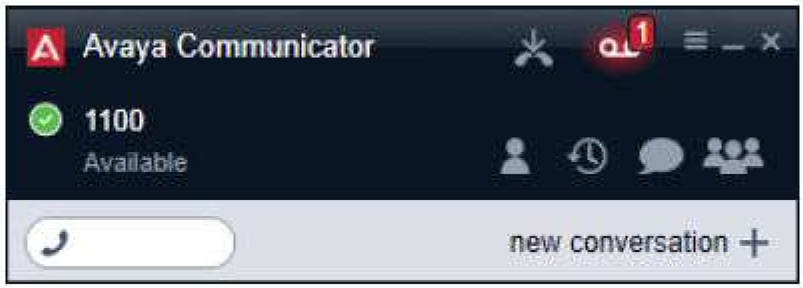


Figure 4: Avaya Communicator for Windows compact view

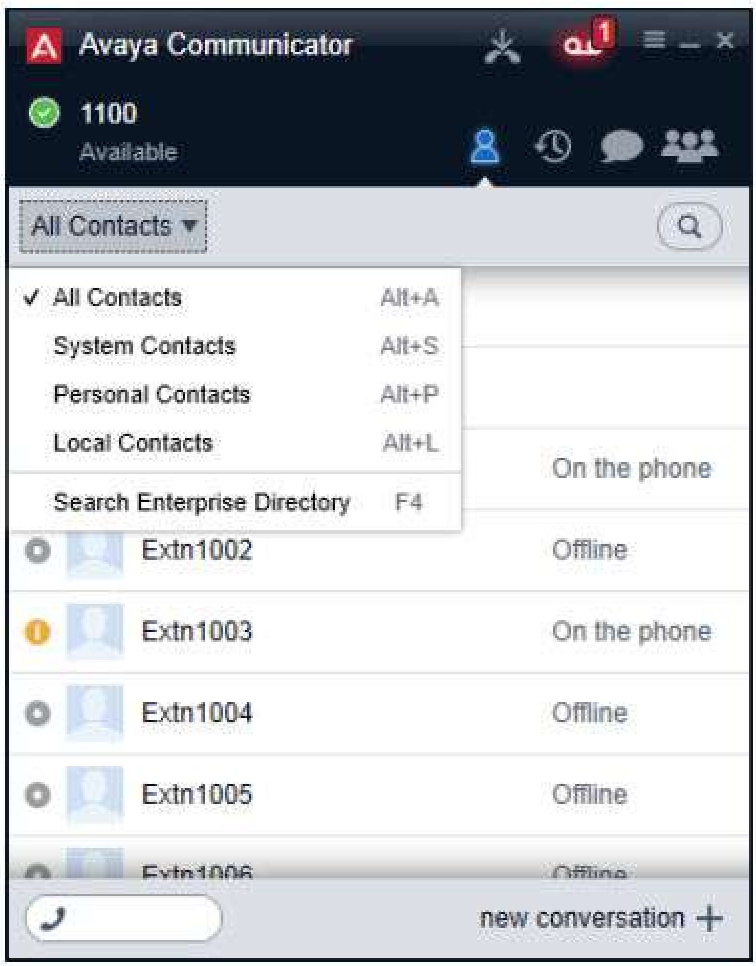


Figure 5: Avaya Communicator for Windows full view

- Secure signaling over TLS and secure media exchange over SRTP for cloud environments
- Contact filtering according to criteria and choosing to view only system, local, or personal contacts
- Web conferencing integration
- Unsupervised transfers

- Auto-answer
- Simultaneous mode for interfaces to one-X Portal, Outlook and Salesforce
- Password changing
- Account codes

Related Links

Avaya Communicator on page 77

IP Office Video Softphone

The IP Office Video Softphone is a full feature telephony client that supports standard telephony features on Mac operating systems.

An IP Office Video Softphone Mac license is required and the user must be licensed as a Power User or Teleworker.

Existing customers can use the older versions on their respective supported operating systems after upgrade, however Avaya will not distribute older versions for Mac and Windows. Existing customers who used IP Office Video Softphone Mac through purchase or Teleworker, Power User or Mobile User license (or upgrade) are entitled to use the new version of the Mac client after upgrading to the latest version of IP Office. IP Office Video Softphone works on Mac OS 10.8 or 10.9 in the following languages: English, Spanish, French and Russian.

Note:

IP Office Video Softphone for Windows is no longer supported. Existing users must use Avaya Communicator for Windows.

IP Office Video Softphone includes the following features:

- Single message window to view all messages
- Busy Lamp Field (BLF) busy beep support
- Instant messaging
- Video conference for up to six participants
- Support for the G.722 codec option
- Multiple tabs for calls, contacts and logs
  - On the **Phone** tab, users can type a number or name and then make a phone or video call
  - On the **Contacts** tab, users can type a name in the search field to find matching contacts, then right-click for possible actions (audio call, video call, instant message)
- Two operating modes: client mode and application mode
- Several audio headset options for wireless headsets and full hook-switch support

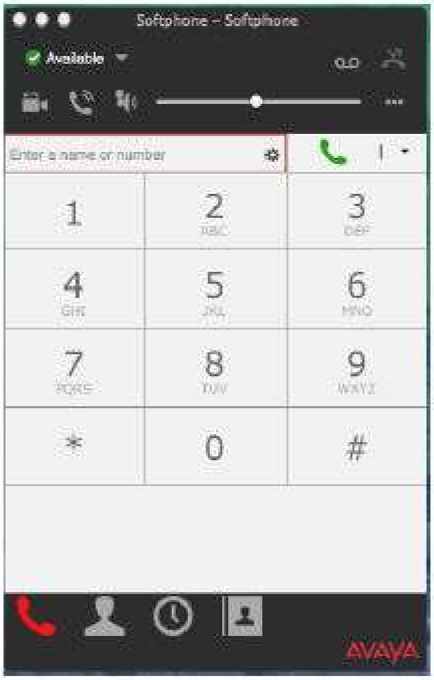


Figure 6: IP Office Video Softphone Mac keypad

SoftConsole

SoftConsole is the PC-based Windows receptionist application for IP Office. It can be purchased with the Receptionist user license.

SoftConsole provides enterprise receptionists and operators with call information and call actions to simplify call handling and instant messaging. With SoftConsole, users see the status of other users and adjust basic telephony settings of other users, such as forwarding numbers. Avaya recommends using phones that support Auto Answer. Users can use instant messaging features provided by Avaya one-X® Portal, if available.

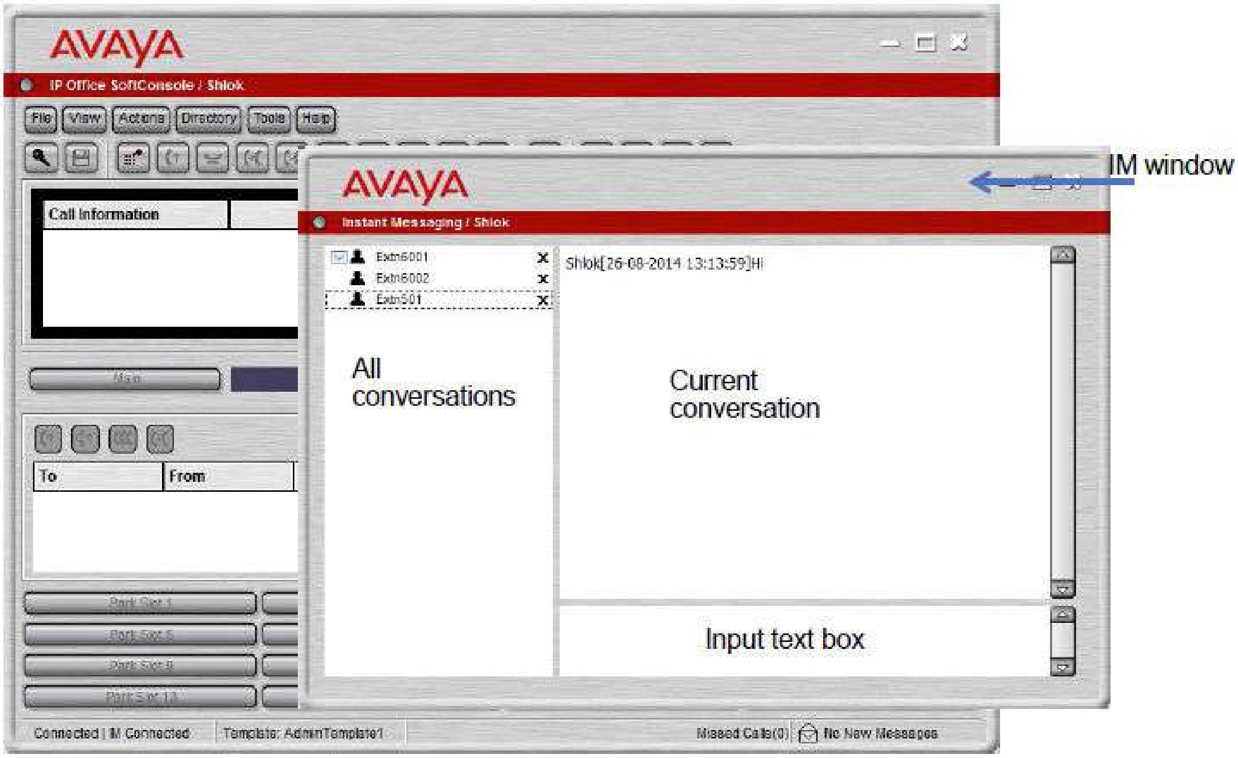


Figure 7: SoftConsole instant messaging window

WebSocket communication allows SoftConsole clients to communicate with IP Office and Avaya one-X® Portal. The WebSocket protocol is bidirectional between the client and the server. As the communication is done over port 80 or 443 (same port used for HTTP), there are no issues with firewall traversal. In a hosted environment, WebSocket communication provides security.

SoftConsole can be minimized in the Windows system tray when not in use, but will pop up on the screen when a call is received. Sound and media files can be associated with calls. If this feature is used, the PC requires a sound card and speakers.

SoftConsole supports the following features:

- Answering calls
- Making outgoing calls
- Supervised and unsupervised transfers
- Transfer calls to voicemail
- Hold and park calls
- Monitoring queues and answering queue calls
- Using and viewing conference rooms
- Conferencing held calls
- Adding users to a conference
- Adding text to a call

- Door release
- Intrude
- Sending text messages
- Paging
- Recording calls
- Sending email
- Using dial pad
- Multiple language support, users can select language

Embedded Voicemail

In environments like retail or home office, where space, noise or cost considerations rule out using a PC for voicemail, Embedded Voicemail provides basic voicemail services. Embedded Voicemail is on the IP500 V2 control unit and does not require a separate voicemail server.

Embedded Voicemail is available with IP Office Essential Edition. No additional licenses are required.

Voicemail Pro

Voicemail Pro is provided with IP Office Preferred Edition and is an advanced messaging and call flow application for IP Office systems. Voicemail Pro can handle 40 (up to 250/500 on Server Edition/ Server Edition Select) simultaneous calls depending on license and system settings. Each user has the option of turning their voicemail on or off. When on, the system automatically answers their telephone when they are not available to take a call, plays a personal greeting, and records a message.

When a message has been left, the user will see a message-waiting lamp lit on their telephone and can press a retrieval button to collect their messages.

Voicemail Pro can also ring the user to deliver any new messages. Voicemail messages are time and date stamped and the caller's number recorded. Voicemail Pro can be configured to delete read messages automatically, unless the user chooses to save the message permanently.

Voicemails can be collected remotely by dialing into the Voicemail Pro server. If the number the user is dialing from is recognized (home number or mobile/cell phone for example), the user will listen to their voicemail straight away. If the source number is not recognized, the user will be prompted for a mailbox number and a PIN code for that mailbox, before they can listen to their voicemail. Users have the ability to set and change their own PIN codes.

When a voicemail needs to be forwarded to other users, Voicemail Pro provides many options:

- Voicemails can be forwarded to another mailbox, or group of mailboxes

- Recipients can add their comments to the voicemail before forwarding to another mailbox or mailboxes.
- Voicemails can be forwarded as email WAV attachments.

All options are available in a choice of languages; both spoken voice prompts and graphical programming interfaces and have the choice of IP Office TUI and INTUITY emulation TUI.

One Active Voicemail Pro server

Server Edition supports one active Voicemail Pro server on the primary server. A non-active Voicemail Pro server is supported on the secondary server for resiliency.

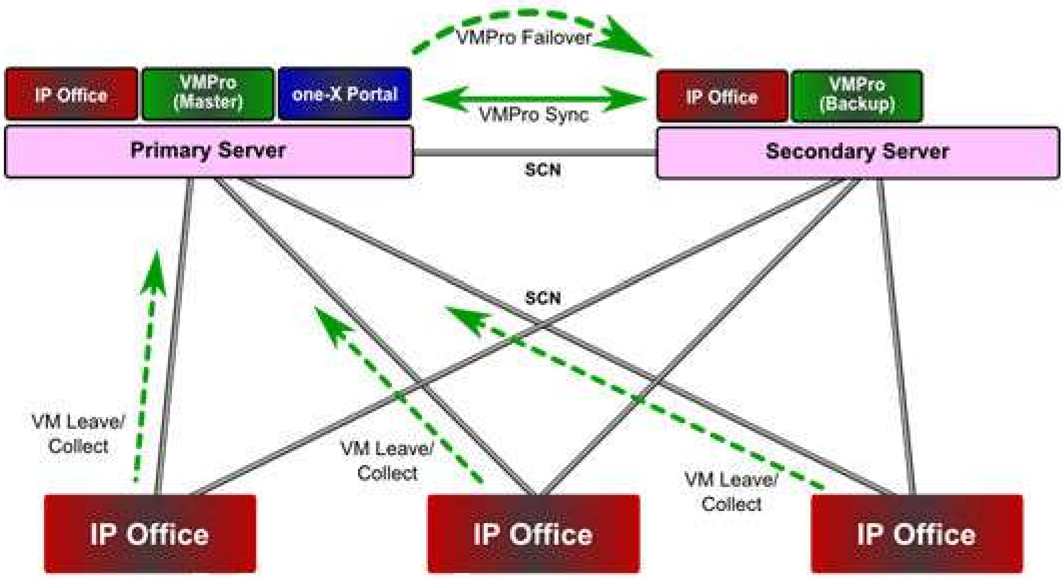


Figure 8: One active Voicemail Pro server

Dual Active Voicemail Pro servers

Server Edition Select systems support two active Voicemail Pro servers, doubling the maximum channel capacity and dual processing locations. Each expansion system and all contained users can be configured to use one or the other. Each Voicemail Pro server provides backup for the other. The two Voicemail Pro servers are both active for a configured subset of users. They share a common configuration and message store. Each can support all mailboxes, MWI and call flows under failure conditions.

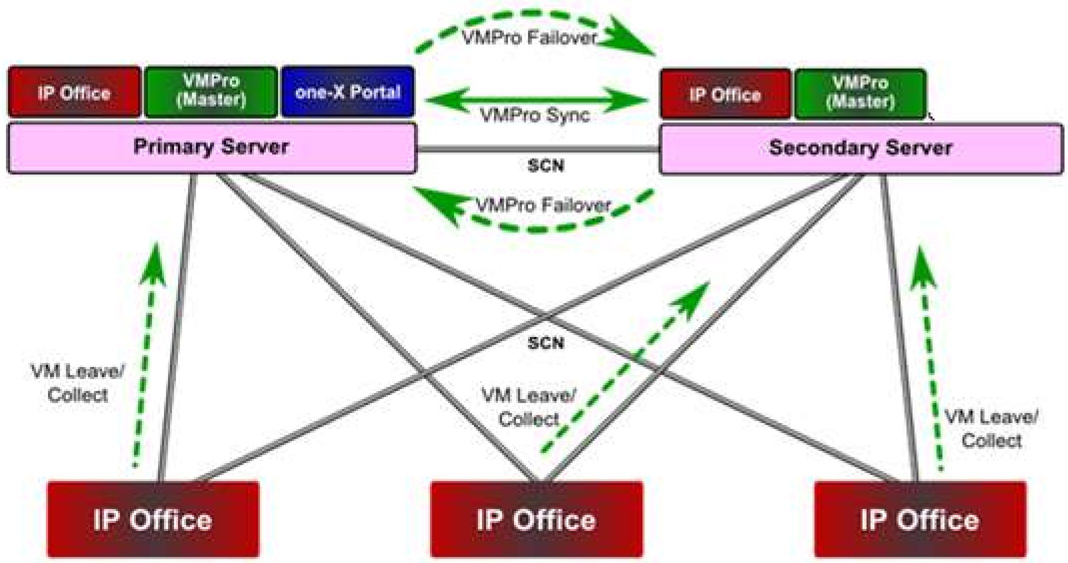


Figure 9: Dual Active Voicemail Pro servers

Conferencing

Users can place calls on hold and a create a conference using either the telephone or desktop applications. Additional conference members may be added, however a single conference may not have more than 64 members (with IP500 V2 only and more on Server Edition).

For ad-hoc conferencing, the system requires as many digital trunks/VoIP channels as external participants (as well as Preferred Edition for Meet-Me conferences). The system supports 128 conferencing channels on the IP500 V2, allowing multiple conferences of any size from 3 to 64 parties. The system support 42 3-party conferences, 2 64-party conferences or any combination in between. Meet-Me capabilities require Preferred Edition for direct dial into a conference bridge with PIN code security. In an SCN network, only one centralized Preferred Edition license is required to host Meet-Me conferences at any of the sites. Conference IDs are also shared across the SCN sites.

The following conference channel capacities are available:

Table 2: Conferencing channel capacities

Platform	Non-Select	Select	Avaya Contact Center Select	IP Office Contact Center
HP DL120 Dell R210	128	128	414	414
HP DL360	256	256	825	825
Dell R620	256	512	825	825

Table continues…

Platform	Non-Select	Select	Avaya Contact Center Select	IP Office Contact Center
OVA	256	512	825	825
IP500V2	128	128	128	128

To initiate a conference, users dial the direct number allocated to the conference bridge, type in the PIN (require Preferred Edition and Voicemail Pro) if required. For ad-hoc conferences with a few participants, users can easily set up immediate conferences by calling all parties and bringing them to the conference bridge. With Avaya one-X® Portal for IP Office, the originator of the conference can keep control: the Caller ID number (and the associated name if recognized) of each participant is displayed. If required, they can selectively hang-up a specific participant. The system plays a single beep on entry and a double beep on exit. The owner of the conference may use their extension number as the conference ID. The owner of the conference has control of the conference with the ability to mute and drop calls of participants. All participants will hear the system Music on Hold (MOH) until the owner joins, and will hear MOH when the owner drops. Note that any internal party has the option to view and drop participants (not just the conference originator).

Users can record a personalized greeting for a conference (requires Preferred Edition and Voicemail Pro).

Users can record the conference using Avaya one-X® Portal for IP Office, digital or IP display phone or a short code (requires Preferred Edition and Voicemail Pro). To prevent unauthorized access to the conference bridge, PIN codes, Caller ID number screening as well as time and date profiles can be set-up using Voicemail Pro. One user can manage the conferencing bridge facility from any location.

Conferencing has the following restrictions:

- Only two calls connecting through analog trunks are permitted in any single conference.
- Each external caller requires a digital trunk/VoIP channel (for example 1 T1 allows 23/24 external parties, 1 E1 allows 30 parties and a fully licensed VCM-64 allows 64 parties).
- There are no limits on the mix of internal and external calls in conference, but if all internal participants disconnect from the conference bridge, the external participants can be disconnected automatically by the system for added security (configurable system setting).
- System features such as call intrusion, call recording and silent monitoring all use conference resources, as does automatic recording if enabled. When any of these features are active the number of slots available for conference parties is reduced. For example, a conference call between 3 parties and being recorded will use 4 conference slots.

Related Links

Meet-Me conferencing on page 87
Video collaboration on page 88
Collaboration Agent on page 89

Meet-Me conferencing

Meet-Me conferencing enables multiple callers to talk in an audio conference. Callers can be on-site personnel as well as external parties whether field-based engineers, sales staff on the road, customers or suppliers. Conference calls can be planned in advance or established ad-hoc as and when required.

Related Links

Conferencing on page 33

Video collaboration

IP Office provides Bring Your Own Device (BYOD) and HD room system support for video collaboration.

IP Office supports video collaboration with data sharing through Avaya Scopia® desktop and mobile applications when using Radvision MCU or Video Collaboration for IP Office. Flare clients can also participate in multiparty video conferences. Avaya Scopia® connects to IP Office as a SIP endpoint using an Avaya IP license.

Avaya Video Collaboration for IP Office provides the following features:

- Direct integration including a common dial plan with IP Office
- “Virtual conference room” for up to eight participants with click-to-join capabilities form any standards-based room system, desktop or mobile device
- Freely distributed desktop and mobile video clients for PCs, Macs and most popular iOS and Android devices, enabling people inside and outside an organization to easily join a video meeting
- Low bandwidth HD multiparty video conferencing with data collabration using native SIP/H.323
- Automatic firewall transversal to engage with participants outside the network

The following diagram shows the topology of IP Office deployed with video endpoints.

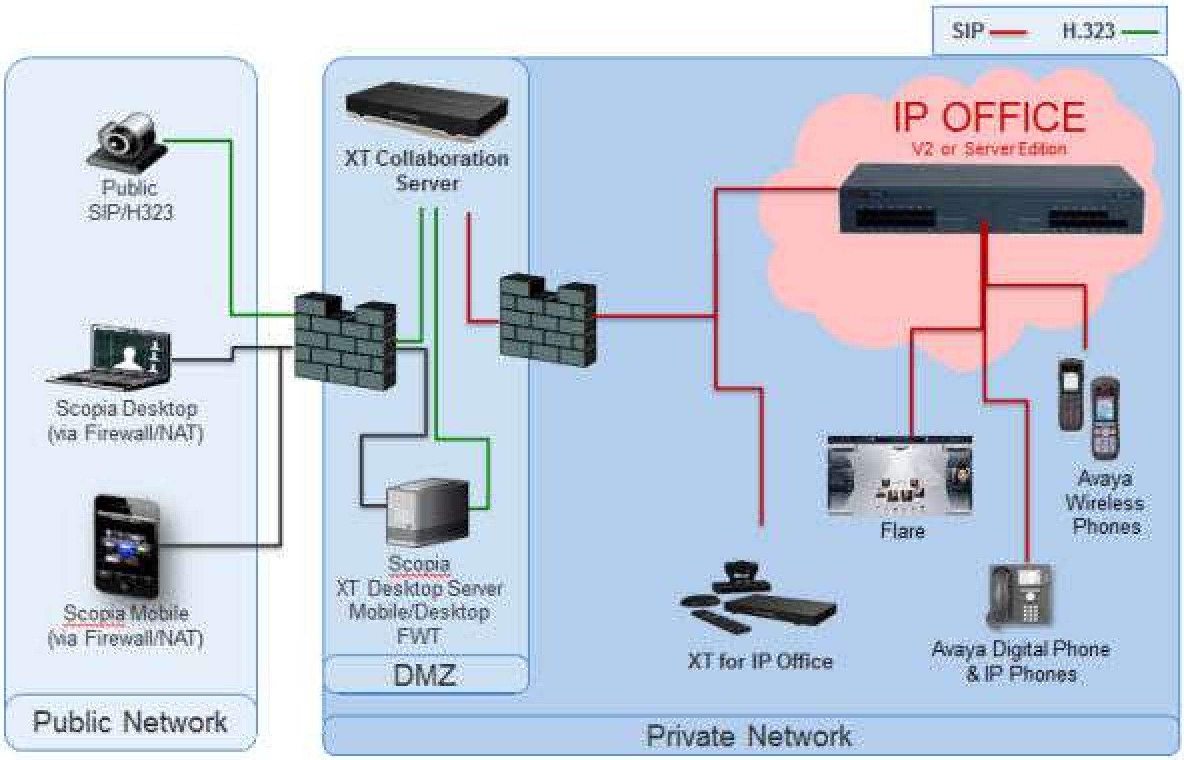


Figure 10: Video endpoints

Related Links

Conferencing on page 33

Collaboration Agent

Collaboration Agent is an application that provides web collaboration and conferencing tools. Users with Avaya Aura® Conferencing accounts and invited guests can use the tools to manage conferences and participate and collaborate in conferences.

Conference participants can join conferences by logging in to Collaboration Agent and dialing in to the audio bridge assigned to the conference. Participants can also use the integrated audio and video feature of Collaboration Agent. Participants can use the Collaboration Agent tools to boost productivity and track action items even after the conference ends. Conference moderators can:

- Record all aspects of conferences.
- Record and edit meeting minutes.
- Create and distribute meeting reports based on the meeting minutes.

Collaboration Agent features

In Collaboration Agent, the participants and moderators can perform multiple tasks such as:

- View a list of other participants.
- Virtually raise a hand and seek permission to speak.
- Send messages.

- Annotate shared content.
- Record or edit minutes.
- Set the entry and exit tones.
- Dial out to other users and the users to the conference.
- Disconnect participants.
- Promote participants to the moderator role.
- Invite more participants to join an active conference.

During the conference, participants can view the following information in Collaboration Agent:

- The participants who joined only on the audio bridge
- The participants active on web collaboration
- The participant currently speaking
- The current presenter

Related Links

Conferencing on page 33

Installation and administration applications

IP Office Manager

IP Office Manager supports complete centralized administration for Server Edition Primary, Server Edition Secondary, and Server Edition Expansion Systems. Manager also provides IP Office telephony and Unified Communications features.

Manager enables management of all the components within the solution for activities such as:

- Single point of configuration for IP Office and voicemail
- Simple initial installation wizard
- Overview of the system with inventory and status
- Common settings consolidated to the Server Edition Primary
- Integrated Voicemail Proclient, System Status Application, and Linux Platform settings access
- Supports online, offline administration, and configuring a complete solution
- Template operations
- Centralized configuration and template storage
- Administrator account management utility
- Retains existing IP Office expertise
- Context sensitive help

Even though Manager is a Windows application, Manager can be installed directly from the Web administration portal of Server Edition Primary server. This enables you to use any Windows personal computer that has any IP Office Manager that is pre-installed immediately.

Using Manager, the administrator can create templates for many management items such as users, extensions, Hunt Groups, and Lines. The administrator can then create any new item using the default settings or the template. You can create multiple users and extensions using one template.

Call Routing Support:

- Full IP Office ARS and dial plan support
- Default routing simplifies configuration
- Solution wide auto line group numbering
- Common incoming call routes provide resilience
- Resilient Hunt Groups

Offline Operation:

- Complete solution can be created and/or managed offline if required
- Can still manage when some deices offline
- On/offline configuration sync options to harmonize as required

Solution Management:

- Complete solution view with status and inventory
- Users and Hunt Groups are solution wide
- Centralized User Rights, feature short codes, Time Profiles, Incoming Call Routes, and Account Codes
- Permits advanced per-device configuration if desired
- All configurations stored on primary server
- Solution wide system directory
- Easy management of central and per-device licenses

Resilience management:

- You can manage every device locally for ‘rainy day’ events
- You can manage the solution through a secondary server when the primary server fails or in a split WAN setup
- On/Offline configuration sync options to harmonize as required

Add or Remove Devices:

- Single process for addition or removal of device
- Built-in Initial Configuration Utility (ICU) to simplify adding a new device
- Common configuration items from primary server is auto populated
- Can configure before you install a new device

Validation :

- Configuration validation on read and any change.
- Solution wide validations

Template:

- Create a local and centralized template from an existing Line, Extension, User, Hunt Group, Time Profile, Firewall Profile, IP Route and Service entries
- Recreate multiple Extension and Users from one template

Remote access:

- Supports access from service through SSL VPN

Security:

- Single Sign On to all except one-X Portal administration

Simplified Manager

Use the Simplified Manager to manage IP Office Essential Edition Quick Mode. Simplified Manager tracks system configuration changes, manages upgrades, and configuration imports and exports.

IP Office has a built-in audit trail that tracks changes to the system configuration, and who has made them. Manager can display the audit trail to assist with problem resolution. The audit trail records the last 15 changes in the configuration and records the following elements:

- Configuration Changed - For configuration changes, the log will report at a high level on all configuration categories (users, hunt group...) that have been changed.
- Configuration Erased
- Configuration merged
- Reboot - user instigated reboot
- Upgrade
- Cold Start
- Warm Start
- Write at HH:MM - This is when the administrator saved the configuration via the schedule option
- Write with Immediate Reboot
- Write with Reboot When Free

IP Office Manager is also used for maintenance functions such as:

- Upgrade to the IP Office system software
- Ability to send software over an IP network link to a system and have it validated before committing to the upgrade

- Backwards compatibility with systems from Release 2.1 onwards to allow a single management application
- Importing and Exporting IP Office configuration information in ACSII-CSV files.

Web Manager

Web Manager is a browser-based management tool designed to simplify the installation and maintenance process and provides access to most, but not all, IP Office configuration settings. Web Manager eliminates the need to have windows operating system because it can run on any device that supports standard browsers.

Solution Management Application

IP Office Manager and Web Manager use the Solution Management Application (SMA) to access the system configuration.

SMA resides on the primary or secondary server. Settings are available for remote access and Server Edition Central Access. Central Access communicates with the primary or secondary server rather than to each node individually. Avaya requires Central Access for a hosted environment and recommends it for non-hosted environments with more than 32 nodes.

SoftConsole Administrator mode

System administrators can start SoftConsole in administrator mode. When run in this mode, there is no access to the telephony functions.

SoftConsole administrator mode enables users to configure the following functions:

- Create and edit user profiles
- Amend the length of call notes
- Create and edit templates
- Remove or display the interface panels

SNMP Management Console

Simple Network Management Protocol (SNMP) is an industry standard designed to allow the management of data equipment from different vendors using a single Network Manager application. The Network Manager periodically polls equipment to solicit a response, if no response is received an alarm is raised. In addition to responding to polls, IP Office monitors the state of its Extensions, Trunk cards, Expansion Modules and Media cards so that if an error is detected IP Office will notify the Network Manager.

As the IP Office platform comprises many applications, the core software notifies SNMP events from both Voicemail Pro and Embedded Voicemail to warn of approaching storage capacity limits.

IP Office sends email notifications directly to the email server; no additional PC client is needed.

On customer sites where SNMP management is not available, IP Office can email events using up to 3 email addresses each containing a different set of alarms.

The following system event categories can be chosen for email notification, if installed on the system:

- Generic
- Trunk lines
- Embedded Voicemail Card
- VCM
- Expansion modules
- Applications
- License
- Phone change
- CSU Loop-Back

IP Office has been tested against CastleRock's SNMPc-EE™ and HP's Network Node Manager (part of the OpenView application suite).

System Status Application (SSA)

The System Status Application (SSA) is a diagnostic tool for system managers and administrators to monitor and check the status of IP Office systems locally or remotely. SSA shows both the current state of an IP Office system and details of any problems that have occurred. The information reported is a combination of real-time events, historical events, status and configuration data to assist fault finding and diagnosis. SSA provides real-time status, historic utilization and alarm information for ports, modules and expansion cards on the system. SSA connects to all variants of IP Office using an IP connection that can be remote or local. Modem connections at 14.4kbps or above are supported for remote diagnostics.

SSA provides information on the following:

Alarms	SSA displays all alarms which are recorded within IP Office for each device in error. The number, date and time of the occurrence is recorded. The last 50 alarms are stored within IP Office to avoid need for local PC.
Call Details	Information on incoming and outgoing calls, including call length, call ID and routing information.

Extensions	SSA details all extensions (including device type and port location) on the IP Office system. Information on the current status of a device is also displayed.
Trunks	IP Office trunks and connections (VoIP, analog and digital) and their current status are displayed. For VoIP trunks, QoS information is also displayed (e.g. round trip delay, jitter and packet loss).
System Resources	IP Office includes central resources that are utilized to perform various functions. Diagnosing these resources is often critical to the successful operation of the system. This includes details on resources for VCM, Voicemail and conferencing.
QoS Monitoring	QoS Parameters from connected calls, such as jitter and roundtrip delay, are monitored.

SSA can be launched independently or from IP Office Manager and there can be up to two (2) SSA clients connected to an IP Office unit at one time.

Note: SSA is not a configuration tool for IP Office systems.

SysMonitor

Use SysMonitor to troubleshoot IP Office from both local (LAN) and remote locations (WAN).

Select the protocols and interfaces to monitor and diagnose through a graphical interface. Capture traces directly to the screen or as a log file for later analysis. Color code different traces to improve the clarity in large files. The utility also captures system alarms and displays the activity log of the last 20 alarms that have occurred.

Data Migration Manager (DMM)

The Data Migration Manager (DMM) facilitates migration from BCM and Norstar systems to IP Office. There are three steps in the migration process: extract, convert and apply.

DMM migrates:

- Announcements and greetings
- Voicemail messages
- Extract Call Pilot configuration

IP Office Branch applications

Centralized management

With the distributed, mixed, and centralized deployment models, you can use Avaya Aura® System Manager to centrally manage all components in the solution. System Manager manages the centralized applications and services included in the solution, IP Office systems in the branch, as well as centralized users and IP Office users. For certain capabilities that cannot be managed centrally, System Manager launches IP Office Manager in the appropriate mode where you can remotely administer individual IP Office systems.

Centralized management of components through Avaya Aura® System Manager is optional. For example, you can choose to directly manage IP Office systems through IP Office Manager.

With the stand-alone IP Office branch option, centralized management is not available. You must manage all IP Office systems directly though IP Office Manager.

Centralized licensing

With a distributed, mixed, or centralized deployment connected to the Avaya Aura® network, you can access centralized licensing capabilities through the System Manager Avaya WebLM server. With centralized licensing, a single license file is generated in the Product Licensing and Delivery System (PLDS) for multiple branches.

To use centralized licensing, the enterprise must obtain a WebLM licence from PLDS for each IP Office branch. Centralized licensing is not available in stand-alone IP Office branch environments.

Voice mail systems

The IP Office Branch solution supports IP Office voice mail systems and centralized voice mail systems.

The IP Office Embedded Voicemail system is included with the IP Office Essential Edition, and the IP Office Voicemail Pro system is included with the IP Office Preferred and Advanced Editions.

The Branch solution supports the following three centralized voice mail systems as additional components within the solution:

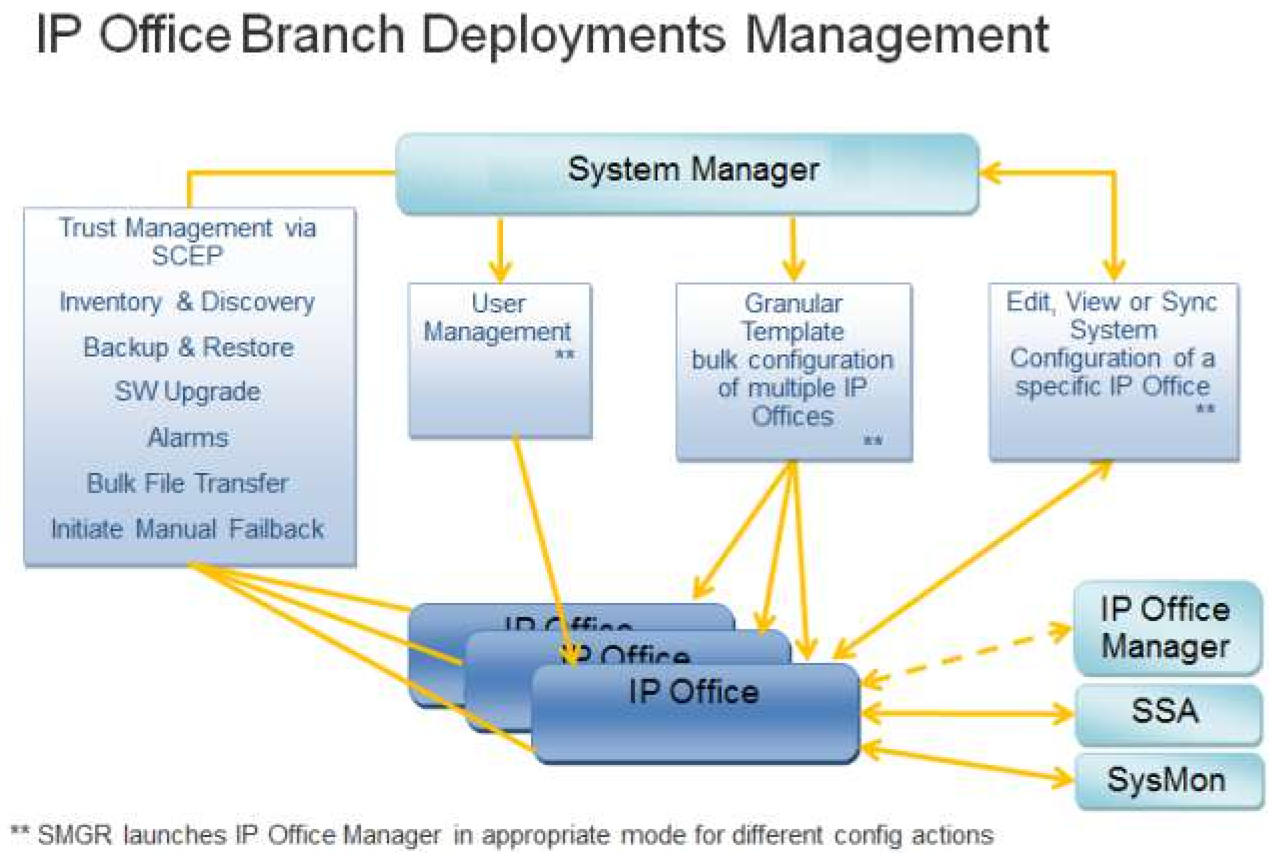
- Avaya Aura® Messaging
- Avaya Modular Messaging
- Avaya CallPilot®: Only supported in distributed branch environments connected to CS 1000.

Avaya Aura® System Manager

Avaya Aura® System Manager allows administrators in Distributed. Mixed, and Centralized deployment environments connected to Avaya Aura® to centrally manage all users and IP Office systems in the enterprise branch. In a Distributed branch environment connected to CS 1000, you can also configure Avaya Aura® System Manager to centrally manage CS 1000.

System Manager provides the following Centralized administration and management functionality:

- Upgrade IP Office systems.
- Add IP Office devices from the network to System Manager.
- Create IP Office endpoint templates that are used to create IP Office users and Centralized users. These templates can be edited, duplicated, or deleted.
- Create IP Office system configuration templates that can be applied to selected IP Office systems. These templates are used for initial device provisioning. These templates can be edited, duplicated, or deleted.
- Upload and convert audio files to System Manager to be used in the IP Office System Configuration Auto Attendant feature.
- Manage IP Office system configurations. From System Manager, you are able to launch IP Office Manager to view or edit a system configuration. With this feature, you make changes directly to the IP Office device. You are able to apply the changes immediately or schedule the changes to run at a specified time.
- Manage IP Office security configuration. From System Manager, you are able to launch IP Office Manager to view or edit a system security configuration. With this feature, you make changes directly to the IP Office device.
- Create user templates. These templates can be edited or deleted. Templates can be created for Centralized users or IP Office users.
- Perform an IP Office backup with the option of storing the backup output in System Manager or creating a local backup where the system stores the backup output on the local storage attached to the IP Office device.
- Perform an IP Office restore. This feature allows you to restore:
    - a saved IP Office system configuration onto an IP Office from System Manager.
    - a backup of an IP Office system configuration onto an IP Office from the device SD card.
    - users from System Manager to the IP Office.
    - a saved IP Office system configuration and user from System Manager onto an IP Office.
- View events and alarms regarding various operations that occur on the IP Office.



Avaya Aura® Session Manager

Avaya Aura® Session Manager handles call admission control, call re-direction, digit analysis, dial plan management, internal network call accounting feeds, toll by-pass, inter-office routing and international least cost routing. All administration and management of the enterprise-wide private global dial plan network is handled by this communications appliance, and managed as a single enterprise with Avaya Aura® System Manager.

Session Manager plays a different role for centralized users and IP Office users in deployment environments connected to Avaya Aura®. For IP Office users, Avaya Aura® Session Manager acts as a SIP proxy to route SIP sessions to and from the SIP connections to the IP Office. For centralized users, Avaya Aura® Session Manager is also the main interface that handles user registration and call routing.

Avaya Aura® Communication Manager

Centralized users register to Avaya Aura® Session Manager and obtain telephony services from the Avaya Aura® Communication Manager Feature Server or Evolution Server in the enterprise core. Avaya Aura® Communication Manager does not provide any functionality to IP Office users.

Contact Center applications

Avaya IP Office Contact Center overview

Avaya is the market leader in call center technology, and IP Office Contact Center can take your business to a new level. Avaya IP Office Contact Center provides integrated contact center capabilities specifically designed for businesses supporting between 5 and 250 contact center agents and supervisors.

IP Office Contact Center provides the following features and characteristics:

- All-in-one customer service solution that delivers consistent service to customers across multiple media channels and locations. IP Office Contact Center includes a user interface (UI) on Microsoft Windows and a Chrome UI. The Chrome UI is supported on Chrome devices.

  Note:

  The functionality available on the Customer Engagement OnAvaya (IP Office Contact Center) User Interface for Chrome and the IP Office Contact Center User Interface for Windows varies.
- Access to Agent UI functionality, including call control, from a SalesForce (SFDC) plug-in or SAP CRM connector.
- Fast implementation with minimum disruption to the business. IP Office Contact Center also includes an automatic synchronization feature for configuration. This feature can be enabled and disabled as needed during implementation.
- Flexible, common administration and management.
- Inbound and outbound voice calls with telephony and dialer capabilities.
- Email and chat capabilities in the Windows UI.
- Skills-based routing.
- Address book access so agents can quickly find the contact information they need to make calls and send emails.
- Real time and historical reporting for all media channels.
- Interactive Voice Response (IVR) and Task Flow Editor scripts.

- User profile and agent group privilege configuration to determine which features are available to users of the interface. Administrators must assign privileges and create agent groups. The IP Office Contact Center interface supports the following user types:
  - Agents: Make and receive telephone calls. If configured, agents can also communicate using email and instant messaging chats.
  - Supervisors: Monitor the activities agents perform on the IP Office Contact Center interface. Supervisors can also create, view, and edit reports, real-time information in the interface, and call statistics.
  - Administrators: Perform system administration, such as configuring email and chat services. Administrators can also create and edit topics, objects, call flows, and scripts.
- Access to a web-based administration portal that allows you to perform initial configuration, upload certificates, collect logs, and download IP Office Contact Center User Interface for Windows. Additional administration tasks must be performed on IP Office Contact Center User Interface for Windows.
- Optional integration with Avaya Contact Recorder. Calls are recorded with Voicemail Pro and the details of the complete recording are stored in the Avaya Contact Recorder database. You can search for and manage recordings using a web browser.
- Access to a wallboard that displays IP Office Contact Center statistics.

Avaya Contact Center Select overview

Avaya Contact Center Select is a context-sensitive, collaborative, voice and multimedia customer experience solution that allows small to midsize enterprises to anticipate, accelerate, and enhance customer interactions. Avaya Contact Center Select uses the telephone system to provide a real-time telephony platform. is a flexible and scalable phone system designed specifically for small and midsize enterprises. supports a wide range of phones and devices for use in contact centers.

Agent Desktop is a single-interface client application used to interact with customers. You can respond to customer contacts through a variety of media, including phone, outbound contacts, email, Web communication, fax, scanned documents, and Short Message Service (SMS) text messages. Agent Desktop provides automation for customer responses to eliminate repetitive actions, such as typing a common response in an email message. Agent Desktop supports specified phones and continues to support multimedia contact types.

Agent Desktop, in an Avaya Contact Center Select solution, supports the following routed contact types:

- Voice contacts
- Email messages
- Web communications contacts
- SMS text messages
- Fax messages
- Scanned documents

- Voice mail messages

Your administrator determines which contact types you can handle. Avaya Contact Center Select also supports peer-to-peer Instant Messaging. To support the email-based contact types, you must add an email server to your solution. To support the Web communications contact type, you must add a Web communications server to your solution.

Agent Desktop uses Microsoft .NET Framework Click Once Deployment technology, which means that you can install and start the application by entering a URL address in Windows Explorer or Internet Explorer.

Note:

Agent Desktop does not support touch screen or tablet devices.

Appendix A: Standards

Regulatory standards

Quality of Service standards

Every customer will have different expectations and different budgets to work to. Some will be willing to upgrade their networks to use the best possible equipment and practices. To others the additional expense may be viewed as unnecessary. Examples of standards based Quality of Service protocols include:

- 802.1Q (Layer 2)
- DiffServ (Layer 3)
- Port Range (Layer 4)
- 802.1X (MD-5)

Voice compression codecs

The bandwidth used varies depending on the compression method chosen. IP Office supports standards listed below. These will occupy approximately 10K and 13K of bandwidth respectively. Use the following chart to choose the most appropriate compression algorithm for your available bandwidth.

Audio Codec	RTP Voice Data Payload (bytes)	Packets per second	LAN (bps)	% overhead LAN	WAN (bps)	% overhead WAN	Algorithmic delay (ms)
G.723.1 (6.3K)	24	33.33	20,800	225%	9,867	54%	80
G.729a	20	50	29,600	270%	13,200	65%	40
G.711 (64K)	160	50	85,600	34%	69,200	8%	20
G.722 (64K)	160	50	85,600	34%	69,200	8%	20

VoIP standards

IP Office supports the following protocols and standards:

H.323 V2 (1998)	Packet-based multimedia communications systems.
Q.931	ISDN user-network interface layer 3 specification for basic call control.
H.225.0 (1998)	Call signaling protocols and media stream packetization for packet-based multimedia communication systems.

H.245 (1998) Control protocol for multimedia communication.

SIP Session Initiation Protocol

T.38 Fax standard

Internet standards (In addition to TCP/UDP/IP.)

Standard	Description
RFC 1889	Real Time Protocol (RTP) and Real Time Control Protocol (RTCP)
RFC 2507, 2508, 2509	Header compression
RFC 2474	DiffServ, Type of Service field configurable
RFC 1990	PPP fragmentation
RFC 1490	Encapsulation for Frame Relay
RFC 2686	Multiclass Extensions to Multilink PPP
RFC 3261	SIP
RFC 3489	STUN

Analog trunk standards

IP Office analog trunk cards conform to the standards:

TIA/EIA-646-B Loop Start

GR-188-CORE and GR-31-CORE Incoming Caller line identification (ICLID)

ANSI T1.401 and TIA/EIA-646-B Ground Start (not available in all localities)

Database interface standards

IP Office supports the ActiveX Data Object (ADO) interface standard.

PCI Security Standard Council standards

Leading credit card companies defined standards in the PCI Security Standard Council and one of these standards is not recording credit card numbers given by the customer.

Wireless WiFi standards

The 3641 and 3645 telephones provide an improved user-interface, a new lightweight design and a radio that supports several WiFi standards (802.11 a/b/g). With these handsets customers have an increased choice to fit their needs and infrastructure. Based on global standards for wireless LAN's, the Avaya IP Wireless Telephone Solution simplifies network infrastructure by enabling voice traffic to be carried along with data traffic over the same wireless network. 3616, 3620 and 3626 telephones are supported but no longer available from Avaya for direct sequence 802.11b wifi networks; the 3641 and 3645 will also work in 802.11a and 802.11g networks. These telephones are also field upgradeable through external TFTP clients (not included), so telephones can be updated with new protocols, features, and capabilities as they become available.

Networking protocol standards

Protocol	RFC	Description
Point-to-Point Protocol (PPP)	RFC1661	WAN protocol that allows interworking with a wide range of third-party routers. PPP is used over leased line circuits where a single channel is used to connect the two locations together. For example, a single channel maybe a 64K channel on a dial-up circuit or a 256K leased line etc.
Link Control Protocol (LCP)	RFC1570	In PPP, LCP establishes, configures and tests data-link Internet connections.
Multi-Link Point-to-Point Protocol (ML-PPP)	RFC1990	Allows additional calls to be made where bandwidth greater than a single channel is required. The maximum number of channels available to data can be set on a service-by-service basis. When the available bandwidth reaches a user defined limit additional channels can be automatically added. Similarly, when traffic falls then the number of channels in use can be automatically reduced. If there is no data traffic on any of the channels in use then all lines can be cleared. Since most carriers have a minimum charge for calls, the period that a channel has to be idle before clearing is configurable. Through these mechanisms call costs can be effectively controlled while ensuring that bandwidth is available as and when it is needed.
Internet Protocol Control Protocol (IPCP)	RFC1332	A Network Control Protocol (NCP) for establishing and configuring IP over a PPP.
Internet Protocol Header Compression (IPHC)		Reduces the header size of the data packet to gain bandwidth efficiency over WANs, but adds to transmission latency.
Password Authentication Protocol (PAP)	RFC1334	A method of authenticating the remote end of a connection using unencrypted passwords.
Real-time Transport Protocol (RTP) Real-time Transport Control Protocol (RTCP)	RFC1889	RTP defines a standardized packet format for delivering audio and video over IP networks. RTCP works with RTP to send control packets to call participants to provide feedback on the quality of service.
Challenge Handshake Authentication Protocol (CHAP)	RFC1994	Allows an incoming data call to be authenticated using encrypted passwords. The system also provides the option to periodically reaffirm the authenticity of the caller during the data call.
Compression Control Protocol (CCP)	RFC1962	Configures, enables and disables data compression algorithms on both ends of the PPP link. Also used for signal a failure.
Light-weight Directory Access Protocol (LDAP)	RFC4510	Allows the telephone number directory (names and telephone numbers) held in IP Office to be synchronized with the information on an LDAP server (limited to 5000

Table continues…

Protocol	RFC	Description
		entries). Although targeted for interoperation with Windows 2000 Server Active Directory, the feature is sufficiently configurable to interoperate with any server that supports LDAP version 2 or higher.
Microsoft Point-to-Point Compression (MPPC)	RFC2118	Data compression method for greater throughput on slow speed WAN links.
Bandwidth Allocation Control Protocol (BACP)	RFC2125	Allows the negotiation with the remote end of the data call to request additional calls to be made to improve aggregate data throughput.
User Datagram Protocol (UDP)	RFC768	A simple connectionless transmission model with a minimum of protocol mechanism used to allow applications to send messages (datagrams) to other hosts on an IP network without prior communications to set up special transmission channels or data paths.
Internet Protocol (IP)	RFC791	A set of rules governing the format of data sent over the Internet or other network.
Transmission Control Protocol (TCP)	RFC793	A connection is established an maintained until the application at each end have finished engaging messages.
Dynamic Host Configuration Protocol (DHCP)	RFC1533	Dynamically distributes network configuration parameters on and IP network such as IP addresses for interfaces and services.
Network Address Translation (NAT)	RFC1631	A mechanism that allows the use of different IP address on a private network behind a router with a public IP Address. When connecting to the Internet, ISPs typically want a customer to use an IP address they have allocated. Using NAT this is easily accommodated, eradicating the need for the customer to change their network numbering scheme and providing additional security to the internal users as their address in hidden to the public. Typically, a company maps its internal network addresses to a global external IP address and unmaps the global IP address on incoming packets back into internal IP addresses. This helps ensure security since each outgoing or incoming request must go through a translation process. This also offers the opportunity to qualify or authenticate the request or match it to a previous request. NAT also conserves the number of global IP addresses that a company needs.
Bootstrap Protocol (BOOTP)	RFC951	Automatically assigns an IP address to network devices from a configuration server on an IP network.
Trivial File Transfer Protocol (TFTP)	RFC1350	A simple protocol to transfer files implemented on top of the UDP using port number 69.
Network Time Protocol (NTP)	RFC868	Provides clock synchronization between computer systems over packet-switched, variable latency data networks.

Table continues…

Protocol	RFC	Description
Proxy Address Resolution Protocol (ARP)		Support for Proxy Address Resolution Protocol allows IP Office to respond on behalf of the IP address of a device connected to it when receiving an ARP request.
Simple Network Managment Protocol (SNMPv1)	RFC1157 RFC1155 RFC1212 RFC1215	Simple Network Management Protocol. (STD15) Structure and identification of management information for TCP/IP based internets. (STD16) Concise MIB Definitions. (STD16) A convention for defining traps for use with SNMP
Managment Information Base (MIB-II)	RFC1213	Management Information base for network management of TCP/IP based internets: MIB-II. (STD17)
ENTITY MIB	RFC2737	Entity MIB (Version 2)
Routing Information Protocol (RIP)	RFC1058 RFC2453 RFC1722	Adistance vector protocol that allows routers to determine the shortest route to a destination network. It does this by measuring the number of intermediary routers that need to be traversed to reach the destination network. If more than one route exists to the same destination the shortest route is used. If a fault occurs on the shortest route it will be remarked as being infinite and any alternative route will become the new shortest route. This behavior can be used to add resilience into a data network. Where a customer has an existing data network comprising of third party routers, IP Office added to the network can provide back up using its routing and dial-up capability. RIP enabled routers share their knowledge of the network with each other by advertising and listening to routing table changes. IP Office Supports both the RIP I and RIP II standards.
Internet Protocol Security (IPSec)	RFC2401 RFC2402 RFC2403 RFC2404 RFC2405 RFC2406 RFC2407 RFC2408 RFC2409 RFC2410 RFC2411	Security Architecture for the Internet Protocol IP Authentication Header The Use of HMAC-MD5-96 within ESP and AH The Use of HMAC-SHA-1-96 within ESP and AH The ESP DES-CBC Cipher Algorithm with Explicit IV IP Encapsulation Security Payload. (ESP) The Internet IP Security Domain of Interpolation for ISAKMP Internet Security Association and Key Management Protocol The Internet Key Exchange The NULL Encryption Algorithm and its Use with IPSec IP Security Document Roadmap

Table continues…

Protocol	RFC	Description
Layer 2 Tunneling Protocol (L2TP)	RFC2661 RFC3193	PPP authentication using PAP or CHAP takes place between directly connected routers only. When using a public IP Network to connect sites this authentication takes place between the customers router and the service provide router that it is connected to. In some circumstances it is desirable to authenticate between the customer owned routers, jumping over all the intermediary routers of the service provider's network. Layer 2 Tunneling Protocol allow this to happen by facilitating a two stage authentication, firstly with the service provider router then the customer router on the remote network. IPSec tunnels allow a company to pass data between locations over unsecured IP networks such as the public internet. The company data is secured using 3DES encryption making it unintelligible to other parties that might be 'eaves dropping' on the traffic. Tunneling can be applied to link offices together or provide workers access to the office over the internet. All IP Office systems support up to a total of 256K worth of encrypted traffic to multiple locations. Initially, inter-working is supported only between IP Offices that are connected either directly on a WAN port or via the LAN using a third-party router. IPSec is optional and enabled on IP Office through a License Key.
Differentiated Services (DiffServ)	RFC2474	Networking architecture that specifies a simple, scalable and coarse-grained mechanism for classifying and managing network traffic and providing quality of service (QoS) on IP networks.
Frame Relay Encapsulation	RFC 1490	Multi protocol Interconnect over Frame Relay

Session Initiation Protocol (SIP) standards

Rec. E.164 [2]	ITU-T Recommendation E.164: The international public telecommunication numbering plan
RFC 2833 [7]	RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
RFC 3261 [8]	SIP: Session Initiation Protocol
RFC 3263 [10]	Session Initiation Protocol (SIP): Locating SIP Servers
RFC 3264 [11]	An Offer/Answer Model with Session Description Protocol (SDP)
RFC 3323 [14]	A Privacy Mechanism for the Session Initiation Protocol (SIP)
RFC 3489 [18]	STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)

RFC 3824 [24]	Using E.164 numbers with the Session Initiation Protocol (SIP)
RFC 1889	RTP
RFC 1890	RTP Audio
RFC 4566	SDP
RFC 3265	Event Notification
RFC 3515	SIP Refer
RFC 3842	Message Waiting
RFC 3310	Authentication
RFC 2976	INFO
RFC 3323	Privacy for SIP (PAI) and draft-ietf-sip-privacy-04 (RPID)
RFC 3325	Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
RFC 3581	An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing
RFC 3311	The Session Initiation Protocol (SIP) UPDATE Method

Appendix B: Supported TAPI functions and data

Supported TAPI 2.1 functions

TAPILink Lite provides the following functionality for TAPI 2.1.

- lineAddToConference
- lineAnswer
- lineBlindtransfer
- lineCompleteTransfer
- lineConfigDialog
- lineClose
- lineDeallocateCall
- lineDial
- lineDrop
- lineGetAddressCaps
- lineGetAddressID
- lineGetAddressStatus
- lineGetAppPriority
- lineGetCallInfo
- lineGetCallStatus
- lineGetDevCaps
- lineGetID
- lineGetLineDevStatus
- lineHold
- lineInitialiseEx
- lineMakeCall
- lineNegotiateTAPIVersion
- lineOpen
- linePark

- lineRedirect
- lineRemoveFromConference
- lineSetAppPriority
- lineSetAppSpecific
- lineSetCallPrivilege
- lineSetStatusMessages
- lineSetupTransfer
- lineShutdown
- lineSwapHold
- lineUnhold
- lineUnpark
- lineSetCallData
- lineDevSpecific
- lineGenerateDigits
- lineGenerateTone
- lineMonitorDigits
- lineMonitorTones

Supported TAPI 3.0 functions

The following functions are supported using TAPI 3.0:

ITTAPI	• Initialize • Shutdown • EnumerateAddresses • RegisterCallNotifications • Put_EventFilter
ITAddress	• get_AddressName • get_dialableAddress • get_ServiceProviderName • CreateCall
ITMediaSupport	get_MediaTypes
ITCallInfo	• get_Address

	• get_CallState • get_CallInfoString • SetCallInfoBuffer
ITBasicCallControl	• Connect • Answer • Disconnect • Hold • SwapHold • ParkDirect • Unpark • BlindTransfer • Transfer
ITCallStateEvent	• get_Cause • get_State • get_Call
ITCallNotificationEvent	get_Call
ITCallInfoChangeEvent	get_Call
ITCallHubEvent	• get_Event • get_Call

Note:

TAPILink Lite can be used from C, C++ and Delphi. Visual Basic cannot directly use TAPI 2.1, but does support TAPI 3.0 without any third-party tools.

TAPILink Lite provides detailed information on telephony events, including the ability to screen-pop based on CLI and/or DDI.

Supported TAPILink Pro functions

TAPILink Pro also supports additional TAPI functionality that is not available through TAPILink Lite. This functionality is supported through the LineGetLineDevStatus and LineDevSpecific calls.

The additional TAPILink Pro features are:

- Agent login
- Agent logout
- Set and retrieve divert destination

- Set and retrieve extended divert status
  - Forward All Calls
  - Forward On Busy
  - Forward On No Answer
  - Do Not Disturb
- Retrieving the extension locale (language)
- Set and clear the message waiting lamp
- Enable and disable group membership
- Generate and detect DTMF digits and tones (requires the TAPI-WAV driver)

TAPI device-specific data

The following table shows the device specific data available through TAPI:

- Phone's extension number
- Forward on busy flag
- Forward on no answer flag
- Forward unconditional flag
- Forward hunt group flag
- Do not disturb flag
- Outgoing call bar flag
- Call waiting on flag
- Voicemail on flag
- Voicemail ring-back flag
- Number of voicemail messages
- Number of unread voicemail messages
- Outside call sequence number
- Inside call sequence number
- Ring back sequence number
- No answer timeout period
- Wrap up time period
- Can intrude flag
- Cannot be intruded upon flag
- X directory flag
- Force login flag

- Login code flag
- System phone flag
- Absent message id
- Absent message set flag
- Voicemail email mode
- User's extension number
- Users Locale
- Forward number
- Follow me number
- Absent text
- Do not disturb exception list
- Forward on busy number
- User's priority
- Number of groups the user is a member of
- Number of groups that the user is a member of that are currently outside their time profile
- Number of groups the user is currently disabled from
- Number of groups that the user is a member of that are currently out of service
- Number of groups that the user is a member of that are currently on night service

DevLink device-specific field data

The following table shows the device specific data available via DevLink.

#	Field Data (S Message)	#	Field Data (S Message)
1	A call id	26	Voicemail disallow
2	B call id	27	Sending complete
3	A state	28	Bc.tc,bc.tm
4	B state	29	Owner hunt group name
5	A connected	30	Original hunt group name
6	A is music	31	Original user name
7	B connected	32	Target hunt group name
8	B is music	33	Target user name
9	A name	34	Target RAS name
10	B name	35	Is internal call

Table continues…

#	Field Data (S Message)	#	Field Data (S Message)
11	B list (possible targets for the call)	36	Time stamp
12	A slot ,channel	37	Connected time
13	B slot , channel	38	Ring time
14	Called party presentation and type	39	Connected duration
15	Called party number	40	Ring duration
16	Calling party presentation and type	41	Locale
17	Calling party number	42	Park slot number
18	Called sub address	43	Call waiting
19	Calling sub address	44	Tag
20	Dialled party type	45	Transferring
21	Dialled party number	46	Sv active
22	Keypad type	47	Sv quota used
23	Keypad number	48	Sv quota time
24	Ring attempt count	49	Account code
25	Cause	50	Unique call identifier

#	Field Data (D Message)	#	Field Data (A Message)
1	A call id	1	A call id
2	B call id	2	B call id
3	Unique call identifier	3	Unique call identifier

Glossary list

Automatic Route Selection — A feature of some telephone systems in which the system automatically chooses the most cost-effective way to send a toll call.

Busy Hour Call Completions — A measure of dynamic traffic calls that can be completed in an average busy hour.

Communication Manager — A key component of Avaya Aura®. It delivers rich voice and video capabilities and provides a resilient, distributed network for media gateways and analog, digital, and IP-based communication devices. It includes advanced mobility features, built-in conference calling, contact center applications and E911 capabilities.

Computer Supported Telecommunications Application (CSTA) — A standard interface for Computer Telephony Integration (CTI) applications, such as voice mail and auto-attendant, to interact with telephony equipment.

Digital Communications Protocol — A proprietary protocol that is used to transmit both digitized voice and digitized data over the same communications link. A Digital Communications Protocol (DCP) link consists of two 64-kbps information (I) channels, and one 8-kbps signaling (S) channel. The DCP protocol supports two information-bearing channels and two telephones or data modules.

Directory Enabled Management — An interface that uses Avaya Directory Server to facilitate administration of Modular Messaging from a centralized location.

Distributed Communications System — A proprietary inter-networking protocol from Avaya with which you can configure two or more Avaya-based private communication networks to operate as one, large network.

Domain Name System (DNS) — An Internet Engineering Task Force (IETF) standard for ASCII strings to represent IP addresses. The DNS is a distributed internal directory service used mostly to translate between domain names and IP addresses. Avaya 9600 Series IP Telephones can use DNS to resolve names into IP addresses. In DHCP, TFTP, and HTTP files, DNS names can be used whenever IP addresses are available as long as a valid DNS server is identified first.

Dynamic Data Exchange (DDE)	An interprocess communication (IPC) method.
Dynamic Host Configuration Protocol (DHCP)	An Internet Engineering Task Force (IETF) protocol used to automate IP address allocation and management.
Ethernet Routing Switch (ERS)	The Avaya stackable chassis system that provides high-performance, convergence-ready, secure, and resilient Ethernet switching connectivity.
Expansion Interface	A port circuit pack in a port network (PN) that provides the interface between a time-division multiplex (TDM) bus or a packet bus on the PN and a fiber-optic link. Expansion interface (EI) carries circuit-switched data, packet-switched data, network control, timing control, and digital signal-1 (DS1) control. EI in an expansion port network (EPN) also communicates with the master maintenance circuit pack to provide the environmental status and the alarm status of the EPN to the switch processing element (SPE).
Expansion port network	In Intuity Audix Server configurations, a port network (PN) that is connected to the time-division multiplex (TDM) bus and the packet bus of a processor port network (PPN). Control is achieved by indirect connection of the EPN to the PPN by way of a port network link (PNL).
Extension to Cellular access number	The phone number dialed to connect to the Avaya server that is running Communication Manager. The Extension to Cellular access number initiates the process of enabling or disabling Extension to Cellular or changing the station security code.
Federal Communications Commission (FCC)	A United States federal agency that regulates communications such as wire-line communications and the Internet.
Global Technical Services	An Avaya team that answers customer calls about products in Avaya Integrated Management.
Internet Protocol	A connectionless protocol that operates at Layer 3 of the Open Systems Interconnect (OSI) model. Internet Protocol (IP) is used for Internet addressing and routing packets over multiple networks to a final destination. IP works in conjunction with Transmission Control Protocol (TCP), and is identified as TCP/IP.
Local Survivable Processor	A configuration of the S8300 media server in which the server acts as an alternate server or gatekeeper for IP entities such as IP telephones and G700 media gateways. These IP entities use the Local Survivable Processor (LSP) when the IP entities lose connectivity with the primary server.

Media gateway	An application-enabling hardware element that is part of a family of such elements. This family includes intra-switch connectivity, control interfaces, port interfaces, and cabinets. Avaya media gateways support both bearer traffic and signaling traffic that is routed between packet-switched networks and circuit-switched networks to deliver data, voice, fax, and messaging capabilities. Media gateways provide protocol conversion, such as IP to ATM to TDM, conferencing, presence, such as on-hook or off-hook, connectivity to private networks and public networks, such as IP, ATM, TDM, and networking, such as QSIG, DCS, ISDN. Media gateways support optional form factors.
Network Address Port Translation	A network routing technique. Network Address Port Translation (NAPT) is used to access systems on the same subnet as an IP Office.
Network Routing Policy	An application for centrally managing SIP routing for Session Manager instances. A routing policy describes how a call is routed: where it comes from, where it's going, what its dial pattern is, what time of day it is routed, and its cost for a particular route.
Novell® eDirectory™	An X.500-compatible directory service software product initially released in 1993 by Novell® for centrally managing access to resources on multiple servers and computers within a given network. Novell® eDirectory™ was formerly known as Novell® Directory Services. It is sometimes referred to as Netware Directory Services. Novell® eDirectory™ is a hierarchical, object-oriented database used to represent certain assets in an organization in a logical tree, including people, positions, servers, workstations, applications, printers, services, and groups.
OFCOM	The United Kingdom Office of Communication for the regulation of telecommunications.
PARTNER® Contact Closure Adjunct	A device that is connected to the chassis of a media gateway and provides contact closures. Contact Closure Adjunct (CCA) closes a relay in response to a dial-in command from the media gateway to operate a door or perform a similar action.
Product Information Presentation System	The Product Information Presentation System (PIPS) reports provide data from the Product Information Expert (PIE), a data mining tool that extracts Avaya customer switch and adjunct configuration information and stores it in a database.
Product Licensing and Delivery System (PLDS)	The Avaya licensing and download website and management system. Avaya Business Partners and customers use this site to obtain ISO image files and other software downloads.
Public Switched Telephone Network (PSTN)	A telephone network that includes many communication technologies such as microwave transmission, satellites, and undersea cables.

Remote Feature Activation	A Web-based Avaya application to remotely activate features and increase capacities on the system of a customer by delivering a new license file.
System Manager	A common management framework for Avaya Aura® that provides centralized management functions for provisioning and administration to reduce management complexity.
System Status Application	An IP Office application that shows the status of things such as outgoing calls.
Telecommuter	The configuration where Communication Manager establishes the voice connection to a circuit-switched telephone. Requires two connections: a TCP/IP connection for signaling control and a circuit-switched connection for voice.
Telephony Application Program Interface (TAPI)	A Microsoft® Windows API that enables computers running Windows to use telephony services. TAPI is used for data, FAX, and voice communications. Applications can use TAPI to control telephony functions, such as dial, answer, and hang up.
Telephony Service Provider Interface (TSPI)	A Microsoft-defined interface to the telephony service provider (TSP). Microsoft® Windows comes with an H.323 TSP, an IP conference TSP, a kernel-mode device driver TSP, and a unimodem TSP.

Index