



Avaya Proactive Contact Overview and Specification

Release 5.2
Issue 1.1
January 2019

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

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

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. 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 types

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.

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

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at <https://support.avaya.com/LicenseInfo> under the link "Heritage Nortel Products" or such successor site as designated by Avaya. For

Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

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

INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://WWW.MPEGLA.COM).

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing

contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction	8
Purpose	8
Chapter 2: Avaya Proactive Contact overview	9
Avaya Proactive Contact overview	9
New in Avaya Proactive Contact Release 5.2	11
Supported languages	12
Avaya Proactive Contact Features	13
Batch Campaign Update enhancement	13
Configurable password lockout attempts	13
de_reject process enhancement	13
Display of a warning on the Agent Monitor if agent transfers are unsuccessful	13
Increase in the number of time zones supported to 150	14
Java, WebLM, and Tomcat upgrades	14
Log customization	14
Manual Dialing	14
Maximum password length aligned across client applications	14
OFCOM-72 hour rule compliance enhancement	15
Reduction in the value of the VIRT_PORT_TIMEOUT parameter to 10 minutes	15
Support for acceptance of double-digit reason codes in the soft dialer mode	15
Support for Avayatized Red Hat Enterprise Linux 6.9 version	15
Support for Common Server 3 for fresh installations	16
Support for an external syslog server for logging	16
Support for configuring Answer Supervision by job	16
Support for displaying notification messages to ACD agents when an outbound job ends	16
Support for identifying the time zone based on the zip code	16
Support for Music on Hold	17
Support for passing called party number for opt out calls to VDN	17
Support for shadow jobs in the preview mode	17
Support for strong ciphers	17
Support for virtualized servers as a deployment platform	17
Updates to the browsers supported for Internet Monitor	17
Microsoft Windows versions supported	18
Multitenancy	18
Increased dialer support in a pod	18
Backup logs	18
Enhanced ID field for calling list names	18
Enhanced IQ Reporting	19
Out of time zone phone support	19
Automated Release Agent to Ready feature for Voicemail	19
Enhanced Access Security Gateway	20

Oracle 11g.....	20
Simplified Supervisor installation.....	20
USB support.....	20
Implementation of FCC 12-21 regulation.....	21
Feature description.....	21
Configured features list.....	23
Chapter 3: Interoperability.....	28
Interoperability.....	28
Product compatibility.....	28
Hardware requirements.....	28
Operating system compatibility.....	32
Browser compatibility.....	35
Databases versions supported in Proactive Contact.....	36
Database client connector for Proactive Contact.....	36
VMWare versions supported in Proactive Contact.....	36
Supported versions of Tomcat, Java, and WebLM.....	37
Chapter 4: Performance specifications.....	38
Capacity and scalability specification.....	38
Avaya Proactive Contact Traffic specification.....	45
Difference between boundary conditions and steady-state behavior.....	46
Redundancy and high availability.....	47
Chapter 5: Environmental requirements.....	48
Environmental checklist.....	48
Avaya PG230RM cabinet specifications.....	48
Avaya PG230RM system cabinet environmental specifications.....	49
Safety specifications.....	50
Safety and regulatory information.....	50
Federal Communications Commission regulations.....	51
Office of Communication (OFCOM).....	53
Answer supervision.....	53
Industry Canada regulations.....	54
European Union regulations.....	55
China Regulations.....	55
Safety instructions.....	56
Contacting support.....	59
Chapter 6: Security.....	60
Port utilization.....	60
Security specification.....	60
Chapter 7: Licensing requirements.....	62
Licensing requirements.....	62
Chapter 8: Resources.....	63
Documentation.....	63

Finding documents on the Avaya Support website..... 63

Training..... 64

Viewing Avaya Mentor videos..... 64

Support..... 65

Glossary..... 66

Chapter 1: Introduction

Purpose

This document describes tested Avaya Proactive Contact characteristics and capabilities, including feature descriptions, interoperability, performance specifications, security and licensing requirements.

This document is intended for people who want to gain a high-level understanding of the Avaya Proactive Contact features, functions, capacities, and limitations.

Chapter 2: Avaya Proactive Contact overview

Avaya Proactive Contact overview

Avaya Proactive Contact is a flexible product for real-time outbound and blended customer contact. Avaya Proactive Contact leads the Contact Center industry in Predictive Dialing algorithms and best-in-class call classification. Avaya Proactive Contact helps your contact center stay productive and the cost for each call stays at the lowest possible levels.

Avaya Proactive Contact integrates with a variety of Automatic Call Distribution systems to blend agents between outbound and inbound missions to meet the needs of your company and lines of business.

You can manage call pacing based on flexible real-time control or you can set call pacing in cruise control mode. Managing call pacing increases agent productivity and results in a higher Return on Investment (ROI).

The following features make the product flexible:

- Adding call recording solutions, such as Verint Contact Store and NICE Call Recorders.
- Customizing the agent desktop solutions, from built-in screen and key changes to creating your own desktop client with real-time updates to other business systems.
- Managing flexible line capacity through control of multiple systems with one interface.
- Sharing calling lists across systems with the capability to share up to ten systems and 4300 plus active agents access to the same customer data.
- Integrating with the best time to call applications.
- Delivering virtual notification campaigns, using which customers can immediately opt out of speaking with an agent.
- Delivering customer-specific automated messages based on account details.
- Integrating with Avaya Aura® Experience Portal to provide automated notification customized for each individual customer.

Assigning agents to specific campaigns so that the agents never log into the wrong job.

- Creating a multitenant environment where multiple business units share the same system without affecting the calling mission of another business unit.

- Assigning customers to specific agents with agent work skills. For instance, agents can be assigned any combination of client spoken language, for example, Spanish, French, English, Portuguese.
- Having infinite campaigns and adding new customer contact information without interrupting the job flow.
- Modifying the calling focus with real-time record selections.
- Specifying the outbound caller ID for each job or each record based on customer criteria, for example, Gold status, Silver Status, and standard status.
- Having flexible built-in reporting and blended reporting with Avaya Aura[®] Performance Center or creating custom reporting with a flexible suite of real-time and historical reporting from the built-in Oracle database or data event stream.
- Having the preview or managed dialing feature for high touch accounts.
- Providing support to SIPREC media duplication for the recording system by passing the CALLID as an identifier for every outbound call to PG230 and then passed to Avaya Aura[®] Communication Manager by PG230 for further processing.

Avaya Proactive Contact is available in the following versions:

- The high capacity hard dialer for enterprise level environments, that is, a rack-mounted product with its own switching equipment.
- The soft dialer or Computer Telephony Integration (CTI) version for small to medium business environments that leverages the hardware of Avaya Aura[®] Communication Manager.
- The virtualized option of using Avaya-provided Appliance Virtualization Platform (AVP) on Common Server 3 (CSR3).
- The virtualized option using customer-provided VMware.

 Note:

An Appliance Virtualization Platform host and all virtual machines running on the host must be on the same subnet mask. However, PG230 must be on a different subnet.

If Out of Band Management is configured in an Appliance Virtualization Platform deployment, you need three subnet masks, one for each of the following:

- Public or signaling traffic, AVP, and all virtual machines public traffic
- Traffic towards PG230
- Management, Appliance Virtualization Platform, and all virtual machine management ports

With the wide range of features and technology that Avaya Proactive Contact offers, your business can gain a further competitive edge.

New in Avaya Proactive Contact Release 5.2

Support for Avayitized Red Hat Enterprise Linux 6.9 version

Avaya Proactive Contact Release 5.2 supports version 6.9 of Avayitized Red Hat Enterprise Linux (RHEL).

Supports Transport Layer Security 1.2 including High Ciphers

Avaya Proactive Contact Release 5.2 supports Transport Layer Security (TLS) 1.2 for connections between the dialer server and the clients including high ciphers. Dialer is configured, by default, to support TLS 1.2. Customers have an option to configure security setting of their choice.

To support TLS 1.2, following components are modified:

- Agent binary
- Listserver
- PC Agent
- Agent API
- Event SDK
- Internet Monitor
- WebLM
- Supervisor

TLS 1.2 and SHA-2 certificates are now supported between the dialer server and the Avaya Application Enablement Server (AES).

Supports SIP Recording

Avaya Proactive Contact Release 5.2 introduces a unique call-id on the ISDN and H.323 trunks when using the PG230 trunks. The function of such an ID is to enable SIP Recording (SIPREC) recording solutions in cases where PG230 trunks are converted to SIP. The ID provided within the trunks can be correlated with the ID provided by the Event SDK to identify individual calls on the SIP trunks.

Support for custom certificate

Avaya Proactive Contact Release 5.2, introduces deployment of the custom certificate into Proactive Contact system including Dialer, Supervisor, Agent, and Event SDK. Customers can create and install their own certificates into PC system and the certificate may be signed by any third party Certificate authority (CA).

Java, WebLM, and Tomcat upgrades

Avaya Proactive Contact Release 5.2 upgrades the Java platform on the dialer and supports the following versions of Java, WebLM, and Tomcat:

- Azul JDK version 1.8 and JacORB version 3.2
- WebLM version 7.1.0
- Tomcat version 9.0

Secure System Access

The Access Security Gateway, effective from Avaya Proactive Contact Release 5.1, is a system access challenge and response feature. It is a multi-user, one-time token system that is able to

securely generate responses for the challenges posed by administrative and support access from remote systems. The Enhanced Access Security Gateway has been integrated with Avaya Proactive Contact Release 5.2 to further improve remote access security.

The Enhanced Access Security Gateway (EASG) has been integrated into the Avaya Proactive Contact system. EASG provides secure authentication and auditing of all remote access into the maintenance ports.

Area codes with Time Zone Mapping (U.S and Canada)

Avaya Proactive Contact Release 5.2 includes updated area code mapping tables for the United States and Canada. The area code and time zone information is stored in `locale.cfg`, `timezone.cfg`, and `sttday.cfg` files located at `/opt/avaya/pds/config` directory.

Migration from Avaya Proactive Contact Release 5.1.x to Avaya Proactive Contact Release 5.2 creates a backup of the original Avaya Proactive Contact Release 5.2 `locale.cfg`, `timezone.cfg`, and `sttday.cfg` files in `/opt/avaya/pds/pc52_orig/pds/config` backup directory for migration. Customer's custom files are restored to the `/opt/avaya/pds/config` directory.

To use the latest area codes from Avaya Proactive Contact Release 5.2, refer to the files in `/opt/avaya/pds/pc52_orig` directory. Customers must manually update their customized `locale.cfg` file with the new area codes.

If customer does not have any customization and require to use updated area code information, then the `locale.cfg`, `timezone.cfg`, and `sttday.cfg` files can be copied from the backup directory to the active directory.

For detailed instructions for migration, see *Migrating to Proactive Contact, 5.2, - Release Notes*.

Supported languages

The Proactive Contact user interface, the Agent, and the Supervisor documents are available in the following languages:

- English
- French
- German
- Italian
- Japanese
- Simplified Chinese
- Korean
- Portuguese for Brazil
- Russian
- Latin Spanish

*** Note:**

For the Supervisor to work in Latin Spanish, the users must set Windows OS Locale to Spanish (Spanish).

Avaya Proactive Contact Features

Batch Campaign Update enhancement

Avaya Proactive Contact enhances the Batch Campaign Update (BCU) feature to update all matching records, and not just the first or the last. You can configure a parameter in the `master.cfg` file to control the functioning of the BCU feature and ensure backward compatibility.

Configurable password lockout attempts

In Avaya Proactive Contact Release 5.1.2, you can configure the LDAP password lockout policy. The dialer administrator specifies the number of attempts that can be made for entering a password before the password gets locked at the sysadm prompt. If the administrator enters zero, then the lockout policy is disabled.

de_reject process enhancement

Avaya Proactive Contact enhances the de_reject process with the ability to mark cancelled records as duplicate. This ensures that records that are already cancelled are not called even if you download the cancelled records subsequently.

You can choose between the old or the new functioning of the de_reject process.

Display of a warning on the Agent Monitor if agent transfers are unsuccessful

Avaya Proactive Contact enhances the Agent Monitor to display a warning if agent transfers between jobs are unsuccessful. The system displays a message that some agent transfers are unsuccessful, along with a list of agents who did not get transferred.

Increase in the number of time zones supported to 150

In Avaya Proactive Contact Release 5.1.2, the number of time zones supported has been increased from 62 to 150.

Java, WebLM, and Tomcat upgrades

Avaya Proactive Contact upgrades the Java platform on the dialer and supports the following versions of Java, WebLM, and Tomcat:

- Java version 7.0.91
- WebLM version 6.3
- Tomcat version 7.0.55

Log customization

Prior to Proactive Contact Release 5.1.2, users collected logs using the `get_logs` tool. However, the `get_logs` tool collected all the logs and users could not select specific logs. In Proactive Contact Release 5.1.2, users can capture specific logs or system details using the following scripts:

- `collect_logs`
- `get_info`
- `config_debug`

For more information about how to customize logs, see *Implementing Avaya Proactive Contact*.

Manual Dialing

Proactive Contact introduces a new dialing mode called the Manual Dialing mode that is available only with Preview jobs. In the Manual Dialing mode, the dialer presents the call record to the agents for previewing and does not automatically dial the number. The agent must click a button to dial or cancel the call. Using Manual Dialing, an agent can dial a number through Proactive Contact or a third-party application.

Maximum password length aligned across client applications

Avaya Proactive Contact aligns the maximum password length across client applications. The maximum password length for the client applications is 20 characters.

OFCOM-72 hour rule compliance enhancement

Proactive Contact supported compliance to OFCOM 72-hour regulation for a customer in older releases. In Release 5.1.2, Proactive Contact supports compliance to OFCOM 72-hour regulation for a phone number also.

The OFCOM 72-hour regulation specifies that you must have a 72-hour period before a telephone number receiving an abandoned call might be called again without the guaranteed presence of an agent. There must be a live operator if you are making a repeat call to a number to which a nuisance call was made. Proactive Contact supported the OFCOM 72-hour regulation on a per-record basis. From Proactive Contact 5.1.2, Proactive Contact also supports the OFCOM 72-hour regulation on a phone number basis.

To comply with the OFCOM 72-hour regulation, Proactive Contact adds a new parameter, OFCOM72 in the `master.cfg` file. You can set the OFCOM72 parameter for a job, a tenant, or a dialer. If you set this parameter, without the guaranteed presence of a live operator, no repeat call is made to a number that received a nuisance call in the prior 72 hours.

Reduction in the value of the VIRT_PORT_TIMEOUT parameter to 10 minutes

In Avaya Proactive Contact Release 5.1.2, the value of the VIRT_PORT_TIMEOUT parameter that is present in the `master.cfg` file is reduced to 10 minutes. 10 minutes is the recommended value for the following reasons:

- Virtual ports can time out and get freed up so that the dialer does not run out of virtual ports.
- The dialer can initiate dial backs and acquire calls, and agents can log on to the dialer.

Support for acceptance of double-digit reason codes in the soft dialer mode

In Avaya Proactive Contact Release 5.1.2, the dialer accepts double-digit reason codes from Communication Manager in the soft dialer mode. The new supported reason code range is 1–99. For backward compatibility, single-digit reason codes are also supported.

Support for Avayitized Red Hat Enterprise Linux 6.9 version

Avaya Proactive Contact supports version 6.9 of Avayitized Red Hat Enterprise Linux (RHEL).

Support for Common Server 3 for fresh installations

With HP DL 360 G8 servers going end of sale, Common Server 3 (CSR3), that is, HP DL 360 G9, is the new supported platform for deploying Avaya Proactive Contact. The deployment of Proactive Contact on CSR3 is done only through either customer procured VMWare or through Avaya Virtualized Platform.

You can deploy Avaya Proactive Contact 5.1.2 OVA on VMWare ESXi Version 5.0, 5.1, 5.5, or 6.0.

Older releases of Proactive Contact are not supported on CSR3. However, you can migrate from any of the current supported hardware running any version of Proactive Contact to CSR3 running Proactive Contact 5.1.2. You can either upgrade on the existing Proactive Contact 5.1.1 server or install PC 5.1.1 using CSR3 and virtualized platform, and then upgrade to PC 5.1.2.

Support for an external syslog server for logging

Avaya Proactive Contact supports storing of logs on an external syslog server. Users can configure the logs that need to be stored.

Support for configuring Answer Supervision by job

In Avaya Proactive Contact, you can configure Answer Supervision by job using the Editor application. You can also configure Answer Supervision feature at the campaign level using the job configuration files.

Support for displaying notification messages to ACD agents when an outbound job ends

If an ACD agent is released to an inbound job, and the outbound job to which the agent is logged in ends, Avaya Proactive Contact displays the following job end notification to the agent:

`The job was shut down.`

Support for identifying the time zone based on the zip code

Avaya Proactive Contact supports determining the time zone of a telephone number on the basis of zip code. You can configure the ZIP_TO_ZONE parameter in the `master.cfg` file.

Support for Music on Hold

In Avaya Proactive Contact, supervisors can configure a script for Music on Hold. Then the dialer plays music when an agent puts a customer on hold. Otherwise the customer hears silence.

Support for passing called party number for opt out calls to VDN

Avaya Proactive Contact enhances the Opt-out to VDN feature so that the TRANSID feature works with a virtual job to allow one of the calling lists field data to be transferred as ANI to the agent.

Support for shadow jobs in the preview mode

In Avaya Proactive Contact, you can configure shadow jobs in the preview mode. If supervisors configure the shadow job feature in the preview mode, then an agent can view the record in the preview mode before dialing out to a customer.

Support for strong ciphers

In Avaya Proactive Contact Release 5.1.2, you can configure the system to use only strong ciphers with ≥ 128 bits key size. Using strong ciphers enhances the security of your system.

Support for virtualized servers as a deployment platform

In addition to the current supported hardware, you can deploy Proactive Contact Dialer on virtualized servers. For more information , see *Implementing Avaya Proactive Contact*.

Updates to the browsers supported for Internet Monitor

Avaya Proactive Contact supports Internet Monitor (IMON) on the following browsers:

- Microsoft Internet Explorer 10 and 11
- Mozilla Firefox 38 and 39

Microsoft Windows versions supported

Avaya Proactive Contact Release 5.1.2 applications (PC Agent, Supervisor suite, APIs (Agent API), and Event SDK) support Microsoft Windows Vista Enterprise Edition, Microsoft Windows 7, 8.1, and 10, and Microsoft Windows Server 2008.

Avaya Proactive Contact Release 5.1.2 does not support Microsoft Windows XP.

Multitenancy

Multitenancy is an optional feature in Avaya Proactive Contact. Multitenancy creates separate instances of configuration so that multiple individual business units can use the same Avaya Proactive Contact system but not have access to configurations of other business units. Using Multitenancy, you can create various tenants on the Dialer. Within these tenants, you can administer and use the functionalities of the dialer so that each tenant performs actions on the dialer without hampering the work of other tenants working on the dialer. Therefore, each tenant can work as an individual dialer while residing on the same setup. You can allocate campaigns, agents, calling lists, schedules, agent keys, and other components to the tenants.

You can continue to use Avaya Proactive Contact as the default resource group, without Multitenancy. The other new features in this release such as, Increased Dialer Support and Out of Time Zone Cellphone Support, are available in both tenantised and non-tenantised environments.

For more information on Multitenancy, see *Administering Avaya Proactive Contact 5.1*.

Increased dialer support in a pod

In Avaya Proactive Contact 5.1, the number of dialers that you can include in a pod setup has been increased from four to ten.

The pod capacity for Avaya Proactive Contact with CTI is four dialers.

Backup logs

In Avaya Proactive Contact 5.1, backup and restore activities that you perform on the dialer are logged in a separate log file which is at `/opt/avaya/logs/archive_mgr.log`. The log file contains the actions and user inputs during the backup and restore activities.

Enhanced ID field for calling list names

In the current release, you can provide meaningful names to calling lists, for example, to indicate the reason for creating the calling list.

In releases prior to Avaya Proactive Contact 5.1, the calling list name only indicated the nature of the calling list, such as inbound or outbound, and the pre-assigned number. You can use customized calling list names in strategy, call selections, and jobs. You can also create, download, upload, and install a campaign template for a calling list with a customized name. All the reports display customized calling list names.

The calling list name must be unique at the tenant level. You can use the same calling list name for multiple tenants, but within a tenant, you cannot have more than one list with the same name.

Enhanced IQ Reporting

Avaya Proactive Contact 5.1 integrates with Avaya IQ to support call transfers and conference. A pod environment also supports Enhanced IQ Reporting.

Out of time zone phone support

In some countries, telemarketers are restricted from calling outside the calling hours of the called party whatever the local time zone might be. In previous releases, when a person kept the original mobile phone number after moving to a different time zone, the Avaya Proactive Contact dialer placed a call to the mobile phones outside of the regulatory time zone hours. In this release, you can support calls to mobile phones with an additional time zone identifier assigned.

Automated Release Agent to Ready feature for Voicemail

In the United Kingdom, Avaya Proactive Contact must connect the called party with an agent within two seconds. Therefore, the customers are unable to use the Answering Machine Detection (AMD) feature of Avaya Proactive Contact to eliminate agent intervention for a call. The customers typically turn off AMD and answer all calls with a live agent. The live agent passes the call to the correct message, selects the completion code for this result, and then goes back to the ready state. However, this procedure impacts agent productivity significantly.

With the Automated Agent Release to Ready feature, Avaya Proactive Contact connects all calls to a live agent and the system continues to detect answering machines. If the system detects an answering machine, the administrator can configure the Avaya Proactive Contact system to perform one of the following actions:

- End the call without playing a message and place the agent in the ready mode.
- Play a message on the answering machine but also place the agent in the ready mode.
- Leave the answering machine with an agent.

Enhanced Access Security Gateway

Enhanced Access Security Gateway (EASG) is a challenge and response protocol that eliminates the need for a shared password. EASG is supported by Avaya Services. The accounts that require EASG authentication are the admin, craft and sroot accounts. Currently, Proactive Contact provides sroot and admin accounts that are shared among Avaya Services, business partners, and customers. Avaya Services periodically updates the passwords through a manual process several times a year. Change of passwords is done by a personal visit to the customer site which incurs significant costs. All the shared accounts do not provide the Services team the ability to determine who made changes on the system. The shared accounts also prevent Avaya Services from using other authentication technologies for Services access. To overcome the problems of sharing passwords, you must implement EASG on Proactive Contact.

The following are the key points for EASG implementation:

- A single EASG RPM deploys all required files, such as scripts and product certificates, to setup EASG.
- A single product certificate for Proactive Contact 5.2 is installed through EASG RPM installation.
- Proactive Contact 5.2 uses the single EASG certificate for all customers which is deployed during installation.
- The product certificate is always located at - `/etc/asg/Product.p7b`.
- EASG utilities have manual (man) pages that describe the EASG commands or utilities.

Oracle 11g

The Oracle version on the dialer is 11.2.0.4. The Oracle version on the Supervisor application is 11.2.0.4.

Simplified Supervisor installation

Using Avaya Proactive Contact 5.1 Supervisor, you can skip the installation of third-party components, such as Oracle Instant Client, Microsoft .NET Framework, or SAP Crystal Reports Runtime Engine. For example, if your system already has a version of Oracle Instant Client, then you can skip the installation of Oracle Instant Client in Supervisor setup. To skip installing specific third-party components, you must skip installing specific Avaya Proactive Contact components.

USB support

In addition to the earlier supported media types, in Avaya Proactive Contact 5.1 you can also use USB (Flash Memory Drive) to install dialers, perform backups, and restore. USB devices do not support Mondo backup.

Implementation of FCC 12-21 regulation

In the earlier release of Avaya Proactive Contact, in case of a live call, you can use the Do Not Call (DNC) feature to allow agents to mark the called party record as DNC and mark all the matching records with the same unique called party identifier in other selected calling lists as DNC.

In view of the FCC 12-21 regulation, in case of virtual job, a pre-recorded message plays to the called party that provides the DNC opt-out option for automatic indication to mark the record as DNC.

In case of an outbound live call on Avaya Proactive Contact, if a welcome message is played to the called party before connecting to the agent, the system provides the DNC opt-out option to the called party throughout the duration of the welcome and wait queue messages. After the welcome message, the call must connect to a live agent within two seconds, otherwise the system marks the call as an FCC nuisance call. Also, a report has been added to the Analyst module that provides the details of FCC nuisance calls for a 30-day period.

Feature description

The following table describes the standard features of Avaya Proactive Contact:

Feature	Description
Detect the beep	You can use the Detect the Beep feature to leave a message after detecting the last beep on an answering machine. Detect the beep is not available in Avaya Proactive Contact with CTI.
Expert Calling Ratio	You can use the Expert Calling Ratio feature to provide the supervisors the ability to control the dialing pace of a Job.
Cruise Control	You can use the Cruise Control feature to automatically maintain the service level of outbound dialing during a Job. The Cruise Control feature also connects the calls to agents within a specified period of time. The system manages the call pacing during the Job based on the service level configured at the start of the Job.
Agent Blending	You can use the Agent Blending feature to integrate outbound calling activities on Proactive Contact with inbound calling activities on your Automatic Call Distribution (ACD). In an Agent Blending system, ACD agents log in to both Proactive Contact and the ACD. The Agent Blending feature monitors the activity on the ACD. Agent Blending uses the information gathered to determine when to acquire agents for outbound calling and when to release ACD agents to handle inbound calls.

Table continues...

Feature	Description
Intelligent Call Blending	You can use the Intelligent Call Blending (ICB) feature that Avaya Proactive Contact uses as a call blending method for call centers whose priority is outbound dialing. ICB distributes a blend of inbound and outbound calls to Proactive Contact agents. The ACD transfers inbound calls to available inbound or blend agents on Avaya Proactive Contact. When an agent is unavailable, Avaya Proactive Contact places calls in the inbound wait queue. If your system does not use an ACD, Avaya Proactive Contact transfers inbound calls to available inbound or blend agents.  Note: Intelligent Call Blending feature is not available on CTI.
Job Linking	You can use the Job Linking feature to identify Jobs that start automatically when the current Job is complete. When you link a Job, the system transfers agents to the next Job as the agents complete their last calls and release the records. The system displays a message that the agents are changing Jobs.
Letter Generation	You can use the Letter Generation feature to help supervisors create a list of customer data, such as names, addresses, and other record information, to develop customized form letters from their calling lists. Letter Generation extracts the information that the system exports locally. Supervisors can then create a mail merge letter using the extracted information.
Line Pool	You can use the Line Pool feature to allow multiple Jobs to share common line pools. Using Line pooling, Avaya Proactive Contact can distribute lines to active Jobs.
List Distribution	You can use the List Distribution feature to analyze the records in an outbound calling list and create reports that count the records in the specified categories or distributions. With List Distribution, you can do Job planning and analysis.
Managed Dialing	You can use the Managed Dialing feature to facilitate agents to preview a customer record before calling that customer.
PC Analysis	You can use the PC Analysis feature to generate reports from Jobs, agents, calling list information, and calling activity.
Record Edit	You can use the Record Edit feature to facilitate a supervisor to view, edit, or mark a record uncallable or deleted on a calling list. The supervisor can specify data to locate the customer record and display the data on the Supervisor workstation where the supervisor can view, edit, or mark a record uncallable or deleted. Record edit has two options: Standard Record Edit and Quick Search. By default, both the options are configured on the system unless otherwise requested.

Table continues...

Feature	Description
Standard Record Edit	You can use the Standard Record Edit feature to search through a calling list based on the values entered in the fields. Standard Record Edit is slower than Quick Search, but Standard Record Edit accepts field values that contain special characters, such as hyphens (-) and wildcard characters (*). With Standard Record Edit, you can also perform searches on multiple fields.
Quick Search	You can use the Quick Search feature to use the value entered in a single field to locate a record. The system also uses the same single field to index your calling lists. The value for this single field must be unique to each record. Quick Search is a fast retrieval method that you can use for large calling lists. Quick Search does not accept field values that contain special characters.
Screenbuilder	You can use the Screenbuilder feature to help supervisors design and modify agent screens.
Ziptones	You can use the Ziptones feature to indicate the tones that Avaya Proactive Contact transmits to the headset of an agent immediately before the agent connects with a customer. The two ziptones defined during the specification process are distinct: one for inbound calls and the other for outbound calls. Agents can quickly determine by the tone whether the call is an inbound or an outbound call.

Configured features list

The following table describes the features that Avaya configures and provides with Avaya Proactive Contact:

Feature name	Description
Agent owned recall (AOR)	You can use the Agent Owned Recall feature to facilitate an agent to set a recall for a customer. The agent who initially set the recall handles the call when the call is placed again.
ANI/DNIS	You can use the ANI/DNIS feature to display Automatic Number Identification (ANI) to indicate the number of the calling party. The ANI/DNIS feature displays Dialed Number Identification Service (DNIS) or the number dialed.
Autoplay	You can use the Autoplay feature to facilitate Avaya Proactive Contact to automatically deliver a message during a campaign when Autoplay detects an answering machine at the other end.

Table continues...

Feature name	Description
Completion codes	The system or an agent uses the Completion Codes to specify individual call results. When a customer answers a phone call, Avaya Proactive Contact transfers the call to an agent. The completion code can be an agent-generated code that is pre-specified or a standard system completion code. If the system does not pass the call to an agent, Avaya Proactive Contact generates the completion code. Avaya Proactive Contact stores the completion codes and uses these codes to select records for calling and to generate reports. The system identifies completion codes by a code number, a call result, and a description. • The call result is a short name that makes the code easier for agents to identify. • The description provides call center supervisors with a more concise description of the codes. Each system has one set of completion codes. You must specify the agent-generated codes to use in the specification process.
Campaign update	You can use the Campaign update feature to stop outbound calls to customers who are already in contact with an agent. If the customer calls an inbound agent, the system removes the record from the calling activities of the day. You can configure the Campaign update feature as Real Time, Batch, or Both.
Do not call list	Using the Do not call feature, agents can mark a record as uncallable. Using the Do not call feature, you can also mark a matching record uncallable on multiple lists as configured. The uncallable records are then not called on any other jobs. Agents can mark numbers as Do Not Call (DNC) on request. You can also upload DNC requests to the host database for future exclusion. This marking of DNC, however, is valid only for a day, if you download the list every day.

Table continues...

Feature name	Description
File transfer and schedules	You can use the File transfer and schedules feature to identify the information that Avaya Proactive Contact uses to receive and transfer data to the host. The system gathers the following information during the specification process: • The time to start the data transfer, even to retry transfers when an attempt fails • The time between each transfer attempt • The time to stop transfer attempts • The days to conduct the data transfer • The calling lists to process Type of transfer: Download from the host to Avaya Proactive Contact, and upload from Avaya Proactive Contact to the host.
Infinite job	You can use the Infinite Job feature the system to append new records to a calling list during calling activities and automatically add these records to the active Infinite Job campaign.
List processing	You can use the List processing feature for flexible configuration options for extracting and updating information on the calling list, such as retaining data from previous lists, marking duplicate accounts, and running reports.
Native voice and data transfer	Voice can be transferred by the phone or softphone. Data can be transferred if the application utilizes the UCID. Outbound Contact Agent is not using the UCID. You can use the Native voice and data transfer feature to transfer a call and the associated call data to an available inbound or blend agent. Outbound or blend agents use this feature. Native voice and data transfer is not available on Proactive Contact with CTI.
Record specific messaging	You can use the Record specific messaging feature to link outbound wait queue messages to selected criteria in the calling list fields. During calling activities, Proactive Contact plays messages specific to zip code, city, account type, or any other specified field in the calling list. During the specification process, you specify the messages that a customer hears while waiting in the outbound wait queue. This feature is not available on Proactive Contact with CTI.

Table continues...

Feature name	Description
Sales verification	You can use the Sales verification feature to use a second calling campaign to confirm sales or commitments obtained in a prior campaign. You can choose the keys needed to support a sales job in a sales verification scenario. When you use Sales Verification, agents use a specific code to release records that resulted in a successful sale. The system automatically sends these records to a second verification Job where agents call up each record and the agent verifies and confirms the sale.
System wait queue messages	You can use the System Wait Queue Messages feature to provide the messages that customers hear while waiting for an agent or when customers call after business hours. You can also create customized messages for agent keys so that when an agent presses the agent key, Avaya Proactive Contact plays the assigned messages. System wait queue messages are commonly strung together to create a script. When creating system wait queue messages, create individual messages, and then assign messages to a message script. This feature also indicates the time, in seconds, that Avaya Proactive Contact pauses between messages. The following is a sample message script: 1. "Hold the line. I have a call for this number." 2. Pause for 5 seconds 3. "Sorry to keep you waiting. I'm still trying to connect." 4. Pause for 5 seconds. 5. "Still trying to connect, continue to hold." 6. Pause for 5 seconds. 7. "Thank you for waiting. Sorry I could not connect you. Try again later." 8. Avaya Proactive Contact disconnects the line.
Virtual agent	You can use the Virtual Agent feature to deliver outbound messages to customers. This feature is a part of an agentless Job.
Wait queues	You can use the Wait queues features to assign calls to a holding area. These calls are the calls that the system cannot pass immediately to agents. Customers often hear system messages while waiting in a wait queue.

Table continues...

Feature name	Description
Wait queue indicators	The Wait Queue Indicators feature is a message that appears on the screen of an agent when Avaya Proactive Contact passes a call from the wait queue to the agent. Wait queue indicators display the amount of time that the customer waited for the agent and a brief message that the agent reads to the customer. Base each indicator on how long customers waited for an agent. An agent screen can display up to four wait queue indicators in one set.

Chapter 3: Interoperability

Interoperability

Product compatibility

For the latest and most accurate compatibility information, go to <https://support.avaya.com/CompatibilityMatrix/Index.aspx>.

Hardware requirements

Supervisor workstation hardware requirements

Supervisor workstations are network-attached computers. Supervisor workstations require a headset or phone. Identify and dedicate workstations for each Avaya Proactive Contact Supervisor license purchased. The location of the Supervisor workstation can vary based on your operational requirements.

Avaya Proactive Contact Supervisors use these workstations to:

- Set up and manage system settings.
- Set up jobs.
- Monitor calling activity.
- Produce call center reports.

Table 1: Supervisor workstation hardware requirements

Component	Minimum requirements
Processor	1.3GHz (Dual Core) Processor
RAM	2 GB
Free disk space	2 GB
Drive	DVD

The data in all the Monitor applications connected to a dialer might freeze for 15 minutes when a user runs the Monitor application from the Supervisor workstation in the following case:

- The Supervisor workstation machine has multiple network interfaces, and
- The dialer is not accessible through any network interface on the workstation.

For more information about additional hardware requirements to support:

- Microsoft Windows 7 Enterprise Edition, see the Microsoft website: <http://windows.microsoft.com/en-IN/windows7/products/system-requirements>
- Microsoft Windows Server 2008 SP2 Enterprise version, go to the Microsoft website: <http://www.microsoft.com/windowsserver2008/en/us/system-requirements.aspx>
- Microsoft Windows 8.1 Enterprise version, see the Microsoft website: <http://windows.microsoft.com/en-SG/windows-8/system-requirements>
- Microsoft Windows 10 Enterprise version, see the Microsoft website: <http://www.microsoft.com/en-gb/windows/windows-10-specifications#sysreqs>
<http://www.microsoft.com/en-gb/windows/windows-10-specifications#sysreqs>

Agent workstation hardware requirements

Each agent workstation consists of a computer and a voice connection. During jobs, agents use the workstation to talk to customers and update customer records. Avaya Proactive Contact agent workstation can use Avaya Proactive Contact agent application or Agent API to perform tasks.

Agent workstations can be network connected or directly through a serial connection.

The Avaya Proactive Contact system:

- provides quality service using network-connected computers
- supports connections to an Ethernet network
- uses the TCP/IP protocol to move data to the agent workstations and back

Table 2: Agent workstation hardware requirements

Component	Minimum requirements
Processor	1.3GHz (Dual Core) Processor
RAM	2 GB
Free disk space	2 GB
Drive	DVD  Note: For Microsoft Windows Vista Enterprise Edition (32-bit or 64-bit) and Microsoft Windows 7 Enterprise Edition (32-bit or 64-bit), operating systems CD drives are also supported.

For additional hardware requirements to support

- Microsoft Windows 7 Enterprise Edition, see the Microsoft website: <http://windows.microsoft.com/en-IN/windows7/products/system-requirements>
- Microsoft Windows Server 2008 SP2 Enterprise version, go to the Microsoft website: <http://www.microsoft.com/windowsserver2008/en/us/system-requirements.aspx>
- Microsoft Windows 8.1 Enterprise version, see the Microsoft website: <http://windows.microsoft.com/en-SG/windows-8/system-requirements>
- Microsoft Windows 10 Enterprise version, see the Microsoft website: <http://www.microsoft.com/en-gb/windows/windows-10-specifications#sysreqs><http://www.microsoft.com/en-gb/windows/windows-10-specifications#sysreqs>

Hardware requirements for HP DL 360 G9 server

HP DL 360 G9, also known as Common Server 3 (CSR3) is the new supported platform for deploying Avaya Proactive Contact. The deployment of Proactive Contact on CSR3 is done only through either customer procured VMWare or through Avaya Virtualized Platform.

Hardware requirements for HP DL 360 G9 are:

- Form Factor Rack Server (1 U Rack Height)
- Six Core Intel Xeon E5-2620v3at 2.4 GHz, 15MB Cache
- 32GB (4GB x 8) DDR3 1600MHz Memory
- Integrated 4-port Gigabit Ethernet NIC
- Hot swappable power supplies, fans, and hard drives
- Internal SATA DVD RW drive
- RAID 1 configuration: Hot Pluggable 300GB 10K 2.5 SAS HDD (qty 2)
- RAID 5 configuration: Hot Pluggable 300GB 10K 2.5 SAS HDD (qty 3)
- Power supply: 500W AC (qty. 2)

Note:

From Avaya Proactive Contact Release 5.2, the dialer uses only 16GB of the allocated RAM.

Hardware requirements for Avaya Converged Platform

Avaya Dell PowerEdge R640, is the underlying server hardware for the Avaya Converged Platform100 series. Proactive Contact 5.2.0.1 supports Avaya Converged Platform 130 Appliance, which is pre-loaded with standard VMware (EXSi 6.5) virtualization software.

- Form Factor Rack Server (1 U Rack Height)
- Twenty Core Intel(R) Xeon(R) Silver 4114 CPU @2.20GHz
- 48GB (8GB x 6) Memory
- Integrated 6-port Gigabit Ethernet NIC

- Hot swappable power supplies, fans, and hard drives
- Internal SATA DVD RW drive
- External RW USB DVD/CD-ROM (Model No : DIG - 72032)
- Four HDDs 2.5" 10K SAS
- RAID 1 configuration: 600GB 10K 2.5 SAS HDD (qty 4), 1.2 TB storage
- RAID 5 configuration: 600GB 10K 2.5 SAS HDD (qty 4), 1.8 TB storage
- RAID 6 configuration: 600GB 10K 2.5 SAS HDD (qty 4), 1.2 TB storage
- Power supply: 495W AC/750W AC (qty. 2)

Administrator console requirements

Using the administrator console, you can gain access to the Avaya Proactive Contact system CPU and digital switch. The administrator console connects directly to the access server inside the system cabinet. This interface requires a monitor and a keyboard. The system administrator uses this interface to perform basic system operations such as monitoring system status, backing up system files, shutting down the system, and setting the time and date of the system.

You can connect the monitor and keyboard directly to the access server inside the system cabinet. Alternatively, you can use any terminal emulation software that supports VT100 terminal emulation on Windows 2000 or later. The computer must have an available RS-232 serial port for connection to the remote access hardware. Alternatively, you can use an available USB port in conjunction with a USB to RS-232 serial adapter. You must provide the cables for either solution.

Placement

The placement specifications of the Administrator console are as follows:

- Minimum of 2 feet x 3 feet (0.6 meters x 0.9 meters) table or computer stand space.
- Maximum of 10 feet (3 meters) from the system cabinet.
- Minimum weight of 19.5 pounds (9 kilograms).

Table placement

If you place the Administrator console and the printer on the same table, use the following guidelines:

- Table dimensions: 4 feet x 2 feet (1.3 meters x 0.6 meters).
- Table weight: 50 pounds (18.65 kilograms).
- Table distance: must not be more than 8 feet (2.66 meters) away from the system cabinet.

Electrical

The workstation power cord plugs can be plugged directly into the system cabinet UPS.

Data connectivity

The workstation connects directly to the system cabinet through an RS-232 serial bus connection.

Avaya supplies a 15-foot RS232 cable terminating in a DB25 connector and is designed for a dumb terminal. Provide a serial-to-USB I/O converter to connect to a computer with terminal emulation software.

Security

For system security, you require the administrator user name and password.

*** Note:**

Avaya recommends that you have the latest updates for your Windows systems.

Operating system compatibility

Server operating systems

Operating system	Proactive Contact 5.2	Proactive Contact 5.1.2	Proactive Contact 5.1.1	Proactive Contact 5.1
Avaya Red Hat Enterprise Linux	Release 6.9	Release 5.11	Release 5.9	Release 5.5

Supervisor workstation-supported operating systems

Operating system	Proactive Contact 5.2	Proactive Contact 5.1.2	Proactive Contact 5.1.1	Proactive Contact 5.1	Proactive Contact 5.0
Microsoft Windows XP Service Pack 2 (32-bit or 64-bit)	N	N	Y If you are using Microsoft Windows XP SP2 with the Windows Firewall turned on, you can set permissions for Avaya applications to run.	Y	Y
Microsoft Windows Vista Enterprise Edition (32-bit or 64-bit)	N	Y	Y	Y	Y
Microsoft Windows 7 Enterprise Edition (32-bit or 64-bit)	Y	Y	Y	Y	Y

Table continues...

Operating system	Proactive Contact 5.2	Proactive Contact 5.1.2	Proactive Contact 5.1.1	Proactive Contact 5.1	Proactive Contact 5.0
Microsoft Windows Server 2008 SP2 Enterprise version (32-bit or 64-bit)	Y	Y	Y	Y	Y
Microsoft Windows 8.1 (32-bit or 64-bit)	Y	Y	N	N	N
Microsoft Windows 10 Enterprise Edition (32-bit or 64-bit)	Y	Y	N	N	N

*** Note:**

If you install a version of an Oracle client and the setup detects the Oracle client environment settings, the setup overwrites the existing Oracle environment variables.

Agent workstation-supported operating systems

Operating system	Proactive Contact 5.2	Proactive Contact 5.1.2	Proactive Contact 5.1.1	Proactive Contact 5.1	Proactive Contact 5.0
Microsoft Windows XP Service Pack 2 (32-bit or 64-bit)	N	N	Y If you are using Microsoft Windows XP SP2 with the Windows Firewall turned on, you can set permissions for Avaya applications to run.	Y	Y
Microsoft Windows Vista Enterprise Edition (32-bit or 64-bit)	N	Y	Y	Y	Y

Table continues...

Operating system	Proactive Contact 5.2	Proactive Contact 5.1.2	Proactive Contact 5.1.1	Proactive Contact 5.1	Proactive Contact 5.0
Microsoft Windows 7 Enterprise Edition (32-bit or 64-bit)	Y	Y	Y	Y	Y
Microsoft Windows Server 2008 SP2 Enterprise version (32-bit or 64-bit)	Y	Y	Y	Y	Y
Microsoft Windows 8.1 (32-bit or 64-bit)	Y	Y	N	N	N
Microsoft Windows 10 Enterprise Edition (32-bit or 64-bit)	Y	Y	N	N	N

*** Note:**

If you install a version of an Oracle client and the setup detects the Oracle client environment settings, the setup overwrites the existing Oracle environment variables.

- If you are not using Avaya Proactive Contact Agent Desktop or Avaya Proactive Contact Agent API, provide VT100 Emulation software for connection to the host and the system. You can install the following:
 - WallData Rumba
 - Attachmate Extra!
 - WRQ Reflections
 - Hummingbird

*** Note:**

Integration development and consulting is not included as part of your services agreement with Avaya Professional Services.

- If you are using an Agent API solution, provide network-connected agent computers. Avaya Proactive Contact communicates with the system through the Agent API. An emulation session is not necessary.

The Avaya Proactive Contact Agent application broadcasts record information using DDE. If you are creating a cut-and-paste solution to your host, the host emulation session must support DDE. You are responsible for creating any cut-and-paste solution, unless you have a contract with Avaya Professional Services (APS) for this work. If you have a contract, you must provide the host emulation software name, for example, Reflections, and the host emulation software type, for example, VT100 or 3270.

Browser compatibility

Table 3: Web browsers supported for Internet Monitor (IMON)

Web browsers	Proactive Contact 5.2	Proactive Contact 5.1.2	Proactive Contact 5.1.1	Proactive Contact 5.1	Proactive Contact 5.0
Microsoft Internet Explorer 6 Service Pack 1	N	N	N	Y	N
Microsoft Internet Explorer 7	N	N	N	Y	N
Microsoft Internet Explorer 8	N	N	Y	Y	N
Microsoft Internet Explorer 9	N	N	Y	N	N
Microsoft Internet Explorer 10	N	Y	N	N	N
Microsoft Internet Explorer 11	Y	Y	N	N	N
Chrome 56.0.2924	Y	N	N	N	N
Microsoft Edge Browser 20.10240 on Microsoft Windows 10	Y	Y	N	N	N
Microsoft Edge Browser 38.14393.1066.0 on Microsoft Windows 10	Y	N	N	N	N
Mozilla Firefox 2.x	N	N	N	Y	N
Mozilla Firefox 3.x	N	N	N	Y	N
Mozilla Firefox 18.x	N	N	Y	N	N

Table continues...

Web browsers	Proactive Contact 5.2	Proactive Contact 5.1.2	Proactive Contact 5.1.1	Proactive Contact 5.1	Proactive Contact 5.0
Mozilla Firefox 31.x	N	Y	N	N	N
Mozilla Firefox 38 and 39	N	Y	N	N	N
Mozilla Firefox 54.0.1	Y	N	N	N	N

Databases versions supported in Proactive Contact

Databases	Proactive Contact 5.2	Proactive Contact 5.1.2	Proactive Contact 5.1.1	Proactive Contact 5.1	Proactive Contact 5.0
Oracle 11g 32-bit (11.2.0.4.0)	Y	N	N	N	N
Oracle 11g 32-bit (11.2.0.3.15)	N	Y	N	N	N
Oracle 11g 32-bit (11.2.0.3.8)	N	N	Y	N	N
Oracle 11g 32-bit (11.2.0.3.3)	N	N	N	Y	N
Oracle 10g 32-bit (10.2.0.5.0)	N	N	N	N	Y
Microsoft 32-bit ODBC	Y	Y	Y	Y	N

Database client connector for Proactive Contact

Databases	Proactive Contact 5.2	Proactive Contact 5.1.2	Proactive Contact 5.1.1	Proactive Contact 5.1	Proactive Contact 5.0
Microsoft 32-bit ODBC	Y	Y	Y	Y	N

VMWare versions supported in Proactive Contact

VMWare versions	Proactive Contact 5.2	Proactive Contact 5.1.3	Proactive Contact 5.1.2	Proactive Contact 5.1.1	Proactive Contact 5.1	Proactive Contact 5.0
5.0	N	Y	Y	N	N	N

Table continues...

VMWare versions	Proactive Contact 5.2	Proactive Contact 5.1.3	Proactive Contact 5.1.2	Proactive Contact 5.1.1	Proactive Contact 5.1	Proactive Contact 5.0
5.1	N	Y	Y	N	N	N
5.5	Y	Y	Y	N	N	N
6.0	Y	Y	Y	N	N	N
6.5	Y	N	N	N	N	N

Supported versions of Tomcat, Java, and WebLM

Component	Proactive Contact 5.2	Proactive Contact 5.1.2	Proactive Contact 5.1.1	Proactive Contact 5.1	Proactive Contact 5.0
Java 1.6	N	N	Y	Y	Y
Java 1.7	N	Y	N	N	N
Azul JDK 1.8	Y	N	N	N	N
Tomcat 6.x	N	N	Y	Y	Y
Tomcat 7.x	N	Y	N	N	N
Tomcat 9.x	Y	N	N	N	N
WebLM 4.7	N	N	Y	Y	Y
WebLM 6.3	N	Y	N	N	N
WebLM 7.1.0	Y	N	N	N	N

Chapter 4: Performance specifications

Capacity and scalability specification

The following table provides information about various capacity parameters and their values for Avaya Proactive Contact:

 Caution:

You must adhere to the maximum capacity limits mentioned for each parameter. If you exceed the prescribed limits, then the system might not function as expected.

Category	Parameter	Value	Notes
Agent	Name recall name length	39	—
Agent	Name length (characters) in English or CJK	8/3	Alphanumeric.
Agent	Headset ID length	13	—
Agent	Maximum number of agents on Avaya Proactive Contact with PG230 per dialer (T1/E1)	432/450	PG230 Enabled.
Agent	Maximum number of agents per pod (T1/E1) in a 10 dialer pod.	4320/4500	PG230 Enabled.
Agent	Maximum number of preview agents on Avaya Proactive Contact with CTI	300	CTI Enabled.
Agent	Maximum number of predictive agents on Avaya Proactive Contact with CTI	300	CTI Enabled.
Agent	Number of users on the system	32K	—
Agent Blending	Number of Vector Directory Numbers (VDNs) Avaya Proactive Contact with PG230 or Avaya Proactive Contact with CTI.	600/300	The limit is 300 for each switch. For Avaya Proactive Contact with PG230, tested limit is up to 600, and for Avaya Proactive Contact with CTI, the tested limit is 300.
Agent Blending	Number of logins	432/450	432 for T1 and 450 for E1.

Table continues...

Category	Parameter	Value	Notes
Campaigns	Number of active supported campaigns (single Dialer)	- Maximum 200 campaigns when AOR is turned off. - Maximum 100 campaigns when AOR is turned on. The maximum value decreases if the number of shadow jobs running are more than 100.	—
Campaigns	Number of active supported campaigns (Pod) for a 10 dialer pod	- Maximum 2000 campaigns when AOR is turned off. - Maximum 1000 campaigns when AOR is turned on. The maximum value decreases if the number of shadow jobs running are more than 1000.	—
Campaigns	Number of active supported campaigns (CTI)	- Maximum 200 campaigns when AOR is turned off. - Maximum 100 campaigns when AOR is turned on. The maximum value decreases if the number of shadow jobs running are more than 100.	Preview and predictive.
Calling List	Record size in bytes	8192	Maximum record size of a calling list on which you can run a job. The record size includes the user added fields, the Proactive Contact added fields in addition to the number of fields, in bytes.

Table continues...

Category	Parameter	Value	Notes
Calling List	Maximum list size in gigabytes	2	Linux limit is 2 GB.
Calling List	Calling list name length in English	15	The calling list name must only be in English and must be alphanumeric.
Calling List	Number of unique calling lists	999	—
Calling List	Maximum records	900000	—
Calling List	Number of fields	Limited only by the record length	Limited only by the record length which is 8192.
Calling List	Number of phone fields	10	—
Calling List	Sortable fields	10	—
Calling List	Phone field digits	20	—
Calling List	Post-update - maximum attempts stored in calling list	5	The maximum number of phones that post update can track is 9.
Calling List	Field Length	1024/75	1024, if the field is not to be viewed by Agent as a part screen. In calling list details, you can set more than 75 characters but you cannot select those fields in screenbuilder for viewing by the agent. You must perform hashing, indexing, sorting, and DNC only on the fields which have a length of less than or equal to 128 bytes.
Calling List	Index field- Campaign Update	40 bytes	The data in the index field must not exceed 40 bytes.
Character Length	Dialer host name in English	12	—
Character Length	DO NOT CALL group name in English or other languages	32/10	—
Character Length	Maximum name length of selection in English or other languages	20/15	—
Character Length	Maximum Job name length in English or other languages	20/15	—
Character Length	Job unit ID length	32	Single byte

Table continues...

Category	Parameter	Value	Notes
Character Length	Job ID length	10	- The system generates the Job ID automatically. - The Job ID in the calling list has a fixed length of ten characters, and you cannot edit the ID.
Character Length	Strategy name length in English and other languages	20/15	—
Character Length	Single message size	Agent-to- supervisor 59 and supervisor-to-agent- 72	From Agent to Supervisor, displays only show on Jobmon.
Character Length	ANI/DNIS field length	15	Tested limit is up to 13.
Character Length	Tenant name in English and other languages	20/10	—
Database	Access	Read only	Chargeable ODBC access.
General	Line pools	50	—
General	Time zones	150	Configuration limit
General	Number of predictive blend gateways	10	—
General	Identification field length	255	The total length of 4 fields can be maximum 255.
General	Number of identification field	4	—
General	Completion codes	0–999	Of the 1000 completion codes, 31 are system codes or reserved codes. Supervisor cannot configure these codes.
General	Telephony script lines	6000	—
General	Screen size	23x80	The number of rows is 23 and the number of columns is 80.
General	Event service clients	20	—
General	Event service refresh in seconds	6	—
General	Internet Monitor refresh in seconds	30	—
General	Average backup size	15–GB	Includes 3 GB for lists and is based on 10% usage of the 148 GB drive.
General	Telnet/SSH sessions	Unlimited	—
General	Busy Hour Call Attempts (BHCA)	172000	172000 BHCA can be achieved only when the PG230 alarming is turned off.

Table continues...

Category	Parameter	Value	Notes
General	Maximum Call Selection	80	Ensure that the value is synchronized with the maximum strategy.
General	Dialed digit support	19	—
General	The number of switches	10	—
General	Maximum number of tenant allocation	20	If a user is a part of the default tenant, then the user can be a part of only 19 other tenants. If the user is not a part of the default tenant, then the user can be a part of only 20 tenants.
Hardware	Agent, outbound, inbound, and transfer	—	All can be on the same card. Minimum of 24.
Hardware	Total LPVC ports	384	128 per card and a maximum of 3 cards.
Hardware	Backup media	Tape/DVD/TPH/USB (Flash Memory Drive)	TDK DVD-R 16x 4.7–GB.
Hardware	The number of NICs	2	One NIC is used for your network, and the other NIC is connected to the PG230 switch.
Hardware	ENBC generic software	—	Switch generic 18.1.4 or later.
Hardware	RAM (Gigabytes) for G5/M2/G7/G8/G9 server	• 16 GB of RAM for IBM Nextgen 3650 M2 server which is also known as S8800 • 16 GB of RAM for HP ProLiant DL385 G5 servers. • 24 GB of RAM for HP ProLiant DL360 G7 • 32 GB of RAM for HP ProLiant DL360 G8 • 32 GB of RAM for HP ProLiant DL360 G9	Podded or high volume systems require 16 GB of RAM. The primary dialer must always have a 24 GB RAM.  Note: • Avaya Proactive Contact Release 5.2 does not support HP DL 385 G2/G5 hardware. • Avaya recommends that customers running HP DL385 G5 or S8800 should upgrade to a newer server.

Table continues...

Category	Parameter	Value	Notes
Integration	Crystal reports professional version	11	—
Integration	IVR agents	100	—
Jobs	Line pools per Job	10	—
Jobs	Number of configured jobs that are tested	500	These Jobs are not necessarily active Jobs.
Jobs	ID fields	4	—
Jobs	Job Description length	40 characters in English	—
Messages	Message storage capacity per LPVC in minutes	34	If multiple LPVC2 cards installed in a specific cabinet have 16-MB of memory, this cabinet will be limited to 16-MB of memory capacity for all LPVC2 cards installed, regardless of actual memory size. Message storage capacity does not increase with more LPVCs. Only the number of LPVC ports increase.
Monitor	Number of Monitor views in a single dialer	20/40	The maximum number of default views is 20 and the maximum number of views is 40. Users can have the viewsets in the following ways: • Monitor session with 20 default views only. • Monitor session with 40 custom views only. • Monitor session with 20 default and 20 custom views only. Use filtering to improve the performance. You must set the refresh interval to 20 seconds for optimal Monitor performance.

Table continues...

Category	Parameter	Value	Notes
Monitor	Number of Monitor views in a pod	10/20	The maximum number of default views is 10 and the maximum number of views is 20. Users can have the viewsets in the following ways: • Monitor session with 10 default views only. • Monitor session with 20 custom views only. • Monitor session with 10 default and 10 custom views only. Use filtering to improve the performance. You must set the refresh interval to 30 seconds for optimal Monitor performance.
Physical	Maximum Dialers per pod	10	On a 10 dialer pod, the minimum supported refresh rate of the Monitor is 15 seconds.
Physical	The number of phone lines per dialer (T1/E1)	912/900	912 is a combination of inbound, outbound, and transfer ports.
Supervisor	The number of Supervisor applications per system	100	The Supervisor application includes Editor, Analyst, Monitor, and Role Editor.
System	Protocols	—	TCP over SSL, and SSLIOP.
System	Java	1.7	—
System	Oracle DB server	Oracle Data base 11g 11.2.0.4.0	—
System	Oracle DB client	Oracle Data base 11g 11.2.0.4.0	—
Network	Network bandwidth minimum in Mbps	100/1000	Contact Centers must set up a 1000-Mbps, full-duplex, auto-negotiation network. Alternatively, the contact center can set up a 100-Mbps, full-duplex network.
Network	D-channel band rate	64kb	—

Table continues...

Category	Parameter	Value	Notes
Unit IDs	Number	50 units	Number of Unit IDs a Job can have.
Work List	Maximum length of line in master.cfg	1023	Each line in master.cfg cannot exceed 1023 bytes. This includes parameter name and the parameter value separated by a colon.
Work List	Maximum Strategy	300	Number of lines in strategy per strategy.
Work List	Maximum allowed units that agent can login to in multiunit Job	15	
System users	Maximum number of supported users	500	You can create a maximum of 500 system users.
rbac/rbacadmin users	Maximum number of supported users	500	You can create a maximum of 500 rbac/rbacadmin users.
sysadm users	Maximum number of supported users	500	You can create a maximum of 500 sysadm users.
Agent users	Maximum number of supported users	6000	You can create a maximum of 6000 agent users on a single dialer.
Pcanal users	Maximum number of supported users	100	You can create a maximum of 100 pcanal users.
Auditor users	Maximum number of supported users	100	You can create a maximum of 100 auditor users.
MAX_EXPANSION_UNIT	Maximum Dynamic Expansion Unit in case of Infinite Job	50	In an Infinite Job, you can add a maximum of 50 units.
Line Assign	Maximum character length of LinePool Name	10	The maximum character length of the LinePool name configured.
Selection Report	Maximum fields, which can be selected for selection fields, for reports.	40	The maximum fields. Must not exceed 40.

Avaya Proactive Contact Traffic specification

Two distinct classes of Avaya Proactive Contact operations are responsible for network traffic. The Avaya Proactive Contact classes are as follows:

- Discretionary activities

- Non-discretionary activities

Discretionary activities

Discretionary activities are activities where you can use your discretion to decide whether or not to perform certain actions. For example, downloading a calling list from a host computer system can often be done outside of peak calling periods, Campaign Monitor sessions do not need to be maintained when nobody is watching the displays, and the Campaign Analyst application can produce reports when fewer agents are online to Avaya Proactive Contact or outside the peak calling period. It is important to control discretionary activities while at the same time it is difficult to estimate the traffic from these activities.

Avaya Proactive Contact does not control these discretionary activities. These activities are unsystematic with respect to outbound calling operations. If a supervisor is careless in the use of the Supervisor suite of applications, the system generates massive amounts of useless traffic. For example, a request for all data from the Campaign Monitor with a short refresh period produces displays that cannot possibly be read or studied within the specified refresh period.

Avaya Proactive Contact does not reduce the rights of a user of the Supervisor suite of applications.

Non-discretionary activities

Non-discretionary activities are those activities where you do not have a choice as to the time or the extent of the activity given your demands for production of outbound call volume. For example, the execution of calling jobs is relatively mandatory for the calling operation, and agent capacity is fixed during a work shift. Avaya Proactive Contact performs non-discretionary activities automatically. The related traffic depends on the configuration of your network components, agent capacity, characteristics of call attempts, characteristics of call handling, and subscriptions to the event service for monitoring by non-Avaya sub-systems. These activities can vary widely. However, the activities are systematic to the calling job and are not subject to unnecessary use. Traffic from non-discretionary activities is more important for capacity planning because the traffic is necessary for the mission of the calling operation.

Difference between boundary conditions and steady-state behavior

Steady-state behavior occurs continually in the course of an activity, while boundary conditions exist at the beginning or end of an activity. The relevant activity is the execution of a calling job.

Emphasis on steady-state behavior

The steady-state behavior of calling jobs consists primarily of getting call records, initiating calls, connecting calls, disconnecting calls, updating call records, and registering agent availability for calls. This behavior happens repeatedly and cyclically for each agent and is asynchronous amongst the agents. The volume of this call-associated behavior depends on the number of agents and the length of the calling job. Most of the job activity is in steady-state. Consequently, the steady-state behavior is important for traffic analysis.

Boundary conditions

The traffic related to boundary conditions is less frequent than the traffic related to steady-state behavior.

Initial job behavior

The start of a job includes the control, monitoring and reporting of message traffic. There might be more call volume at the start of a job in the case where the agents are already logged in the job. More agents are available to handle calls than at any other time during the execution of the job since no agent is presently handling a call. Such conditions do not persist and are not frequent. Consequently, initial job activity is not important for traffic estimation.

Agent session boundaries

Additional traffic occurs when an agent logs in to a job and when the agent logs out of a job. Since each agent typically stays on the job to handle several calls, and since no call traffic exists on behalf of an agent that is logged, the traffic due to boundaries of agent sessions is unimportant.

Terminal job behavior

The end of a job includes the control, monitoring and reporting of message traffic. In the case of a job shutdown, the call handling activity diminishes gradually as agents complete calls without the job distributing more calls to the agents. The traffic due to job termination is not important for traffic estimation.

Agent blending activities

The traffic characteristics due to blending agents between inbound call handling and outbound call handling are similar to the traffic characteristics of Agent session boundaries. However, the rate of agent transitions into and out of handling outbound calls is more systematic.

Redundancy and high availability

Avaya Proactive Contact uses the Lightweight Directory Access Protocol (LDAP) when Avaya Proactive Contact is deployed as a pod. In a pod configuration, without using LDAP, user accounts must be created on each of the dialers in the pod for the following reasons:

- This is a manual process and can be error prone.
- It is possible that the users' accounts get out of sync across pod dialers.
- There is a possibility that some users are added in a dialer in pod and are forgotten to be added in other dialers in pod.
- It is also possible that the same user has different password on dialers in pod.

LDAP addresses all these problems by providing a single repository for user authentication which is available over the network.

Note:

LDAP is mandatory in Avaya Proactive Contact release 5.1. Without using LDAP, pod configuration or a standalone system is not supported by Avaya Proactive Contact.

Avaya Proactive Contact uses OpenLDAP version 2.4.40. Avaya Proactive Contact does not support the use of existing third party LDAP implementation. Avaya Proactive Contact supports OpenLDAP version 2.4.40 and High Availability feature via native support.

Chapter 5: Environmental requirements

Environmental checklist

You must adhere to the specifications mentioned in this section. Avaya is not responsible if you fail to adhere to the specifications mentioned in this section.

The checklist for the external environment setup is explained in the following table:

 Electrostatic alert:

Prepare the cabinet location to meet environmental requirements and to prevent component failure because of extreme temperatures, moisture, static electricity, and bad air quality.

#	Description	Notes	✓
1	Maintain the temperature of the laboratory between 45 degrees and 80 degrees Fahrenheit (7° C to 26° C). The ideal temperature is between 65 degrees Fahrenheit and 75 degrees Fahrenheit.	 Caution: You must consistently maintain this temperature in the mentioned range. The system produces up to 5500 BTUs of heat per hour. In a small room lacking air conditioning, this heat can raise the temperature above the operating limits of the system.	
2	Maintain the humidity between 8% and 80% in the non-condensing state.		
3	Keep the system cabinet 5 ft. (1.7 m.) from any air conditioning or heating ducts.		
4	Protect your system from direct sunlight.		
5	Ensure that the system cabinet is not under an overhead sprinkler or in an area near water such as a damp basement.	 Important: If the sprinkler placement cannot be changed, then note that the warranty provided by Avaya is limited.	

Avaya PG230RM cabinet specifications

The PG230RM cabinet contains the digital switch card cage to place and answer phone calls.

Components that connect to the PG230RM cabinet include:

- Maintenance modem and remote access server for remote technical support of the system.
- Avaya Proactive Contact System CPU to run the system software with a DVD or DDS drive for backing up and restoring the database and files.
- Uninterruptible power supply (UPS) to provide a dual power supply to the system cabinet components in addition to the power supply included at the factory with the PG230RM.
- Administrator console, which is customer provided, for access to the digital switch and system controller.
- Public Switched Telephone Network (PSTN) for placing and receiving calls.
- Local Area Network (LAN) for connecting to agent and supervisor workstations.
- Customer-provided Agent workstations and Supervisor workstation, headsets or phones, using the trunk connections to the switch.
- For CTI deployment options, Application Enablement Services (AES) communicates with the Avaya Aura® Communication Manager switch. The server integrates telephones on the desktops of agents with telephony-enabled applications or telephony-based applications. These applications can reside either on the server as server applications or on the desktop computer as client applications. For more information on installing AE Services, see *AE Services Client Installation Guide*.

For more information about PG230RM, see the *Implementing Avaya Proactive Contact* guide.

Avaya PG230RM system cabinet environmental specifications

The environment can influence PG230RM system performance and reliability. You must control the temperature, humidity, and other environmental factors to meet the operating requirements of PG230RM.

Electrical

Connect the system cabinet ground to the building ground. Use a minimum of 10 AWG (5.26 sq-mm) stranded ground conductor (green insulated wire with at least one yellow stripe).

Air Conditioning

A qualified air conditioning engineer must determine the exact requirements for your environment. Use the following guidelines to estimate air conditioning requirements:

Air conditioning must handle the heat produced by the components in the system cabinet, personnel in the room, and lighting. You must also consider the heat that comes through walls, windows, floors, and ceilings. Because the system requires constant power (even if the system is idle), the system continually generates heat. Ensure that air conditioning requirements are met.

The environment must have a stable ambient operating temperature of approximately 72 degrees Fahrenheit (22 degrees Celsius). A temperature in the range of 45 degrees to 80 degrees Fahrenheit (7 degrees to 26 degrees Celsius) is acceptable. The temperature variation in the equipment room must not exceed ± 5 degrees Fahrenheit (± 3 degrees Celsius).

Heat dissipation from a system is estimated in British Thermal Units (BTUs) per hour. Estimate the amount of air conditioning required based on the heat generated in the equipment area and square feet of occupied floor space. Remember that each person in the occupied area generates heat. Consult your (Heating, Ventilation, and Air Conditioning (HVAC) representative for specific air conditioning, heating, and ventilation requirements.

Use the following guidelines for all the hardware components of the Avaya Proactive Contact system:

- Keep the temperature between 45°F to 80° F (7°C to 26° C).
- Maintain 8% to 80% relative humidity.
- Protect from heat, cold, and water exposure.
- Avoid direct sunlight.

Other environmental factors

In addition to controlling temperature, you must control the following environmental factors in the equipment areas:

Environmental factors	Description
Humidity	Low humidity can increase static electricity buildup, while high humidity can affect the performance of disks and printers. Maintain a non-condensing, relative humidity between 8 percent and 80 percent.
Static electricity	You must place the system cabinet on an antistatic electrical grade matting. When you work on Avaya Proactive Contact System equipment, use an antistatic wrist strap.
Lighting	Avoid direct sunlight.
Ventilation	Do not block the vents on the system cabinet.

Grounding and power requirements

In addition to meeting the requirements in this topic, you must comply with the requirements in *Avaya Proactive Contact Safety and Regulatory Information*.

Warning:

If you fail to follow the grounding procedures, the installation can be unsafe for personnel, unprotected from lightning or power transients, and subject to service interruptions and degraded performance. The power supply conductors must be dedicated and uninterrupted from the service panel to the system cabinet.

Safety specifications

Safety and regulatory information

This section contains regulatory, safety, and support information essential to the installation and operation of Avaya Proactive Contact implementation. This document covers Avaya Proactive

Contact implementations using the Avaya Proactive Contact System and the Avaya PG230 Proactive Contact Gateway cabinet or rack mounted (PG230-RM). For regulatory purposes, the system is also known as PDS2-100, PDS2-120, PDS2-230, Avaya Programmable Adjunct Switch - APAS, and APAS-RM. Statements made in this document apply to all implementation options.

Read each section carefully. Follow the requirements in the regulation and safety sections before operating the system. If you need system support, read [Contacting support](#) on page 59 to gather the information identified before you call an Avaya representative.

The following table identifies the sections of this document that apply to the systems installed in the listed locations.

Country and related regulations

Country	FCC Regulations	Answer Supervision	IC Regulations	China Regulations	European Union Regulations	Safety Instructions	Contacting Support
Argentina	-	-	-	-	-	Yes	Yes
Australia	-	Yes	-	-	-	Yes	Yes
Brazil	Yes	-	-	-	-	Yes	Yes
Canada	-	-	Yes	-	-	Yes	Yes
Chile	-	-	-	-	-	Yes	Yes
China	-	-	-	Yes	-	Yes	Yes
Colombia	-	-	-	-	-	Yes	Yes
European Union	-	-	-	-	Yes	Yes	Yes
Hong Kong	-	-	-	-	-	Yes	Yes
Japan	-	-	-	-	-	Yes	Yes
Korea	-	-	-	-	-	Yes	Yes
Malaysia	-	-	-	-	-	Yes	Yes
Mexico	Yes	-	-	-	-	Yes	Yes
South Africa	-	-	-	-	-	Yes	Yes
United States	Yes	Yes	-	-	-	Yes	Yes

Federal Communications Commission regulations

To comply with Federal Communications Commission (FCC) regulations, ensure that you meet the specified requirements.

*** Note:**

Many FCC reports refer to the PG230 Gateway as the Avaya Programmable Adjunct Switch (PAS).

This document covers Avaya Proactive Contact implementations using the Avaya Proactive Contact system and the Avaya PG230 Gateway (also known as Avaya Programmable Adjunct Switch - PAS). Statements made in this document apply to both of these implementation methods.

- The FCC Part 68 registration number of this equipment AV1USA-28011-MA-T and the Ringer Equivalence (UTC) Number (0.7B) must report to the Centralized Operations Group of your local telephone company. Centralized Operations Groups are better equipped to process TELCO line requests for this telephone system.
- The Facility Interface Codes (FIC) for the following types of cards are as follows:

Card	FIC	Description
EUTC	O2LS2	2-wire, local switched access, loop start
EUTC	O2GS2	2-wire, local switched access, loop start
QT1	04DU9-BN	1.544 Mbps SF and ESF format
QT1 PRI	04DUS-1SN	1.544 Mbps SF and ESF format

- The order codes for the following services are as follows:

Service	Code	Description
Analog	9.0F	Provides full protection for the network using live voice. Only registered terminal equipment can be connected to station ports.
Digital	6.0P	Provides billing and encoded analog content protection.

- The sum of the Ringer Equivalence Numbers for all devices connected to a single telephone line should not exceed 5.0 for reliable operation.
- Do not install Avaya Proactive Contact on coin-operated telephone lines or party lines.
- Avaya Proactive Contact complies with the requirements in Part 15 of FCC Rules. Operation is subject to the following two conditions:
 1. The system must not cause harmful interference.
 2. The system must accept any interference received, including interference that may cause undesired operation.
- Repair work on Avaya Proactive Contact must be done by Avaya Inc. or the Avaya Proactive Contact vendor.

Office of Communication (OFCOM)

The Office of Communication (OFCOM) U.K. releases a statement of policy on the persistent misuse of an electronic communication network or service. This policy applies to predictive dialers that make calls in U.K. For details refer to:

http://www.ofcom.org.uk/consult/condocs/persistent_misuse/statement/

OFCOM specified changes in their Revised statement of policy on the persistent misuse of an electronic communications network or service on October 30, 2009.

The changes in this policy (applicable only to the United Kingdom) are as follows:

http://www.ofcom.org.uk/consult/condocs/persistent_misuse/amendment/amendment.pdf

Editor application has been updated to enable the new OFCOM policy.

 Note:

Hard Dialer with PG230 environment	CTI Dialer/Soft Dialer environment
The OFCOM feature is available only on the Proactive Contact PG230RM dialer. To use the OFCOM feature in Proactive Contact, you might need to configure some parameters in the <code>master.cfg</code> file. To configure these parameters, contact Avaya Professional Services.	The OFCOM feature is available only on the Avaya Proactive Contact PG230RM dialer. This feature is not supported on the Proactive Contact with CTI dialer. The Avaya OFCOM feature is not approved for use in the Proactive Contact CTI Dialer (Soft Dialer). If the OFCOM feature is enabled in the customer's Proactive Contact CTI Dialer (Soft Dialer), it will be subject to the Support Limitations and Exclusions contained in the applicable Service Agreement Supplement, and Avaya will have no obligation to support, diagnose or correct problems caused by or associated with the OFCOM feature.

Answer supervision

Allowing Avaya Proactive Contact to operate in a manner that does not provide proper answer supervision signaling violates FCC Part 68 rules. The system returns answer supervision signals to the Public Switched Telephone Network (PSTN) when:

- The called station answers.
- The attendant answers.
- The system is routed to a recorded announcement that the Customer Premise Equipment (CPE) user can administer.
- The system is routed to a dial prompt.

Avaya Proactive Contact returns answer supervision on all Direct Inward Dialing (DID) calls forwarded back to the PSTN. Permissible exceptions are when:

- The call is unanswered.
- A Busy tone is received.
- A Reorder (Fast Busy) tone is received.

 Note:

FCC regulations are applicable only to the United States. If you are outside the United States, refer to the regulations applicable for your country.

Emergency service support

The Avaya Proactive Contact system will not support the dialing of emergency service numbers in the event of a loss of mains power according to AS/ACIF-038,5.1.2.3.

Industry Canada regulations

Avaya Proactive Contact meets the following requirements established by Industry Canada:

Industry Canada registration

The Industry Canada (IC) label identifies certified equipment. The certificate means that Avaya Proactive Contact meets specific telecommunications network protective, operational, and safety requirements. Industry Canada does not guarantee that Avaya Proactive Contact will operate to user satisfaction. Before installing Avaya Proactive Contact, ensure you are permitted to connect it to the facilities of the local telecommunications company. You must also install the system using an acceptable method of connection. For example, you may extend the company's inside wiring for single line individual service by means of a certified connector assembly (telephone extension cord). You should be aware, however, that compliance with the above conditions might not prevent degradation of service in some situations. For your own protection, ensure that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution might be particularly important in a rural area.

 Caution:

Do not attempt to make electrical ground connections yourself. Contact the appropriate electrical inspection authority or electrician.

IC compliance notice

This digital apparatus does not exceed the Class A limits for radio noise emissions for digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Ringer Equivalence Number (REN): 07

The Ring Equivalence Number (REN) is an indication of the maximum number of devices allowed to be connected to a telephone interface. The termination on the interface may consist of any combination of devices subject only to the requirement that the sum of the RENs of all the devices does not exceed five.

European Union regulations

Avaya Proactive Contact conforms to the following directives established by the European Union:

- Low Voltage Directive
- EMC Directive
- R&TTE Directive

For details, refer to each Declaration of Conformity.

China Regulations

This information is required for all products imported or sold in the People's Republic of China.

Table of toxic substances

The following table shows where you can find the substances in the list of electronic information products of Avaya as of the date of manufacture of the enclosed product. Some of the component types listed may or may not be a part of the enclosed product.

Part Name	Pb	Hg	Cd	Cr	PBB	PBDE
Metal Parts	O	O	O	O	O	O
Circuit Modules	X	O	O	O	O	O
Cables and Cable Assemblies	X	O	O	O	O	O
Plastic and Polymeric Parts	O	O	O	O	O	O
Circuit Switch/Breakers	O	O	O	O	O	O
Power Assemblies	X	O	O	O	O	O

O: SJ/T 11363 2006. Indicates that the concentration of the hazardous substance in all homogeneous materials in the parts is below the relevant threshold of the SJ/T 11363 2006 standard.

X: SJ/T 11363 2006. Indicates that the concentration of the hazardous substance of at least one of all homogeneous materials in the parts is above the relevant threshold of the SJ/T 11363 2006 standard.

Environmentally Friendly Use Period

The Environmentally Friendly Use Period (EFUP) for all enclosed products and their parts are per the symbol shown here, unless otherwise marked. Certain products have a different EFUP (for example, telephones) and so are marked to reflect such. The Environmentally Friendly Use Period is valid only when the product is operated under the conditions defined in the product manual.

Safety instructions

Only service personnel trained to maintain and service the equipment must install and service Avaya Proactive Contact and related components.

Safety precautions

When using Avaya Proactive Contact, follow basic safety precautions to reduce the risk of fire, electric shock, and injury to people. The basic precautions include the following:

- Read and understand all instructions.
- Follow all warnings and instructions marked on the Avaya Proactive Contact hardware.
- Unplug the equipment from the wall outlet before cleaning. Use a damp cloth for cleaning. Do not use liquid cleaners or aerosol cleaners.
- Do not use the equipment near water or in a wet room.
- Do not place the equipment on an unstable cart, stand, or table. The equipment may fall, causing serious damage.
- Slots and openings in the cabinet and the back or bottom provide ventilation (to protect it from overheating). Do not block or cover these openings. Never place the equipment near or over a radiator or heat register. Do not place the equipment in a built-in installation, unless there is proper ventilation.
- Operate this equipment only from the type of power source indicated on the marking label. If you are not sure of the type of power source, ask your Avaya Proactive Contact representative or system vendor.
- This equipment is required to use a three-wire grounding plug, a plug having a third (grounding) pin. This plug only fits into a grounding-type power outlet. This is a safety feature. If you are unable to insert the plug into the outlet, contact your electrician to replace your obsolete outlet. Do not defeat the safety purpose of the grounding-type plug.
- Do not rest anything on the power cord. Do not locate this equipment where the cord will be damaged by people walking on it.
- Do not overload wall outlets and extension cords to avoid the risk of a fire or electric shock.

- Never push objects of any kind into this equipment through the cabinet slots. This action might cause a fire or electric shock by touching dangerous voltage points or shorting of parts. Never spill liquid of any kind on the equipment.
- To reduce the risk of electric shock, do not disassemble this equipment. Contact a qualified service person when service or repair work is required. Opening or removing covers may expose you to dangerous voltages or other risks. Incorrect assembly can cause electric shock when the equipment is subsequently used.
- Unplug this equipment from the wall outlet and refer servicing to qualified service personnel under the following conditions:
 - When the power supply cord or plug is damaged or frayed
 - If liquid has been spilled into the equipment
 - If the equipment has been exposed to rain or water
 - If the equipment does not operate normally by following the operating instructions
 - If the equipment has been dropped or the cabinet has been damaged
 - If the equipment exhibits a distinct change in performance
- Avoid using a telephone (other than a cordless type) during an electrical storm to prevent a risk of electric shock from lightning.
- Do not use the telephone near a gas leak to report the leak.
- Use the same type of attachment-plug receptacles and grounding as used by the equipment or system. Connect the grounding conductors of the equipment to the earth ground.
- Connect the supplementary equipment grounding conductor before connecting any telecommunication lines to the equipment or system.

Warnings and cautions

Read the following sections for instructions on safety:

- Electrical ratings.
- Leakage.
- Grounding.
- Power supply (PG230 and PG230-RM only).
- Circuit protection.
- Telecommunications network.
- Telephone wiring.
- Battery disposal.

Electrical ratings

System type	Rating
Avaya PG230 and PG230-RM	100-240 VAC, 50-60 Hz, 10-4A
Avaya Proactive Contact system cabinet 100 VAC (Japan)	100 VAC, 50-60 Hz, 20A
Avaya Proactive Contact system cabinet 120 VAC	120 VAC, 50-60 Hz, 16A
Avaya Proactive Contact system cabinet 220-240 VAC	220-240 VAC, 50-60 Hz, 8A

Leakage

HIGH LEAKAGE CURRENT, earth connection essential before connecting supply.

Grounding

Warning:

ELECTROSTATIC ALERT: Install a wire to connect the system cabinet to the building earth ground. A protective earthing terminal is located on the rear of the equipment and must be connected to earth. Use a 10 AWG (5.26 mm) ground conductor (green insulated wire with one or more yellow stripes) wire to connect to this terminal. Install according to the applicable national electrical codes.

Power supply (PG230 and PG230-RM only)

Caution:

The power supply cord is the main device for disconnection. Ensure that the socket outlet is located or installed near the equipment and is easily accessible. Use a certified power supply cord suitable for the country of installation. Ensure that the conductors are 16AWG (1.0 mm) or larger.

Circuit protection

Maximum 30A current protection required.

Telecommunications network

Warning:

High Touch Current. Earth connection is essential before making telecommunication network connection.

Telephone wiring

- Use caution when installing or modifying telephone lines.
- Never install telephone wiring during an electrical storm.
- Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
- Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.

- Use 26AWG minimum telephone line cords for connection to the EUTC card.

Battery disposal



Warning:

The ENBC card contains a lithium battery clip. Dispose off this battery according to the national regulations, or return it to the manufacturer for disposal.

Contacting support

To contact your Avaya representative for customer support:

- Call the customer support number provided by your Avaya representative if:
 - You purchased your system from a third-party organization or partner
 - Your installation is not in the United States, Canada, or the United Kingdom
- If your installation is in the United States and Canada, call the following Avaya Inc. support number: (425) 885-7678 or (888) 782-3343
- If your installation is in Europe, the Middle East, or Asia, call the 24-hour support number: +44 (0)1753 727272
- When you call , provide the following information to your customer support representative:
 - Your site name.
 - Your site number.
 - The problem you encountered.
 - Any questions you might have about the problem.

Chapter 6: Security

Port utilization

For information about port utilization, see www.support.avaya.com/security.

Security specification

The following actions ensure that Avaya Proactive Contact is protected against cyber attacks:

- Using Secured Socket Communication Compliance, for example, SSL, SSH, SFTP.
- Discarding packets from outside entities.
- Displaying login details.
- Logging.
- Using Client-Server authentication, for example, SSL certificates, encrypted key generation.
- Practicing secured installation, upgrade and removal of product.
- Validating port matrix.
- Using enhanced password and lockout functionality.
- Restricting users as per the roles assigned.
- Restricting undocumented users.
- Ensuring that backup copies of files have permissions and format that is no less restrictive or secure than the original file.
- Ensuring database security with authentication.
- Preventing high privilege level login.
- Ensuring logon banner display for unauthorized access.
- Ensuring secured, authenticated, encrypted, with integrity, method of product or feature activation.
- Complying to SNMPv3 and SNMPv2.
- Denying service attacks.

- Performing virus scanning.
- Performing vulnerability analysis by Nessus scan or by an equivalent security scanning software.
- Using Enhanced Access Security Gateway (EASG) provides secure authentication and auditing of all remote access into the maintenance ports.

Chapter 7: Licensing requirements

Licensing requirements

The Avaya Product Licensing and Delivery System (PLDS) provides customers, Avaya Partners, distributors, and Avaya Associates with tools for managing license entitlements and electronic delivery of software and related license files. Using PLDS, you can perform operations such as license activations, license upgrades, license moves, and software downloads.

Installation software packages for Avaya products are available as ISO files on PLDS. Users can download the ISO images to a system, and choose to either burn a DVD for installation or transfer the ISO file to the target server for installation. You can check PLDS to determine if a later service pack or software release is available. If updates exist, see the appropriate upgrade procedures, or contact Avaya, or contact the Avaya Partner Service representative.

When you place an order for a PLDS-licensed software product, the license entitlements on the order are automatically created in PLDS. Once these license entitlements are created, you receive an e-mail notification from PLDS. This e-mail notification includes a License Activation Code (LAC). Using the LAC, you can quickly find and activate the newly purchased license entitlements in PLDS. You can then download the license file.

Important:

You must provide the WebLM host ID to activate the license file in PLDS. The primary WebLM host ID is the MAC address of a physical network interface card (NIC) on the server. You can view the WebLM host ID in the WebLM Server Properties page.

Examples of license management tasks that you can perform in PLDS include:

- Adding more license entitlements to an existing activation.
- Upgrading a license file to a new major release.
- Moving license entitlement activations between license hosts.
- Regenerating a license file with a new host ID.

Chapter 8: Resources

Documentation

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

Title	Description	Audience
<i>Using Avaya Proactive Contact Agent</i>	Provides detailed description of Avaya Proactive Contact Agent.	Agents of contact centers and end users.
<i>Using Avaya Proactive Contact Supervisor</i>	Provides detailed description of the Avaya Proactive Contact Supervisor suite of applications.	Supervisors of contact centers and end users.
<i>Planning for Avaya Proactive Contact</i>	Provides detailed description of the planning process of Avaya Proactive Contact.	Sales engineers, Avaya Professional Services, and design engineers.
<i>Maintaining and Troubleshooting Avaya Proactive Contact</i>	Provides detailed information about hardware and software maintenance of Avaya Proactive Contact.	Avaya Professional Services and business partners.
<i>Avaya Proactive Contact Safety and Regulatory Information</i>	Provides information about safety regulations.	Avaya Professional Services and end users.
<i>Administering Avaya Proactive Contact</i>	Provides detailed information about the operation of the Avaya Proactive Contact system through a Linux-based menu.	Administrators, design engineers, and business partners.

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

The following courses are available on the Avaya Learning website at www.avaya-learning.com. Enter the course code in the **Search** field, and click **Go** to search for the course.

Course code	Course title
1C00010W	What's New with Proactive Contact 5.2
AVA00989H00	Avaya Proactive Contact 5.0 Basic System Supervisor
AVA00990H00	Avaya Proactive Contact 5.0 Advanced System Supervisor
AVA01013WEN	Avaya Proactive Contact Solutions 5.0 Overview - Assessment

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.

- To find videos on the Avaya Support website, go to <http://support.avaya.com> and perform one of the following actions:
 - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
 - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.

- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
 - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
 - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

 Note:

Videos are not available for all products.

Support

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

Glossary

Access Security Gateway	An authentication interface that protects the system administration, maintenance ports, and logins associated with Avaya Aura®.
Agent Blending	Agent Blending is a tool that integrates outbound calling activities on your Avaya Proactive Contact system with inbound calling activities on your ACD.
Analyst	Avaya Proactive Contact Analyst generates call management reports with job, agent, and system details based on the activities of Avaya Proactive Contact.
Application Enablement Services (AES)	A set of enhanced telephony APIs, protocols, and web services that are available to developers. These capabilities support access to the powerful call processing, media, and administrative features available in Communication Manager.
Automatic Call Distribution	A programmable feature at the contact center. Automatic Call Distribution (ACD) handles and routes voice communications to queues and available agents. ACD also provides management information that can be used to determine the operational efficiency of the contact center.
Avaya Aura®	A converged communications platform unifying media, modes, network, devices, applications. Avaya Aura® is based on the SIP architecture with Session Manager at the core.
Avaya Interactive Response	A powerful voice-response system that may include automated call routing, announcement storage, message retrieval, and callback. Avaya Interactive Response was formerly called CONVERSANT®.
Health Manager	Using the Health Manager application, you can start and stop only the Mid-Tier all services.
Hierarchy Manager	Hierarchy Manager is a tool that helps you group and organize data.
Jobs	A job contains all the information that Avaya Proactive Contact needs to place phone calls to customers. A job integrates a calling list, phone strategy, record selection, and other settings to place outbound calls and receive inbound calls.

Monitor	Using the Monitor application, you can monitor real-time calling activities in Avaya Proactive Contact, and also specify how to view real-time calling activities.
PC Analysis Telnet	PC Analysis Telnet is a tool that helps you to access the Linux-based PC Analysis menus.
Role Editor	Using Role Editor you can create and manage users and tenants, create roles, and assign users to appropriate roles.
Schedule	The Schedule feature provides the flexibility to automatically schedule activities, create a new dialer activity, and view schedule reports. Avaya Proactive Contact provides the ability to define and manage schedules.
Supervisor	Using Avaya Proactive Contact Supervisor, you can perform system monitoring and reporting of real-time and historical operations.

Index

A

ACP	30
administrator console	
data connectivity	31
specifications	31
table placement	31
agent blending	
displaying notification message	16
Agent Monitor	
display warning for unsuccessful agent transfers	13
agent workstation	
supported operating system	33
agent workstations	
hardware requirements	29
answer supervision	53
audience	63
Avaya PG230RM system cabinet	48 , 49
Avayatized RHEL	
support for 6.9 version	15

B

Battery disposal	59
browser	
interoperability	35

C

capacity	38
China	55
Circuit protection	58
client applications	
maximum password length	14
collect_logs	14
config_debug	14
configure	
password lockout attempts	13
configuring	
Answer Supervision by job	16
strong ciphers	17

D

database client connector	36
databases	
support	36
de_reject process	
handling of cancelled records	13
deployment	
virtualized server	17
discretionary activities	45

displaying notification message	
outbound job	16
display warning	
unsuccessful agent transfers	13
documentation	63

E

EASG	
overview	20
Enhanced Access Security Gateway	20
enhancement	
Batch Campaign Update	13
BCU	13
de_reject process	13
enhancements	
Agent Monitor	13
environmental checklist	48
Environmentally Friendly Use Period	56
environmental specifications	49
external syslog server	
logging	16

F

features	21
features 5.1.2	
accepting double-digit reason codes	15
Agent Monitor enhancement	13
Answer Supervision by job	16
BCU enhancement	13
browsers supported for IMON	17
configurable lockouts	13
de_reject process enhancement	13
displaying notification message	16
external syslog server support	16
Java, WebLM and Tomcat upgrades	14
log customization	14
manual dialing	14
maximum password length	14
music on hold	17
number of time zones supported increased to 150	14
OFCOM-72 hour rule compliance enhancement	15
passing called party number for opt out calls to VDN	17
shadow jobs in the preview mode	17
strong ciphers	17
support for windows 8.1	18
VIRT_PORT_TIMEOUT value reduced to 10 minutes	15
virtualized server	17
zip to zone	16
features 5.2	
Avayatized RHEL 6.9 version supported	15
features list	23

G

get_info	14
grounding	58

H

hardware requirements	
agent workstations	29
supervisor workstations	28

I

IMON	
support for Firefox 31	17
support for Firefox 34	17
support for Internet Explorer 10	17
support for Internet Explorer 11	17
increase number of time zones	
150	14
interoperability	28
browser	35

J

java	
support	37
Java upgrade to 7.x	14

L

languages supported, supported languages	12
logging	
customization	14
external syslog server	16

M

maximum password length	
client applications	14
mode	
manual dialing	14
Multitenancy	18

N

network	
telecommunications	58
new in this release	11
New in this release	
CSR3	16
HP DL 360p G9	16
non-discretionary activities	45
not supported	
Windows XP	18

O

office of communication	53
Opt-out to VDN	
TRANSID feature	17
out of time zone phone support	19

P

ports	60
power supply PG230 and PG230-RM	58
preview mode	
shadow jobs	17
Proactive Contact	
hardware requirements	30

R

regulation Federal Communications Commission	51
regulations	55
related resources	63

S

safety and regulatory	50
server	
supported operating system	32
soft dialer	
accepting double-digit reason codes	15
Supervisor suite	45
supervisor workstation	
supported operating system	32
supervisor workstations	
hardware requirements	28
support	65
acceptance of double-digit reason codes	15
Avayitized RHEL 6.9 version	15
databases	36
external syslog server	16
java	37
music on hold	17
passing called party number for opt out calls to VDN ...	17
passing numeric calling list fieldname for opt out calls to VDN	17
tomcat	37
virtualized server	17
VMWare versions	36
WebLM	37
Windows 8.1	18
supported operating system	
agent workstation	33
supported operating systems	
server	32
supervisor workstation	32

T

table of toxic substances	55
time zone dertermination	
zip code	16
tomcat	
support	37
Tomcat upgrade to 7.x	14
traffic	45
Traffic Estimator Tool	45
training	64

V

value	38
videos	64
VIRT_PORT_TIMEOUT	
value reduced to 10 minutes	15
VMWare versions	
support	36

W

WebLM	
support	37
WebLM upgrade to 6.x	14
wiring	
telephone	58