



Avaya Contact Recorder
Release 12.0
Planning, Installation and
Administration Guide

Issue 3
March 2013

Confidential & Proprietary
Information

© 2003 - 2013 Verint Systems Inc. All Rights Reserved. THIS AVAYA PRODUCT ('Product') CONTAINS CONFIDENTIAL AND PROPRIETARY INFORMATION OF VERINT SYSTEMS INC. OR ITS SUBSIDIARIES. USE OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE AT <http://support.avaya.com/LicenseInfo/>, including the following AVAYA GLOBAL SOFTWARE LICENSE TERMS (or "Software License Terms"); AVAYA GLOBAL SOFTWARE LICENSE TERMS REVISED: OCTOBER 2010

THIS END USER LICENSE AGREEMENT ("SOFTWARE LICENSE TERMS") GOVERNS THE USE OF AVAYA'S PROPRIETARY SOFTWARE AND THIRD-PARTY PROPRIETARY SOFTWARE. READ THESE SOFTWARE LICENSE TERMS CAREFULLY, IN THEIR ENTIRETY, BEFORE INSTALLING, DOWNLOADING OR USING THE AVAYA SOFTWARE (AS DEFINED BELOW). BY INSTALLING, DOWNLOADING OR USING THE AVAYA 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"). IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE SOFTWARE LICENSE TERMS. ANY USE OF THE SOFTWARE WILL CONSTITUTE YOUR ASSENT TO THESE SOFTWARE LICENSE TERMS (OR RATIFICATION OF PREVIOUS CONSENT). IF YOU DO NOT HAVE SUCH AUTHORITY OR DO NOT WISH TO BE BOUND BY THESE SOFTWARE LICENSE TERMS, YOU MUST RETURN OR DELETE THE SOFTWARE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OF THE FEE, IF ANY, YOU PAID FOR THE LICENSE OR IF SOFTWARE IS ACCESSED ELECTRONICALLY, SELECT THE "DECLINE" BUTTON AT THE END OF THESE SOFTWARE LICENSE TERMS.

A. Scope. These Software License Terms are applicable to anyone who downloads and/or installs Avaya Software and Documentation, purchased from Avaya Inc., any Avaya Affiliate, or an authorized Avaya reseller (as applicable) under a commercial agreement with Avaya or an authorized Avaya reseller ("Agreement"). Unless otherwise agreed to by Avaya in writing, Avaya does not extend this license if the Software was obtained from anyone other than Avaya, an Avaya Affiliate or an Avaya authorized reseller, and Avaya reserves the right to take legal action against you and anyone else using or selling the Software without a license. To the extent there is a conflict between these Software License Terms and another Agreement, the order of precedence shall be (i) your Agreement with Avaya if you purchased from Avaya Inc. or an Avaya Affiliate, or (ii) these Software License Terms if you purchased from an authorized Avaya reseller, except with respect to third party elements subject to a Shrinkwrap License or other Third Party Terms, in which case the Shrinkwrap License or other Third Party Terms will prevail. "Affiliate" means any entity that is directly or indirectly controlling, controlled by, or under common control with Avaya Inc. or End User. For purposes of this definition, "control" means the power to direct the management and policies of such party, directly or indirectly, whether through ownership of voting securities, by contract or otherwise; and the terms "controlling" and "controlled" have meanings correlative to the foregoing.

B. License Grant. Avaya grants you a personal, non-sublicensable, non-exclusive, non-transferable license to use Software and Documentation obtained from Avaya or an Avaya authorized reseller and for which applicable fees have been paid for your internal business purposes at the indicated capacity and features and within the scope of the applicable license types described below and at locations where the Software is initially installed. "Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Software installed on mobile-devices, such as a laptop or mobile phone, may be used outside of the country where the software was originally installed, provided that such use is on a temporary basis only.

(i) Right to Move License Entitlements. Notwithstanding the foregoing, You may move right to use license entitlements (RTU's) from one location to another in accordance with Avaya's then-current software license move policy for that Software ("License Portability Policy") which is available upon request subject to the following conditions:

(a) You shall provide written notice within ten (10) days to Avaya of any RTU moves including but not limited to, the number and type of licenses moved, the location of the original Server and the location of the new Server, the date of such RTU moves and any other information that Avaya may reasonably request;

(b) You may only move RTU's to and from Designated Processors or Servers supporting the same Software application;

(c) You must reduce the quantity of the licenses on the original Server by the number of RTU's being moved to the new Server.

(d) You acknowledge that (1) you may be charged additional fees when moving RTU's as per Avaya's then-current License Portability Policy, (2) maintenance services do not cover system errors caused by moves not performed by Avaya, (3) you are responsible for any programming, administration, design assurance, translation or other activity to make sure the Software will scale and perform as specified as a result of any license moves, and if any such transfer results in a requirement for Avaya system engineering or requires the use of on-site Avaya personnel, you will be charged the Time & Materials fees for such activity;

(e) If your maintenance coverage differs on licenses on the same product instance at the location of the new Server, Service updates, recasts and/or fees may apply and any fee adjustments for differences in coverage will only be made on a going forward basis as of the date Avaya receives notice of the RTU move; and

(f) You may move RTU's from one Affiliate to another Affiliate provided that you comply with all of the conditions of this section, including, without limitation, providing the name and address of the new Affiliate in your written notice under subpart (a) above, and such new Affiliate shall be bound by these Software License Terms.

(ii) Non-Production License Grant. With respect to Software distributed by Avaya to you for non-production purposes, Avaya grants to you, subject to the terms and conditions contained herein, a personal, nonexclusive, nontransferable and non-sublicensable right to use the Software in a non-production environment solely for testing, development or other non-commercial purposes on a single computer ("Non-Production License").

C. All Rights Reserved. Except for the limited license rights expressly granted in these Software License Terms, Avaya reserves all rights in and to the Software and Documentation and any modifications or copies thereto.

D. General License Restrictions. To the extent permissible under applicable law, you agree not to: (i) decompile, disassemble, or reverse engineer the Software; (ii) alter, modify or create any derivative works based on the Software or Documentation; (iii) use, copy, sell, sublicense, lease, rent, loan, assign, convey or otherwise transfer the Software or Documentation except as expressly authorized by the Agreement with a Avaya; (iv) distribute, disclose or allow use of the Software or Documentation, in any format, through any timesharing service, service bureau, network or by any other means; (v) allow any service provider or other third party, with the exception of Avaya's authorized resellers and their designated employees ("Authorized Providers") who are acting solely on behalf of and for the benefit of End User, to use or execute any software commands that cause the Software to perform functions that facilitate the maintenance or repair of any product except that a service provider or other third party may execute those software commands that, as designed by Avaya, would operate if a user is logged into a product using a customer level login and Maintenance Software Permissions ("MSPs") were not enabled or activated; (vi) gain access to or the use of any Software or part thereof without authorization from Avaya; (vii) enable or activate, or cause, permit or allow others to enable or activate any logins reserved for use by Avaya or Authorized Providers; or (viii) permit or encourage any third party to do so. You shall provide Authorized Providers the terms and provisions of this Agreement and shall obligate Authorized Providers to comply with such terms and provisions. End User shall be responsible for any third party's failure to comply and shall indemnify Avaya for any damages, loss, expenses or costs, including attorneys' fees and costs of suit, incurred by Avaya as a result of non-compliance with this section. Notwithstanding the foregoing, if the Software is rightfully located in a member state of the European Union and End User needs information about the Software in order to achieve interoperability of an independently created software program with the Software, End User will first request such information from Avaya. Avaya may charge End User a reasonable fee for the provision of such information. If Avaya refuses to make such information available, then End User may take steps, such as reverse assembly or reverse compilation, to the extent necessary solely in order to achieve interoperability of the Software with an independently created software program. To the extent that the End User is expressly permitted by applicable mandatory law to undertake any of the activities listed in this section End User will not exercise those rights until End User has given Avaya twenty (20) days written notice of its intent to exercise any such rights.

E. Backup Copies. End User may create a reasonable number of archival and backup copies of the Software and the Documentation, provided all proprietary rights notices, names and logos of Avaya and its suppliers are duplicated on each copy.

F. Warranty. Avaya provides a limited warranty on its Software. Avaya's standard warranty language as well as information regarding support while under warranty, is available through the following website: <http://support.avaya.com>. Please note that if you are acquiring the Software from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. EXCEPT AS REFERENCED HEREIN, THE SOFTWARE IS PROVIDED "AS IS" AND NEITHER AVAYA NOR ITS SUPPLIERS MAKES ANY EXPRESS REPRESENTATIONS OR WARRANTIES WITH REGARD TO ANY PRODUCTS OR SERVICES OR OTHERWISE RELATED TO THE AGREEMENT OR SOFTWARE LICENSE TERMS. AVAYA DOES NOT WARRANT UNINTERRUPTED OR ERROR FREE

OPERATION OF PRODUCTS. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, AVAYA DISCLAIMS ALL WARRANTIES IMPLIED OR STATUTORY, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.

G. Compliance. Avaya will have the right to inspect End User's compliance with these Software License Terms.

H. Termination of License. If you breach the license limitations or restrictions in these Software License Terms and if within ten (10) business days of your receipt of a reasonably detailed written request to cure, you have not cured all breaches of license limitations or restrictions, Avaya may, with immediate effect, terminate the Software licenses granted in these Software License Terms without prejudice to any available rights and remedies. Upon termination or expiration of the license for any reason, you shall immediately return the Software and any copies to Avaya, or, at Avaya's discretion and written notice to you, you shall permanently destroy all copies of the Software and any related materials in your possession or control. Inadvertent copies of the Software and any related materials remaining in the possession of the End User subsequent to termination or expiration shall not be implied or construed as Avaya consenting to transfer ownership of the Software and any related materials to the End User. The provisions concerning confidentiality, indemnity, license restrictions, export control, and all limitations of liability and disclaimers and restrictions of warranty (as well as any other terms which, by their nature, are intended to survive termination) will survive any termination or expiration of the Software License Terms.

I. License Types. Avaya grants you a license within the scope of the license types described 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. "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. "Software" means the computer programs in object code, originally provided by Avaya and ultimately utilized by you, whether as stand-alone products or pre-installed on hardware products, originally sold by Avaya and ultimately utilized by you.

Designated System(s) License (DS). End User may install and use each copy 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, 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.

Database License (DL). End User may install and use each copy of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than a single instance of the same database.

CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User," means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

J. Third-party Components. Certain software programs or portions thereof included in the Software may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Software ("Third Party Terms"). Information

identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya's website at: <http://support.avaya.com/Copyright>.

K. Limitation of Liability. EXCEPT FOR PERSONAL INJURY CLAIMS, WILLFUL MISCONDUCT AND END USER'S VIOLATION OF AVAYA'S OR ITS SUPPLIERS INTELLECTUAL PROPERTY RIGHTS, INCLUDING THROUGH A BREACH OF THE SOFTWARE LICENSE TERMS AND TO THE EXTENT PERMITTED UNDER APPLICABLE LAW, NEITHER AVAYA OR ITS SUPPLIERS NOR END USER SHALL BE LIABLE FOR (i) ANY INCIDENTAL, SPECIAL, STATUTORY, INDIRECT OR CONSEQUENTIAL DAMAGES, OR (ii) FOR ANY LOSS OF PROFITS, REVENUE, OR DATA, TOLL FRAUD, OR COST OF COVER AND (iii) DIRECT DAMAGES ARISING UNDER THESE SOFTWARE LICENSE TERMS IN EXCESS OF THE PURCHASE PRICE AND FEES PAID FOR THE PRODUCTS OR SERVICES GIVING RISE TO THE CLAIM.

L. Protection of Confidential Software and Documentation. End User acknowledges that the Software and Documentation are regarded as confidential information by Avaya and its suppliers, ("Confidential Information") and End User agrees at all times to protect and preserve in strict confidence the Software and Documentation.

M. Protection of Personal Data. The use of the Software may require the processing of personal data pertaining to you or to your personnel. Personal data required to use the Software will need to be submitted to Avaya. Failing the submission of such data, the use of the Software will not be possible. You or your personnel have a right to access and correct erroneous personal data pertaining to you or your personnel and to object for legitimate reasons to the processing and transfer of these data. You can exercise this right by contacting in writing the Data Privacy Officer of the applicable Avaya Affiliate.

N. High Risk Activities. The Software is not fault-tolerant and is not designed, manufactured or intended for any use in any environment that requires fail-safe performance in which the failure of the Software could lead to death, personal injury or significant property damage ("High Risk Activities"). Such environments include, among others, control systems in a nuclear, chemical, biological or other hazardous facility, aircraft navigation and communications, air traffic control, and life support systems in a healthcare facility. End User assumes the risks for its use of the Software in any such High Risk Activities.

O. Export Control. End User is advised that the Software is of U.S. origin and subject to the U.S. Export Administration Regulations (EAR). The Software also may be subject to applicable local laws and regulations. Diversion contrary to U.S. and applicable local country law and regulation is prohibited. You agree not to directly or indirectly export, re-export, import, download, or transmit the Software to any country, end user or for any use that is prohibited by applicable U.S. and local country regulation or statute (including but not limited to those countries embargoed by the U.S. government). You represent that neither the U.S. Bureau of Industry and Security (BIS) nor any other governmental agency has issued sanctions against End User or otherwise suspended, revoked or denied End User's export privileges. You agree not to use or transfer the Software for any use relating to nuclear, chemical or biological weapons, or missile technology, unless authorized by the U.S. and applicable local government by regulation or specific written license. Additionally, you are advised that the Software may contain encryption algorithm or source code that may be limited for export to government or military end users without a license issued by the U.S. BIS and any other country's governmental agencies, where applicable. Lastly, you agree not to directly or indirectly export, reexport, import, or transmit the Software contrary to the laws or regulations of any other governmental entity that has jurisdiction over such export, import, transmission, or use.

P. U.S Government End Users. The Software is classified as "commercial computer software" and the Documentation is classified as "commercial computer software documentation" or "commercial items," pursuant to FAR 12.212 or DFAR 227.7202, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software or Documentation by the Government of the United States shall be governed solely by the terms of these Software License Terms and shall be prohibited except to the extent expressly permitted by the terms of these Software License Terms.

Q. Acknowledgement. End User acknowledges that certain Software may contain programming that: (i) restricts, limits and/or disables access to certain features, functionality or capacity of such Software subject to the End User making payment for licenses to such features, functionality or capacity; or (ii) periodically deletes or archives data generated by use of the Software and stored on the applicable storage device if not backed up on an alternative storage medium after a certain period of time.

R. Miscellaneous. These Software License Terms will be governed by New York State laws, excluding conflict of law principles and the United Nations Convention on Contracts for the International Sale of Goods. If a dispute cannot be settled by good faith negotiation between the parties within a reasonable period of time, and to the extent authorized by applicable law, it must be finally settled upon request of either party by arbitration to be held in accordance with the Rules of Arbitration of the International Chamber of Commerce by a single arbitrator appointed by the parties or (failing agreement) by an arbitrator appointed by the President of the International Chamber of Commerce (from time to time). The arbitration will be conducted in the English language, at a location

agreed by the parties or (failing agreement) ordered by the arbitrator. The arbitrator will have authority only to award compensatory damages and will not award punitive or exemplary damages. The arbitrator will not have the authority to limit, expand or otherwise modify the Software License Terms. The ruling by the arbitrator will be final and binding on the parties and may be entered in any court having jurisdiction. Avaya and you will each bear its own attorneys' fees associated with the arbitration. Notwithstanding the foregoing, Avaya shall be entitled to take immediate legal action where required to protect its confidential or proprietary information, or to obtain any interim injunction. If any provision of these Software License Terms is determined to be unenforceable or invalid, these Software License Terms will not be rendered unenforceable or invalid as a whole, and the provision will be changed and interpreted so as to best accomplish the objectives of the original provision within the limits of applicable law. The failure to assert any rights under the Software License Terms, including, but not limited to, the right to terminate in the event of breach or default, will not be deemed to constitute a waiver of the right to enforce each and every provision of the Software License Terms in accordance with their terms. If you move any Software, and as a result of such move, a jurisdiction imposes a duty, tax, levy or fee (including withholding taxes, fees, customs or other duties for the import and export of any such Software), then you are solely liable for, and agree to pay, any such duty, taxes, levy or other fees.

S. Agreement in English. The parties confirm that it is their wish that these Software License Terms, as well as all other documents relating hereto, including all notices, have been and shall be drawn up in the English language only. Les parties aux présentes confirment leur volonté que cette convention, de même que tous les documents, y compris tout avis, qui s'y rattachent, soient rédigés en langue anglaise. Las partes ratifican que es su voluntad que este Contrato, así como cualquier otro documento relacionado con el mismo, incluyendo todo tipo de notificaciones, han sido redactados y deberán continuar siendo redactados únicamente en el idioma inglés.

AVAYA RESERVES THE RIGHT TO MODIFY, SUPPLEMENT OR REPLACE ITS AVAYA GLOBAL SOFTWARE LICENSE TERMS, EFFECTIVE UPON POSTING AT <http://support.avaya.com/LicenseInfo/> OR NOTIFYING YOU OTHERWISE. YOU ACKNOWLEDGE AND AGREE THAT IT IS YOUR OBLIGATION TO REGULARLY VISIT THE AFOREMENTIONED WEBSITE AND TO CHECK FOR ANY UPDATED INCLUDING CHANGES TO THE TERMS HEREIN AND/OR AVAILABLE ON THE ABOVE REFERENCE WEBSITE, INCLUDING UPDATED CHANGES TO THE AVAYA GLOBAL SOFTWARE LICENSE TERMS .

IN THE EVENT OF ANY CONFLICT OR INCONSISTENCY BETWEEN THE TERMS SET FORTH HEREIN AND ANY WRITTEN AGREEMENT WITH AVAYA AND/OR AVAYA EULA, THE TERMS OF SUCH EITHER WRITTEN AGREEMENT WITH AVAYA AND/OR AVAYA EULA SHALL GOVERN. IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT. Avaya grants End User a license within the scope of the license types described below. 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 End User. 'Software' means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. 'Hardware' means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User. License Type(s): "Channel" means a physical connection between or logical address associated with a recording device and an audio source. "Enterprise" means a license to use, without limitation on the number of copies or users applicable to that End User, that Software within that End User's technical environment in conjunction with other Software licensed. "Seat" means the number of uniquely identified work-stations (i) on which the Software is licensed to be installed, (ii) from or to which the Software will send or receive data, or (iii) about which the Software generates data. Any one or more of the foregoing, in the aggregate, applicable to a work-station shall qualify that work-station as a licensed Seat. Seat licenses are not concurrent, except that licenses relating to a work-station may be transferred to another work-station so long as such transfer is on a permanent basis. "Server" means a license to install the Software on a single central computer server. "Site" means a license to use the Software at a physical End User location, without limitation on the number of copies or users applicable to that physical End User location.

Copyright:

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party Components: This computer program is protected by U.S. and international copyright laws, patent laws, and other intellectual property laws and treaties. Unauthorized use, duplication, publication and distribution of all or any portion of this computer program are expressly prohibited and will be prosecuted to the maximum extent provided by law. Your rights in this computer program are limited to the license rights granted under the license agreement executed by you in

hardcopy form (or if none, by acceptance of the clickwrap terms included with this computer program). If needed, please contact your vendor for an additional copy of those terms. All other rights, title and interest are expressly restricted and retained by Verint Systems, Inc. and its licensors. Certain open source applications ("Open Source") may be included with this computer program. For specific ownership information and license rights relating to those open source applications, please see the "Free and Open Source Licensing Information" guide ("Guide") provided with your computer program, or contact your vendor for a copy of that Guide. A license in each Open Source software application is provided to you in accordance with the specific license terms specified in the Guide. EXCEPT WITH REGARD TO ANY WARRANTIES OR OTHER RIGHTS AND OBLIGATIONS EXPRESSLY PROVIDED DIRECTLY TO YOU FROM VERINT, ALL OPEN SOURCE SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OWNERS OF THE OPEN SOURCE SOFTWARE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THE OPEN SOURCE SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. Certain other software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them is available on Avaya's web site at: <http://support.avaya.com/ThirdPartyLicense/>. In addition, this product may contain the ReportNet application from Cognos Corporation. If so, you are granted a limited for use: (i) by an unlimited number of "Anonymous Users" to set personal preferences, view, run, schedule and output reports, subscribe to scheduled reports, create and manage personal folders, and personalize standard reports, and (ii) by one "Named User" (unless otherwise specified on this Order) to, in addition to the rights of an Anonymous User, use the Query Studio module.

Avaya 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. Suspected security vulnerabilities with Avaya Products should be reported to Avaya by sending mail to: securityalerts@avaya.com

Trademarks:

Avaya and the Avaya Logo are trademarks of Avaya Inc. and are registered in the United States and/or other countries. Avaya may also have trademark rights in other terms used herein. References to Avaya include the Nortel Enterprise business, which was acquired as of December 18, 2009.

All trademarks identified by ®, TM or SM are registered marks, trademarks, and service marks, respectively, of Avaya Inc. or the property of their respective owners.

Patents: The Verint Systems Inc. products are protected by one or more of the following U.S., European or International Patents: USPN 5,659,768; USPN 5,790,798; USPN 6,278,978; USPN 6,370,574; USPN 6,404,857; USPN 6,510,220; USPN 6,724,887; USPN 6,751,297; USPN 6,757,361; USPN 6,782,093; USPN 6,952,732; USPN 6,959,078; USPN 6,959,405; USPN 7,047,296; USPN 7,149,788; USPN 7,155,399; USPN 7,203,285; USPN 7,216,162; USPN 7,219,138; USPN 7,254,546; USPN 7,281,173; USPN 7,284,049; USPN 7,325,190; USPN 7,376,735; USPN 7,424,715; USPN 7,424,718; USPN 7,466,816; USPN 7,478,051; USPN 7,558,322; USPN 7,570,755; USPN 7,574,000; USPN 7,587,041; USPN 7,613,290; USPN 7,633,930; USPN 7,634,422; USPN 7,650,293; USPN 7,660,307; USPN 7,660,406; USPN 7,660,407; USPN 7,672,746; USPN 7,680,264; USPN 7,701,972; USPN 7,734,783; USPN 7,752,043; USPN 7,752,508; USPN 7,769,176; USPN 7,774,854; USPN 7,787,974; USPN 7,788,286; USPN 7,792,278; USPN 7,792,671; USPN 7,801,055; USPN 7,817,795; USPN 7,822,018; USPN 7,826,608; USPN 7,836,171; USPN 7,848,524; USPN 7,853,006; USPN 7,852,994; USPN 7,853,800; USPN 7,853,753; USPN 7,864,946; USPN 7,873,156; USPN 7,881,216; USPN 7,881,471; USPN 7,882,212; USPN 7,882,217; USPN 7,885,813; USPN 7,899,178; USPN 7,899,180; USPN 7,899,176; USPN 7,904,481; USPN 7,903,568; USPN 7,904,325; USPN 7,907,142; USPN 7,913,063; USPN 7,920,482; USPN 7,925,889; USPN 7,930,314; USPN 7,949,552; USPN 7,953,621; USPN 7,953,719; USPN 7,953,750; USPN 7,965,828; USPN 7,966,397; USPN 7,991,613; USPN 7,995,612; USPN 8,000,465; USPN 8,005,676; USPN 8,015,042; USPN 8,050,923; USPN 8,059,154; USPN 8,068,602; USPN 8,078,486; USPN 8,090,204; USPN 8,102,976; USPN 8,108,237; USPN 8,112,298; USPN 8,112,306; USPN 8,117,064; USPN 8,126,134; USPN 8,130,926; USPN 8,130,938; USPN 8,131,578; USPN 8,132,089; USPN 8,139,741; USPN 8,155,275; USPN 8,160,156; USPN 8,160,233; USPN 8,170,184; USPN 8,189,763; USPN 8,195,459; USPN 8,199,886; USPN 8,200,022; USPN 8,204,053; USPN 8,204,056; USPN

8,224,028; USPN 8,238,915; USPN 8,249,413; USPN 8,254,262; USPN 8,258,945; USPN 8,275,944; USPN 8,280,011; USPN 8,285,833; USPN 8,290,469; USPN 8,290,871; USPN D606,983; USPN RE40,634; USPN RE41,534; USPN RE41,608; USPN RE43,183; USPN RE43,255; RE43,324; RE43,386; AU 2003214926; CA 2,474,735; CA 2,563,960; CA 2,564,127; CA 2,564,760; CA 2,564,798; CA 2,565,822; CA 2,567,232; CA 2,574,546; CA 2,600,378; CA 2,600,579; CA 2,623,178; CA 2,623,315; CA 2,627,060; CA 2,627,064; CA 2,628,553; EP 1096382; EP 1248449; EP 1530865; EP 1284077; EP 2020812; DE 1284077; FR 1284077; DE 833489; FR 833489; GB 833489; GB 2374249; IE 84821; IE 85519; IL 135324; IL 150856; IL 135324; NZ 534642; and other provisional rights from one or more of the following Published U.S. Patent Applications: US 10/633,357; US 11/166,630; US 11/359,195; US 11/359,357; US 11/361,208; US 11/394,408; US 11/394,410; US 11/479,267; US 11/540,320; US 11/567,808; US 11/621,134; US 11/693,828; US 11/693,923; US 11/712,933; US 11/723,010; US 11/742,733; US 11/752,458; US 11/824,980; US 11/831,250; US 11/831,257; US 11/831,260; US 11/844,759; US 11/937,553; US 11/959,650; US 11/968,428; US 12/015,375; US 12/015,621; US 12/057,442; US 12/057,476; US 12/118,789; US 12/118,792; US 12/164,480; US 12/245,781; US 12/416,906; US 12/464,694; US 12/466,673; US 12/483,075; US 12/497,799; US 12/504,492; US 12/539,640; US 12/608,474; US 12/628,089; US 12/630,030; US 12/684,027; US 12/686,213; US 12/708,558; US 12/725,127; US 12/762,402; US 12/768,194; US 12/792,796; US 12/840,227; US 12/852,144; US 12/879,868; US 12/887,059; US 12/887,089; US 12/888,445; US 12/891,620; US 12/915,868; US 12/915,941; US 12/916,006; US 12/940,508; US 12/942,111; US 12/964,891; US 13/005,996; US 13/008,283; US 13/011,870; US 13/011,871; US 13/016,998; US 13/036,923; US 13/096,145; US 13/096,148; US 13/096,153; US 13/114,620; US 13/149,655; US 13/155,343; US 13/182,672; US 13/187,438; US 13/189,514; US 13/232,526; US 13/244,462; US 13/253,935; US 13/283,507; US 13/283,532; US 13/284,498; US 13/299,805; US 13/312,410; US 13/315,703; US 13/323,240; US 13/354,919; US 13/355,112; US 13/358,476; US 13/358,477; US 13/358,482; US 13/358,485; US 13/370,073; US 13/406,506; US 13/446,338; US 13/457,373; US 13/457,377; US 13/464,662; US 13/474,761; US 13/550,859; US 13/557,359; US 13/557,365; US 13/567,730; US 13/589,611; US 13/592,972; US 13/606,322; US 13/609,904; US 13/611,912; US 13/622,611; and other U.S. and International Patents and Patents Pending.

VERINT, the VERINT logo, ACTIONABLE INTELLIGENCE, POWERING ACTIONABLE INTELLIGENCE, INTELLIGENCE IN ACTION, ACTIONABLE INTELLIGENCE FOR A SMARTER WORKFORCE, VERINT VERIFIED, WITNESS ACTIONABLE SOLUTIONS, STAR-GATE, RELIANT, VANTAGE, X-TRACT, NEXTIVA, EDGEVR, ULTRA, AUDIOLOG, WITNESS, the WITNESS logo, IMPACT 360, the IMPACT 360 logo, IMPROVE EVERYTHING, EQUALITY, CONTACTSTORE, and CLICK2STAFF are trademarks or registered trademarks of Verint Systems Inc. or its subsidiaries. Other trademarks mentioned are the property of their respective owners. BY CLICKING "ACCEPT" OR "I ACCEPT" OR "AGREE" OR "I AGREE" OR "YES" OR BY USING THE PRODUCT YOU HEREBY ACKNOWLEDGE THAT YOU HAVE READ AND UNDERSTOOD THE TERMS AND CONDITIONS OF THIS AGREEMENT AND THAT YOU HEREBY AGREE TO BE BOUND BY ALL OF ITS PROVISIONS. BY CLICKING OR "ACCEPT" OR "I ACCEPT" OR "AGREE" OR "I AGREE" OR "YES" BY USING THE PRODUCT, YOU ALSO CONSENT TO USE ELECTRONIC SIGNATURES AND ACKNOWLEDGE YOUR CLICK OF "ACCEPT" OR "I ACCEPT" OR "AGREE" OR "I AGREE" OR "YES" BUTTON AS ONE.

**Avaya Contact Recorder
Release 12.0**

Planning, Installation and Administration Guide

About This Guide	17
Intended audience	18
Summary of information included in this guide	18
Conventions used in this guide	20
Additional references	21
For additional information:	22
Chapter 1: System Overview	23
Introduction	24
What's New.	24
Recording Options	29
Communication Manager	29
CS1000	33
Avaya Aura Contact Center	37
Server components.	39
Avaya Contact Recorder Server	39
Optional Server Applications.	40
End-User tools	42
Workforce Optimization ("WFO").	42
Search and Replay	42
Contact Recording Desktop	43
Administration Tools.	43
Recording Functionality.	44
Sampled Recording for Quality Assessment	44
Bulk Recording	44
Ad-hoc or Occasional Recording Modes (Communication Manager only).	46
Replay Options	47
Miscellaneous	48
Beep Tone	48
International support	48
Liability	49

Contents

Chapter 2: Planning and Prerequisites	51
Introduction	52
Recording Bandwidth	53
Voice Recording	53
Screen Recording	54
Storage Requirements	56
Storage at Each Recorder	56
Workforce Optimization ("WFO")	58
Central Database Storage	58
Archive Call Storage	58
Backup Storage	59
TDM Interfaces	60
Cards Supported	60
Chassis Requirements	60
Platform Restrictions	60
Server Platform	61
Sizing	61
Component Co-residency	63
DVD+RW / Blu-ray Drive	63
Network Issues	64
Load	64
Ports Used	64
Network Address Translation Routing	64
Licensing	66
Recording Limit	66
Backup Recording Channels Limit	66
Concurrent Screen Recording Limit	66
Quality Monitoring Seat Limit	66
Telephone Replay Channel Count	67
Dialer Integration	67
Secure Call Recording	67
Selective Recording	67
Timed Trials	67
Communication Manager system prerequisites	69
Communication Manager	69
Gateway Resources	70
AE Services	70
Expansion Interface Boards (TN570)	71
C-LAN	71
VoIP Resources	72
Multi-Connect Capacity	75
DMCC (IP_API_A) Licenses	75
TSAPI Licenses	75
VoIP Network Design	75
CS1000 System Prerequisites	76
Contact Center Requirements	76
CS 1000 Systems and IP Client Requirements	76

Confidential and Proprietary Information

AACC System Prerequisites	78
Supported Topologies	78
Required Components	79
Version Compatibility	79
Licensing	80
Topologies	81
Bulk Recording System	81
Bulk Recording + Quality Monitoring System	81
Large Bulk Recording Systems	82
Integrating with other systems.	87
Standardized Dialer Integrations	87
Supplementary Tagging of Bulk Recordings	87
Explicit External Control of Recording	88
Chapter 3: Installation	89
Overview	90
Avaya System Configuration	91
Prerequisites	91
Communication Manager Configuration	91
CS1000 Configuration	98
AACC Configuration.	100
Test Phonesets	101
Order in which to Install Applications	102
Platform Prerequisites	103
Linux (Communication Manager, DMCC and Passive IP recording only)	103
Windows	106
DVD+RW / Blu-ray Drive(s)	106
Time Synchronization	108
Java Timezone (TZ) Update	108
Network Connectivity	109
Installing Avaya Contact Recorder.	110
Linux	110
Windows	110
Installing Workforce Optimization ("WFO").	112
Installing Avaya Contact Recording Desktop (CRD)	113
Installing CRD on the Agent's PC	113
Configure the master Avaya Contact Recorder	113
Configure the Contact Recording Desktop application on the agent's PC	116
Installing Screen Capture Software	117
Chapter 4: Configuration	119
Overview	120
Accessing the System	121
URL	121
Initial User Account	121
Key Points	122

Contents

Licensing	123
Terminology	123
Obtaining a License Activation Key	124
Standby and Slave Servers	125
Adding additional licenses	125
Reinstalling on the same PC	125
Reinstalling the Recorder on a new PC	125
Security	127
Securing the System	127
Windows Authentication	128
Windows Accounts for Screen Recording	128
General Setup	129
Recorder	129
Contact Center Interface	131
Avaya Aura Contact Center Interface	137
TDM Tap Points	138
Email Configuration	141
System Monitoring	142
Via the Administration Pages	142
Via Email	143
Application Logs	143
Tomcat Logs	144
Remote logging via Syslog Server(s)	144
SNMP	145
Operations	146
Common Settings	146
Assigning Ports	147
Bulk Recording	150
On Demand Recording (Communication Manager only)	157
Meeting Recording (Communication Manager only)	158
(Telephone) Replay Ports (Communication Manager only)	160
Archive	161
Overall Settings	161
Downloading the EMC drivers	161
Archive Destinations	162
Hard Disk Archiving	166
DVD+RW/Blu-ray Archiving	167
Search and Replay	171
Search and Replay Access Rights	171
ActiveX Control Download	173
Installing the ActiveX Controls Manually	174
Restricting Access to Replay Layouts	176
Miscellaneous Security Features	176
Locking Recordings	176
Enabling Lock/Unlock	176
Replay Authorization Process	178
Modify Default Behavior	180
Backup/Restore	182

Confidential and Proprietary Information

Application	182
Backing up the Database	182
Restoring data to a new PostgreSQL database	183
Backing up Voice Recordings	184
Distributing User Instructions	186
Those Using Recording	187
Those entitled to replay calls.	188
Configuring Avaya Support Remote Access	189
Chapter 5: Operations, Administration & Maintenance	191
Introduction	192
Status Monitoring	193
System	193
Server	194
CTI Monitors	195
Ports	197
Alarms	199
Audit Trail.	200
Preventative Maintenance	201
Daily	201
Weekly	202
Monthly.	203
Every Six Months	204
Restarting the System	205
Be patient	205
CS1000 Agents	205
Chapter 6: System Security	207
Access to the Recorder	208
Windows Domain Authentication	208
Use of SSL	209
Allow search and replay from this server?	210
Session Inactivity Timeout	210
Minimum Password Length	210
Force strong password	210
Password expires after (days)	211
Password cannot be reused within (days)	211
Minimum changes between reuse of same password	211
Replay Authorization Process	211
Server Hardening	212
Linux	212
Windows	212
ACR Firewall ports	213
Single Login	214
Dual Sign-in	215
How it Works	215
Applying this Mode	215

Contents

Making this the Default	215
Audit Trail	216
Using this Mode	216
Changing Passwords	217
User Accounts	217
Postgres Database Owner.	217
Encrypted File Storage	219
PCI Compliance	220
Chapter 7: Advanced Configuration	223
Properties File	224
Slave Server	233
Standby Server.	234
Central Replay Server	235
Installation	235
Configuration	235
Configuring other Recorders.	235
Installing Multiple Central Replay Servers	236
Customizing Search and Replay with Layout Builder	237
Usage Report	243
Enabling the Report.	243
Content	243
Accessing through URL:.	243
Accessing the Usage report in a log file	244
Selective Record Barring	245
Configuration	245
Example	245
Limitations	245
Contact Recording Desktop (CRD)	246
Overview	246
Status	247
Persistence of Commands.	247
Desktop Layout XML File on Avaya Contact Recorder Master/Standby.	248
Operations › Bulk Recording.	248
Client PCs	248
Command Line Options	249
Fault Tolerant Configurations	251
XML Configuration File Format	251
Restarting a Recorder.	256
Altering Translations	257
Migrating from Central Archive Manager (CAM)	258
Limitations	258
Replace Viewer with Central Replay Server	258
Preparation	258
Import a CAM Folder	260

Confidential and Proprietary Information

Appendix A: Technical Reference	261
Recording files	262
WAV files	262
XML files	262
SCN files	262
Internal Database	263
Recording details	263
Configuration details	263
Recorder Interfaces	264
HTTP/HTTPS Interfaces Offered	264
Communication Manager	265
CS1000	266
Avaya Aura Contact Center	267
Screen Recordings	267
Workforce Optimization ("WFO")	268
Other Recorders	268
External Control Interface	269
AET/DPA Interface	269
Database Upload Interface	269
Summary	270
Recording Attributes	272
Overview	272
Definitions	273
Call Identifiers	276
User Defined Fields	277
Search and Replay Attributes	278
WFO Integration	281
 Appendix B: Troubleshooting	 291
Hints and Tips	292
Where to Look for Clues	292
Determining Current Version	292
Specific Problems	293
System Administration page problems	293
Connectivity	294
Search and Replay problems	294
Recording Problems	299
 Appendix C: Alarms	 301
Alarms	302
Alarms Table	303
 Appendix D: External Control Interface	 321
Introduction	322
When to Use External Control	322
CAUTION	322

Contents

This Appendix	323
Port Allocations (Communication Manager only)	323
Master + Slave Systems (Communication Manager)	323
Java API Toolkit	324
RecordingParty	324
RecordingData	326
Reconnection	328
TCP/IP Protocol Overview	329
Connection Method	329
Enabling Control	329
Persistence of Commands	329
Channel Identification	329
General Protocol Specification	330
XML Tagging	331
Basic Call Tagging (Communication Manager only)	331
Fallback Mode	332
Examples	333
Third-party CTI Control	333
Additional Call Tagging	334
TCP/IP Message Sequences	335
Appendix E: Fault Tolerant Systems	343
Redundant SAN	344
Duplicated recording (Communication Manager only)	345
Standby Recorder Options	346
Prerequisites for high availability	346
Standby recorder licensing	348
Configuration Options	348
Known limitations	348
Fault Tolerant Topologies	349
"Main" Site	350
Disaster Recovery ("DR") Site	351
ESS or LSP Satellite Sites	353
Distributed Recording System	354
Supported failure modes	354
Standby recorders and Unify/External Control	355
CS1000 Master/Standby Topologies	355
Mode of operation	356
Standby configuration (automatic)	356
Standby configuration (manual)	356
Power-On	356
Standby mode	356
Failure Detection	357
Disk Space Monitoring	357
Active mode	358
Return to Standby mode	358
Switchover Implications	358
Restoring the Master	359

Confidential and Proprietary Information

Comparison with hardware switch-over units	360
Standby Recorder Configuration	361
Configuration Differences	361
Appendix F: Auto-Dialer Integrations	363
Introduction	364
Functionality	364
How it Works	365
Status Monitoring	365
Configuration	366
Licensing	366
Dialer List	366
Generic Dialer Configuration	366
Tagging of Calls	368
Avaya PCS/PDS Dialer	369
Versions Supported	369
Limitations	369
Configuration	369
PCS/PDS Settings Summary	372
SER Dialer	374
Configuration	374
FieldMappings	375
Davox Dialer	377
Configuration	377
FieldMappings	377
Agent IDs	378
Proactive Outreach Manager (POM) Dialer	379
Configuration	379
Limitations	380
Versions Supported	380
Configuration	380
Appendix G: Non-standard Hardware	381
Overview	382
Disks	382
NICS	382
DVD	382
Kickstart (Linux only)	383
Appendix H: Advanced Security Settings	385
Installing Unlimited Strength Encryption	386
Installing a Signed SSL Certificate	387
Selecting a Certificate Authority (CA)	387
Backing up the Keystore file	387
Creating the new Certificate	387
Generating a Certificate Signing Request	389

Contents

Importing the CA's certificates	389
Backing up the keystore file	390
Adding Additional AES CA Root Certificates to ACR	390
Changing Tomcat Port Numbers	391
Encrypting Properties File entries	392
Glossary	393

Confidential and Proprietary Information



About This Guide

The *Avaya Contact Recorder Planning, Installation and Administration Guide* provides details of the Avaya Contact Recorder system, as well as recommended and required components.

Intended audience

This guide is intended to be used by:

- Pre-sales Systems Engineers developing system topologies and designs
- Professional Services staff installing and deploying systems
- Systems Administrators
- Support personnel

The reader is expected to be familiar with:

- System administration of Microsoft Windows servers and/or Linux servers
- TCP/IP Networking and Voice over IP (VoIP)
- Avaya contact center systems administration

Summary of information included in this guide

The following table provides information about this guide.







Chapter Title	Description
Chapter 1: System Overview	This chapter provides an overview of the design options for an Avaya Contact Recorder system.
Chapter 2: Planning and Prerequisites	This chapter gives details of the prerequisites for an Avaya Contact Recorder system. You should also review Chapter 6 System Security as some of the optional elements described there may also require additional cost and/or effort.
Chapter 3: Installation	This chapter gives details of the steps to install an Avaya Contact Recorder system.
Chapter 4: Configuration	This chapter gives details of the steps to configure an Avaya Contact Recorder system.
Chapter 5: Operation, Administration and Maintenance	This chapter provides details of regular maintenance required for an Avaya Contact Recorder system.

Confidential and Proprietary Information

Chapter Title	Description
Chapter 6: System Security	Security of customer recordings is very important. This Chapter discusses the various features - some optional - that you can use to ensure the safety and integrity of recordings.
Chapter 7: Advanced Configuration	This chapter provides an overview of the more complex and rarely used options for an Avaya Contact Recorder system
Appendix A: Technical Reference	This appendix provides technical details about the Avaya Contact Recorder system.
Appendix B: Troubleshooting	This appendix covers general troubleshooting tips and specific common issues.
Appendix C: Alarms	This appendix provides details of the alarms that can be raised by the system.
Appendix D: External Control Interfaces	This appendix provides details of the external control protocols and associated Java class library.
Appendix E: Fault Tolerant Systems	In addition to using fault tolerant components within servers as described in the High Availability Systems section, recording systems can be made tolerant of many server and network failure conditions. This appendix details how such systems are designed and configured, how they handle failures and how to upgrade them.
Appendix F: Auto-Dialer Integrations	This appendix describes how the system can be connected to a number of popular auto-dialers.
Appendix G: Non-standard Hardware	This appendix discusses considerations for non-standard hardware such as blade servers
Appendix H: Advanced Security Settings	This appendix discusses some features and prerequisites for advanced security.
Glossary	The glossary defines the terms you need to understand this manual.

Conventions used in this guide

The following table shows how user input, output and instructions are highlighted in this guide, as well as special notations that you will see as you use this guide.

To show...	This style is used	For example...
Information shown on screen	Fixed width	You should see the prompt below: login:
Characters that you should type exactly as shown	Fixed width, bold	Enter the following command: mount /mnt/cdrom
Characters that you should replace with appropriate information	<i>Fixed width, bold italic</i>	Browse to the new server by entering http://servername:8080
Menu selections, buttons and tabs	Sans Serif, Bold	Click on the Install button.
Helpful hints that can improve the efficiency or effectiveness of your work	Tip:	Tip: If no part-time licenses are available, a full time license may be used instead.
Important details that we want to make sure that you do not overlook	Note:	Note: Media Encryption may or may not show up on this form.
Advice that can help you avoid undesirable results	 Important:	 Important: If the network does not meet the three conditions listed, there will be no media resources.
Situations that can result in: <ul style="list-style-type: none"> ● Harm to software ● Loss of data ● An interruption in service 	 CAUTION:	 CAUTION: Perform this procedure only after normal business hours. This procedure restarts all links on the interface, and can cause a temporary loss of service.
Situations that can result in harm to hardware or equipment	 WARNING:	 WARNING: Make sure that the disks are the Update you require. RedHat and other vendors still sometimes supply Update 0 disks.

Confidential and Proprietary Information

Additional references

The following guides contain additional information you may find helpful.

- *Avaya Communication Manager Call Recording: A Design Approach for Device Media and Call Control (DMCC, previously called CMAPI) (Compas ID 128862)*
- *Avaya Contact Recorder User Guide*
- *Avaya Contact Recorder - Remote Administration API*
- *Avaya WFO Security Configuration Guide*
- *Avaya Contact Recorder, Release 12, Technical Note: Migration from previous versions of Avaya proprietary recorders (CSCM, ACR and NES) to ACR 12.0*
- *Avaya Contact Recorder Integration to Workforce Optimization Guide*
- *Avaya Aura Contact Center, Planning and Engineering Guide (NN44400-210)*
- *Avaya Aura Contact Center, SIP Commissioning Guide (NN44400-511)*
- *Avaya Communication Manager Guide to ACD Contact Centers*
- *Administrator's Guide for Avaya Communication Manager*
- *Administration for Network Connectivity for Avaya Communication Manager*
- *Avaya Contact Recorder and Screen Capture Technical Note*
- *Avaya WFO 12.0 Distributor Technical Reference (DTR)*

Note:

Avaya Communication Manager documentation is available through the Avaya online support Web site, <http://www.avaya.com>.

For additional information:

- Contact us at the Avaya Support Web site: <http://www.avaya.com/support>
- Send an email with your application questions or issues to Avaya email support at: crmsupport@avaya.com
Place in the subject line: "Avaya support question"

Note:

You may be asked to email one or more files to technical support for analysis of your application and its environment.

You may also contact Avaya at any of the following numbers:

- U.S. and Canada (toll-free): 888.TECHSPT (888.832.4778)
- International and domestic (direct): 512.425.2200
- Fax: 512.997.4330

Confidential and Proprietary Information

■ ■ ■ ■ ■ ■

Chapter 1: System Overview

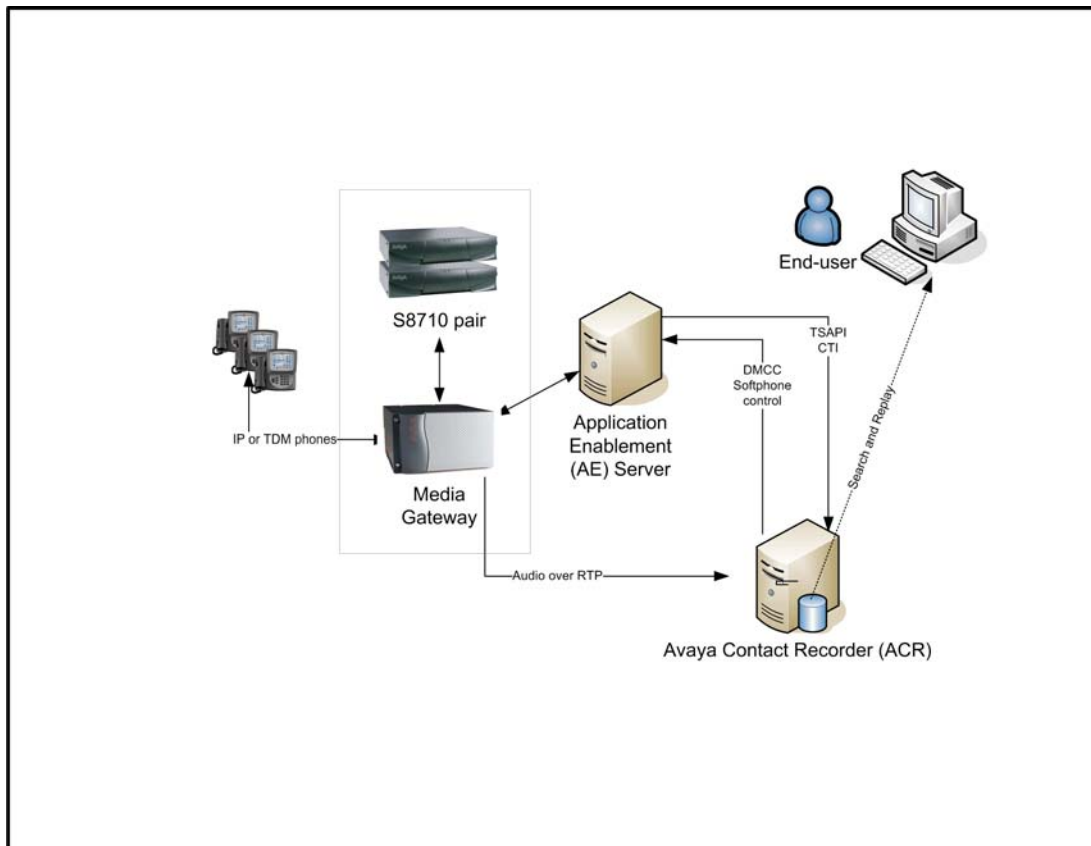
This chapter provides an overview of the design options for an Avaya Contact Recorder system.

Introduction

Avaya Contact Recorder provides an extremely efficient and scalable, voice recording platform, running on standard PC Hardware.

This chapter describes how Avaya Contact Recorder can be used to record calls on several different Avaya switch types. It describes the Avaya Contact Recorder (which is a mandatory component) and the optional components

Example Topology. ACR deployed against Communication Manager.



What's New

In Version 10.0

- Supports Avaya Communication Manager (CM) Version 5 and Application Enablement Services (AES) Version 5

Confidential and Proprietary Information

- Supports Redhat Enterprise Linux (RHEL) Versions 4 and 5. (Existing installations on RHEL 3 or 4 can be upgraded to ACR 10.0 but this version is no longer supported for new installations).
- The user interface has been refreshed and brought in line with that of the rest of the workforce optimization suite.
- One or more Avaya Contact Recorder servers may be used as a central replay server for other IP recorders, removing the need for a separate Viewer server in all but the largest systems.
- The "archive" feature has been extensively enhanced, removing the need for a separate Archive Manager. Blu-ray drives and media are also supported - though currently only on a Linux platform.
- A status screen on Master and Standby recorders now shows the status of all recorder servers in the system, simplifying day to day operation.
- Quality Monitoring has been simplified as the Avaya Contact Recorder now provides CTI information to the Quality Monitoring server in place of the additional TSAPI link previously required.
- Avaya Contact Recorder may no longer require the separate purchase and installation of IP_API_A or TSAPI licenses when connected to CM 5.1 or higher and AES 4.2.2 or higher. See [DMCC \(IP API A\) Licenses](#) on page 75
- As an alternative to specifying which stations are to be recorded, one or more Classes of Restriction (CoR) can be targeted for recording, reducing the administration effort needed to keep the recording rules in line with the switch.
- Integration to auto-dialers such as Avaya Proactive Contact has been simplified and brought within the recorder itself. Dialer integration is controlled by a license key setting.
- Licensing rules have been simplified.

In Version 10.1

- Support for Communication Manager 6.0
- Supports Redhat Enterprise Linux (RHEL) Version 5 ONLY. Existing users on earlier versions of RHEL must backup their database, upgrade the operating system, upgrade ACR and restore the database.
- Recording of calls on Avaya Aura Contact Center ("AACC")
- Recording of calls on Avaya Communication Server 1000 (CS1000) and Communication Server 2x00 (CS2x00) (and is an upgrade path from NES Contact Recording and Quality Monitoring 7.0) when installed on Windows 2008 server
- Recording details can be uploaded to more than one Viewer database
- Date limited licensing
- Bulk export of recordings includes a standalone replay capability

Confidential and Proprietary Information

System Overview

- Selective recording bar now also applies to calls on AACC, CS1000 and CS2x00 switches
- Recording of screen content (where license permits)
- Enhanced security
- Support for Windows 7 and Internet Explorer 8 client access
- User asked to confirm before configuration settings are deleted
- Replay control remains visible when search results scroll
- Enhanced event types passed to Quality Monitoring application (held, transfer, conference)
- Call Recording Card ("CRC") is no longer supported

In Version 10.1 Service Pack 2

CAUTION:

This release is not certified for use with TDM recording channels or CS2x00 switches at this time.

- The "Conferenced" recording mode previously provided for Communication Manager systems has been merged with the "Bulk" recording mode of CS1000/CS2x00 systems. Configuration has been rationalised and enhanced to provide a superset of features. For example, the "Designated Recorder" and "Record Internal calls only" settings are now available across switch types.
- Quality Monitoring recording on Communication Manager now uses single-step conferencing rather than service observe.
- "Station Bulk" and "Station Executive" recordings modes using service observe on Communication Manager have been removed. (Existing customers who feel they must continue with these recording modes should consult Avaya).
- TSAPI integration has been tightened so as to no longer require the Avaya TSAPI client or associated separate process.
- Support for Windows operating system when recording calls on Communication Manager.
- Configurable recording retention period on the disk buffer.
- PCS Dialer integration now includes tagging by any of the "IDENT" fields.
- Authentication mechanisms have been enhanced - to include Kerberos for client access and NTLM2 access to the Quality Monitoring application's fileshare.
- Search and Replay supports proxy servers.
- Incoming AACC calls can be recorded without having to connect to the CTI feed of a Communication Manager or CS1000.

Confidential and Proprietary Information

- Local archiving now supports Blu-ray on Windows as well as on Linux.

In Version 11.0

CAUTION:

This release is not certified for use with CS2x00 switches at this time.

- Now a 64-bit application on both Linux and Windows
- User accounts can be restricted from logging in unless explicitly authorized by an appropriate second user ("dual sign-in")
- A number of other security enhancements - including showing the time of last login and the forced use of a temporary password when an account is created.
- A new Remote Administration API allows most day-to-day configuration to be done through Avaya Control Manager.
- Audit log entries can be exported to ".csv" format.
- Supports "free-seating" for screen recording
- Archive destinations can be configured to store voice only, screen only or both.
- Beep Tone can be configured for specific bulk recording targets and supports a third mode in which beep tone is generated only after a decision to retain a recording has been made. (Note that beep tone is only available in some recording modes on certain switch types).
- Status page now shows total calls observed today and since last restart.
- Support for Proactive Contact ("PC") 5.0 and for Proactive Outreach Manager ("POM") 3.0
- Support for bridged Line appearances in Bulk mode (except where two or more parties on a call are on the same bridged line).
- Pause and Resume (which mask and unmask recordings with a double-beep tone) have been enhanced to allow different degrees of persistence of the mask command. Screen recordings are also masked by showing a black screen for the duration of the pause.
- Recording calls via TDM trunks and extensions within the ACR itself (rather than requiring a separate type of recorder) on Communication Manager as well as CS1000 (on a Windows platform only).
- Recording calls on Communication Manager stations via passive IP tapping (unencrypted, G.711 and G.729A on a Linux platform only)
- Central Replay Server now supports up to 5000 channels.
- Support for Internet Explorer 9 (32 bit)
- User account details are now transferred automatically from Master to Standby recorder(s).

Confidential and Proprietary Information

In Version 12.0

- (Optional) Replay Authorization process
- Interactive search and replay layout designer allows greatly increased scope and flexibility. Access to the layouts can also be restricted to particular user accounts.
- Recording lock and unlock mechanisms
- Compliance screen capture enhanced to work with Windows thin client sessions and to allow recording and replay of multiple screens per recording.
- SNMP monitoring now supports up to Version 3.
- Log file output can be directed to one or more syslog servers at INFO, WARN or ERROR level.
- Where the SMS interface is used (for CoR based recording rules) the interface now defaults to https.
- Contact and session level tracking of interactions provide hold, transfer and conference counts and times as well as overall contact duration.
- Selective Bulk recording (where licensed) allows random recording of a selected percentage of all or specific recording targets.
- Non-recorded stations on Communication Manager can be monitored to improve tagging of calls transferred on to recorded stations.
- Password security has been improved by forcing the use of strong passwords and enforcing change of password while blocking reuse of previous passwords.
- PCS dialer integration now handles hold and transfer scenarios better.
- A standalone archive media verification tool is available on request.
- Can archive recordings to EMC Centera storage systems.
- Can retrieve recordings from NAS storage that were archived there using Central Archive Manager (CAM).
- Can be integrated with Workforce Optimization (WFO)

Confidential and Proprietary Information

Recording Options

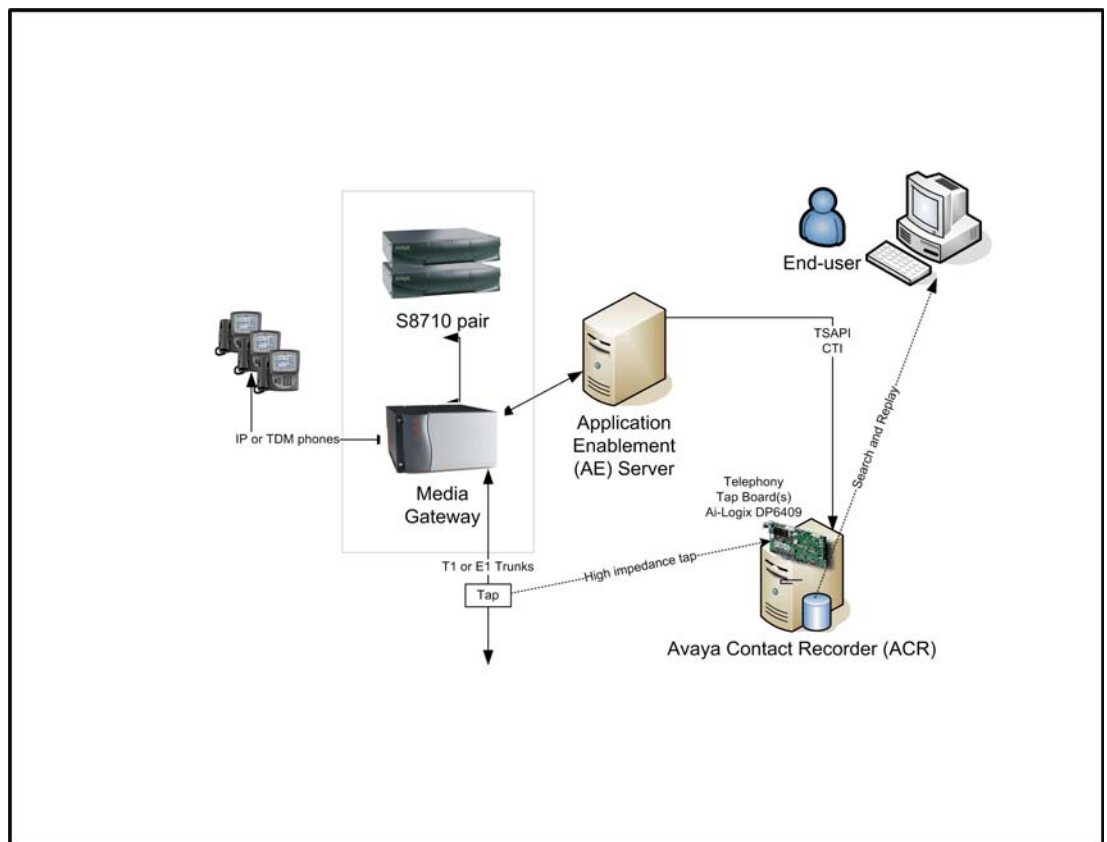
Communication Manager

Avaya Contact Recorder can record calls made on a Communication Manager system in several ways: tapping into the TDM trunks or stations; tapping the IP packets or - the preferred option - to conference into the calls to be recorded.

Trunk-side Tap

Where the bulk of telephone sets are not IP or the number of trunks carrying recordable calls is limited, tapping into the trunks may be appropriate. Using E1 or T1 passive tap cards, Avaya Contact Recorders can record any of the time slots as shown below. When using this method, internal calls cannot be recorded. This makes it unsuitable for quality monitoring.

Trunk-side Recording on Communication Manager

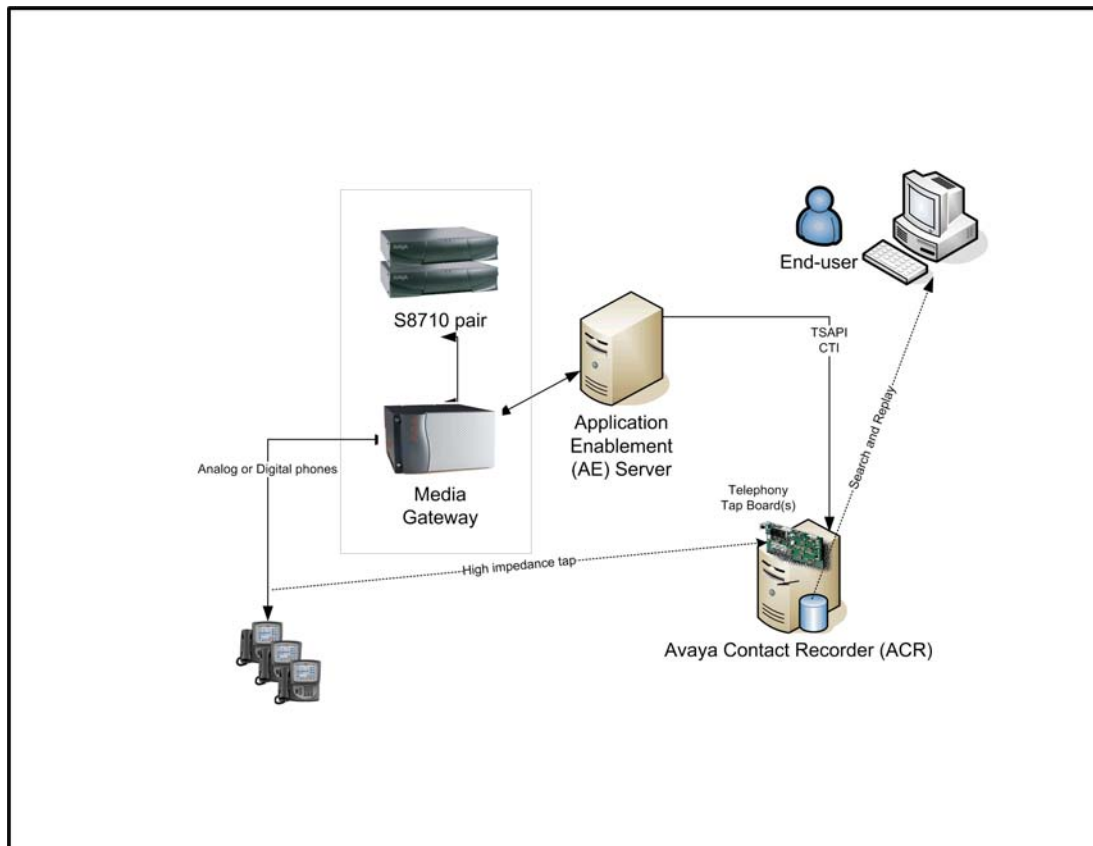


Confidential and Proprietary Information

TDM Station-side Tap

Where the telephone sets are digital and you only need to record a limited number of telephones, tapping into the extensions may be appropriate. Using digital extension tap cards allows an Avaya Contact Recorder to access the audio passing to or from the tapped telephones as shown below.

TDM Station Recording on Communication Manager

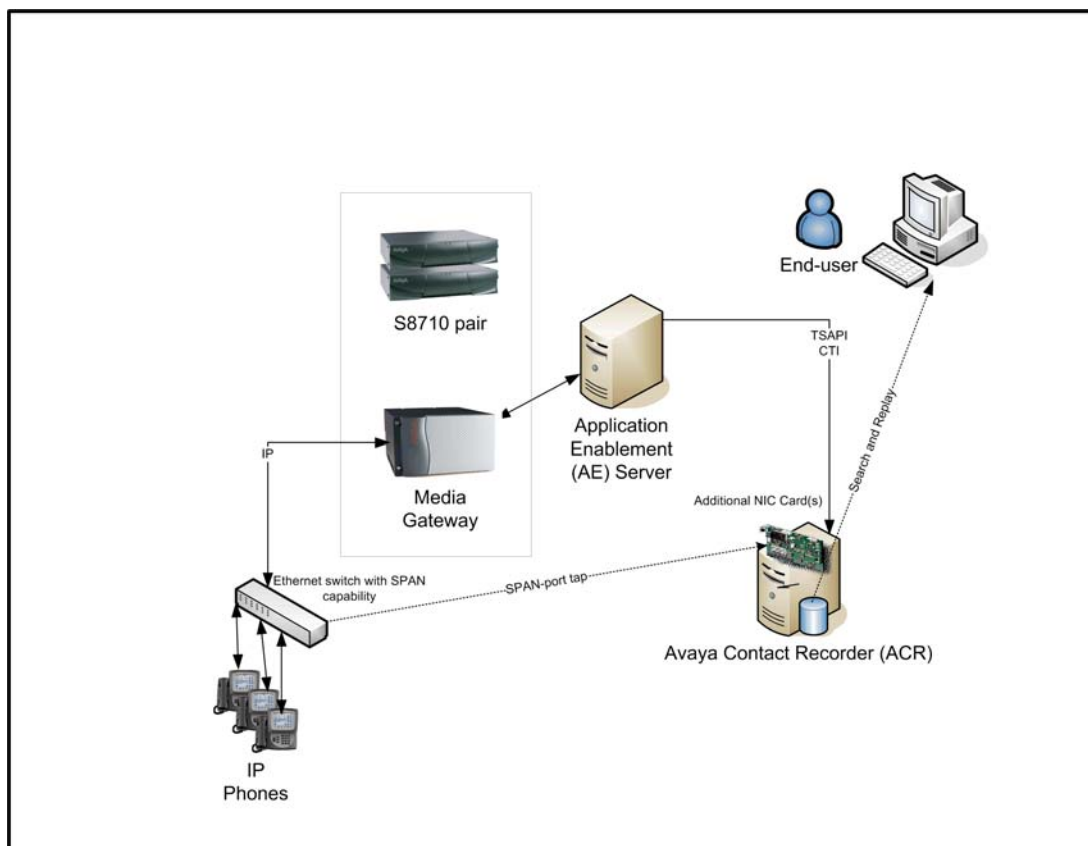


Passive IP Tap

Where IP phones are used and the audio transmitted is unencrypted, a passive IP tapping solution may be appropriate. This does not load the Communication Manager itself as a conferenced approach would. In this approach, one or more additional Network Interface cards (NICs) tap into the Ethernet segment(s) over which the voice traffic is flowing - as shown below.

Confidential and Proprietary Information

Passive IP Tapping on Communication Manager



Limitations

As the passive IP recorder first has to learn the location of IP phones, it may not be able to record the first call made on each station after the recorder starts up.

Conferencing into Calls ("DMCC recording")

The preferred approach to recording calls on this switch is to use Avaya's Device, Media and Call Control (DMCC) features to provide a wide range of recording modes with all the benefits of VoIP-based recording but without the limitations of passive tap IP recording systems.

This approach to recording offers the following benefits:

- The recorder can record potentially any call on the switch. Traditional trunk and extension modes cannot record internal and tandem calls respectively.
- There is no cabling to maintain as new trunks or extensions are added to the switch.
- Uses standard PC servers with no proprietary cards

Confidential and Proprietary Information

System Overview

The recorder uses two different methods to record calls. The table below shows which mode is used by each mode.

Recording Mode	Uses
On Demand Recording	Conference
Meeting Recording	
Bulk Recording	Single-step Conference
On Demand with External Controller	
Quality Monitoring	

Note:

Regardless of which recording method is used, when a recorder port joins a Communication Manager call to record it counts as an additional party on that call. Hence your normal limit of 6 parties on a call includes one party through which all of the recordings are made. This reduces the number of real parties on the call to five.

Single-step Conference

Single-step conferencing as used by Bulk recording, Quality Monitoring and Externally controlled (single-step conference option) has the following characteristics and limitations:

Exclusion

Prior to Communication Manager 6.2, this recording mode cannot be used to record calls in which any user invokes the Exclusion feature.

Conference with Party still Ringing

If a conference contains a party that is still ringing, the call cannot be recorded until that party answers the call.

Timeslots

Single-step conferences require an additional timeslot on the switch if (and only if) beep tone is used.

Device Names

To avoid excessive load on the system, the recorder caches the "name" of each device rather than request it on every call. These names are refreshed overnight so any changes are picked up the next day unless you restart the recorder.

Confidential and Proprietary Information

Call Segmentation

"Bulk" recordings are broken into separate segments whenever the parties on the call change. The recorder continues to record only so long as the real parties on the call are connected. If the call is on hold, recording stops.

If an external controller is used, it may segment calls at points it chooses.

Bridged Lines

Because of an inherent limitation in the underlying call/connection model, calls involving more than one instance of the same (bridged) line may not be recorded correctly.

Beep Tone

If you choose to inject beep tone on a single-step conferenced recording, the recorder becomes a full member of the call rather than a listen-only member and therefore:

- Becomes visible to the agent, who can see that the call is conferenced
- Uses an extra timeslot on the switch

Conference

In some modes a user or an external application will dial a port on the recorder. When this happens, the recorder answers the call and is therefore a normal party on the call.

Timeslots

As "just another party" on the call, the recorder port will use the single additional timeslot that any other phone would use when added to a call.

Call Segmentation

As the recorder port is a normal party on the call, it is still connected even if one or more other parties on the call places the call on hold. It will receive the same audio that the parties remaining on the call receive. This may include music on hold or silence.

If an external controller is used, it may segment calls at points it chooses.

CS1000

Avaya Contact Recorder can record calls made on the CS1000 switch via IP streaming (preferred) or via traditional TDM tapping - or a combination of the two. In this mode Avaya Contact Recorder must be installed on Windows.

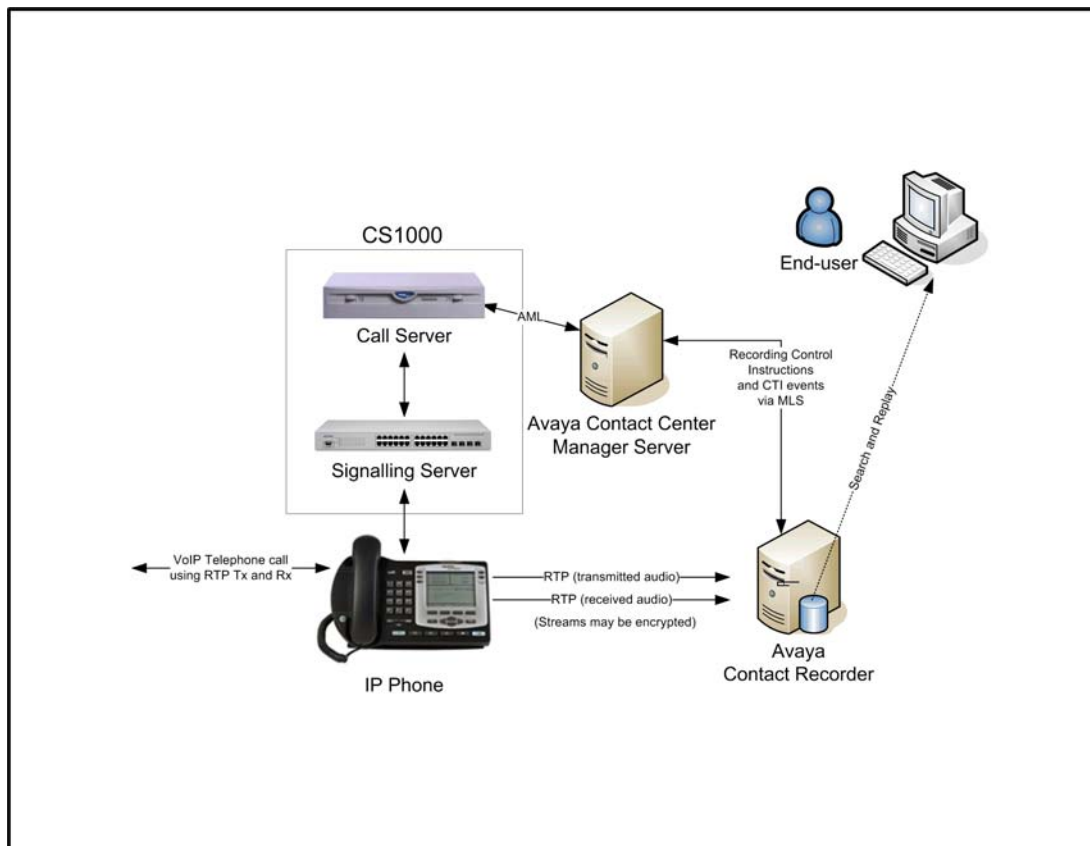
Duplicate Media Streaming over IP

This mechanism overcomes the difficulties inherent in passive-tap IP approaches and allows greater flexibility in the location of recorders as well as increased capacity and reliability of recorders. It requires only a standard full-duplex Ethernet card in the recorder. It can be used on any type of switched Ethernet system, as it does not require port mirroring. Ensure that the bandwidth is adequate. Above 100 channels, gigabit ethernet will be required.

This is the preferred method of recording calls on CS1000 and should be used where possible as it provides the simplest, most flexible and usually the most cost effective approach to recording. In this approach, the recorder instructs the telephone system to stream a duplicate copy of the audio directly to it over IP.

On CS1000 systems, the audio is streamed by the IP phone itself; this approach is only available for systems using Phase II (or later) IP phones. The recorder sends instructions via a Meridian Link Services (MLS) interface as shown below.

Duplicate Media Streaming in CS 1000



You should use this option for Bulk Recording or Quality Monitoring if both of these requirements are met:

Confidential and Proprietary Information

- your Avaya system meets the prerequisite requirements for Duplicate Media Streaming as shown in [CS1000 System Prerequisites](#) on page 76.
- the required bandwidth is available between the Avaya Contact Recorder(s) and the IP phonesets.

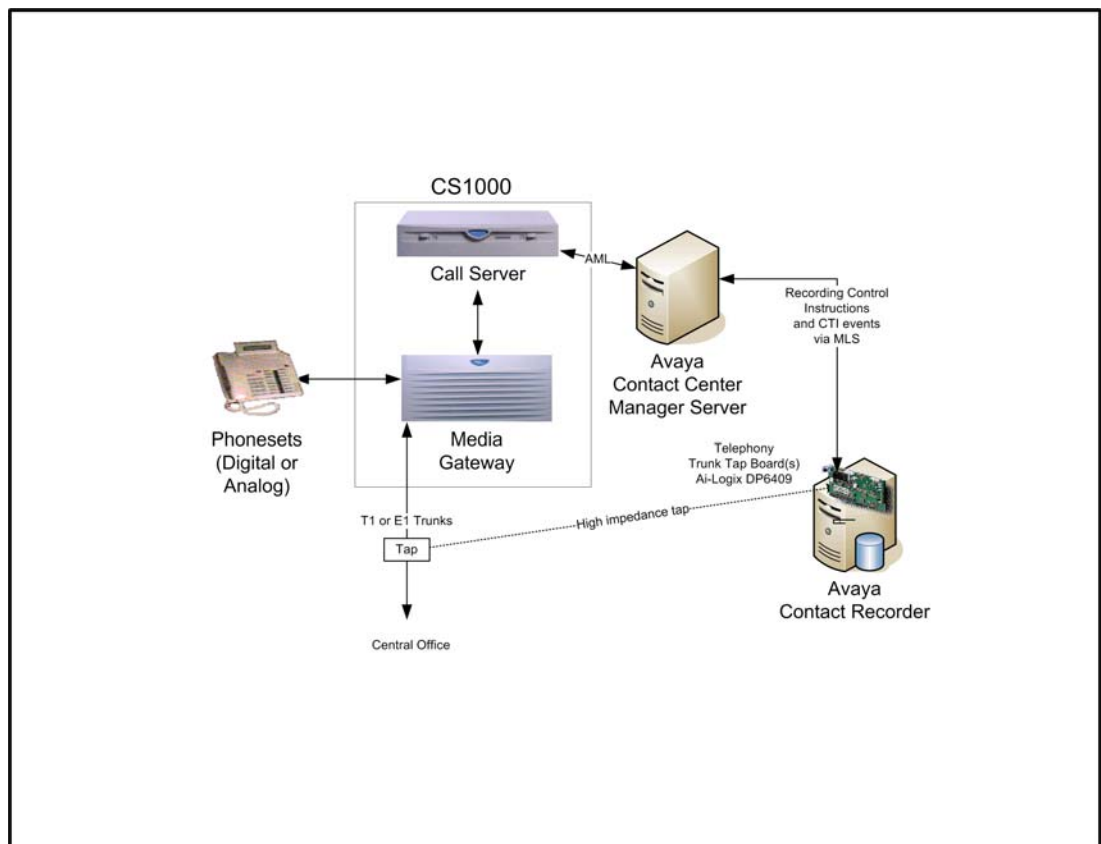
The recorder can be used with either G.711 (A- or μ -law), or compressed G.729A data streams - the latter with or without Voice Activity Detection (VAD).

Trunk-side tap

Where the bulk of telephone sets are not IP or the number of trunks carrying recordable calls is limited, tapping into the trunks may be appropriate. Using E1 or T1 passive tap cards, Avaya Contact Recorder can record any of the time slots as required. When using this method:

- Internal calls cannot be recorded. This makes it unsuitable for quality monitoring.
- An Avaya Contact Center Manager Server is required

Trunk-side Recording on CS1000

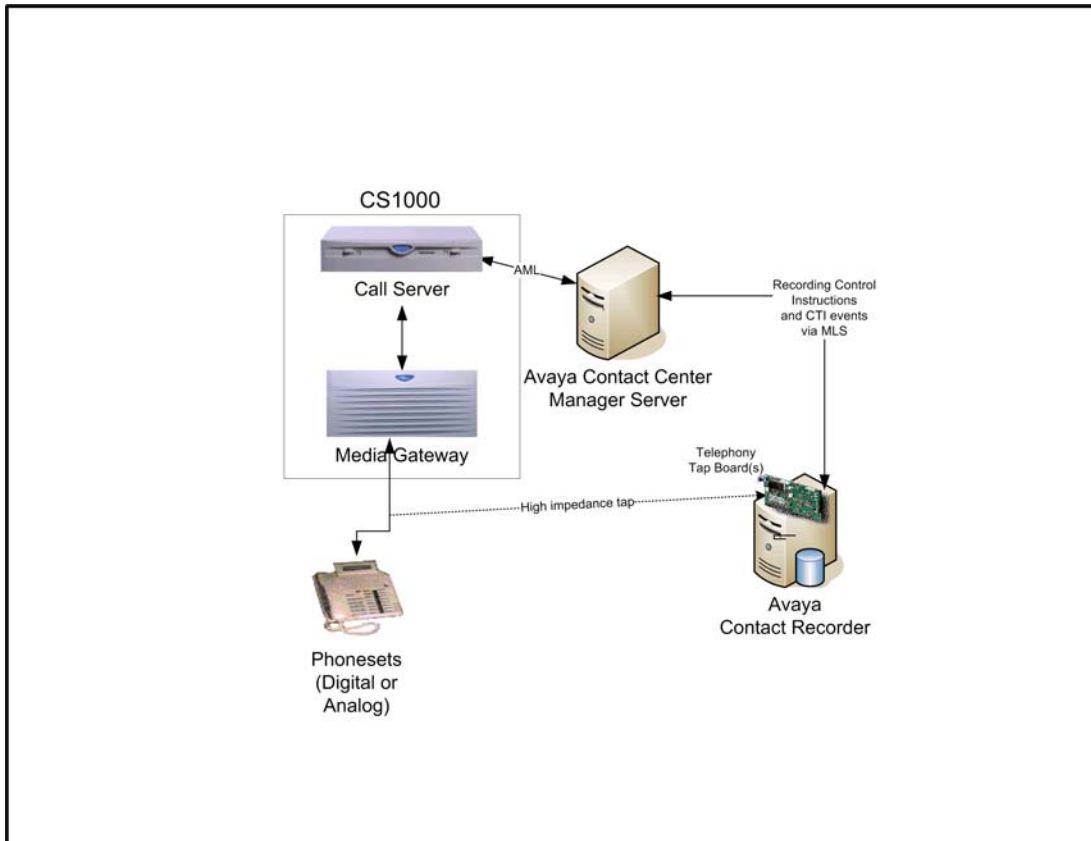


Confidential and Proprietary Information

TDM Station-side tap

Where the telephone sets are digital and you only need to record a limited number of telephones, tapping into the extensions may be appropriate. Using digital extension tap cards allows an Avaya Contact Recorder to access the audio passing to or from the tapped telephones as shown below.

Digital Extension Recording on CS 1000



⚠ CAUTION:

CS1000 switches support many different types of extension. Check the Ai-Logix cards' manuals to confirm precise models supported.

Limitations

Actions by Unobserved Positions/DNs

CTI events are only received for the positions/DNs being recorded. When another, unrecorded and hence unobserved position/DN is involved in a call, not all actions taken by that other party are visible to the recorded DN. If such an internal "far-end" places the call on hold, transfers to another party or conferences in another party, the recorder will not

Confidential and Proprietary Information

be aware and hence cannot tag the call with the details of the third parties to whom the call is transferred or who are conferenced into the call.

Emergency Calls

Calls received by a phone as a result of someone using the Emergency key may be recorded more than once.

Supervisor Calls

Calls received by a phone as a result of someone using the Supervisor call feature may be recorded more than once.

Beep tone

Beep tone is only supported in Duplicate Media Streaming recording modes. It is not supported in any of the TDM recording modes.

Agent Status

In CC V6, agent status is not visible to the recorder at startup. Agents must log out and in again after the recorder has started before calls can be recorded by and tagged with agent numbers.

MARP/MADN

Multiple Appearance DNs ("MARP" and "MADN") can only be recorded when in Bulk Recording mode in a knowledge worker environment. These are not supported by the Quality Monitoring application, or the Avaya Contact Center environment.

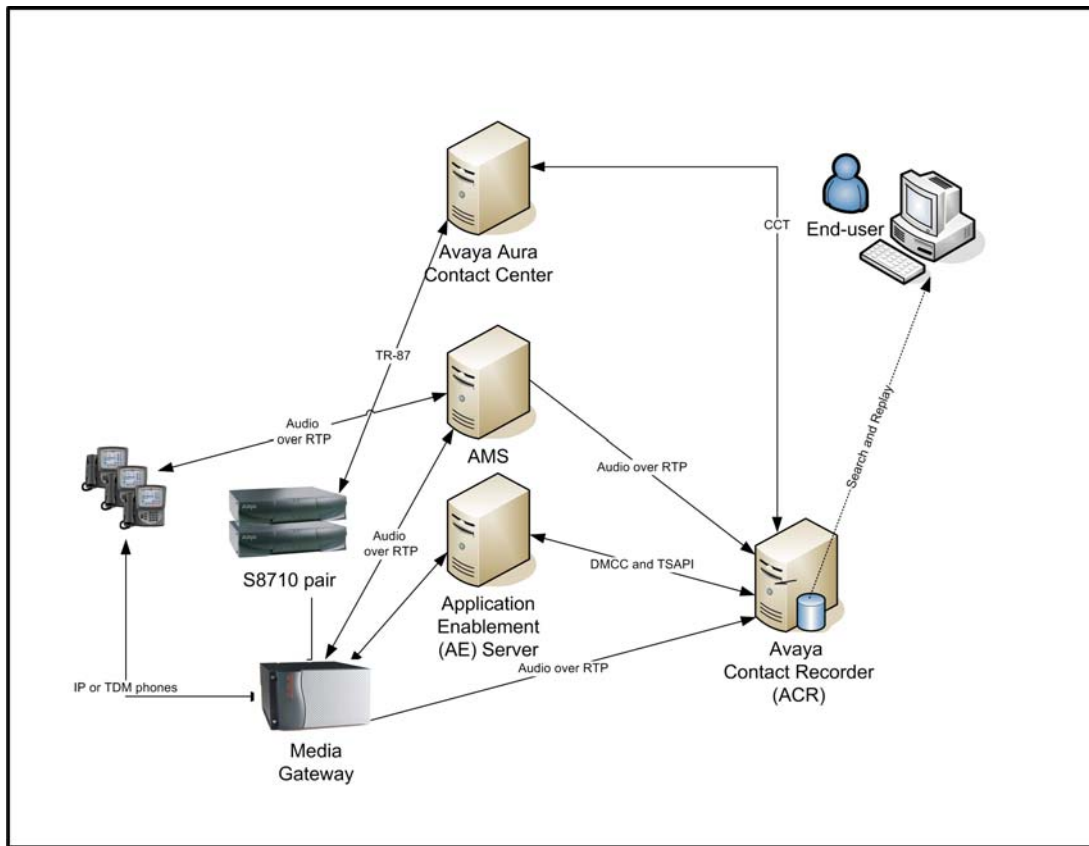
Recording of calls made from one instance of a number to another line key on the same number are NOT supported. The CSTA computer telephony model which underpins the call state tracking cannot handle the same address being involved in two separate connections on the same call.

Avaya Aura Contact Center

Avaya Contact Recorder can record calls controlled by an Avaya Aura Contact Center using the CTI information and SIP recording path shown below. If the AACC is hosted on a CS1000 or Communication Manager, then other calls made by these same telephones will be recorded using one of the methods described above for the appropriate underlying switch platform. In such cases, you must plan and configure your system to support both the underlying recording mechanism appropriate to your switch platform and with the CTI links shown below.

Confidential and Proprietary Information

ACR recording Avaya Aura Contact Center (based on Communication Manager)



The Avaya Contact Recorder receives CTI information from the CCT feed and passes instructions through this same feed when it wants to record a call. The Avaya Aura Contact Center then invites the specified recorder port to join the call which is recorded over IP.

Confidential and Proprietary Information

Server components

The Avaya Contact Recorder system can be installed as a single server solution providing recording and replay of calls. Large systems can be built from several independent recorders or in a master/slave or master/standby/slave topology.

You can extend the scope of the system by adding additional optional server applications to create a comprehensive Workforce Optimization system.

The Avaya Contact Recorder runs on Windows or Linux but certain recording modes are only supported on one or other, as shown in the table below

Environment	Recording Mode	Windows	Linux
Communication Manager	DMCC	Yes	Yes
	SIP (of AACC calls)	Yes	Yes
	TDM tap	Yes	No
	IP Passive tap	No	Yes
CS1000	Duplicate Media Streaming	Yes	No
	TDM		
	SIP (of AACC calls)		

All of the other applications in the suite require Windows. The optional server applications normally require their own physical server, but may sometimes be installed together on the same server. See [Component Co-residency](#) on page 63 for details.

Each of the other components has a corresponding guide (as detailed in [Additional references](#) on page 21 which you should refer to for more detail.

Avaya Contact Recorder Server

In most small to medium-sized (up to several hundred channels) Bulk Recording systems, one of these applications provides the entire recording and replay system (as shown in [Introduction](#) on page 24).

In larger systems (where a single physical server is not powerful enough), you should install multiple instances of this application on different physical servers, each providing a subset of the system's overall functionality. The Avaya Contact Recorder can:

- connect to your Avaya switches CTI feed(s) and control all voice recordings

Confidential and Proprietary Information

System Overview

- record and store telephone calls
- record and store screen content of Windows desktops during phone calls
- archive the recordings it makes to one or more local DVD+RW or Blu-ray drives, network fileshares and/or EMC Centera file stores.
- provide search and replay services to users connecting via their browser or via their telephone
- provide voice recording services to Workforce Optimization
- control other Avaya Contact Recorders
- be controlled by another Avaya Contact Recorder
- act as a Standby to an Avaya Contact Recorder Master
- act as a centralized replay server, holding details of recordings made by other Avaya Contact Recorders

Optional Server Applications

Workforce Optimization ("WFO")

This application suite provides comprehensive Workforce Optimization tools that can control and exploit the voice and screen recordings made by Avaya Contact Recorder. These include Quality Monitoring, coaching and Workforce Management tools among others.

See the WFO manuals listed under [Additional references](#) on page 21 for full details of this application suite and [Installing Workforce Optimization \("WFO"\)](#) on page 112 for how to integrate it into the overall system.

Centralized Replay Server(s)

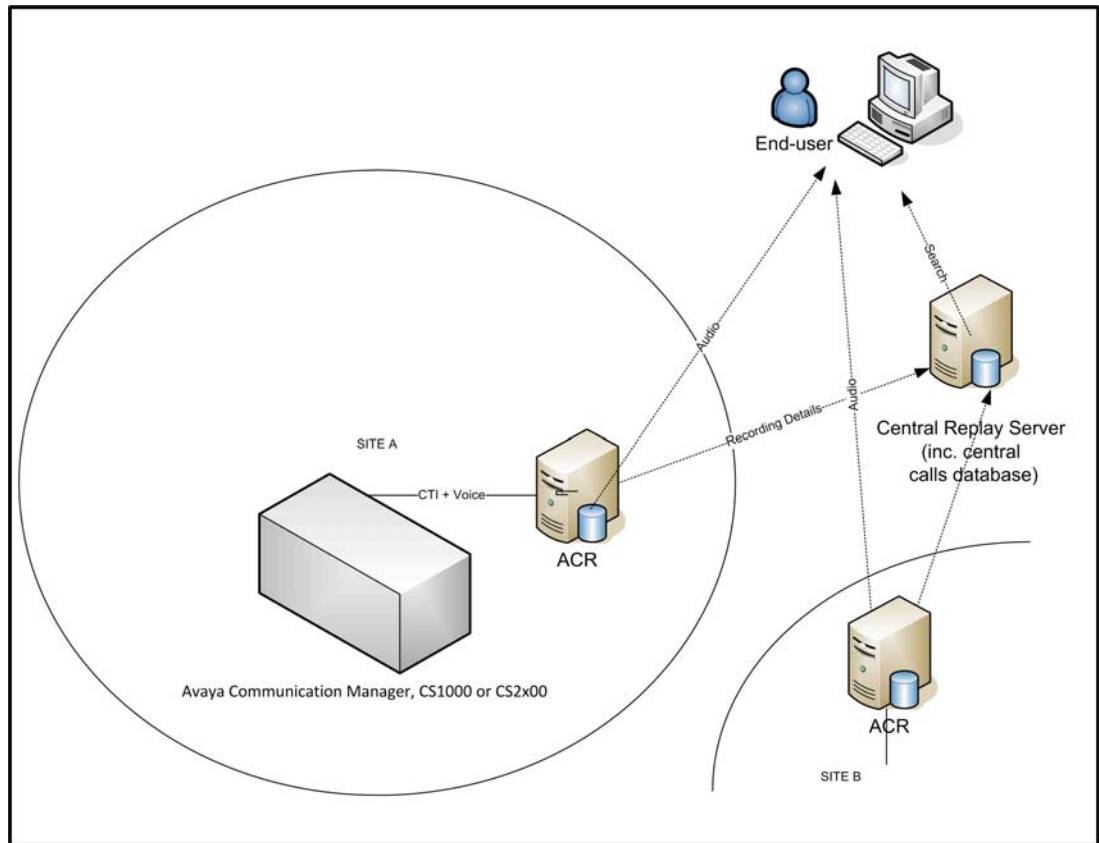
In any system with more than one Avaya Contact Recorder, details of recordings are (by default) uploaded to the Master (and Standby if present). This allows users to search for and replay calls recorded on any of the servers in a single query. On large (>5000 channel) systems, you should dedicate a server to this search and replay task.

This server should be another instance of the Avaya Contact Recorder, licensed and configured as a "Central Replay Server".

Note that the recording system is designed to continue recording regardless of the state of these central servers. This means that the availability of the central applications cannot affect the reliability of the recorders themselves. However, should you wish to deploy independent and hence fault tolerant central search and replay servers, this is also supported.

Confidential and Proprietary Information

Centralized Search and Replay



External Control

In addition to the data provided by the Avaya switches main CTI link(s), you may wish to control and/or tag your recordings with details from other CTI feeds or application interfaces. These may include third party systems and/or your own in-house applications. The recorder supports a wide range of systems and allows them to be connected to your recording system. These include:

- Avaya Proactive Contact and other auto-dialers as described in Appendix F.

End-User tools

To access the recordings held in the system, users have a variety of options.

Workforce Optimization ("WFO")

If you have integrated Avaya Contact Recorder with a WFO system, the user interfaces of that system are available to search for, replay and evaluate the recordings. See [Additional references](#) on page 21 for further details.

Search and Replay

Integral Search and Replay

The Avaya Contact Recorder includes a search and replay application within it. This replay mechanism is a very simple and intuitive browser-based interface, requiring the user to access it via (32-bit) Internet Explorer Version 8.0 or higher. For further details see *Avaya Contact Recorder User Guide*.

The Search and Replay application is hosted on a web server running on the recorder itself. It uses a local database of recordings to allow users to search for recordings by:

- Call start date/time
- The name(s) and number(s) where provided of any party on the call or through which the call was routed. This includes stations, ANI, DID, Skill or hunt group, VDN etc. where provided by the switch.
- Agent ID and name
- Call duration
- Call Identifier
- User defined fields supplied by external controllers

A full description of the attributes that recordings are tagged with is given in [Recording Attributes](#) on page 272. Access restrictions determine which calls individual users are able to replay. Each recording is assigned one or more "owners" at recording time (see [Search and Replay Access Rights](#) on page 171 for further details).

The user can play and view details of any call that matches their search criteria and access rights. When a call is played, a graphical representation of the audio level of the call, the audio wave form, is displayed. The audio wave form shows silence and tones, so the user can click beyond irrelevant sections and pinpoint parts of the call that are of interest.

Confidential and Proprietary Information

Screen content, where recorded, can also be viewed. See the accompanying User Guide for further details of this application.

Central Search and Replay

Where multiple Avaya Contact Recorders are deployed, an additional server can be nominated as a Central Replay Server. This server is not used for recording but can provide telephony replay ports (on Communication Manager only).

The other recorders upload details of the recordings they have made into this server's database allowing users to search for and replay recordings made on any recorder without having to know which one recorded a particular call.

Contact Recording Desktop

This is a very simple desktop application that lets users on CS1000 systems control recording of a DN or Position ID line that they are using alongside the PC on which they are running this application. The application typically shows as an icon in the tool tray. Users can then use the right-click menu or restore the main window to:

- Start or stop recording
- Request that a recording is deleted or retained
- Tag a recording with additional details

Note:

Users with IP phones can perform the first two directly from keys on their phone.

[Contact Recording Desktop \(CRD\)](#) on page 246 describes how to configure and use this application.

Administration Tools

As the suite is designed specifically for Avaya systems, much of the complexity associated with generic recording systems has been removed resulting in a system that is easy to configure and maintain. The recorders are administered via a web interface. The detailed use of this interface is the subject of later Sections in this guide.

Alternatively, on Communication Manager systems, much of the day-to-day administration can be performed on Avaya Contact Center Control Manager and pushed to the Avaya Contact Recorder.

Recording Functionality

The first task in designing any recording system is to define what is to be recorded. This in turn is often driven by the reason for wanting the recordings. This section introduces the various ways in which recorders' ports can be used but you should refer to [Operations](#) on page 146 for detailed functionality and limitations of each mode.

Sampled Recording for Quality Assessment

If the end goal is to record only a sample of calls in order to assess the quality of your interactions with customers, Workforce Optimization ("WFO") can be used alongside the Avaya Contact Recorder. See *Avaya Contact Recorder Integration to Workforce Optimization Guide* to determine how you will use the WFO system to control recording. Note that this document also highlights a number of limitations.

Licensing

The Avaya Contact Recorder must be provided with a license key that specifies how many different telephone stations can be recorded by WFO.

Bulk Recording

If you need to record all of the calls taken by specific stations, agents, skill groups or Vector Directory Numbers (VDNs) then you require Bulk Recording:

CS1000

You can record specific positions and DN's.

Communication Manager

CTI Information received over an AES TSAPI link allows the Avaya Contact Recorder to record calls on specific stations, agents, skill groups, VDNs or CoRs. Advanced configuration options let you filter the calls by VDN or Skill Group rather than have to record every call on the nominated addresses.

Confidential and Proprietary Information

AACC SIP Contact Center

Where an AACC is configured as a "SIP Contact Center", on either Communication Manager or CS1000 platforms, calls that are routed via the AACC will be recorded using SIP. Other calls will be recorded as described above for the relevant underlying platform.

Externally Controlled Recording

More complex recording requirements may be met by customized or specialist applications that interface to other CTI feeds or customers' own applications. Such an application can control ports on the Avaya Contact Recorder, allowing it to record exactly what and when it requires. The application may also "tag" the recordings with additional details such as customer number or account number.

Refer to [Integrating with other systems](#) on page 87 for more detail..

Screen Recording

As well as recording the audio content of a call, you can also associate a telephone with a Windows PC and record the content of its screen in Bulk Recording mode. Alternatively, the recorder can track where an agent logs in and record the screen of that agent's Windows desktop. In this case, as well as a dedicated Windows PC the recorder can record the user's desktop on any of the following thin client topologies:

- Citrix Presentation Server 4.5
- Microsoft Windows 2003 Terminal Services
- Microsoft Windows 2008 Terminal Services
- VMWare 3.5 VDI solutions hosted on any of the above client operating systems.

Recordings may contain multiple screen recordings (up to 4) where more than one party on the call is configured for screen recording.

Note:

Avaya Contact Recorder does not currently support encryption of the screen recording transport.

Licensing

The recording capacity across the whole system is restricted according to the license key entered. (This encompasses all voice recordings being made except the number of screen recordings which are separately licensed).

Ad-hoc or Occasional Recording Modes (Communication Manager only)

Although Bulk Recording can be configured to delete most calls and only retain those a user selects during a call, this still requires a recording port to be assigned throughout the duration of a call. Two other recording modes are provided for those requiring occasional recording:

On Demand Recording

This mode lets users of any phone on your system dial into or conference in a recording port as and when they want to start recording a call.

One or more "pools" of ports on the recorder can be assigned to this recording mode and accessed via Hunt Group numbers so that callers automatically reach an available port. The recorder automatically answers the incoming call on its port and starts recording.

Refer to [On Demand Recording \(Communication Manager only\)](#) on page 157 for a full description of this mode and how to configure it.

Meeting Recording

A novel use for recording is in taking a detailed log of a meeting, either as an audio record for those attending, or as a way to include non-attendees later. You can use any meeting room or office with a telephone that has a speakerphone or, ideally, conference phone capabilities to record the meeting.

 **Important:**

The audio recorded with Meeting Recording is the same as someone dialing in would hear it on the phone used to record it. Place the phone so it picks up the speech of all participants. They should speak loudly and clearly. Experiment with this recording mode before relying on it to provide full and complete records of your meetings. Avaya cannot be held responsible for the failure to pick up all of the audio intelligibly. Use this recording mode as an aid to note taking, not a replacement for it.

One or more "pools" of ports on the recorder can be assigned to this recording mode and accessed via Hunt Group numbers so that callers automatically reach an available port. The user follows the spoken instructions to start the recording and specify which user(s) can access it.

Refer to [Meeting Recording \(Communication Manager only\)](#) on page 158 for a full description of this mode and how to configure it.

Confidential and Proprietary Information

Port Requirements

Ports assigned to On Demand or Meeting recording

- can be assigned to one or more hunt groups making them easily shared across one or more user populations
- can be used not only by stations on the switch but also from outside the switch if they are made accessible via a DID number.

Licensing

Each recording is counted as part of the overall recording capacity and is restricted according to the license key entered.

Replay Options

Soundcard Replay

Many users choose to replay recordings via their browser and the soundcard on their PC. This does not use any ports on the recorder and does not require any additional licensing.

Telephone Replay (Communication Manager only)

However, the recorder also supports replay via the user's telephone on Communication Manager and this does use a port on the recorder.

Refer to [\(Telephone\) Replay Ports \(Communication Manager only\)](#) on page 160 for a full description of this mode and how to configure it.

Licensing

To use Telephone Replay Ports you will need the purchase the required number of replay channel licenses.

Miscellaneous

Beep Tone

Some states and countries require that both parties on a call be made aware that the call is being recorded. One way to do this is to apply a tone to the line. Note, however, that most telephone users are unaware of the significance of this tone and might, in fact, regard it as a fault. There are more effective means of informing the user that the call is being recorded. For example, you can inform users on advertising and in contract literature or play a recorded announcement before the call is connected. Check the legal position in your jurisdiction and apply the appropriate settings.

See the discussions of how each recording mode works earlier in this chapter to determine whether or not you need to turn on this warning tone within the recorder. In most cases, it is recommended that you set this option to No and use the other mechanisms described there.

In cases where the recorder is able to control beep tone, you can set this to be on, off or on only when the recording will be retained.

International support

The recorder's browser-based Administration and Search/Replay interfaces are provided in several languages. Check with Avaya for availability of specific languages. International support includes:

- Time zone and DST support. All dates and times are stored in the database in Coordinated Universal Time (UTC). However, when you view records using the search and replay application, these are converted to your local time. If you view the records using a database query tool, the times will be shown in the time zone of the client machine, which may be different from the server time. Note that the XML files relating to the recordings include ISO standard timestamps, giving both UTC and offset from Greenwich Mean Time (GMT).
- Number ranges are stored in the system database in left-to-right format (e.g. 100-200) unless you configure the property "system.forcertl=true" in the properties file. This affects alarms and audit trail entries.

Confidential and Proprietary Information

Liability

Liability of Avaya for failure to record any calls is limited under the terms of supply.

Confidential and Proprietary Information

■ ■ ■ ■ ■ ■

Chapter 2: Planning and Prerequisites

This chapter gives details of the prerequisites for an Avaya Contact Recorder system. You should also review Chapter 6 System Security as some of the optional elements described there may also require additional cost and/or effort.

The main sections in this chapter are:

- [Introduction](#) on page 52
- [Recording Bandwidth](#) on page 53
- [Storage Requirements](#) on page 56
- [Server Platform](#) on page 61
- [Network Issues](#) on page 64
- [Licensing](#) on page 66
- [Communication Manager system prerequisites](#) on page 69
- [CS1000 System Prerequisites](#) on page 76
- [AACC System Prerequisites](#) on page 78
- [Topologies](#) on page 81
- [Integrating with other systems](#) on page 87

Introduction

Unfortunately, there is no one "right" order in which to plan a system. A number of the requirements and pre-requisites are inter-dependent and it may be necessary to iterate through this section several times, refining your plans each time. This Chapter assumes that you have read the previous one and know the type and quantity of recording and replay that you require - and hence your total license requirements.

This Chapter will now guide you through:

- identifying what is to be recorded, the options for doing so and the relevant license requirements for the preferred option
- determining the storage needed to hold your recordings
- sizing the servers needed for each application
- quantifying the network bandwidth needed

You can then determine an appropriate system topology.

Confidential and Proprietary Information

Recording Bandwidth

Each type of recording requires a certain amount of data to be passed between components of the systems, processed and ultimately stored on disk and/or archive drives. This section explains the implications of each type of recording and - where choices can be made in terms of configuration or topology - the implications of these.

Voice Recording

The Avaya Contact Recorder supports two types of audio codec: G.711 (64kbps) and G.729 (8kbps). The choice of format depends on your switch type and network topology.

G.711

If the recorder receives audio in G.711, recordings will be compressed by the recorder and stored as G.729 (8kbps) files. (unless compression is deliberately disabled by setting `acr.disablecompress=true` in the properties file.)

The implications of receiving G.711 (and compressing it) rather than receiving G.729 in the first place are:

- Several times more bandwidth will be needed between the recorder and the source of the audio
- Bulk recording capacity of a given server will be about halved

G.729A

If the recorder receives G.729, the recorder will not have to perform any compression tasks. The pros and cons are therefore roughly reversed from those shown above.

Communication Manager

With TDM and passive tapping, the recorder does not impose any load on the switching fabric of the Communication Manager. When using DMCC softphones, however, calls are recorded using resources on the Avaya Communication Manager to conference a recorder port into a live telephone call. One of the benefits of this approach is that the recorder can ask to receive audio in a format that suits it - without impacting the experience of the parties actually speaking on the call.

The recorder requests either G.711 (μ -law), or compressed G.729A data streams. The above approach also means that audio is received at the recorder already mixed - so a G.729 recording requires much less processing power than a G.711 call (which is compressed to G.729A by the recorder).

Confidential and Proprietary Information

Planning and Prerequisites

G.729 is definitely preferable from the recorder's point of view but uses about twice as much audio processing resource within the Communication Manager. You must choose which is appropriate for your recording needs, network and server sizing.

Note:

When using G.711, the recorder always requests μ -law, never A-law. This applies to all countries regardless of that country's national preference.

If using IP passive tap recording, the Avaya Contact Recorder receives packets in whatever format you have configured your Communication Manager to use. This mode results in "stereo" recording of the call but if received in G.711 the two streams are combined prior to compressing into a single G.729A (8kbps) recording.

TDM recordings are compressed by the line interface cards which should be configured to provide G.729A (8kbps).

CS1000

On a CS1000 system with IP call recording, IP phones stream copies of the audio packets they are sending and receiving to the Avaya Contact Recorder. As packets are simply copied to the recorder, they are always in the same format (G.711 or G.729) that is being used on the call itself. If you wish to take advantage of the benefits of G.729 recording, you must configure your CS1000 system to use this format.

Duplicate Media Streaming results in "stereo" recording of the call. Two separate streams of audio are received. In the case of G.711 these are mixed and compressed to a G.729A (8kbps) file. In the case of G.729, they are kept as two separate streams and so occupy 16kbps. Hence the storage requirement is doubled but the recorder will support a much higher channel count if it receives G.729.

Note that a phoneset using bandwidth of X kbps to make a phone call will require an additional 2X kbps (twice X) for the streams being copied to the recorder. This results in a new total bandwidth of 3X kbps (three times the bandwidth of the unrecorded call) from the phone being recorded. The quality of service (QoS) of the network between the IP phones being recorded and the recorder must be the same QoS as required for a voice call.

If you have limited wide area bandwidth, consider placing slave recorders on the same sites close to populations of phones to be recorded. You can force recordings to be made on specific recorders.

TDM recordings are compressed by the line interface cards which should be configured to provide G.729A (8kbps).

Screen Recording

Screen content is also transmitted via IP. In this case, when a screen is associated with a phone that is being bulk recorded, or a user is seen to log on with a domain account for which the recorder has an Agent ID set the screen content is sent from the workstation

Confidential and Proprietary Information

being recorded to the recorder. If Quality Monitoring is also performing screen recording, then a further stream of data will be sent from the workstation to the Avaya Contact Recorder system. Note that, in the case of thin client workstations, the recorder interacts with the terminal server providing the services, not directly with the user's desktop display device.

Typical storage requirements for screen recordings are shown below but these can vary enormously according to how dynamic the users' screens are.

Screen Resolution	Color Reduction	No Color Reduction
1024 x 768	200 KB / min	800 KB / min
1280 x 1024	239 KB / min	1200 KB / min
1600 x 1200	301 KB / min	1800 KB / min

Screen recordings must be taken into account when sizing storage requirements as well as network bandwidth.

Storage Requirements

Having determined the type, size and location of your recording capacity, you must now determine how much storage is required within the system. Storage requirements of many terabytes are not uncommon.

Storage is required for:

- the operating system and applications installed on each server
- the audio and screen content of recordings
- the database holding the searchable details of these recordings

In each case you should consider requirements locally at each recorder and centrally.

To do this, you will need to know:

- how many recordings will be made on the recording channels already identified (typically expressed in channel hours per day). In other words, how many hours of audio and/or screen you expect to record on each recorder every day.
- how long you wish to retain recordings (typically expressed in days).
- the average duration of a call (typically expressed in seconds).

Storage at Each Recorder

In addition to the operating system, installed software and its configuration data, each recorder stores:

- details of the recordings it has made in a local database
- the recordings it has made as files on its hard disk

In all cases, the system automatically notes the location of the recordings so that when a user wishes to replay a call that is no longer in local online (disk) storage, the application prompts them to insert the appropriate removable media (if any).

Voice recordings are stored in G.729A format - in either mono (8kbps) or stereo (16kbps) according to the recording method and format in which the audio was received as described above. This allows for high volumes of recordings to be stored on the available disk space.

Avaya strongly recommends RAID arrays or fault tolerant Storage Attached Network (SAN) devices for online storage of recordings on the recorder platform. The operating system and calls database should be RAID 1 and the (typically much larger) recording storage area should be RAID 5.

Confidential and Proprietary Information

The recorder automatically manages the available recording storage space. This is used as a circular buffer providing instant access to the most recent recordings and deleting the oldest, as space is required for new recordings or as they reach the retention period configured.

Rather than storing bulk recordings on RAID arrays in each recorder, many customers prefer to use Storage Attached Networks. These must be connected directly to recorders.

Hierarchical File Storage (HFS) Systems and Network Attached Storage (NAS), however, can only be supported via the recorder's Archive features. These act as secondary recording storage.

 **Important:**

The storage used for recordings **must** be local to the server making the recordings. It must **not** be accessed via a network connection.

The table below summarizes the requirements for Bulk Recording on an Avaya Contact Recorder.

	Details of Recordings	Content of Recordings
Stored	In local postgres database	Stored as files on local disk in a hierarchical folder structure
Purged	Nightly, after user defined period (default 60 months)	100 at a time as disk space is needed for new recordings
Volume	Approximately 2KB per recording . So total ~ 2KB x recordings/day x days retained	Approximately 7.2MB (G.729 stereo) or 3.6MB (G.729 mono) per channel hour of audio. So total ~ 7.2MB (or 3.6MB) x channel hrs/day x days retained
Location (Linux)	/var (in addition to the normal contents of /var)	/calls
Location (Windows)	Install path	User Configurable. Dedicated partition required.
Type	RAID 1 (mirrored) or 5 (striped) strongly recommended. Local hard drive or SAN, not NAS.	RAID 1 (mirrored) or 5 (striped) strongly recommended. Local hard drive or SAN, not NAS.

Workforce Optimization ("WFO")

If Avaya Contact Recorder is integrated with a WFO system, then it is likely to require more storage space for both screen and audio content.

By default, all recordings made on Avaya Contact Recorder are made available to the WFO database. You can override this by setting the property entry `core.consolidateall=false`. Thereafter, only details of recordings involving parties configured appropriately within WFO will be sent to the WFO database. Further details are given in [Sessions Visible to WFO](#) on page 283. You must first determine what proportion of recordings will be made visible to WFO. For those calls, you will require additional storage.

WFO stores details of recordings by "session" - that is, according to the internal party involved in the call. Each internal party needs a separate session - and hence separate recordings. Normally, Avaya Contact Recorder makes a single recording of each call segment regardless of how many parties are on the call. However, where WFO must be advised of multiple sessions, each one requires a separate copy of the audio and, if present, screen content.

Furthermore, if WFO requires screen recordings, then Avaya Contact Recorder must record an additional copy of the screen data, running for the entire duration of the session, including periods when voice recording has stopped - such as when the internal party has the call on hold.

Additional storage capacity for these recordings must be provided. Where screen recording is used or where a high proportion of internal calls are to be recorded this can be significant.

Central Database Storage

Follow the guidance above to size the storage needed for the call details using the total call volumes across all recorders that are feeding into the Central Replay Server.

Archive Call Storage

Where you wish to retain calls for longer than it takes to fill the hard disk storage on a recorder, two options are available:

- Connect one or more DVD+RW or Blu-ray drives to the recorder. This requires only 1GB of buffer space on the recorder. Recorders that capture more than 4GB per day should use Blu-ray.

Confidential and Proprietary Information

- provide one or more fileshares and/or EMC Centera file stores onto which the recorders can archive their recordings.

Backup Storage

See [Backup/Restore](#) on page 182 for a discussion of Backup and Restore options. You should determine whether additional storage space is required in your corporate backup system to accommodate the new recording system.

TDM Interfaces

Cards Supported

The following Ai-Logix cards can be used:

- DP Series (trunk taps)
- NGX Series (digital extension taps)
- LDA Series (analog taps)

Chassis Requirements

As far as performance is concerned, up to 510 channels can be supported in a single chassis but the capacity is normally limited by the number of card slots available.

An extension chassis may be used if the motherboard does not provide sufficient slots.

Platform Restrictions

As the software tools provided for these cards are 32 bit Windows applications, any Avaya Contact Recorder using TDM cards must run on Windows (not Linux) regardless of which telephony switch is being recorded.

A separate (32 bit) process runs as part of the Avaya Contact Recorder and passes audio to the main (64 bit) service.

Confidential and Proprietary Information

Server Platform

Taking the above factors and the potential location(s) of your recorders into consideration, you must determine how many channels of each type of recording you wish to deploy and on which site.

Having decided the total recording capacity at each of your locations, you must translate this into one or more server platforms capable of handling the load identified.

Apart from the specific exceptions listed in [Component Co-residency](#) on page 63, Dedicated server(s) must be provided with no other applications running on them.

Sizing

The benchmarks given below are for the following server specification, which is the minimum required for new installations (upgraded systems can be assumed to continue supporting the load for which they were sized on the version originally installed):

- 2.67GHz six-core CPU with Intel Supplemental SSE3 (SSSE3) support
- 1Gbps Ethernet NIC port
- 8GB RAM
- RAID 1 or 5 strongly recommended
- DVD drive for installation of software (capable of writing DVD+RW and/or Blu-ray disks if local archiving is required)
- RedHat Enterprise Linux 6 Update 2 (64 bit) (Communication Manager IP and/or DMCC recording only) or Windows 2008 Server R2

Planning and Prerequisites

Recording Method (all supported codecs)	Max concurrent channels (Notes 1, 2)
Communication Manager via DMCC	1000
Communication Manager via Passive IP	500 (Note 7)
CS1000 Duplicate Media Streaming	650
Avaya Aura Contact Centre via SIP	1000
Either switch via TDM	510 (hardware limited)

BUT WHEN USING	Reduce max concurrent channels by
24 hour loading rather than 8 hour day	30%
Screen Capture	50% (typical but highly variable)
Workforce Optimization ("WFO")	10%
More than 10 concurrent replays per recorder	N/A. Install dedicated Central Replay Server instead. (Note 4)
Average call duration less than 1 minute	25%
Virtualized environment (under Linux or Windows)	10%
G.711 input Server that does not support Intel Supplemental SSE3 (SSSE3). Most AMD servers do not support this.	30%

Notes:

1. Check the limits imposed by your switch infrastructure (later in this chapter) as these may limit the capacity of individual servers and/or the overall system to lower figures than the recorder hardware does.
2. Where more than one factor from the second table applies, the effects are cumulative. For example, the acceptable channel count for AACC is 1000 but if KMS, a virtualized environment and WFO recording are to be used, the capacity is $1000 \times 80\% \times 90\% \times 90\% = 648$ channels.
3. Where combinations of different recording channels are used, add up the fraction of a server each group of channels would need. The total must be less than one. For example, $400 \text{ channels} \times (\text{Communication Manager, DMCC}) + 200 \text{ channels} \times (\text{Communication Manager, G.711 voice} + \text{screen}) = (400/1000) + (200/500)$ of a server

Confidential and Proprietary Information

= 0.84 of a server - so OK. Do not forget to apply any reductions (as per point 2 above) first.

4. A dedicated Central Replay Server can support systems of up to 5000 channels and (Communication Manager only) 40 phone replay ports.
5. Passive IP figures assume 20ms packet interval over Gigabit ethernet ports with no unwanted traffic appearing on the SPAN ports. Where unwanted packets are received and/or different packet intervals are used, measure TOTAL packets per second (Npps) across ALL NIC ports being tapped and apply the appropriate formula below to find channel count C:

$$C = 500 - Npps/500$$

Component Co-residency

Recorder + Unify

When running on Windows a single server IP recorder of up to 180 channels (codec dependant) will support the co-existence of the following application and components:

- Avaya Contact Recording Master - provides IP recording, local calls database and search and replay application
- Custom adapter (Unify component) - if applicable

See [Recording Bandwidth](#) on page 53 for more details about the codec dependencies.

DVD+RW / Blu-ray Drive

A wide range of DVD drives has been used successfully and Avaya is not aware of any specific model limitations at this time. The following media types are supported:

- On Linux: DVD+RW (single layer) or BD-R (single layer)
- On Windows: DVD+RW (single layer) or BD-RE (single layer)

Note:

Most drives are advertised as supporting a wide range of subtly different media types (e.g. DVD+R, DVD-R, DVD+RW, DVD-RW, single and double layer etc.). Regardless of which media the drive supports, the recorder ONLY supports writing of the above media types. You must confirm that the drive supports at least one of these media types, that it works under the version of operating system you are using and that you only insert this type of media.

Network Issues

In planning the network that will support your Avaya Contact Recorder system, you must consider:

- the additional load imposed on the network
- the IP ports used - so that firewalls can be configured appropriately
- (passive IP recording only) the paths over which audio is transmitted - so that the recorder is able to tap into all the calls that are to be recorded.

Load

You must design your network topology to accommodate the additional traffic created by the recording system. See [Recording Bandwidth](#) on page 53 for a discussion of the bandwidth required for each type of recording.

Ports Used

The components of the system use a number of IP ports to communicate:

- between each other
- with various other Avaya components
- with end-users and administrators

[Recorder Interfaces](#) on page 264 provides a diagram and table listing all of the interfaces to and from the Avaya Contact Recorder software. Your network and firewalls must be configured to permit traffic to pass over these links.

Network Address Translation Routing

The IP address of an Avaya Contact Recorder is sent to the telephone system as part of the recording process. It is therefore essential that when the telephone system components transmit to this address, the packets are routed correctly to the recorder. The recorder must therefore be visible to the media processing resources, IP phones, Media Access Server or Border Control Point as appropriate on the IP address that it uses itself. Additionally, if the recorder has more than one NIC card and these are not "teamed" or "bonded" into a single address, it is imperative to ensure that all VoIP packets are

Confidential and Proprietary Information

transmitted over the same NIC card (i.e. the network route for all recorded audio streams must be the same).

Licensing

A license key is only needed for each recording system. This may be a "standalone" recorder or any number of slaves and/or standby recorders connected to a Master recorder. Slaves and standbys are controlled by the Master and do not require their own license key. Central Replay Servers require a license key each.

Recording Limit

The license key determines the maximum number of Recordings that can occur in the system as a whole. Recording a call uses one recording channel license - regardless of whether this was triggered by Bulk recording configuration, WFO Business Rules or both. Duplicate copies of recordings with multiple sessions, made for WFO's benefit do not use up additional licenses.

Where a recording system includes multiple servers (master plus standby and/or slaves) the limit is applied across all of these recorders.

Backup Recording Channels Limit

To use one or more standby recorders to provide fault tolerant backup capability, you must license as many backup recording channels as are to be configured on standby recorders.

Concurrent Screen Recording Limit

The license determines the maximum concurrent number of screens that can be recorded across the system as a whole. Each screen may be recorded more than once (e.g. for WFO as well as bulk recording) but still only uses one screen recording license.

Quality Monitoring Seat Limit

The license determines how many different stations can be recorded by the WFO application. This is not a concurrent limit. Each station that is recorded for Quality monitoring counts against this license.

Confidential and Proprietary Information

Telephone Replay Channel Count

The license determines how many recorder channels can be assigned to telephone replay. This feature is only available on Communication Manager based systems.

Dialer Integration

The license key will enable or disable integration to predictive dialers using the recorder's integral support for these. It is not required where integration is via a separate (and hence separately licensed) controller, nor is it required for integration between a CS1000 system and the SER dialer.

Secure Call Recording

For CS1000 systems, the license determines whether or not the audio streams sent to the recorder can be encrypted.

Communication Manager based systems support this as standard when using DMCC recording but this cannot be recorded using passive IP tapping.

Selective Recording

The default for Bulk recording mode is that 100% of the calls that match the recording criteria are recorded (subject to capacity limitations). If licensed for this optional feature, you can specify what percentage of such calls are recorded. This can be set overall and/or for specific bulk recording targets.

Timed Trials

Avaya can, at its discretion, issue an activation key which includes an expiration date. This allows for timed trials of any combination of features and capacity. As the expiration date is fixed within the license, the server will stop operating at that date regardless of when you enter the license key.

To extend a timed trial or to upgrade to a full license, contact us for an updated license activation key. Contact details in the section titled [For additional information:](#) on page 22.

Planning and Prerequisites

A five day trial license is available automatically from the license key entry page. This will allow you to try out Avaya Contact Recorder in a single server topology.

 **CAUTION:**

The five day trial license must not be used for production recording. When a full license is installed, any trial recordings become unplayable

Confidential and Proprietary Information

Communication Manager system prerequisites

To use the Avaya Contact Recorder system with a Communication Manager, you will need to ensure that your Avaya system meets the following requirements. This section discusses the various hardware, software and configuration requirements.

Communication Manager

Avaya Contact Recorder requires AE Services and hence is only supported on the models and versions of Communication Manager that support this platform.

Model

The Avaya media server running Communication Manager must be an S8300 through S8800 system.

Station Count

Each DMCC recording port on a recorder is an additional IP phone on the switch. Do not exceed the total station count for the switch in question.

Loading

Each DMCC recording adds as much load to a switch as a normal call. Hence you can only record 100% of calls using this method if your switch is running at no more than 50% of its design load. For example, S8700 switches running at up to 20,000 BHCA (complex call center call types) can have all calls recorded. Higher loads would require an S8710 or S8720.

Software Version

Avaya Contact Recorder requires one of the following:

- CM 5.0 - CM 6.0

Please check on <http://support.avaya.com> for more recent loads.

Gateway Resources

These house the media switching components of the Avaya system. You must ensure that the system has, or is expanded to have sufficient:

- Card Slots for the C-LANs and Media Processing Resources described below
- Time-slots for the original calls and, where needed, the recording channels.

Card Slots

Each C-LAN and Media Processing card must be located in the appropriate gateway and therefore in an available card slot alongside the existing cards.

Time-slots

When using DMCC softphones, the recorder conferences into calls in order to record them.

- ANY recording in which the recorder is injecting beep-tone will require one additional time-slot per concurrent recording.
- On Demand and Meeting modes use normal conferencing (as opposed to single-step) and therefore use a timeslot per recording.

Where additional timeslots are needed, the total timeslot count must not exceed the maximum available on that port network (484). Therefore, for a 100% recorded system, using beep tone injection do not equip any port network with more than:

- 6 x T1s (=144 calls, 432 timeslots)

or

- 5 x E1s (=150 calls, 450 timeslots)

These guidelines allow for reasonable additional timeslot usage for conferences with other port networks, shared tones and so on.

Rebalance port networks or add new ones to reduce the timeslot requirement on each to this level.

AE Services

Each DMCC recording port on an Avaya Contact Recorder uses a DMCC softphone. The recorder also makes use of TSAPI services. If you wish to configure recording of stations according to the CoR of the station, the recorder will also use the SMS Web Service to determine which CoR each station uses.

These are all provided by Avaya's AE Services platform.

Confidential and Proprietary Information

Loading

Note:

To avoid overloading an AE Server, do not attempt to record more than 20,000 calls per hour through each AE Server. (20,000 BHCA).

Note:

You must not use more than 1,000 softphones (recorder ports) through a single AE Server.

If several small recorders are used, you may connect them to a shared AE Server, but only if the total load on the AE Server does not exceed this figure. If the load imposed by a single recorder exceeds this figure, you must split the load across multiple smaller recorders, spreading the load across multiple AE Servers.

Multiple AE Servers

Most Communication Managers can support up to 15 AE Servers but this is a total count - not just those associated with recording. You may have other AE Servers associated with other CTI applications.

Location

In a multi-site system, you should always aim to install an AE server on the same site as the recorder(s) that is (are) using it. This minimizes the chance of system failure due to loss of connectivity between recorder and switching system.

Vintage

Avaya Contact Recorder 12.0 requires AE Services 5.2 or above. Ensure you are running the latest recommended load of AE Services.

Expansion Interface Boards (TN570)

All Expansion Interface Boards must be TN570C Vintage 3 or later.

C-LAN

C-LANs (TN799 DP) are used for two purposes:

- CTI information may be passed through them
- DMCC softphones register through them.

Confidential and Proprietary Information

Number of C-LANs

To ensure that a C-LAN does not become a single point of failure in a recording system, you should always provide at least two C-LANs for each AE server. As the CTI load and channel count increases, you should provide more C-LANs as shown below.

C-LANs per AE Server	Maximum BHCA through the AE Server	Maximum Recording Channels through the AE Server
1	NOT SUPPORTED	NOT SUPPORTED
2	12,000	200
3	20,000	400
4	20,000 (AE Server limited)	600
5	20,000 (AE Server limited)	800

Location of C-LANs

For maximum resilience, spread C-LANs across multiple port networks.

To avoid bottlenecks between the port network and the switch, do not connect more than 400 DMCC recording ports to the C-LANs in any port network.

Vintage

Refer to the switch documentation for the release of Communication Manager you are running.

Firmware

The latest update is recommended but these cards must be at least at Firmware update 132.

VoIP Resources

Although TDM and passive IP recording do not use any VoIP resources, each DMCC port on the recorder will use media processing resources on the Avaya system when it is active (recording or replaying via the telephone). You must ensure that sufficient media processing resources are available for the recording and replay load - in addition to any existing use of these resources within your system.

Confidential and Proprietary Information

Resource Requirements

G.711 recording or replay uses less resource than G.729A recording. Note that replay is always performed using G.711. Depending on the type and version of your Communication Manager, you may require one or more of the devices shown in the table below.

Resource Type	Comments	G.711 Recording or Replay Ports	G.729A Recording Ports
Media Processing Resource TN2302AP		64	32
MM760 VoIP Module	Included within S8300	64	32
Media Processing Resource 2602AP		320	280

These requirements are solely for the recorder's ports and are in addition to any used by other IP phones or other switch components.

Note:

It is not recommended to dedicate Media Processing resource to recording so it is important to over- rather than under-provide as other users of this resource could otherwise starve the recorder of this capability. On the plus side, you may use existing spare capacity in the switch for recording - but check the location of the resource as well as the amount.

Location of Resources

When adding recording to systems with multiple port networks, it is vital to check that the recordings do not overload the interconnects between port networks.

If a call cannot be recorded using VoIP resources within a port network that the call would have been routed through anyway, then the call must be routed to another port network to reach the VoIP resource. This varies according to whether the phones are digital (DCP) or IP and, with IP phones, whether the system is IP- or Multi-connect based.

Site the VoIP resources according to the table below.

Planning and Prerequisites

Recording System	DCP Phones	IP Phones Multi-Connect	IP Phones IPConnect
Station-side - High % of calls on trunks recorded. (Station Bulk, Station Executive or Unify applying station-based rules.)	Same Port Network as the Phones being recorded.	Same Port Network as the trunks carrying the calls.	
	N x VoIP resources per phone being recorded.	N x VoIP resources per trunk channel on that port network that could be recorded concurrently.	
Station-side - Low % (<25%) of calls on trunks recorded. (Station Bulk, Station Executive or Unify applying station-based rules.)	Dedicated port network(s).		As above
	VoIP resources equal to N x total number of trunk channels that could be recorded concurrently		

Where, N=1 for G.711 recording and N=2 for G.729A recording.

Vintage

Refer to the switch documentation for the release of Communication Manager you are running.

Firmware

The latest update is recommended but Media Processors must be at least at Firmware update 105.

Fault Tolerance

You should consider providing one additional board per port network. In the event of a board failing, a spare is then available to handle the full recording load, without having to look outside the Media Gateway - which could introduce sub-optimal use of back-plane timeslots and potentially impact recording in other gateways.

Confidential and Proprietary Information

Further Information

For more information, refer to Chapter 2: Administering C-LAN and IP Media Processor circuit packs, in the Administering Converged Networks section of the *Administration for Network Connectivity for Avaya Communication Manager* manual.

Multi-Connect Capacity

Keeping in mind the number and location of recorders and VoIP resources as defined above, confirm that the capacity of the Multi-connect switch (if present) is not exceeded.

DMCC (IP_API_A) Licenses

As long as you are running CM5.1 or later, the recorder does not require or use any of your existing IP_API_A licenses.

TSAPI Licenses

As long as you are running CM5.1 or later, the recorder does not require or use any of your existing TSAPI licenses.

VoIP Network Design

The recorder hosts the equivalent of 1 x Avaya 4624 IP Phone per DMCC port - whether used for recording or replay. You must therefore design the connectivity between it and the rest of the Avaya switch infrastructure as if there were a bank of this many IP phones at the location of the recorder. Follow Avaya's network design guidelines for this number of IP softphones operating in either G.711 or G.729A mode, but with 60ms packet intervals.

If the bandwidth between recorder and the media processing resources it uses is less than LAN speeds (100Mbps full duplex) then you should use G.729A recording only.

CS1000 System Prerequisites

To use the Avaya Contact Recorder with a CS1000 system you will need to ensure that your Avaya system meets the following requirements. This section discusses the various hardware, software and configuration requirements.

Contact Center Requirements

To use Duplicate Media Streaming you require SCCS 5.0 or CCMS 6.0 or higher.

If you want to use the MultiDN Recording capability, then a minimum of CCMS 7.0 or later (AACC) is required. MultiDN capability for IP sets allows all physical keys to be recorded on a single IP Phone (Previously there was a 2 key restriction). The CCMS/AACC licence for MultiDN must contain the number of DN's or position ID's that are being recorded, including Multiple Appearance (MADN). AST licences are no longer required on the CS1000 when the multiDN capability is configured.

If you want to use the Record on Demand / Save Conversation feature, CCMS 7.0 or later (AACC) is required. A on/off licence key is required on the CCMS/AACC to enable this functionality.

CS 1000 Systems and IP Client Requirements

To use Avaya Contact Recorder you need:

- CS 1000 Release 4.5 or higher
- For Record on Demand/Save conversation a minimum of CS1000 6.0 is required
- If Secure Call Recording is being deployed, then Unistim 4 or higher is required. Also, a minimum of CS 1000 release 6.0 is required. Note that the Secure Call recording feature is only supported on specific IP Phones equipped with this feature, currently the 11xx phones.
- If not using the MultiDN feature, AST licences are required on the Phoneset keys that you wish to record. Note that the MultiDN feature is only available with CCMS 7.0 or later (AACC) AND CS1000 release 6.0 or later. When using MultiDN, a licence is required on the CCMS server to enable this functionality. Also, MultiDN is only applicable to IP phones, so AST licences will definitely be required for TDM recording.

Note:

Even if you are recording trunk-side, the system still monitors the phonesets you wish to record (not the trunks). You therefore require as many AST ISMs as you have phonesets to be recorded.

Confidential and Proprietary Information

To use Duplicate Media Streaming you require Avaya IP Client Phase 2 sets loaded with firmware that supports Duplicate Media Streaming.

AACC System Prerequisites

Avaya Aura Contact Center (AACC) is the next generation Contact Center product from Avaya. Refer to the *Avaya Aura Contact Center, Planning and Engineering Guide (NN44400-210)* which provides all Server Requirements and prerequisites for AACC.

Supported Topologies

Note that AACC can be configured in multiple ways which can influence the type of recording mode required, as follows:

Avaya MBT or Communication Manager (CM) environment

In this environment, the AACC itself has only one mode of operation and it is installed and configured as an “AACC -SIP” Contact Center. This basically means that the Contact Center interfaces to the Switch infrastructure using SIP trunking for voice sessions (via the SES), and using SIP TR87 (via AES) for CTI events from the switch. From a Call Recorder perspective, the connectivity to AACC is via CCT Web Services, and this is the mechanism by which the Recorder receives CTI information for all agent related call events and agent events (such as Login, Logout, Ready, Not Ready). Additionally the recorder can invoke SIP recording Start/Stop requests via Web Services.

Note that in this environment, the Recorder must also maintain a direct link into the CM via the AES component using the DMCC/TSAPI protocols. This is required as the Recorder needs to retain the ability to record Agent calls that are not associated with the Contact Centre i.e. calls which are physically not anchored on the AMS from a media perspective. This mode of operation is referred to as a “hybrid” mode, as the Recorder uses a combination of both existing legacy CTI mechanisms (TSAPI and, unless using only TDM or passive IP recording, DMCC) and the newer Web Services offered by AACC.

Thus in a CM environment, there are essentially two basic configurations for Call Recording, as follows:

1. Recording of calls on the Communication Manager only (via DMCC, TDM or passive IP). This is sometimes referred to as “Legacy CM Recording”. In this mode of operation, all calls are recorded via DMCC/TSAPI. Usually this is used for recording of Knowledge Workers on CM on Agents on CC elite
2. SIP recording via AACC Web Services and recording Communication Manager calls via DMCC, TDM or passive IP. This is referred to as “CM SIP hybrid Recording”. This configuration is used in conjunction with an AACC installation on CM. Note that this is a superset of the previous configuration described in (1) above. In this mode, the Recorder has two simultaneous CTI Links, and can record via SIP, DMCC, TDM or passive IP tapping.

Confidential and Proprietary Information

Avaya Communications Server 1000 (CS1000) environment

In a CS1k environment, the AACC itself can have 2 modes of operation:

- “AACC -SIP” Contact Center: This is analogous to the CM configuration, in that all of the interfaces for the AACC are using SIP - SIP trunking to the CS1K NRS component and SIP TR87 to the CS1k Signalling Server.
- “AACC- AML” Contact Center: In this configuration, the CTI link to the Switch is via a proprietary AML link.

Therefore in a CS1k environment, there are essentially two basic configurations for Call Recording, as follows:

1. MLS Recording only. This is sometimes referred to as “Legacy CS1k Recording”. In this mode of operation, all calls are recorded via the MLS interface. This is used in an AACC-AML configuration, but can also be used in a knowledge worker environment. Recording is possible using either Duplicate Media Stream or TDM recording.
2. SIP Recording via AACC Web Services and MLS Recording. This is referred to as “CS1K SIP hybrid Recording”. This is used only in conjunction with an AACC-SIP configuration on CS1k. Note that this is a superset of the previous configuration described in (1) above. In this mode, the Recorder has two simultaneous CTI Links, and can record either via SIP or MLS.

Other Switch Types

When hosted on other switch types, only those calls being routed by AACC can be recorded. Other calls made on the underlying switch will not be recorded.

Required Components

Note that for a SIP Contact Center solution, the Avaya Media Server (AMS) and Communications Control Toolkit (CCT) components are always required for the base Contact Center functionality. Ensure that the AMS is sized to accommodate the additional load imposed the recorder. Each recorded call loads the AMS with one additional G729 channel.

Version Compatibility

For SIP call recording, AACC must be running one of the following versions:

- AACC 6.0 (some patches may be required for SIP Call Recording- please contact Avaya Support)

Confidential and Proprietary Information

Planning and Prerequisites

- AACC 6.1 (some patches may be required for SIP Call Recording- please contact Avaya Support)
- AACC 6.2
- AACC 6.3

Licensing

For SIP Call Recording (in both MBT/CM and CS1000 environments), ensure that the following items are included in the AACC license file:

- Open Queue
- SIP Recording
- CCT Web Services

Open Queue is required as it provides an underlying link between the CCT and CCMS components within AACC.

Refer to the *Avaya WFO 12.0 DTR* (Distributor Technical Reference) for more detail on the AACC licencing requirements.

Confidential and Proprietary Information

Topologies

This document has so far discussed functionality in terms of "applications" without being specific as to the physical location of these. As the individual components of the recording system interconnect using IP-based mechanisms, you may distribute the components across your Enterprise's network in a wide range of topologies.

In small systems, a single server can perform recording, storage and retrieval but in larger systems, you can separate these tasks onto different servers in a variety of ways as discussed below. A number of the basic topologies have already been shown in the diagrams of [Recording Options](#) on page 29. The following paragraphs define the rules under which each of these basic topologies can be used and introduce the more advanced topologies required for larger and more fault tolerant systems.

Bulk Recording System

At its simplest level, an Avaya Contact Recorder system consists of a single server running the Avaya Contact Recorder software and configured as a Master. This application provides:

- system administration functions via a browser
- voice recording of Avaya phonesets
- screen content recording of Windows desktops
- integration to the Avaya switch via a CTI feed for real-time control and tagging of recordings
- integral search and replay capabilities.

See the diagram in [Introduction](#) on page 24 for this basic Bulk Recording Topology

For most small to medium sized bulk recording requirements, this single server is all that is required.

Bulk Recording + Quality Monitoring System

Bulk recording and Quality recording can be combined on a single Avaya Contact Recorder but the Quality Monitoring application is provided by the WFO suite which resides on a separate server. It is possible to configure a virtualized environment using VMWare ESXi 5.0 (on Windows or Linux) where the Quality Monitoring System and the ACR are installed in their own guest O/S on the same hardware. Care should be taken to follow VMWare recommendations for ensuring accurate timekeeping in the virtualized guest systems.

Confidential and Proprietary Information

Planning and Prerequisites

On such a system, WFO may be configured with "Business Rules" that instruct the Avaya Contact Recorder to record specific calls. These recordings are made *in addition* to the bulk recordings and all recordings are made available to WFO as each contact ends.

Large Bulk Recording Systems

Where your recording load exceeds the capacity of a single server, or where a distributed topology is more appropriate, you may deploy multiple recorders - in one of two ways.

Partitioned Systems

If your recording requirements can be completely separated, you can deploy multiple independent recorders, each unaware of the others. This is only appropriate if you are Bulk recording isolated populations of phonesets on CS1000 systems.

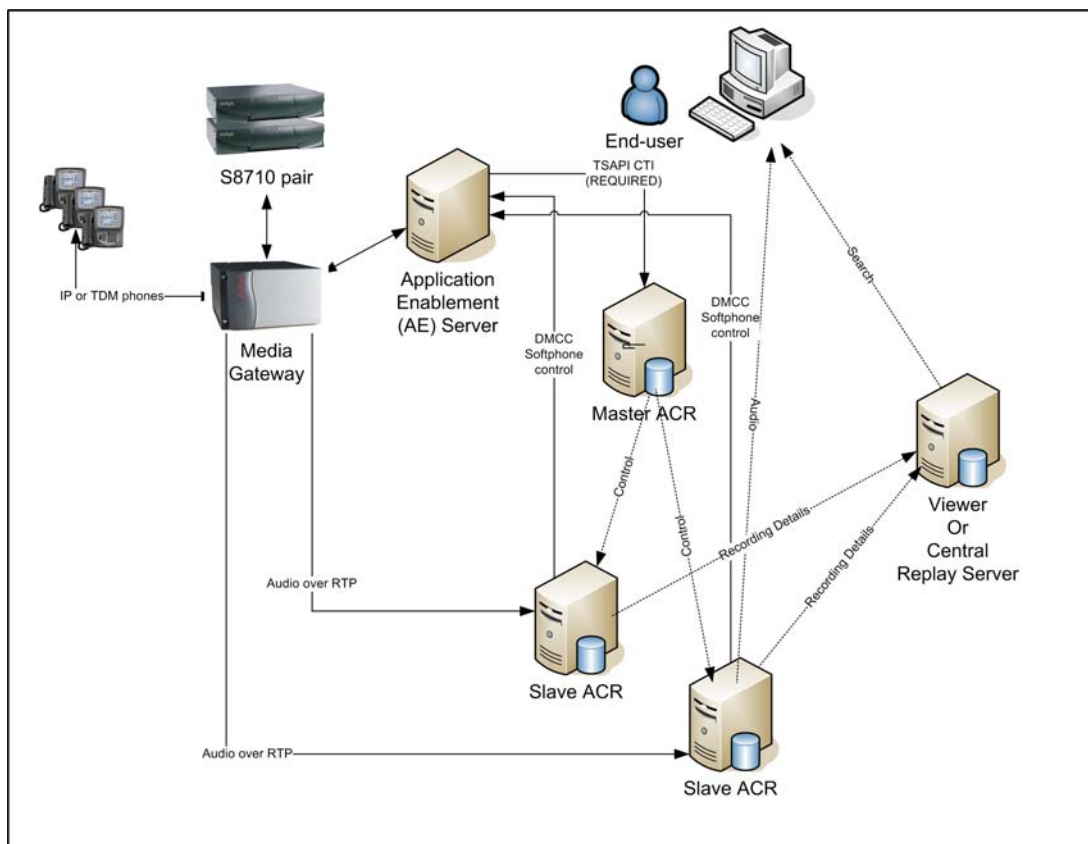
Master/Slave Recorders

Where you are recording Communication Manager calls on the basis of Station, CoR, Agent ID, Skill hunt group or VDN, there must be a single recorder in charge of all recordings. The same is true of all AACC systems and all CS1000 systems except for completely isolated populations of stations.

To support large systems, or to control traffic over your wide area network, you can add further recorders to increase the capacity of the system. Recordings will be load-balanced across the Master recorder and any additional slave and/or standby recorders.

Confidential and Proprietary Information

In such cases, the "Master" recorder is connected to the main CTI feed and is aware of the recording rules - and of the type and locations of the other, "Slave" recorders as shown below for a system recording calls on a Communication Manager.



The Master recorder communicates with each Slave via a TCP/IP link. It instructs the slaves to tag the required data/voice streams with the details it learns from the CTI link. Preferably, one of the slave recorders is actually designated as a "Standby" recorder and can take over should the Master fail (though this requires additional backup channel licenses). All active recorders load balance at all times, regardless of which is in control.

Recorder Type and Location

You may distribute recorders across your network. This lets you trade off network load versus security of storage.

For example, if you wish to record calls on an overseas site to which you have limited bandwidth, you can locate a recorder and media processing resources on that site.

High Availability Systems

Because the recording system is based on industry standard PC hardware, you can spend as much or as little as you like on fault tolerant hardware to increase the reliability of each

Planning and Prerequisites

server. Avaya recommends that you use fault tolerant, hot-swappable RAID disk arrays, redundant power supplies and fans as a matter of course.

Bonded and/or dual NIC cards are strongly recommended.

For still higher availability, you can provide one or more standby recorders. Advanced configuration options let the recorders match your switch failover modes - supporting both ESS and LSP modes when connected to Communication Manager, for example.

In general

- the recorder can be configured with multiple CTI links and will fail over to the next should one fail.
- any internal connections that fail are automatically reconnected using a back-off algorithm
- should a slave recorder fail, the master will attempt to reassign its recordings to other recorders.

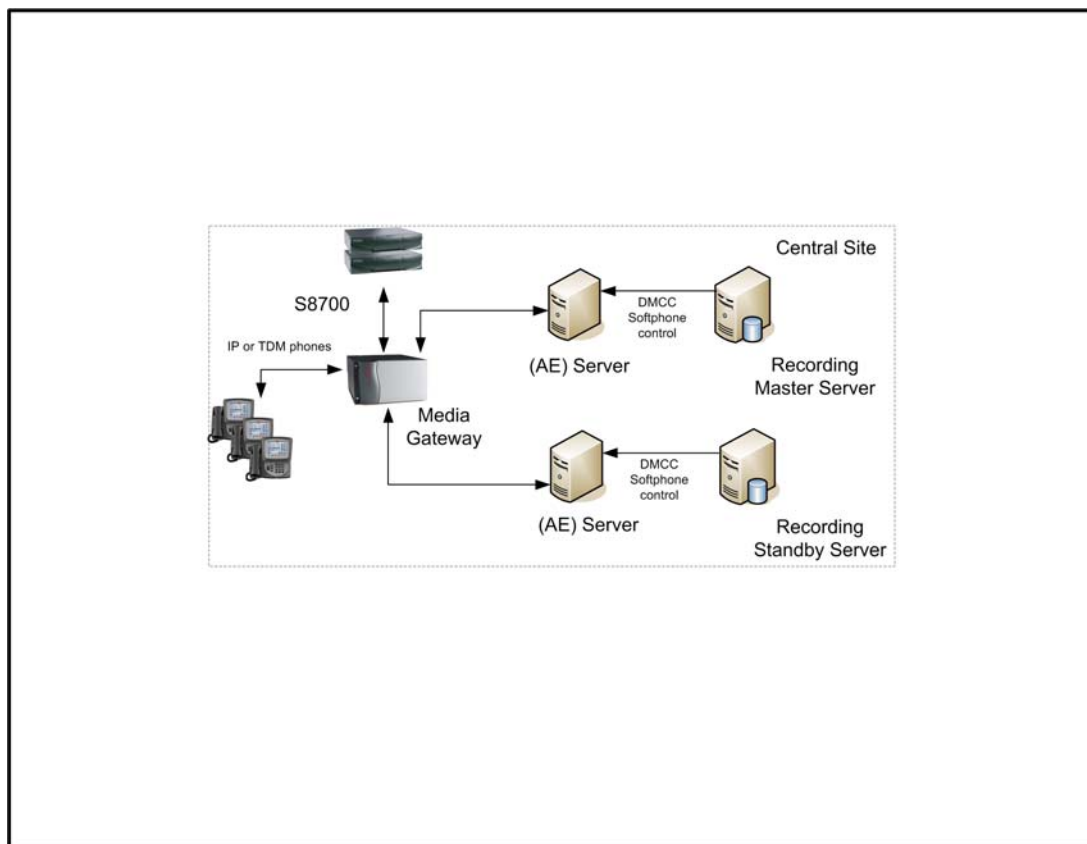
This is a complex topic and a brief summary of the options is given below. (See also [Fault Tolerant Systems](#) on page 343 for further details of how to design and configure fault tolerant systems)

Master/Standby Recorders

Instead of configuring all additional recorders as "Slaves", you can configure one of these as a "Standby" recorder. The standby copies configuration details automatically from the master via a fault-tolerant TCP/IP connection between the two. Over these same links, the two recorders exchange "heartbeats" every few seconds. The standby will take over should the heartbeat fail or should the master request that it do so. This latter case will

Confidential and Proprietary Information

occur, for example, due to the master's disk filling or connection to the CTI link failing. The figure below shows a typical configuration.



In small systems consisting of just a master and standby, details of recordings made on each server are (by default) passed to the other so that users can search for calls from a single location regardless of which of the two recorders actually recorded the call they are looking for. In larger systems, where a Master recorder controls one or more "Slave" recorders, the use of a Standby recorder ensures that the Master does not become a single point of failure for the whole system. In this case, each of the recorders permanently connects to both Master and Standby. This allows the Standby to take over rapidly should the Master fail. In such systems one or more dedicated servers can be provided solely to support search and replay. Details of recordings from all of the recorders are uploaded to these servers allowing a single search to cover all recordings.

Fault Tolerant Pools

When using any of the IP recording mechanisms (i.e. all bar TDM) with a Master, optionally standby and one or more Slave recorders, recordings can be directed towards any available recorder. Therefore a "pool" of recorders can be equipped with one more recorder than is needed for the projected loading. In this configuration, if one fails, the Master recorder will reassign the calls being recorded by the failed unit across the remaining servers.

Centralized Applications

While recorders are often distributed around the network, most other applications are centralized and available to all from one location. See Optional Server Applications on page 20 for further details on these.

Confidential and Proprietary Information

Integrating with other systems

The Avaya Contact Recorder system supports integration with a wide variety of other applications including other CTI feeds, third party and customers' own applications. There are three options, depending on the complexity of the integration required.

Standardized Dialer Integrations

An automated or predictive dialer is often used with Avaya switches. These typically require an agent to connect to a specific port on the switch for the duration of their shift. The basic recording system will see this shift as a single, long call and will not be aware of the individual customer calls that are handled by the agent. Avaya Contact Recorder includes support for a number of commonly encountered dialers. When configured to suit your dialer and data structures, these split and tag the recordings so that each customer call is stored as an individual recording and can be found by searching for one or more data fields provided by the dialer.

See [Appendix F: Auto-Dialer Integrations](#) for details of the current integrations and how to configure these. Note that most of these integrations are charged for and licensed separately.

Supplementary Tagging of Bulk Recordings

It is a common requirement to "tag" recordings with additional details, such as customer account numbers, trouble-ticket numbers etc. This information is often held in a third party or custom application and is known while the call is in progress.

The recorder implements a TCP/IP socket based interface. Applications can:

- receive events as recordings start and end
- send "tag" information to the recorder to be associated with the recording, alongside the basic call details.

Users can then search for recordings based on this enhanced set of call details.

This Recorder Control Protocol is very simple as the recorder makes contact with the application at an IP address specified in the recorder's administration pages. The recorder advises the application as recordings start and stop on each phone. Each start message contains a unique reference (or "INUM") to that recording. If the application wants to tag a call, it sends a "TAG" command specifying the INUM and station number plus the data formatted as XML.

Planning and Prerequisites

In this mode, the recorder continues to be responsible for recording rules. Should the tagging application have a problem, the worst it can do is tag calls incorrectly.

This interface is included within the core Avaya Contact Recorder software and you may use it immediately. A typical tagging project requires the purchase of 2-3 person-days of services to learn how to interface to and control the recorder.

See [External Control Interface](#) on page 321 for further details of the Recorder Control Protocol, associated APIs and example applications that are available.

Explicit External Control of Recording

In normal operation, the recorder is given some basic rules, that it uses to determine which calls are to be recorded. However, you can build more sophisticated recording systems in which the decision to record is made by an existing call routing/handling application. By including control of recording as an integral part of call flow, such applications can, for example,

- automatically mask or stop recording a call during security questions and resume once the customer has been validated
- automatically start recording as the agent accesses the "customer complaint" form
- add additional tagging as the agent traverses a series of menus

Applications can control recording using the same interface as described under [Supplementary Tagging of Bulk Recordings](#) on page 87. By using the additional commands "START", "STOP" and "BREAK", they can override the rules applied by the administration interface.

This interface is included within the core Avaya Contact Recorder software and you may use it immediately. A typical external control project requires the purchase of five person-days of services to learn how to interface to and control the recorder.

Confidential and Proprietary Information

■ ■ ■ ■ ■ ■

Chapter 3: Installation

This chapter gives details of the steps to install an Avaya Contact Recorder system.

The main sections in this chapter are:

- [Overview](#) on page 90
- [Avaya System Configuration](#) on page 91
- [Order in which to Install Applications](#) on page 102
- [Platform Prerequisites](#) on page 103
- [Installing Avaya Contact Recorder](#) on page 110
- [Installing Workforce Optimization \("WFO"\)](#) on page 112
- [Installing Avaya Contact Recording Desktop \(CRD\)](#) on page 113
- [Installing Screen Capture Software](#) on page 117

Note:

Always refer to the Release Notes for the specific patch version you are due to install. These may contain additional information that was not available at the time this manual was prepared.

Note:

Upgrading Existing Systems

This chapter describes how to install the software on a new system. If you are **upgrading** an existing system, you must refer instead to the release notes for the new version and to the *Avaya Contact Recorder, Release 12, Technical Note: Migration from previous versions of Avaya proprietary recorders (CSCM, ACR and NES) to ACR 12.0*. These highlight issues when upgrading from earlier releases and may require you to upgrade via an intermediate release - using the release note for the latest patch of that version.

Overview

Installation of a complete recording system requires:

- Configuration of your Avaya system to support recording.
- Planning the order in which to install the application servers
- Preparing each server
- Installing the Avaya software on each server
- Installing screen capture software on workstations that are to be recorded (if any).

Confidential and Proprietary Information

Avaya System Configuration

Before installing any Avaya Contact Recorder components, you must ensure that your Avaya telephony system is correctly configured and, where necessary, upgraded to support the recording system. As you complete these steps you will be asked to note a number of details which you will need later when configuring the recorder.

Prerequisites

Refer to the appropriate Avaya documentation to apply any prerequisite upgrades and/or additional licenses as detailed in Chapter 2. Then continue with this Chapter, applying the configuration checks and/or changes for your particular switch type(s) as described in the following sections.

Communication Manager Configuration

Use the Avaya administration interface to configure the following items:

Note:

Where page numbers are mentioned on the Avaya administration interface, these are a rough guide only. As new settings are added from one version of Communication Manager to the next, these page numbers tend to increase.

Customer-options

Set the required system parameters as follows:

1. Run the following command
`display system-parameters customer-options`
2. On page 4, verify that **Enhanced Conferencing** is set to **y**.

Features

You must set the following system-wide CM parameters.

1. Enter the following command line:
`change system-parameters features`

Confidential and Proprietary Information

Installation

2. On Page 5, set **Create Universal Call ID (UCID)** to **y** and allocate a number to the switch if it does not already have a unique reference. If there is only one switch, set it to **1**.
3. On Page 13, set **Send UCID to ASAI**.

Device Names

You are strongly advised to ensure that all devices to be observed, recorded or used in recorder (i.e. stations, softphones, agents, splits and VDNs) have a Name configured. Otherwise you may encounter errors when attempting to record these stations.

Adding IP softphones

You must add a station on the Communication Manager for each DMCC recording or replay port you require on the recorder. Create all stations identically. You will subsequently use the recorder's Administration pages to assign them to the various modes.

1. Use the **add station** command to add as many stations as there are ports on your recorders. Note the station numbers as you will need to enter these into the recorder later.
2. Run **add station xxxx**, where **xxxx** is the new station's extension that you want to administer.
3. For **Station Type**, enter **4624**.
4. For **Security Code**, enter the numeric security code the recorder must use to register softphones with the Communication Manager. Note this security code as you will need to enter it into the recorder later. Use the same code for all stations you create for the recorder.
5. In the **IP Softphone field**, enter **y**.
6. Set **Display Language** to **english**.
7. On Page 2:
Set **IP-IP Audio Connections** and **IP Audio Hairpinning** to **n**
8. On Page 4:
 - a. Assign the following feature button in addition to the three default call appearances:
 - i. Button 4: **conf-dsp**
 - b. Clear the **call-appr** setting on Button 3.

Confidential and Proprietary Information

```

change station 11001                                     Page 1 of 4
                                                    STATION
Extension: 11001                                         Lock Messages? n      BCC: 0
  Type: 4624                                             Security Code: 12345  TN: 1
  Port: S00081                                          Coverage Path 1:     COR: 1
  Name: CCE Line 01                                     Coverage Path 2:     COS: 1
                                                    Hunt-to Station:

STATION OPTIONS
  Loss Group: 19                                         Personalized Ringing Pattern: 1
                                                    Message Lamp Ext: 11001
  Speakerphone: 2-way                                    Mute Button Enabled? y
  Display Language: english
  Survivable GK Node Name:
  Survivable COR: internal                               Media Complex Ext:
  Survivable Trunk Dest? y                               IP SoftPhone? y
                                                    IP Video Softphone? n

change station 11001                                     Page 3 of 4
                                                    STATION
SITE DATA
  Room:                                                  Headset? n
  Jack:                                                  Speaker? n
  Cable:                                                 Mounting: d
  Floor:                                                 Cord Length: 0
  Building:                                             Set Color:

ABBREVIATED DIALING
  List1:                                               List2:               List3:

BUTTON ASSIGNMENTS
  1: call-appr                                         7:
  2: call-appr                                         8:
  3:                                                    9:
  4: conf-dsp                                          10:
  5:                                                    11:
  6:                                                    12:

```

Administering hunt groups

If you want to use On Demand Recording or Meeting Recording modes, consider grouping these ports into one or more hunt groups for each mode. Users can then access the recording functionality through the number of the hunt group rather than through individual ports.

Installation

You could assign all ports for a recording mode to a single hunt group to provide a single shared pool of ports, available on a "first come, first served" strategy. Alternatively, you could split the pools into several independent hunt groups - or even leave some individual ports. For example, a dedicated port to be used only by the conference phone in the board room would ensure that meetings there could always be recorded.

For more information about hunt groups, refer to Managing Hunt Groups in Chapter 7: Handling incoming calls, in Volume 1 of the *Administrator Guide for Avaya Communication Manager*.

Note which ports you have assigned to which hunt groups.

Configuring tone detection

The recorder uses tone detection for **Meeting Recording** and for the delete and retain commands in **Bulk Recording**. To configure tone detection:

1. Type `change system-parameters ip-options`.
2. In the **Intra-System IP DTMF Transmission Mode** field on Page 2, enter `rtp-payload`

```
change system-parameters ip-options                               Page 2 of 2
                        IP-OPTIONS SYSTEM PARAMETERS

Always use G.711 (30ms, no SS) for intra-switch Music-On-Hold? n

IP DTMF TRANSMISSION MODE
  Intra-System IP DTMF Transmission Mode: rtp-payload
  Inter-System IP DTMF: See Signaling Group Forms
```

Network Region setup

The recorder requires the following:

- The DMCC softphones used as recorder ports must be in an IP network region that supports G.729A and G.711MU with 60ms packet intervals and NO OTHER CODECS.
- There must be a media gateway or a media processor resource in the same network region or in an interconnected network region.

To set up a network region as above:

Create a Codec Set

Create a new codec set specifically for the recorder(s) as follows:

1. Choose an unused codec set number for the recorders

Confidential and Proprietary Information

2. Use the `change ip-codec-set setnumber` command to create a codec set that uses G.729A and G.711MU
3. Verify that G.711MU and G.729A are the ONLY codecs in the codec set.
4. Set **Silence Suppression** to `n`.
5. Set **Frames Per Pkt** to 6 - which will show a **Packet Size** of 60 (ms).
6. Set the first two **Media Encryption** options to `none` and `aes` respectively.
7. On page 2, ensure that **FAX, Modem, TDD/TTY** are all set to `off`.
8. Also on Page 2, ensure that **Allow Direct-IP Multimedia** is set to `n`.

```

                                IP Codec Set

Codec Set: 4

Audio          Silence          Frames          Packet
Codec          Suppression        Per Pkt        Size(ms)
1: G.711MU      n                6              60
2: G.729A      n                6              60
3:
4:
5:
6:
7:

Media Encryption
1: none
2: aes
3:

```

Refer to the following for further information:

- For an explanation of administering IP codec sets, refer to the Administering IP Codec Sets Section, in Chapter 4: Network Quality Administration, of the *Administration for Network Connectivity for Avaya Communication Manager* guide.
- For a screen reference, refer to the IP Codec Set Section, in Chapter 19: Screen Reference, of the *Administrator Guide for Avaya Communication Manager*.

Create a network region

Create a new network region and assign the previously created codec set to it as follows:

1. Choose an unused network region for the recorders' softphones
2. Type `change ip-network-region region` where `region` is the number of the chosen network region.
3. Specify the Codec Set created in the previous step.

Confidential and Proprietary Information

Installation

4. Set the two **IP-IP Direct Audio** options to **No**.
5. Set **IP Audio Hairpinning** to **n**.
6. Now update the region-region codec table so that all existing regions will use this newly created codec set when communicating with the network region that you have just created for the recorder's softphones.

Refer to the following for detailed information:

- Administering IP Network Regions Section, in Chapter 4: Network Quality Administration of the Administration for *Network Connectivity for Avaya Communication Manager* guide.
- For a screen reference, refer to the IP Network Region Section, in Chapter 19: Screen Reference of the *Administrator Guide for Avaya Communication Manager*.

Assign softphones to the network region

To ensure that the recorder's softphones register in the network region created above, use the `change ip-network-map` command.

Add the IP address of the AE Server to the new network region so that all the recorder's softphones - which register via that AE Server - are created in this network region.

The following example shows how to complete the form. In this example, the AE Server is using network region 10 with an IP address of 192.168.2.100.

```
change ip-network-map                                     Page 1 of 32
                                     IP ADDRESS MAPPING
                                     Subnet
                                     or Mask) Region  VLAN  Emergency
From IP Address  (To IP Address  Location
192.168.2  .100  192.168.2  .100  10      n      Extension
. . .           . . .
. . .           . . .
. . .           . . .
```

AE Server Configuration

The AE Server provides the recorder with DMCC client services, TSAPI services and (if specifying which CoRs are to be recorded) SMS Web Services. The following instructions assume the AE Server has been installed specifically for recording and that OAM and User Management administrative accounts have been created. If the AE Server to be used is already in use for other purposes, check these settings and confirm that its current configuration is appropriate.

Confidential and Proprietary Information

▲ Important:

If you have more than one AES and intend to use ACR's fault tolerant capabilities you must name the Switch Connection the same on each AES

Administer C-LANs

Use the AES Administration Screens to add the C-LANs that will be used to register softphones.

1. From the **CTI OAM Admin OAM** main menu, select:
Communication Manager Interface > Switch Connections
2. Click **Edit H.323 Gatekeeper**. OAM displays the Edit H.323 Gatekeeper - Switch1 page.
3. In the **Name or IP Address** field, type the *hostname* or *IP Address* of the switch C-LAN, and then click **Add Name or IP**.

TSAPI Configuration

Even if there are no explicit CTI clients, you must configure TSAPI (previously known as Avaya CT). Do this after AE Services have been configured as above. If you are using a Security Database as part of your AES TSAPI setup, you must ensure that the recorder is granted access to all the addresses (stations, VDNs and skill hunt groups) that it will need to observe.

SMS Web Services Configuration

If you wish to control which stations are recorded by assigning them to specific CoRs you must enable SMS Web Services to allow the recorder to determine which CoR each station is in. The recorder will use HTTPS to port 443 on the AE Server to determine which stations are in each CoR.

User Account

If you are using the Security Database for Authentication, create a CTI user account on the AE Server as follows:

1. Go to: **User Management > Add User**
2. Complete all of the required fields (indicated by an asterisk).
3. Select **userservice,useradmin** from the **Avaya Role** drop-down menu.
4. Select **Yes** from the **CT User** drop-down menu.
5. Ensure that the new CTI user has access to all TSAPI-controlled devices by going to:
Administration > Security Database > CTI Users > List All Users

Confidential and Proprietary Information

6. Click **Enable** next to the **Unrestricted Access** option.

CS1000 Configuration

Update Call Server

In addition to the prerequisites detailed in Chapter 2, you must ensure that your call server has the latest SU and PEPs.

Check/Set Parameters

Ensure the following parameters are set:

Setting	Description	Value
ISAP	Integrated Services Digital Network/Application Protocol (ACD messages sent across the ISDN/AP link). (Overlay 23)	Default=NO. Set to YES only for Meridian Mail applications. Hence for AML/ELAN messages it should remain NO.
SECU	Security Setting for Meridian Link applications. (Overlay 17, VAS configuration)	When set to NO, the host computer must specify both the TN and DN of the associate set in connect, answer and release messages. For AML/ELAN messaging this should be set to YES.
IAPG	Meridian Link Unsolicited Status Message (USM) group. IAPG assigns AST DNs to a status message group defined in LD 15. These groups determine which status messages are sent for an AST set.	The default Group 0 sends no messages, while Group 1 sends all messages. For AML/ELAN messaging it is better to set it to 1.
ICRA (Rel 6) or RECA (Rel 7)	IP Call recording allowed. (Overlay 11)	Set to YES for each IP phoneset that is to be recorded using duplicate media streaming.

Confidential and Proprietary Information

Configure ROD and SAVE Keys

To configure either a ROD (Record on Demand) or SAVE key on an IP telephone, use the KEY entry in Overlay 11.

Example:

- **KEY 03 ROD** This configures Key 3 with the ROD button
- **KEY 03 SAVE** This configures Key 3 with the SAVE button

Determine Meridian Link Services (MLS) Connection Details

Note the following details that you will need when configuring the Avaya Contact Recording Master later in the installation process:

- the IP address of the Avaya Contact Center Manager Server
- the IP address of any fallback Avaya Contact Center Manager Server to be used in the event of failure of the default server
- your Meridian1 Customer Number (if using a multi-tenanted system)
- your Meridian1 Machine Name (if using a multi-tenanted system)

Record on Demand and Save Keys

Customers running CCMS release 7.0 or higher (AACC) and CS1000 release 6.0 or higher can give users with IP phones control over recording and deletion/retention of recordings. (See the Distributor Technical Reference Bulletin for additional information on this feature).

To use these features:

1. Apply the necessary CCMS licenses.
2. Add ROD and/or SAVE buttons to the appropriate IP phones

As you set up [Bulk Recording](#) on page 150, ensure that you

1. Set the appropriate **Recording Control** options. For standard "on demand recording" you should set:
 - **Start recording automatically at start of call** off
 - **Allow user/external start/restart** on
 - **Allow user/external stop** on

To have recordings deleted unless deliberately saved you should set:

- **Allow user/external delete** on
- **Retain ONLY if requested by user/external** on

2. If using a SAVE key, indicate that this is present on the appropriate DN/Position Ids.

Confidential and Proprietary Information

AACC Configuration

AACC Installation

Refer to the *Avaya Aura Contact Center SIP Commissioning Guide (NN44400-511)* which provides full installation instructions.

Ensure that AACC is running the correct version, contains the required components and is licensed in accordance with the pre-requisite requirements shown on page 83.

CCT Web Services

CCT Web Services are only required for SIP recording. The Avaya Contact Recorder communicates with the AACC (when in SIP mode) via these web services which must be enabled and configured as follows:

- Click on **Start > Programs > Avaya > Contact Center > Communication Control Toolkit > CCT Console**
- In the left hand pane of the CCT console, select **Communications Control Toolkit > Server Configuration > CCT Web Services**
- Ensure the checkbox **Enable CCT Web Services** is ticked
- Increase the **Session Timeout** to a value that suits the deployment. The Default is 120 minutes but this should be increased. This parameter signifies the time after which the SSO token is revoked for the call recorder if the system is completely idle. So if it is expected that no calls occur overnight, this parameter should be set to a longer period (e.g. 24 hours = 1440 minutes).
- Note that for AACC 6.1 or later, there are additional entries in the **CCT Web Services** page for the Call Recording UserID, Domain and Password that must also be configured. With AACC 6.0, a fixed User ID ("CallRecorderUser") must be used.
- AACC 6.2, this issue is resolved and any normal windows userid can be used.
- Note also that the entry "**Domain Authentication Server**" is the actual server name of the Server that is running the Domain Controller Software.
- For Domain Authentication Method, use **Simple**. (If the alternative **Digest-MD5** is used, this then requires that the **reversible encryption** option is enabled on the Domain Controller for the CallRecordUser account)

Trusted Licensing (Communication Manager hybrid systems only)

Under normal conditions, the ACR application works with the AES platform by using default certificates which enables TLS operation. TLS operation is implicit as part of the named licensing implementation for ACR on the AES.

Confidential and Proprietary Information

However, the current installation procedure for AACC requires that an additional CA Root certificate and associated Signed Certificate are installed on the AES server. The impact of this change is that it temporarily breaks the existing default mechanism used by ACR and AES.

Therefore it is necessary to import the Root Certificate from the same CA (Certificate Authority) used by the AACC into the ACR as described in [Adding Additional AES CA Root Certificates to ACR](#) on page 390.

Test Phonesets

You should provide three Avaya phones close to the recorder - in the same or a neighboring rack. Configure these phones with all of the features in use on the phones that you intend to record. You can then use these to place test calls while working on the recorder.

Order in which to Install Applications

In many cases, the recording system will consist solely of a single Avaya Contact Recorder Master server. However, in topologies that are more complex it is important that you install the basic recording infrastructure first and then layer the other applications on top.

Note:

If you have multiple recorders, install and configure all Avaya Contact Recorders BEFORE connecting these to a WFO system.

Install server components in the order shown below:

1. Install one Avaya Contact Recorder (the Master if using Master/Standby and/or Master/Slave). Follow the procedures in [Platform Prerequisites](#) on page 103 and [Installing Avaya Contact Recorder](#) on page 110.
2. Install the Standby (if required) and any additional Slave recorders.
3. Install a central replay server if required as described in [Installing Avaya Contact Recorder](#) on page 110.
4. If using a Key Management Server for encrypted recording storage, install this and configure the recorder(s) as described in [Encrypted File Storage](#) on page 219.

Confidential and Proprietary Information

Platform Prerequisites

Before installing the Avaya Contact Recorder (Master, Slave, Standby or Central Replay Server) software on the designated server(s), you must prepare each server as described below.

Linux (Communication Manager, DMCC and Passive IP recording only)

Version

The operating system must be RedHat Enterprise Linux Version 6.0 (64-bit) Update 2 or higher. The operating system must be installed using the RedHat kickstart process. Avaya supplies a tool to generate the kickstart script automatically. If you cannot use the kickstart process you must contact us (as described in the section [Additional references](#) on page 21) for guidance.

Disk Storage

You must plan the partitioning of your server's disk(s) in line with the storage needs outlined in [Storage Requirements](#) on page 56. The kickstart script supports servers with one logical disk or two physical disks. If using RAID, use the RAID utility to make one large logical volume.

The kickstart script partitions the disk(s) as follows:

Mount Point	Use	One Physical or Logical Disk	Two Physical Disks
/boot	Bootstrap	100 MB	100 MB on first disk
/	Linux and Avaya Software	10.0 GB	10.0 GB on first disk
Swap	Virtual Memory	Twice RAM	Twice RAM on first disk
/var	Linux /var and the database	1 - 99 GB (configurable)	Remainder of the first disk
/calls	The recordings	Remainder of the disk	Whole of the second disk

Confidential and Proprietary Information

WARNING:

The size of /var must be calculated carefully based on the number of recordings per month and how many months the database records will be retained.

Creating the kickstart script

The preferred method requires a Windows machine with a CD drive and a floppy drive. The recorder must also have a (non-USB) floppy. If these requirements cannot be met follow the alternative process described under [Performing a kickstart install without a floppy](#) on page 105.

1. Format a floppy and insert it into the floppy drive of the Windows machine.
2. Insert the installation disk into the CD drive of the Windows machine. The kickstart script generation tool will start automatically.
3. Select the appropriate version of the Redhat operating system (for example, "RH5").
4. Fill in the form with the following information:
 - a. Select the keyboard layout of the recorder server
 - b. Select the timezone of the recorder server
 - c. If you have a corporate NTP server specify its IP address or fully qualified domain name. If you leave the entry empty the tool picks a suitable public server.

WARNING:

Because good time synchronisation is so vital you must take care with this setting and test that it is working after installation.

- d. Fill in the address and netmask for the first NIC.
- e. Specify the address of the default router, which must be in the same subnet as the address that you specify for the first NIC.
- f. Specify the hostname, preferably as a fully qualified domain name (e.g. `cscm1.bigcorp.com`)
- g. Specify the IP address of a DNS server
- h. If there is a second NIC and you want to enable it, fill in the address and netmask. This address must not be in the same subnet as the first NIC.
- i. For one logical drive or physical disk, select **1 disk**, and specify the size of the /var partition.

For two logical drives or physical disks, select **2 disks**, and specify the device names of the two devices. If you do not know the names of the two devices, follow the first few steps of a normal interactive RedHat installation. After selecting the keyboard type, the RedHat installer will display a menu showing the names of the devices.

Confidential and Proprietary Information

- j. Select the number of Linux tools to install. **Minimal** chooses just those parts of Linux needed to run the recorder (Choose this option only if you are familiar with Linux and will perform all installation from the command line.) **Recommended** installs other useful management tools and the Linux windowing system.
5. Click **Generate Floppy**.
 6. Eject the floppy.

Performing the kickstart install

1. Have the floppy just created ready.
2. Boot the target server using the first disk of the RedHat distribution.

 **WARNING:**

Make sure that the disks are the Update you require. RedHat and other vendors still sometimes supply Update 0 disks.

3. Wait for the `boot:` prompt.
4. Insert the floppy.
5. Type `linux ks=floppy`
6. Wait for the automated install to complete and insert the other disks when requested.

Performing a kickstart install without a floppy

If it is not possible to perform the recommended floppy-based kickstart installation, this HTTP based procedure may be used instead.

1. Follow the same procedure to fill in the kickstart script generation tool, except at the last step click **Generate File**. Use the file chooser to specify the location where the file will be saved. Make sure the file is called `ks.cfg`.
2. Copy the `ks.cfg` to a web server and make it available as a web URL. The web server must not use a non-standard port. It must use port 80. Be certain when copying the file that it receives no text processing. If copying it using FTP be sure to use BINARY mode. Do not edit the file. Test that you can view the file using a regular browser.
3. Ensure that the target server will be able to obtain a dynamic IP address using DHCP on its first NIC. If necessary, temporarily cable its first NIC to a corporate LAN segment. Ensure that it will be able to access the web server.
4. Boot the target server using the first RedHat disk, and wait for the `boot:` prompt.
5. Type `linux ks=http://webserveripaddress/path/ks.cfg`

Expert kickstart options

Great care must normally be taken to ensure that the `ks.cfg` file is not corrupted or edited. The process of creating this file directly to a floppy and taking that floppy directly to the target server is the recommended approach.

Confidential and Proprietary Information

Installation

If the file must be edited to access expert options this should be performed on a Unix or Linux computer. Windows editors introduce additional control characters that prevent the script from working properly. Unfortunately the installation of Linux appears to work, but the Avaya software will not install correctly.

There is almost no reason to edit the automatically generated file, but details of the script options are available at

https://access.redhat.com/knowledge/docs/en-US/Red_Hat_Enterprise_Linux/6/pdf/Installation_Guide/Red_Hat_Enterprise_Linux-6-Installation_Guide-en-US.pdf

Windows

Version

Use Windows Server 2008 R2 for all new installations.

Disk Storage

You must plan the partitioning of your server's disk(s) in line with the storage needs outlined in [Storage Requirements](#) on page 56. Partition the disks of all servers so that the operating system and recordings storage are both separated and secure. For the Avaya Contact Recording application, prepare three partitions, shown below as C:, D: and F:. (The E: partition needs no preparation.)

- C: will hold the operating system and other tools/applications - this need only be a few GB. 10 or 20GB is recommended
- D: will hold the Avaya Contact Recording application. This will include the local call details database and should be sized at 10GB + 2GB per million recordings that you want to keep accessible in the local database. Do not forget that the Master and Standby (or dedicated Replay server if you are deploying one) will hold details of recordings made on all recorders, not just their own.
- E: CD/DVD
- F: will hold the actual recordings. See [Storage Requirements](#) on page 56 for sizing guidance.

DVD+RW / Blu-ray Drive(s)

If you intend to use one or more removable optical media drives for archiving calls directly from the Avaya Contact Recorder, you must install and test your drives by writing a test file to each drive before attempting to use it with the recording system.

Confidential and Proprietary Information

You should also confirm that the recorder application will be able to access the drive. The details of this differ according to the operating system in use.

Linux

RedHat Enterprise Linux 5 (or higher) incorporates new features as part of its Hardware Abstraction Layer. You need additional steps to turn off the HAL's media detection service, which interferes with the archiver.

To disable the media detection service follow these steps:

1. Execute the "lshal" command and direct its output to a file

```
lshal > hal.txt
```

2. Open the created file and look for the string `storage.drive_type`. It will list all devices, local and external, so you will find the floppy, cdrom etc.
3. Locate your device. It would be either cdrom, cdrom1..etc, or dvd.

The adjacent lines for storage model and vendor will contain specific details regarding the device, for example:

```
storage.serial = 'HL-DT-ST_DVDRAM_GSA-E50L_P01070913222527'
(string)
storage.vendor = 'HL-DT-ST' (string)
storage.model = 'DVDRAM GSA-E50L' (string)
storage.drive_type = 'cdrom' (string)
```

4. Scroll up until you find the line starting `udi =`

The udi is likely to be in the form

```
/org/freedesktop/Hal/devices/storage_serial_vendor_model_serial
number
```

For example:

```
Udi='/org/freedesktop/Hal/devices/storage_serial_HL_DT_ST_DVDRA
M_GSA_E50L_P01070913222527'
```

5. Test the value of the `media_check_enabled` flag using the `hal-get-property` command. Substitute your actual UDI into the commands:

```
hal-get-property --udi /org/freedesktop/Hal/..... --key
storage.media_check_enabled
```

the result is likely to be "true" - it needs to be "false"

6. Set it to false using `hal-set-property` command:

```
hal-set-property --udi /org/freedesktop/Hal/..... --key
storage.media_check_enabled --bool false
```

7. Re-check that the value is now "false" using the command in step 5.

Confidential and Proprietary Information

Installation

8. Add the command from step 6 into the file `/etc/rc.local` (This will run the command automatically for you every time the machine reboots.)
9. To find the soft link created for the device return to the text file, and look for the value for "block.device" in the Device's settings. It will look something like this:

```
block.device = '/dev/scd0' (string)
```
10. Enter the location in the recorder under **Operations > Archive > Add DVD Drive > Drive path(s)**.

Windows

To use a DVD drive for archiving, you must:

1. Promote the acrservice account to be an administrator account.
2. Check that in Group Policy Editor 'Security Settings' - 'Local Policies' - 'Security options' the setting 'Devices: Restrict CD-ROM access to locally logged-on user only' is disabled.
3. Check that the registry key
HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\AllocateCDRoms is set to 0.
4. On Windows 2008 you must set the **Never Notify** option on **Control Panel > User Accounts > User Accounts > Change User Account Control Settings**

Time Synchronization

You must synchronize all servers to the same source as your telephony switch. This will minimize any time differences if you need to compare events on the telephone system with timestamps of recordings or entries in log files.

Java Timezone (TZ) Update

Avaya ensures that the version of Java installed with Avaya Contact Recorder is up to date. However, governments sometimes change time zone rules. If your time zone rules change, you should update the Java time zone rules using the TZ Updater patch for Java. This patch provides updates to the time zone rules and, without it, the previous rules will be applied. This patch is located at

<http://www.oracle.com/technetwork/java/javase/tzupdater-readme-136440.html>

Please check the instructions carefully. Sometimes the operating system must also be patched.

Confidential and Proprietary Information

Network Connectivity

Disable Media Sensing (Windows only)

 **CAUTION:**

Windows contains a "Media Sensing" feature which can cause problems for recorders. Should all NIC cards in a server lose connectivity at the same time, this feature can lead to the recorder looping with 100% CPU usage. You must disable this feature by following the instructions in <http://support.microsoft.com/kb/239924/en-us>

Domain Name Server (DNS) Entries

Ensure that the IP node names of all servers that make up the recording system are stored in the appropriate Domain Name Servers. Subsequent configuration can then be done by using the host name rather than having to use numeric addresses.

 **Important:**

The Domain Name Server(s) used by the recorders must support reverse name resolution.

Network Routes

You should ensure that valid IP paths exist between each of the servers and from servers to the CTI interfaces, audio sources and recorded workstations. See [Recorder Interfaces](#) on page 264 for details of ports used.

Bonded or Teamed NICs

If you are deploying Master/Standby pairs of Avaya Contact Recorder Servers on the same site, it is imperative that you provide bonded or teamed (same effect, different operating system) NICs in the master and standby servers and fully fault tolerant network connectivity between the master and standby. Failure to do so will leave the system vulnerable to failure should a common component in the network paths between the two fail. In such a case, both recorders will attempt to take control of all recording, with unpredictable results.

Installing Avaya Contact Recorder

Note:

If you are installing a Central Replay Server, a Standby recorder or Slave recorder, you should first read the appropriate section in [Advanced Configuration](#) on page 223.

Linux

To install Avaya Contact Recorder on RedHat 6 (64-bit) from the command line

1. Log onto the server as root.
2. Insert the ACR installation DVD
3. Mount the installation DVD (replace /dev/cdrom with your device name if different)
`mount -r -t iso9660 /dev/cdrom /mnt/cdrom`
It may be necessary to create the /mnt/cdrom mount point using the command
`mkdir /mnt/cdrom`
4. Change directory to the mount point using the command
`cd /mnt/cdrom`
5. Locate the three rpm files on the CD using the command
`ls`
Install the cscm and **one** of the jre rpm files using the following command - replacing **rpmfilename** with the name of the file. Choose the jre rpm with the name including "amd64" for 64-bit systems (which all new installations must use).
`rpm -Uvh --nodeps rpmfilename`
6. Reboot the server.
7. Continue the system configuration as described in [Configuration](#) on page 119.

Note:

Should you need to uninstall Avaya Contact Recorder, use the command
`rpm -e cscm`

Windows

To install Avaya Contact Recorder on a Windows server:

1. Log on to the server using an Administrator's account

Confidential and Proprietary Information

2. Insert the Avaya Contact Recording DVD. This contains the Avaya Contact Recording installation kit.
3. The installation menu should start automatically. If it does not, navigate to the CD and double-click setup.exe found in the \ACR folder.
4. Select Run (not Save) and then follow the instructions on the screen to set the path where you want to install the application. Note that this also determines the location of the call detail database. This must be installed on the D partition which must have adequate space for your call details as described in [Storage Requirements](#) on page 56.

Note:

The installation process creates a local user account.

5. If you require any of the advanced or non-standard features that are controlled by entries in the properties file, set them now. See [Properties File](#) on page 224 for details.

 **Important:**

The default operation of ACR 12.0 with a CS1000 switch assumes that both Contact Center Manager Server 7.0 (or later), CS1000 release 6 (or later) and the appropriate number of MultiDN licences on CCMS (appears as "Multiple DN Registration" on the CCMS License Manager Real Time Usage Screen) are present. If any of these three conditions are not present, then you must manually place an entry into the ACR properties file that ensures the ACR is operating in "CC6 mode". The required entry is: `cc.v6=true`. See [Properties File](#) on page 224 for more details.

6. Complete the system Configuration for a Master recorder server as described in [Configuration](#) on page 119

Installing Workforce Optimization ("WFO")

To configure Avaya Contact Recorder and WFO, please refer to the Technical Note *Avaya Contact Recorder Integration to Workforce Optimization Guide*

Confidential and Proprietary Information

Installing Avaya Contact Recording Desktop (CRD)

Important:

This application is available for CS1000 systems only.

For each agent that requires this application on his PC, you must:

1. Install Avaya Contact Recording Desktop on the agent's PC
2. Configure the master Avaya Contact Recorder with details of this desktop
3. Configure the application on the agent's PC

See the [Contact Recording Desktop \(CRD\)](#) section under "Advanced Configuration" for full details of functionality and configuration options.

Installing CRD on the Agent's PC

1. On the agent's PC, access the CD
2. Open the Avaya Contact Recorder Desktop Installation Folder
3. Double click *setup.exe*.
4. Click OK.
5. Click the computer icon in the upper left corner of the screen.
6. Ensure that Contact Recording Desktop is selected in the Program Group field.
7. Click Continue. The installation will begin.
8. When the installation is complete, a dialog box states Contact Recording Desktop Setup was completed successfully.
9. Click OK.

Configure the master Avaya Contact Recorder

The fields and buttons available on each agent's PC can be configured as required. Different groups of agents can be given different layouts if needed.

To set these up:

1. Navigate to the master Avaya Contact Recorder and login as an administrator.
2. Locate the dcs.xml file. The default location is
D:\ProgramFiles\Avaya\ContactRecording\properties\desktop.

Confidential and Proprietary Information

Installation

3. Make a copy of the dcs.xml file in this directory, giving it a name of your choice. If you need to configure different groups of agents with different desktop layouts, you will need multiple copies - one for each group.

Note:

Do NOT use the example dcs.xml file as this will be overwritten on upgrades. Always take a copy.

4. In the <pcs> section, replace the existing (dummy) entries with the computer name and the DN of the phone(s) you wish to control. Use the following format, substituting the client machine name for Computer1 and the DN for DN1. When you have completed entering client machine names and DNs, ensure that the </pcs> line follows the last entry in your list as below.

```
<pcs>
  <pc name="Computer1" extension="DN1" />
  <pc name="Computer2" extension="DN2" />
</pcs>
```

5. Repeat for each agent.

For example:

Using computer names *xyzcoagt1* and *xyzcoagt2*, and DNs 1000 and 1001 respectively, you would enter:

```
<pcs>
  <pc name="xyzcoagt1" extension="1000" />
  <pc name="xyzcoagt2" extension="1001" />
</pcs>
```

Confidential and Proprietary Information

6. In the `<udfs>` section, you will specify the user-definable fields. These fields are displayed on the Avaya Contact Recording Desktop GUI on the agent's PC. The format is:

```
<udf name="field header1" label="text field" type="text">
  <mask>#</mask>
</udf>
```

Replace "field header1" with a field name of your choice.

Repeat for each field.

Ensure you have `</udfs>` at the end of your field list on the following line.

Example:

```
<udfs>
  <udf name="spare1" label="First Field" type="fixed">
    <entry>Fixed Text Entry</entry>
  </udf>
  <udf name="spare2" label="Second Field" type="text">
    <mask>##/##/####</mask>
    <mask>[abcd]</mask>
    <mask>[!xyz]</mask>
    <mask>##/##/####</mask>
  </udf>
</udfs>
```

7. In the buttons section, define which buttons on the Avaya Contact Recording Desktop GUI you would like the agent to see. There are five options: **start**, **stop**, **update**, **delete**, and **retain**. You control the agent's access to these by editing the `mode="disabled"` to `mode="enabled"` for the buttons you would like them to control.
8. Save your changes to the `dcs.xml` file. These take effect when you next stop and then start the Avaya Contact Recorder service.
9. Login to the Avaya Contact Recorder application on the master.
10. Access the Bulk Recording tab via the Operations tab.
11. You can choose to apply global settings to all of your agents or you can specify the parameters for each DN/PosID to give individual agents their own unique access to the level of control they have over the GUI. You must set the name of the xml file to be used to control the layout of each group of agents.

Installation

- For individual settings click on the Edit field next to the DN/PosID you want to configure and then use the options listed under the advanced button of each DN/PosID.

After you complete the settings for an agent, click **Save** to close the window.

Repeat for each agent that you want to assign individual settings.

- For global settings, edit the fields in the Bulk Recording tab. Choose each of the parameters by clicking on **Edit** and selecting **Yes** or **No**.

Note:

Settings made under the advanced button of each DN/PosID override settings made globally.

Configure the Contact Recording Desktop application on the agent's PC

Complete this procedure to configure the Contact Recording Desktop application for the agent to login to the application from their own desktop. You perform this procedure at each agent's PC.

1. Right-click on the system tray icon and select **Configure**.
2. Enter DN number in the Extension field and the IP address of the master Avaya Contact Recorder in the server field.
3. The port number is preset at 8232. Avaya recommends you use the default.
4. In the Backup server section, enter the IP address of the standby Avaya Contact Recorder, if any.
5. Click **Apply**.
6. You will be prompted to enter a username and password. Leave the default username. The password is *admin*, all lowercase.
7. After successfully saving the parameters, the login page is displayed. Click **Logon**.
8. The status displayed in the tool tip of the system tray icon will be Line Idle. Double click on the system tray icon.
9. The Contact Recording Desktop application will display. You can view the user-defined fields and buttons that you specified in the dcs.xml file.

Confidential and Proprietary Information

Installing Screen Capture Software

To configure Avaya Contact Recorder and Screen Capture, please refer to the Technical Note *Avaya Contact Recorder and Screen Capture*.

Confidential and Proprietary Information



Chapter 4: Configuration

This chapter gives details of the steps to configure an Avaya Contact Recorder system.

The main sections in this chapter are:

- [Overview](#) on page 120
- [Accessing the System](#) on page 121
- [Licensing](#) on page 123
- [Email Configuration](#) on page 141
- [System Monitoring](#) on page 142
- [Operations](#) on page 146
- [Archive](#) on page 161
- [Search and Replay](#) on page 171
- [Backup/Restore](#) on page 182
- [Distributing User Instructions](#) on page 186
- [Configuring Avaya Support Remote Access](#) on page 189

Overview

You must now configure the recording suite to suit your requirements. This section guides you through the various tasks in a logical order. You should follow its steps immediately after installation of the Avaya Contact Recorder application.

Confidential and Proprietary Information

Accessing the System

Before you can configure the system, you must first:

- access the administration web-interface via its URL
- log in

URL

You administer the Avaya Contact Recorder system via a web interface.

1. Open Internet Explorer and navigate to `http://servername:8080` using the name of the server you wish to administer.
2. Enter a username of your choice and leave the password field blank.
3. Click **OK**.

Note:

The login page uses Javascript. If you see the login page but nothing happens when you click **OK**, your Internet Explorer settings may be blocking this. See [ActiveX Control Download](#) on page 173 for detailed instructions on this and other necessary settings.

Initial User Account

The application will accept any username during the first log on attempt after installation and will automatically create a local application account for you under that name and give it full system administrator rights.

As the password of this account has not yet been set, the web application immediately directs you to a page asking you to set the password for this account. In this instance, leave the **Old Password** field blank and enter a new password of your choice into the two other fields. This password must be at least 8 characters long, include upper and lowercase characters, at least one digit and at least one special character (#,@,%,! or \$). Click **OK**.

 **Important:**

Make a note of this username and password otherwise you will not be able to access the web application in the future. Note that both username and password are case sensitive.

Confidential and Proprietary Information

Key Points

Before using the System Administration pages, familiarize yourself with the following key points.

Invalid settings

Any of the system's settings that are known to be invalid are shown in red. Use the information in this guide to change the settings to valid values. If you change a setting, but submit an invalid entry, a message indicates the reason that the entry is rejected and you are prompted to re-enter it. To quit without changing a parameter, click on the **Close Window** link.

Show All

At the top of pages that show a list of entries that spans more than one page, the **Show All** link appears next to the page selection tags. When you click this link, all the search results are presented on a single scrollable page.

Page at a Time

If you have clicked the **Show All** link described above, you can return to seeing one page of entries at a time by clicking this link.

Impact of changes

When you change a setting, the window into which you enter the new setting explains the meaning of that setting and the consequences of changing it. Read these notes carefully. Some settings require you to restart the recorder while others may truncate current recordings.

Confidential and Proprietary Information

Licensing

Until you enter a valid License Activation Key, connect to a licensed Master recorder or select the Five day timed trial license, the application will only show you the license entry screen. Note that the timed trial license only allows you to run a single (master) ACR server.

Terminology

License Generation Key

This is a three digit number that is specific to a particular server. This is shown on the license entry page. You will need it to obtain a valid License Activation key for a Master recorder and Central Replay Server.

License Activation Key

This is a long (30 or more characters) string containing the serial number, server type and other options that you have licensed. You must obtain this key and enter it into the administration pages before your master recorder or central replay server will operate.

Recorder Serial Number

This is a unique identifier for every Avaya Contact Recorder. For Avaya Contact Recorders, this is a 6-digit number starting with 8. The serial number of each Master and Central Replay Server is allocated by Avaya as part of the licensing process.

The serial number of a slave or standby recorder is chosen by you. You should assign each slave and standby recorder in your enterprise a unique number from 2 to 9999 (the master is 1). The serial number for these servers will then be shown as 880000 plus this locally chosen recorder number. The serial number defines the first 6 digits of the unique reference number given to each call recorded by the recorder. For example, the recorder with serial number 800001 records its first call into the following files:

```
8000010000000001.wav
```

```
8000010000000001.xml
```

The serial number is encoded within every activation key issued. Once a master recorder or central replay server has been configured with its initial activation key, subsequent keys must have a matching serial number.

 **Important:**

The 5-day license option uses serial number 800000. This temporary and non-unique serial number is the only serial number that you can subsequently override with the recorder's correct serial number, which is included in the full license key.

Obtaining a License Activation Key

Obtain a license activation key for a Master or standalone recorder or Central Replay Server as follows:

1. Open another browser window (on this or another PC) and ensure that pop-ups are not blocked.
2. Navigate to the Verint licensing website at www.verint.com/ACR.
3. Enter your Username and Password.
4. Click **Log in**
5. Click **License Activation**
6. Choose the Serial Number from the drop-down list.
7. Enter the three-digit License Generation Key from the License page in the Administration application.
8. Enter the appropriate information for the end user.
9. Click **Generate Key**.
10. Your license activation key is:
 - a. Displayed on the screen
 - b. Sent to you through email

Activating the License

1. Return to the **System > License** page that you have open in another browser window.
2. Enter the License Key. The license activation key is not case-sensitive, and you can omit the dashes. If you use a browser on the same machine to obtain the activation key, you can copy and paste the number between the browser windows.
3. Click **Enter**.

The page displays the licensed serial number, server type and channel capacity.

Make a note of the license key and store it safely in case you need to reinstall the application on the same server - in which case you will be able to reuse the key. To reinstall on a different server, you will need a new key, because the MAC address, to which it is tied via the three digit license generation key, will be different.

Confidential and Proprietary Information

Once you have successfully entered a license key, you will be able to access the other pages of the administration interface.

Standby and Slave Servers

These do not require a license key. Simply enter the Recorder Number you wish to assign to the server and provide the IP address(es) of the already licensed server as instructed on the lower half of the **System > License** administration page.

Adding additional licenses

Follow the procedure in the previous section titled "Activating the license" for the installation of additional licenses. You must restart the recorder after changing any license settings so this is best done out of hours.

Note:

Additional licenses may require more switch components (for example, in a Communication Manager system, more C-LAN, VoIP resources, media processing boards).

Reinstalling on the same PC

If you reinstall the recorder software on a new hard disk in the same chassis, you can reuse your existing activation keys.

If you reinstall the recorder from the installation kit, you must re-enter the activation keys.

 **WARNING:**

If you reinstall the software, you must restore the database as described in [Restoring data to a new PostgreSQL database](#) on page 183 before starting recording. Otherwise the recorder will reuse recording identifiers that have already been used.

Reinstalling the Recorder on a new PC

For license security, the installation is tied to the first Network Interface Card (NIC) in the server on which it is installed. To reinstall the recorder on another server, do one of the following:

Configuration

Move the first NIC to the new server and use your existing activation keys

Note the license generation key on the new server and request new activation keys as outlined in [Obtaining a License Activation Key](#) on page 124.



WARNING:

If you reinstall the software, you must restore the database as described in [Restoring data to a new PostgreSQL database](#) on page 183 before starting recording. Otherwise the recorder will reuse recording identifiers that have already been used.

Confidential and Proprietary Information

Security

Security of recordings is very important and is discussed at length in [System Security](#) on page 207. At this stage in the configuration of your system you should immediately create appropriate user accounts as described below.

Note:

If you have installed one or more central replay servers then you should only configure Administrator accounts on each recorder. Create and control end user replay rights on the replay server(s).

Securing the System

The system automatically creates an initial system administrator account as you log in for the first time. If you wish to create additional system administrator accounts, you should do so now. Until you do so, the only means of accessing the system is with the initial account.

To create a new user account:

1. Click on **System > Manage Users** at the top of the Administration screen.
2. Click on **Add User**.
3. Enter the user's name (with domain name and entirely in uppercase if using Windows domain accounts).
4. If using local (non domain) accounts, you must also enter a temporary password for this account. The user will be forced to change this when they log in for the first time. You must tell the new user what this temporary password is.
5. Select the appropriate **Role** for this user. System Administrators have full access to the system including all configuration. Restricted Administrators cannot change the system's recording configuration but may view the overall status, alarm and archive pages; eject DVDs and configure non-administrator accounts.

Note:

The **Comment** field is for your own notes.

See [Search and Replay Access Rights](#) on page 171 for an explanation of how to use the **May Replay calls owned by** field.

Windows Authentication

If you enter a simple username without a domain qualifier (for example, *admin* rather than *ADMIN@DOMAIN.COM*) then the account is administered by the recorder application. Administrators may change this account's password and the user may change their account password and log off from the application using the administration web pages.

However, if you specify a domain and username, the system will attempt to authenticate you via Kerberos. In this case, you will not see **Logoff** or **Change Password** links on the web pages presented by the recorder.

 **CAUTION:**

When adding user accounts user accounts that correspond to Active Directory accounts, enter the username and domain all in uppercase - regardless of the case used in Active Directory.

This feature is also known as "Single Sign On" (SSO) as users only have to log onto their Windows workstation, but do not need to log on to the search and replay application separately. See [Windows Domain Authentication](#) on page 208 for details of how to enable this feature.

Windows Accounts for Screen Recording

In addition to entering the domain accounts of those who will administer the system and replay calls on it, you will also need to enter account details for the domain accounts of any agents that you want to record whenever they are logged on at a Windows desktop configured for screen recording. Simply create the account and set the Agent ID field. This is used to identify which workstation or thin client session they are logged on at and whenever audio is being recorded, then so long as the desktop they are using has screen capture installed, screen content will be recorded too.

Alternatively, if you are using WFO, you can define the relationships between agents, employees and user accounts within WFO. Avaya Contact Recorder will use this information when interpreting WFO Business Rules that specify screen recording.

Confidential and Proprietary Information

General Setup

You should now configure how the system makes recordings and how it interfaces with your Avaya telephony system. Follow the procedures below, clicking on the appropriate tab at the top of the Administration screen for each section.

Recorder

This is the section where you specify information about the recorder hardware and environment.

Note:

It is important that you review and change any of the settings that are not correctly defaulted. On servers designated as Standby, Slave or Central Replay Servers, a number of the settings are irrelevant and hence will not appear. Others are automatically copied from the Master and hence do not show an **Edit** link next to them.

Call storage path

On Windows servers, you must specify the path into which the recorder will store its recordings. This should be the F drive.

On Linux servers this is automatically set to the /calls partition.

Days to retain calls

Enter the number of days after which calls will be deleted from the disk buffer. Set to 0 to disable this feature and keep calls until the space is needed for newer calls.

 **CAUTION:**

Calls will be deleted sooner if the disk buffer fills up.

IP Address to use on this server for RTP

You must specify which IP address (and therefore which NIC) on the server should receive any audio streams that are directed to the recorder. Even if you do not intend to use RTP recording, set this to an appropriate NIC card anyway.

This setting does not affect passive IP tapping. If you configure the recorder to use passive tap IP recording, it will automatically accept packets over any Network Interface Card that does not have an IP address or, if there is only one NIC card in the server, it will default to using that NIC.

Confidential and Proprietary Information

Configuration

Maximum total call duration (hours)

To avoid having recording channels permanently active, the recorder will reset a channel that has been continuously recording for this many hours. Set this field to a value that you can be sure will not occur for a real call - typically just longer than any one person would ever be present on a shift. This setting only affects recordings which are under the direct control of the recorder. Duplicate media streaming from a CS1000 IP phone, for example, may continue beyond this period.

Maximum recording segment duration (mins)

To optimize the playback experience, the recorder cuts long recordings into segments of the designated length. A typical value for call centers is 120 minutes. This is the default. However, if your switch regularly handles longer calls, you may increase this value

Retain call details for (months)

At some point, the size of the call details database will become either unmanageable or will fill the available disk space. Specify, in months, how long the system should retain call detail records before they are purged from the system. This ensures that the database stabilizes at a finite size. Purging is carried out at, or shortly after, 1:00 a.m. each night and does not affect recording or replay.

SNMP Settings

See [SNMP](#) on page 145 for notes on these settings.

Replay Server(s)

By default, each Avaya Contact Recorder server will pass details of calls it has recorded to the Master and Standby (if present). If you have installed one or more dedicated replay servers you must override this default behaviour by entering the address(es) of the replay server(s) here.

- Separate the addresses with a semi-colon.
- When specifying a Viewer server, simply enter its IP address or hostname. If your SQL server implementation is not using the default port (1443) you can override this with a properties file setting as described in [Properties File](#) on page 224.
- When specifying a dedicated Avaya Contact Recorder server - i.e. a "Central Replay Server" - you must also specify the port number (default 8080) that is to be used to contact it. For example, 10.1.1.25:8080
- If you have two Central Replay Servers, you should configure each with the address of the other here - so that recording lock/unlock requests will be passed between them.

Confidential and Proprietary Information

Once you have set this value, it will be acted on within one minute and subsequent recordings will be queued to be sent to the address(es) specified.

Note:

If you intend to install a central replay server and want all call details to be uploaded to it, enter its address in this field before you start recording. Do this even if the replay server is not yet ready. This way, all recordings' details will be queued ready for upload when the server is available. The recorder will raise an alarm daily until you install and correctly configure the replay server. Ignore this alarm.

Allow Full Database Vacuum on Startup if required

Once every 6 months, the recorder must perform essential database functions. It does this on startup, but only after warning you that this will happen. If you receive an alarm saying that this is required but cannot afford to have the recorder do this on its next restart, you can defer this activity by clearing this checkbox. After each restart, this checkbox is reset and you must clear it again if you want to defer the task further. You must allow the recorder to perform these tasks within one month of being alerted.

Key Management Server

If you intend to encrypt recordings, refer to [Encrypted File Storage](#) on page 219 and set the name of your Key Management Server here.

Key Management Certificate Passphrase

If you intend to encrypt recordings, refer to [Encrypted File Storage](#) on page 219 and set the passphrase for your Key Management Certificate here.

URL(s) of external control port(s) to connect to

Specify the IP node name of each external controller. The port number will default to 1414 but to override this add a colon then the port number. If the recorder is supporting multiple servers, list their names separated by semi-colons.

For every URL entered here, the **Recorder Status** › **Server** page will monitor the status of the link and the Alarms page will show any problems with the link.

Contact Center Interface

Use the top setting on this tab to define which type of Avaya switch you are recording. If you have to change this setting, you must restart the recorder, then complete the other

Configuration

settings on this tab. These settings vary according to the type of switch you have specified and a number of subsidiary settings only become visible if required.

Communication Manager

When recording a Communication Manager, configure these settings:

Minutes after which call information indexed by Call ID is discarded

Each call is given a reference number or "Call ID" but these are reused after a period and hence any information gleaned by the recorder must be discarded before that call ID is reused. The default of three hours is appropriate for many switches but if you have, for example, an auto-dialer or very high calling rates you may need to decrease this setting.

The disadvantage of a low setting is that a genuinely long call, which is active for longer than the time specified may not be tagged fully should it subsequently be transferred to another station.

Apply Beep Tone

This setting determines whether or not beep-tone is applied during recording.

Time between beeps (secs)

If you want to inject warning tone onto calls as they being recorded (a mandatory requirement in some countries/regions) you can specify the interval between beeps.

Audio Format

You can choose to stream audio from the switch in G.711 or G.729 format.

Avaya Communication Manager Name

Set this to the name of the AES switch connection you are using.

AE Server Address(es)

This and the following two settings are required on each server that is providing DMCC based recording (as opposed to TDM and passive IP tapping). The IP address of the Avaya Application Enablement Server on which the Device, Media and Call Control (DMCC) API is running. If you are not using a standby recorder but do have a backup AES, add a semicolon before each subsequent address. If the first address in the list is unavailable, the recorder attempts to establish a connection with the next server specified in the list. If you have a standby recorder, connect the master to one AES and the standby to another.

Confidential and Proprietary Information

DMCC User Name

The user name that the recorder should use to log in to the Device, Media and Call Control API.

DMCC Password

The password that the recorder should use to log in to the Device, Media and Call Control API.

Encrypt Media Streams

Check this setting to have the audio between the recorder and VoIP resources encrypted. You can still record calls on which the other party's audio is encrypted without setting this option. If you do set it, ensure that you have configured the codec set used by the recorder's softphones to support encryption. Also note the impact on server capacity.

IP Station Security Code

All IP softphones that register with Communication Manager must provide a security code. The code you enter must match the code entered for all the stations that you created earlier on Communication Manager for the recorder to use. This field entry is masked for security purposes.

The following settings are only shown on Master and Standby servers as they are not required by Slave or Replay servers.

AES TSAPI Server(s)

Enter the IP address of the AE Server that is configured to provide TSAPI services to the recorder. If you are not using a standby recorder but do have a backup AES, you can specify further addresses, separating them with a semi-colon. Names are attempted in order if the first one fails. If you have a standby recorder, connect the master to one AES and the standby to another.

AES TSAPI Switch Name(s)

Enter the name of the switch as configured in TSAPI. If you have specified multiple TSAPI servers and the name differs on each, enter the name that each server uses in order, separated by semi-colons.

AES TSAPI Service Login ID

Enter the login identifier that the recorder should use when accessing TSAPI.

AES TSAPI Service password

Enter the password that the recorder should use when accessing TSAPI.

Non-recorded Stations/IVR ports to Observe

If any of the calls that you wish to record are initially handled by stations that are not themselves recorded (such as a bank of IVR ports) the tagging of those calls may be incomplete. Some information is only available via TSAPI when the call is first answered. To avoid losing this information, you can specify one or more ranges of stations that the recorder will monitor via TSAPI and hence learn the additional details it needs to tag and record these accurately. You can enter contiguous ranges and individual stations. Separate these with semi-colons. For example: 1201-1209;1346;4000-4099

Agent Skill Group(s) to Observe

TSAPI does not let the recorder observe AgentIDs directly. If you wish to record calls based on AgentID - or even to tag recordings with Agent IDs and names, you **MUST** configure this setting. Enter enough skill groups to ensure that each agent you wish to record is in at least one of these groups. Separate skill groups with a semi-colon. You can enter ranges of skills - but only if all values within the range are valid skill hunt groups.

Tip:

Consider creating one dummy skill hunt group and assign all agents to this skill. You then need only enter that one skill hunt group here. This also minimizes the number of TSAPI licenses you need.

VDN(s) to Observe

To ensure accurate tagging of recordings, you must enter all of the VDNs in use here. Separate VDNs with a semi-colon. You can enter ranges of VDNs - but only if all values within the range are valid VDNs.

Tip:

If you have ranges of VDNs within which some numbers are not used, consider creating these as VDNs to allow you to enter the whole range here.

Tag calls with which VDN?

Each recording can only be tagged with a single VDN. You can choose whether this is the first or last VDN that a call went through. As with the following setting, "first" and "last" are "as far as the recorder is aware" i.e. restricted to those VDNs you tell it to observe.

Confidential and Proprietary Information

Add VDN number as additional "owner" of calls

Access to recordings is normally controlled according to the station or agent that is the subject of the recording. You may, however, choose to control access to recordings on the basis of which VDN the call was routed by by setting this option to Yes.

Address of the Communication Manager

This setting and the following two are only required if you intend to control recording in Conferenced mode according to the CoR in which stations are placed. The recorder needs these settings to use the SMS Web services.

Set this entry to the IP address or hostname of the Communication Manager. If using hostname, the AES must be able to resolve this to an IP address.

Username for Switch Administration

See above for when this setting is required. If it is needed, enter the username the recorder should use when accessing the automated switch administration (SMS) services.

Password for Switch Administration

See above for when this setting is required. If it is needed, enter the password the recorder should use when accessing the automated switch administration (SMS) services.

Record with Passive IP Taps

Normally calls on Communication Manager will be recorded using DMCC conferencing if there is no physical TDM tap available. Set this option to force the recorder to use passive IP tapping instead. Ensure that you have sufficient NIC cards in the servers to tap all of the possible paths that calls may follow. Remove the IP stack from NIC cards that are to be used for passive tapping (unless using a single NIC card in a server for both passive tap and normal server interactions). If you change this setting you must restart the recorder.

Extensions assigned to recorder(s)

To use DMCC recording, you must provide enough softphones to support the total recording load.

To make subsequent administration as easy as possible, assign sufficient stations to handle the ultimate load on each server, even if you do not intend to allocate all of these ports immediately.

To add a port range

1. Click **Add Port(s)** at the bottom left.
2. Enter a range of station numbers.

Configuration

3. If you have more than one ACR server, twenty softphones (by default) will be immediately assigned to each server and additional ones added to maintain this headroom as the peak load on each server grows. Normally a single pool is provided and used across all recorders. In some topologies you may need to assign specific softphones to particular ACR servers. To do this, click the **Advanced** button and assign the range of softphones to a particular recorder by entering its serial number in the **Designated Recorder Pool(s)** field.

To edit a port range,

1. Click on the **Edit** link in the right-hand column.
2. Change lowest or highest port number or both.

To delete one or more port ranges:

1. Click the checkbox in the Select column for each station range you want to delete.
2. Click on the **Delete selected port(s)** link.

Once you have configured a range of softphones, these can be used for a number of purposes according to the type of recorder this is:

Master: Use the tabs under **Operations** to assign ports to the various tasks that your license allows.

Standby: Normally, this will adopt the configuration of the master (unless you have forced it to accept local configuration in which case you should use the **Operations** tab as above).

Slave: All ports are automatically assigned under control of the Master.

Central Replay Server: All ports are automatically assigned to the telephone replay pool.

Note:

You can only delete a port range if none of its stations is assigned to any of the recording modes.

 **Important:**

Set these port ranges up correctly before proceeding to the subsequent pages on which you allocate these ports to the various recording and replay tasks.

For a basic, small system, this is all that you need enter here. However, on larger systems you may want to click on the **Advanced** link to set the following:

- You can (although this is NOT recommended) force the ports to register through a specific C-LAN(s) rather than allowing AES to determine this automatically. Enter the IP address of the C-LAN they should use.

 **Important:**

These settings will not take effect until you restart the recorder.

Once you have set any of these Advanced options, this setting will be shown on the list of ports.

Confidential and Proprietary Information

CS1000

When recording a CS1000, configure these settings:

Minutes after which call information indexed by Call ID is discarded

Each call is given a reference number or "Call ID" but these are reused after a period and hence any information gleaned by the recorder must be discarded before that call ID is reused. The default of three hours is appropriate for many switches but if you have, for example, an auto-dialer or very high calling rates you may need to decrease this setting. The disadvantage of a low setting is that a genuinely long call, which is active for longer than the time specified may not be tagged fully should it subsequently be transferred to another DN or Position ID.

Apply Beep Tone

This setting determines whether or not beep-tone is applied during recording. (Note that TDM recording does not support this feature).

Avaya Contact Center Manager Server Address(es)

Enter the IP address of the Contact Center Manager Server(s) that the recorder is to establish an MLS link to. There is no need to add a port number as MLS always uses a fixed port number. If you have a standby CCMS, this should be configured to use the same "managed" IP address as the master.

To find the correct IP address of the CCMS, login in to CCMA, choose Config and pick the CCMS server. You will find the IP address in Properties.

Meridian 1 Machine Name and Customer Number

If you share a multi-customer system, you must specify your Machine Name and Meridian 1 Customer Number. Otherwise, leave these fields at their default values (blank and 0 respectively).

Option 11

If your switch is an Option 11, you must indicate this here.

Avaya Aura Contact Center Interface

If you are using an Avaya Aura Contact Center in SIP mode (in either CM or CS1000 environment), you must enter the following information to allow the recorder to communicate with it. Note that if there is a requirement to record agent outbound or

Confidential and Proprietary Information

Configuration

personal calls in a SIP contact Center configuration, it is necessary to have an additional CTI link configured. For CM, use the existing TSAPI link and for CS1000, use a separate MLS Server.

Also, refer to Chapter 7 “Properties File” for any settings that are specific to SIP Contact Center configurations.

CCT Server

Enter the IP address of the server running CCT. The port number defaults to 9080 but can be changed by adding a colon followed by the required port number.

CCT Username

Enter Windows the username that the recorder should use when connecting to the server running CCT. This defaults to "CallRecordUser". Note that with AACC 6.2 or later, any normal username can be used.

CCT Password

Enter the Windows password the recorder should use when connecting to the server running CCT.

Windows Domain

Enter the Windows domain name that your AACC uses, in which the above **CCT Username** and password are configured..

TDM Tap Points

If you are recording any TDM trunks and/or phones, you must install the appropriate Ai-Logix cards into one or more Avaya Contact Recorders. These servers must be running Windows (not Linux). Use the supplied SmartView tools to confirm that your cards are connected and are receiving the appropriate audio from your trunks and/or phones. You must then use this administration page to specify which trunks or phones you have connected to the input channels on these cards. Enter all information into the Master Avaya Contact Recorder as follows.

1. On the **Operations** tab, select the **TDM Tap Points** sub-tab.
2. Click the **Add Tap(s)** button to enter details of the phones and/or trunks to which the TDM recorders' ports are connected.
3. Enter the connections according to the table below:

Confidential and Proprietary Information

	Extension-side Taps	Trunk-side Taps
Communication Manager	Enter the numbers of the stations connected to the TDM cards. If you are tapping a contiguous range of stations and you have connected these to a contiguous range of input channels, you can enter these as a single entry. If your connections are not sequential, enter each one individually.	First determine whether the trunk is a T1 or E1 and if T1, whether 23 or 24 channels of audio are present. Then determine the trunk group number for each trunk. Once these have been found, set the type of trunk and enter the trunk group number for each trunk being tapped.
CS 1000	Enter the TNs of the phone sets connected to the TDM cards. If you are tapping a contiguous range of TNs and you have connected these to a contiguous range of input channels, you can enter these as a single entry. If your connections are not sequential, enter each one individually.	First determine whether the trunk is a T1, E1 or DPNSS trunk and if T1, whether 23 or 24 channels of audio are present. Then determine the loop number for each trunk. These are determined from the switch using LD21 on the switch console and entering LTM (List Trunk Map). Once these have been found, set the type of trunk and enter the loop number for each trunk being tapped.

Tip:

If extension side tapping, connect phone sets with consecutively numbered TNs/DNs/PositionIDs/Stations) to consecutively numbered media channels so that you can enter ranges of phones rather than have to specify each one separately.

4. Enter an optional comment to describe the device or trunk being tapped.
5. Select the serial number of the Avaya Contact Recorder that is tapping this device/trunk.
6. Each trunk or range of phones will be connected to the appropriate number of input channels on a TDM card. These number from 1 as shown on SmartView. Enter the lowest (first) channel number used here. The recorder will then associate the appropriate number of channels starting with this one to the trunk or phone(s) entered above.
7. Repeat steps 2 through 6 for each trunk and phone or group of consecutively numbered phones.

Note:

(For CS 1000 Systems) Even though you enter TNs in the TDM tap points page to tell Avaya Contact Recorder which physical phones or loops are being tapped, you still enter DNs when specifying what to record. The recorder uses CTI information to determine which TN is involved when a recordable DN is active, and enables the relevant port on the TDM recorder. The DNs are administered in **Operations > Bulk Recording** as described in [Bulk Recording](#) on page 150.

"Unable to Record" Alarms

When using trunk-side recording, the system may raise alarms warning you that it could not record specific calls. These occur when the recorder attempts to record a call that it believes includes an external party but none of the devices to which they are connected are recordable. The reasons for this, and the appropriate actions to take are listed below:

1. The call is actually internal. Set **Record internal calls** to **No** on the **Operations > Bulk Recording** page.
2. The call does go via an external trunk, but one that has not been tapped so cannot be recorded. If you have genuine external trunks that do not have a recorder connected to them, you should either connect a recorder or accept that calls over these trunks will not be recorded. You can suppress the alarms on a specific trunk as shown below.
3. (CS1000 only) The TN reported in the CTI message is actually a conference bridge. In four (or more) way conferences, where an external party is present the recorder needs to be told to ignore the loops which are actually conference bridge loops. (The call should be recorded on the external trunk loop and hence does not need to be recorded on the conference loop as well.)

You can suppress these alarms on a particular trunk by creating an appropriate entry in the properties file (see [Properties File](#) on page 224).

On a	Add this to the properties file	Where...
Communication Manager	<code>trunkgroup.ignore.nnn=true</code>	<i>nnn</i> is the trunk group number to be ignored. Do not use leading zeroes.
CS 1000	<code>loop.ignore.nnn=true</code>	<i>nnn</i> is the loop number to be ignored - from 1 to 255. Do not use leading zeroes.

(CS1000 only) Note that the recorder assumes that trunks will be digital when it converts from the "packed TN" provided by the switch into a "loop number". This algorithm differs for analog trunks and the recorder may report a trunk number that does not actually exist. This is the number that the TN would represent if it were a digital trunk. You should examine the

Confidential and Proprietary Information

packed TN to determine what this really is. When setting the "loop.ignore" value in the properties file, use the loop number reported by the recorder.

Email Configuration

The Avaya Contact Recorder sends Emails as part of the Replay Authorization process and can also be configured to email support staff with details of alarms that occur. If you require either of these features, create an email account that the recorder can use to send emails. Click the **System** › **Email Server** tabs at the top of the Administration page and enter the following details:

SMTP Mail "From" Address

Set the name from which alarm email messages should originate, for example, *recorder1@alt.bigcorp.com*.

SMTP Mail Server

Enter the name of the SMTP mail server on which you have established the email account that the recorder will use to send email messages. If you leave this blank, the system will not send email messages when alarms occur - and you can then leave the remaining settings on this page blank. The system uses the standard SMTP port (25) unless overridden by the property setting `smtp.port=nnnn`.

SMTP Username

Leave this blank if your SMTP server allows unauthenticated sending. If it requires authentication, set the username of the SMTP account here.

SMTP Password

Leave this blank if your SMTP server allows unauthenticated sending. If it requires authentication, set the password of the SMTP account here. The password is masked when entered in this field.

Send Alarm/event emails to

Specify the email address(es) to which alarm and event messages should sent. Separate multiple addresses with a semi-colon (;).

Note:

Confirm that you are receiving emails correctly after you make any changes to these settings.

Confidential and Proprietary Information

System Monitoring

There are several ways to track the operation of the Avaya Contact Recording system:

- You can browse the status and alarms pages via the administration pages
- The system can proactively send emails to warn of problems
- You can analyze log files produced by the application and its Tomcat web servlet container
- You can have application logging information sent to a Syslog server
- You can interrogate the system and have it send notifications via SNMP

These options are described in detail below. You are strongly advised to set up one of the proactive mechanisms to ensure that any problems are brought to your attention in a timely fashion. This can be done via Email, SNMP or Syslog monitoring.

Via the Administration Pages

The status of your recording system is shown on several web pages beneath the **Recorder Status** link on the Administration interface. Here you can see:

- overall **System** Status (Master and Standby recorders only). This shows the status of all recording servers in your system and provides links to the administration interface of the other servers should you wish to investigate any issues that are highlighted there. Problems are highlighted in red or amber according to their severity.
- overall status summary for the **Server** and its interfaces to other components
- loading levels - both current and peak
- **CTI Monitors** and current call states
- the state of all recorder **Ports**

Having just configured the recorder's main settings, you should now review the status and address any problems highlighted on these pages or the **Alarms** page.

Alarms and events occurring within the system are stored in its local database. You can view them via the **Alarms** tab at the top of the Administration page. If this link is red, it indicates that there are one or more uncleared alarms. As you address the cause of an alarm, you should clear it by clicking the checkbox to the left of it and then clicking the **Clear Selected Event(s)** link.

Confidential and Proprietary Information

Via Email

Use the **Send Alarm/event emails to** setting on the **System > Email Server** page to specify the email address(es) to which alarm and event messages should sent. Separate multiple addresses with a semi-colon (;). The email recipient can be a local system administrator, a manned help-desk and/or suppliers' support desks if you have a support agreement that includes this facility.

The system sends an email message each time an alarm occurs or is resolved. It also sends an email once per day as a "heartbeat" to let you know it is still operating. This email is sent overnight and also advises you of the available disk space after the log files have been purged. You should investigate any failure to receive the daily heartbeat message as it could indicate that the server has failed.

Note:

The system will batch emails for up to 10 minutes to avoid flooding users' inboxes. The default configuration is that all alarms and events are sent via E-mail. You can change this so that only alarms above a specified severity are sent by E-mail. Be aware that if you do so, you may be unaware of issues that are affecting your system. See "**email.minalarmlevel**" in [Properties File](#) on page 224.

Application Logs

The Avaya Contact Recorder writes log files to the /logs directory beneath its install path (typically /opt/witness on Linux, **D:\Program Files\Avaya\ContactRecorder** on Windows). The current day's log file is called **acr.log**. At midnight the current log file is closed, renamed to **acr.log.<date>**, and a new log file opened. These log files are automatically purged after 30 days by default but this can be overridden with a properties file entry.

Setting the server log level

You can set the level of messages logged by the Avaya Contact Recorder to **DEBUG**, **INFO** (the default), **WARN**, **ERROR** or **FATAL** in one of two ways. Note that the logging levels of some components within the Avaya Contact Recorder are controlled by other settings - which are not to be altered by end users.

Permanently from next restart

To change the level permanently, enter the following line in the properties file **acr.properties** and restart the Avaya Contact Recorder service to have it take effect.

```
log.level=DEBUG
```

Confidential and Proprietary Information

Configuration

If you change the log level in the properties file, it remains set on subsequent restarts. When logging at DEBUG level, note that the log files grow very quickly and can overflow the disk if left at this level. You may therefore also wish to change the number of days log files are retained. Set this with `acr.logkeepdays=nn` in the properties file.

Temporarily, immediately

To change the level temporarily, without restarting the service, simply use a browser to request the URL:

```
http://myrecorder:8080/log?level=DEBUG
```

using the name of your server.

Alternatively, on Linux systems if you do not have access to the web administration screens, but do have access via secure shell, execute the following command:

```
perl /opt/witness/bin/loglevel.pl DEBUG
```

You do not have to stop recording in order to change the logging level. To set it back again, enter the same URL, replacing `DEBUG` with `INFO`. The command is case-sensitive. Using this method changes the log level temporarily. It will revert to normal the next time that the system is rebooted.

Tomcat Logs

Avaya Contact Recorder uses the Tomcat web servlet container, which writes log files to `/tomcat7/logs` beneath the install path (typically `/opt/witness` on Linux, `D:\Program Files\Avaya>ContactRecorder` on Windows).

Remote logging via Syslog Server(s)

A subset of the information sent to the application logs can also be forwarded to one or more Syslog servers. To configure this, use the maintenance page at `/servlet/acr?cmd=mtce`

There you can

- enter the IP hostname or address of one or more syslog servers
- filter the events to only those at or more severe than INFO, WARN or ERROR level.

The recorder announces these events as coming from facility "LOCAL1" but this can be overridden using the property file entry `syslog.facility`.

Confidential and Proprietary Information

SNMP

You can use an SNMP monitoring system such as HP OpenView to monitor Avaya Contact Recorders. To do so, you must first set the name of the SNMP Read Community in the **General Setup › Recorder** page. The recorder will then respond to SNMPV1 Get messages using Version 1, 2c or 3 as configured on this page. Version 3 is recommended but may require additional settings to be made via the properties file as shown in the table below. If you change any of these settings you should restart the recorder.

For security reasons, recorders:

- do not allow "well known" community names like "private" or "public"
- do not respond to SNMP Gets until a community name has been set
- do not use the usual port of 161, but instead use 2161.

You can also specify the SNMP Notification Destination (again, on the **General Setup > Recorder** page).

Once set, SNMP traps will be sent to your monitoring system at the address specified.

Property	Default	Description
snmp.port	2161	The port number to use for SNMP
snmp.authtype	SHA	Set to "MD5" to override the default SHA authorization type with MD5.
snmp.privtype	AES128	Set to "DES", "3DES" or "AES256" to change the privacy type from AES128. Note that AES256 requires the java unlimited strength patch as described in Installing Unlimited Strength Encryption on page 386.
snmp.mainusername	acrsnmpuser	The main username the Network Management System will use to connect to the recorder.
snmp.username. <i>nn</i>	no default value	Additional usernames can be entered. Replace <i>nn</i> with 1, 2, 3 etc.
snmp.password. <i>nn</i>	no default value	Encrypted password to be used in conjunction with the corresponding snmp.username. <i>nn</i> entry. This requires the java unlimited strength patch as described in Installing Unlimited Strength Encryption on page 386

Operations

After initial setup, configuration of the recorder on a day-to-day basis largely consists of changing what is being recorded. You should also regularly check the status of any archive locations that you have configured here.

Beneath this tab therefore are administration pages that let you manage Archiving and each of the different recording and replay functions that the recorder provides.

Common Settings

The following settings are used on more than one **Operations** page and have the same meaning on each. This does not imply that all of these settings are applicable to ALL modes.

Apply Beep Tone within recorder

In some recording modes, you can specify whether or not the recorder injects beep tone. For a full discussion, see [Beep Tone](#) on page 48.

Audio format

In some recording modes, you can specify whether the VoIP audio is sent to and from the recorder in G.729A or in G.711. See [Recording Bandwidth](#) on page 53 for a discussion of compression formats. You must restart the recorder for changes to this setting to take effect.

Stop recording if the call drops to just one other party

In some modes, users call a port on the recorder in order to record a call. Because the recorder port is then itself a party to the call being recorded, the call will stay active if any one of the other parties fails to hang up.

To avoid the port getting stuck in this way, you can set the recorder to hang up if other parties on the call hang up - leaving only the recorder and one other party left on the call.

Ports Configured

This figure shows how many ports you have allocated to this recording mode - as detailed in the table at the bottom of the page.

Confidential and Proprietary Information

Designated Recorder/Pool(s)

Use this field to force recordings to happen on a specific recorder (by entering its six digit serial number) or a specific "pool" of recorders (by entering a pool name). The latter allows for load-sharing and fault tolerance. To place a recorder in a pool, set `recorder.pool=poolname` - where `poolname` is the name of the pool. See [Properties File](#) on page 224 for further details.

This feature is normally used to ensure that recording takes place on a remote site. If you specify a designated recorder, and there is an AES on the remote site, you can configure that recorder as a standby rather than a slave. It will then record the targets for which it is the designated recorder should it lose contact with the master recorder. However, this also means that if you do specify any targets with a designated recorder and have a centralised standby recorder that should take over the entire function of the master in the event of it failing, you **MUST** set `standby.main=true` on the central standby.

Warn when free port count falls BELOW

Where a pool of ports is used as a shared resource, this setting triggers an alarm warning that a pool is running short of available capacity. The warning message identifies the pool of ports using the **Comment** field (or the port number range if no comment was entered). The default for this setting is zero - and as a pool can never have less than zero ports available, the warning is effectively turned off by this setting. If you set it to 1 the recorder will alarm when the free count falls below 1 - that is to zero. And so forth.

Recording owner

See [Search and Replay Access Rights](#) on page 171 for details of how a recording's "owner" determines which user(s) can replay it. You can use this setting to override the default ownership (phone number or agent number).

For example, if you are configuring a pool of ports for use by the human resources department, you might find it more convenient to have all recordings made on them owned by "hr" rather than several different phone numbers, as would be the case if you left the default ownership in place. You can then control access to all of these recordings by assigning replay rights over "hr" to those users entitled to play them. You can enter an alphanumeric string or a number. Leading zeroes, if entered, are significant and are retained. All characters are stored in lowercase, so replay rights are applied case insensitively.

Assigning Ports

Each of the sub-tabs beneath **Operations** (except the **Archive** one) lets you assign ports to any of the uses that are appropriate given the type of Avaya switch you are recording,

Configuration

server and channels licenses you have installed. You allocate these ports to specific uses in two ways:

- **Explicit Allocation** - where you specify exactly which ports should be used. This approach is used where users dial in to or conference in to the ports in order to use them. An example is a pool of On Demand recording ports. The station numbers assigned to this pool must match those you have placed in the hunt group that you are going to tell your users they should dial for a recorder port.
- **Automatic Allocation** - where you specify what you want the ports to record or simply how many ports are to be used. This approach is used for modes where users do not need to dial into ports and hence it does not matter which ports the recorder selects for a given task. An example is Bulk recording of a particular station. You tell the recorder which station you want to record but don't care which of the recorder's ports is used.

Read the text in the pop-up dialogs carefully to see whether you are being asked to specify recorder ports or targets to be recorded.

Ranges

When assigning ports or specifying which stations or addresses are to be recorded, you can enter single numbers or ranges of numbers. For example, entering "4000-4099" is much easier to enter than 100 different numbers. Typically you need to enter some contiguous ranges and some individual port numbers.

A set of recorder ports is referred to as a "pool" and is configured on the appropriate page of the administration application by entering one or more port ranges. As you enter port numbers, keep the following in mind:

- A range can be a single number or a set of contiguously numbered ports or phone numbers.
- The lowest and highest port numbers in a range must have the same number of digits. Therefore, if you have some 4 and some 5-digit ports, you must enter these as two separate ranges.
- It is possible to have port or phone numbers that have one or more leading zeros. It is therefore important that you enter any leading zeros. The start and end ports in any port range must have the same number of digits even if some of these are leading zeros.

Entering a range

Enter a range of ports as follows (phone and address ranges are entered in the same way):

1. Click the **Add port(s)/address(es)** button. The **Station Range** dialog is displayed.
 - To enter a single port, type the number in the top text box.
 - To enter a range, type the number of the first port in the range into the top text box and the final port in the range into the second text box.

Confidential and Proprietary Information

2. Add a **Comment** (optional).

For pooled modes, you can use this field to name a range of ports and to note any hunt group number that you assigned to these ports. The text you enter appears in status reports and warning messages as labels for the specified range. For more information about pooled modes, see [Using pooled port modes](#) on page 150.

3. To quit without entering the port numbers, click **Close Window**.

To enter the port numbers and keep the window open to specify additional port numbers, click **Enter and Stay Open**. Your previous settings are retained. Change those that differ for the next range and repeat as necessary.

To enter the port numbers and close the window, click **Enter and Close**.

Port ranges are checked for consistency with other ranges and with license conditions as they are entered. If an entry is invalid, a message indicating the error is displayed; you can change the information as necessary.

Editing ranges

You can either change or delete the ranges listed. You can change the following fields without interrupting any recordings that might be active on the port(s) affected:

- **Comment**
- **Prompt User in...**
- **Warning Level**
- **Recording Owner**
- **Recording Rules**

Some changes require that the recording channel be reset and hence active recordings will be truncated. These are:

- **C-LAN address**
- **Designated Recorder/Poolname(s)**
- Any change to the number of ports in the range
- Any change to the port numbers in the range
- A change to the Codec (will only take effect on next restart)

To edit a range:

1. Click the **Edit** link to the right of the range you want to alter.
2. Edit the range in the port entry form.
3. Click **Enter**.

Configuration

Deleting ranges

Delete one or more ranges as follows:

1. Click the checkbox in the **Select** column for each range that you want to delete.
2. Click **Delete selected port(s)/address(es)**. In some recording modes, this will truncate any recording in progress on the port(s).

Advanced settings

To implement advanced settings on a range of ports, phone numbers or addresses:

1. Add or edit a range as above.
2. Click the **Advanced** button.
3. Enter data in the **Advanced** fields.
4. To quit without saving the settings, click **Close Window**.

To enter the port numbers and keep the window open to specify additional port numbers, click **Enter and Stay Open**.

To enter the port numbers and close the window, click **Enter and Close**.

Using pooled port modes

If you use On Demand Recording, Meeting Recording or Phone Replay, you can manage each range of ports dedicated to a recording mode separately. For example, if you assign two ranges of ports to Meeting Recording, you can use one for English speakers and one for French speakers. You can also track usage of individual pools. You could, for example, set up two different On Demand pools, one for a particular department on one hunt group and one for everyone else on another hunt group. You can track the status of these pools through the **Recorder Status** pages. For each port range assigned to a mode, you can view activity for that port range in the **Recorder Status > System** page.

Bulk Recording

This tab is only visible if your license includes bulk recording channels. You configure this screen on the Master recorder only. The top part of the screen lets you choose how bulk recording works for all ports but you can override most of these settings for specific recording targets - using the **Advanced** settings of the phone number ranges which are shown in the bottom section of the screen. The type of address that you can enter as a

Confidential and Proprietary Information

"recording target" in the bottom section of the screen depends on the switch type you are using as follows:

	Recording Targets Can Be	Notes
Communication Manager (To switch between CoR, Style and other target types you must first delete all recording targets then change the Specify recording targets setting.)	Station	Ideally, choose one type of recording target rather than mix these as the results of the latter can be complex and confusing. The recorder assumes that an address never changes type. Address names are refreshed nightly but if you change the type of device associated with an address you must restart the recorder for this to be noticed.
	Agent	
	Split	
	VDN	Requires SMS services as described under the Communication Manager section within Contact Center Interface on page 131. If you change recording targets, click the Refresh CoR membership button (otherwise this only happens overnight as it may take several minutes). Check the Alarms page after 10 minutes to confirm this completed successfully. Ensure the Standby is also successful.
	CoR	
Recording Style	Use the recorder's administration page to define the Advanced settings for each recording "style" but use Avaya Contact Center Control Manager to specify which phones are to be recorded in a given style.	
CS1000	DN	Single occurrence on a single phone set
	PositionID	NB. Not AgentID. (And cannot be used with AACC agents as they log on to DNs not positions).
	IDN	Single occurrence on a position
	MARP	Only on Knowledge Worker sets. On CC6, enable MARP/MADN for specific recording targets using Advanced setting. Always on for CC7 and higher.
AACC (only)	Agent	Only applicable if neither Communication Manager nor CS1000 is connected

The advanced settings, for the recording mode as a whole and/or specific recording targets are:

Confidential and Proprietary Information

Configuration

Designated Recorder/Pool(s) (specific recording targets only)

If set to a recorder's 6 digit identifier or pool name, this will determine which recorder or pool of recorders should record this/these addresses. Leave blank for automatic recorder allocation. To specify a list of recorders or pools to be used in descending priority order, separate recorder numbers or pool names with semi-colons. (Note that TDM channels are physically connected to specific recorders and must, therefore be recorded on those servers. This setting only applies to IP recordings.)

Screen to Record (specific recording targets only)

To record screen content at a particular Windows workstation whenever audio is recorded on a Communication Manager station, CS1000 DN or Position or (if running AACC without CM or CS1000) AACC Agent, enter the IP address or host name of the workstation. Where a range of phones is used, enter the screen name for each in order, separated by a semi-colon. This cannot be used when targeting Communication Manager Agents, Splits or VDNs as it indicates a physical relationship between a telephone and a screen.

If, on the other hand, you wish to record the screen content for particular agents, you can use **System > Manage Users** to associate an AgentID with a Windows domain account. If you do this, the screen of that agent will be recorded along with the audio whenever they are logged in to a screen that has been configured with the "Capture Service". This approach works not only for physical workstations but also for a range of thin client desktop topologies.

Note:

When using WFO Business Rules to drive screen recordings, the Agent/Employee/User Account mappings defined within WFO are used to determine which screen should be recorded - rather than this setting.

Recording owner

As described on [Recording owner](#) on page 147, this will override the normal owner of any recording made. It can be any alphanumeric entry.

Apply Beep Tone

You can override the default beep tone set for the switch or recording mode as a whole. Beep tone can be on, off or on only when the recording is being made and will be retained at the end.

Record Internal Calls

Whether or not to record internal calls. You must set this to **No** if you only have trunk-side recording taps.

Confidential and Proprietary Information

Percentage of calls to record

If your system has been licensed for this optional feature, you can choose what percentage of calls that meet the criteria for bulk recording are actually recorded. The decision to record or not is taken when a call first becomes recordable and will persist for subsequent segments of that call and any related calls i.e. those to which people connected to the original call are also connected. You can set this percentage for the recording mode as a whole. You can also override this default by setting it as an **Advanced** property for one or more recording target ranges.

Recording Control

By default, recording occurs whenever a call is connected to the phone number(s) specified and cannot be influenced by external controls such as Unify, instructions from the phone or desktop applications. Using this setting you can change this behaviour:

- to **Trigger on alerting** - i.e. to record even if the phone only rang and was subsequently answered by another party.
- to not **Start recording automatically at start of call** - i.e. to wait for a manual or external start signal.
- to **Follow the call** - i.e. continue recording even if the phone number that triggered recording is no longer on the call. Note that this only supported on Communication Manager (and then only when using DMCC recording) and requires the recorder to keep a recording port connected to the call at all times. This may restrict calls to 4, rather than 5 way conferences as there may, briefly, be two recording ports present on a call as a consult call merges into a conference call. Also note that the scope of this capability varies from switch to switch and is also limited where calls are controlled by external dialers.
- to **Allow user/external start/restart** - i.e. to act on START commands from manual or external control applications.
- to **Allow user/external stop** - i.e. to act on STOP commands from manual or external control applications.
- to **Allow user/external delete** - i.e. to act on DELETE commands from manual or external control applications. Not supported for TDM recording. Database records within Viewer (if used) will not be deleted.
- to **Retain ONLY if requested by user/external** - i.e. to delete the recording unless a RETAIN command has been received. Not supported for TDM recording.

Warn when available channel license count falls BELOW

If the recorder is loaded to the point where there are very few licenses available, it will raise an alarm.

Confidential and Proprietary Information

Configuration

XML file to use for Contact Recording Desktop (specific recording targets on CS1000 only)

If left blank, desktop control will be defined by dcs.xml. To change this, specify an alternative configuration file.

Recording Rules

These settings let you control whether or not to record on the basis of a particular piece of CTI information. The fields available vary according to the switch type as shown below.

Switch Type	Fields	Notes
Communication Manager	Agent	Must be observing an appropriate set of skills (see Settings > Contact Center Interface)
	DNIS	
	Split	Must be observing an appropriate set of skills (see Settings / Contact Center Interface)
	VDN	Must be observing an appropriate set of VDNs (see Settings > Contact Center Interface)
CS1000	Activity Code	Set during call so call has to be recorded and then deleted at the end if not wanted. Manual entry is prone to error. An activity code entered by one user does not affect the call once it has been transferred to another user. Use with caution.
	Agent	In CC6 agent location cannot be determined at recorder startup - only when the agent next logs in.
	DNIS	
	Skillset	Alphanumeric name
AACC	Agent	
	CDN	
	Skillset	Alphanumeric name

For each filter setting, you can set one of the following options:

Confidential and Proprietary Information

- Record only those where the field has specific values.
- Record only those where the field does NOT have specific values
- (only when overriding a rule on the recording mode as a whole) to ignore this field.

You can also choose:

- whether to record or not if this attribute is blank on a call.
- whether the rule applies to the first, last, current or any values of this attribute on the call. Note that some - such as split/skillset and VDN - are never actually connected to the call while it is active, hence "current" is not an option.

You can add rules to bulk recording as a whole or to specific recording targets using the **Add Rule** buttons at the bottom of the **Bulk Recording** and **Advanced** settings pages respectively. To delete a rule, click its **Edit** link and then click the **Delete Rule** button.

Each recording is only tagged with a single split/skillset or VDN - though as a call is handled and transferred it may actually have passed through several of these. You can choose whether the recorded segment is tagged with the "first" (earliest) or "last" (latest) VDN but in the case of splits/skillsets it is always the latest that is tagged. Because recording rules on these fields can be applied to the "first", "last" or "any" of the splits/skillsets or VDNs on the call, the resulting recordings will not necessarily be tagged with the split/skillset or VDN that triggered the recording.

Specify Recording targets (Communication Manager only)

On Communication Manager, you can choose to record specific Stations, Agents, Splits and VDNs or you can choose to specify one or more Classes of Restriction (CoR). In the latter case, all stations in that CoR will be recorded. You can also choose to administer recording targets via Avaya Contact Center Control Manager.

Delete Recording by entering (Communication Manager only)

Use this setting to specify a digit string that a user can dial during a recorded call to instruct the recorder to delete a recording. This will only work if you have also set **Allow user/external delete** under the **Recording Control** setting.

Retain Recording by entering (Communication Manager only)

Use this setting to specify a digit string that a user can dial during a recorded call to instruct the recorder to retain a recording. This will only work if you have also set **Retain ONLY if requested by user/external** under the **Recording Control** setting.

Configuration

Block IP recording (force TDM)

If there is a TDM tap onto an extension being recording, that will be used. If not, the recorder will try to use IP recording if possible and only use TDM trunkside as a last resort. Stop it using IP recording using this setting.

Save/Delete Key Present (specific recording targets on CS1000 CC7 and higher only)

If you have configured a Save/Delete key on a CS1000 phone, check this setting to ensure the recorder updates the lamp on the button appropriately.

Allow MARP/MADN (specific recording targets on CS1000 CC6 only)

By default, CC6 DN's are assumed to be single line appearances. If multiple appearances are used, check this setting.

Number of Addresses Targeted

This is not set directly, but summarizes how many different recording targets have been configured in the table at the foot of the page. Note that some targeted addresses (e.g. bridged lines, Splits, MADNs) may result in multiple calls being in progress at the same time so the maximum number of concurrent recordings that may be attempted could be higher.

Delayed Call Deletion (Communication Manager only)

Optionally, you can configure the recorder to wait before deleting a recording made in this mode. If a user decides to retain a call after it has completed, he can do so by ringing a specific number (the "Retain Port") on the recorder.

Note:

This feature requires one additional DMCC port on the recorder.

To implement this configuration, you must add the following lines to the properties file:

```
execmode.deletedelaymins=NN
```

```
execmode.retainnumber=NNNNN
```

Where

- ***NN*** is a number of minutes from the end of the call within which the user can call the "retain" number to retain the call
- ***NNNNN*** is the station number of an otherwise unallocated port on the recorder that will be dedicated to receiving Retain commands after hang up.

Confidential and Proprietary Information

If you set these properties, call segments recorded in Bulk mode with the **Retain ONLY if requested by user/external** setting enabled are not deleted until the time specified has elapsed after the end of that recording segment. A retain command entered during or after the recording ends (within the specified period) will preserve the calls. When determining an appropriate value for this delay, consider the following:

- You want to maximize the chance of retaining all segments of a call that the Station Executive user chooses to Retain, but
- You should minimize the time in which unwanted or unauthorized recordings are available for replay.

The **Retain** command applies only to the most recent call on a station. So, if a call is placed on hold and a consultation call is made, this consultation call is now the most recent.

Calling the retain number when the previous call is still on hold results in the consultation call being retained. However, if the user resumes the held call, hangs up, then dials the retain number, the original (and final) call is retained. In this case, the segment before the call was placed on hold is retained, as long as it ended less than **NN** minutes before the retain command was given.

On Demand Recording (Communication Manager only)

This type of recording uses a pool of ports on the recorder that you can access via one or more hunt groups.

Mode Setup

At the top of the page are the following settings:

- **Recording Owner**
- **Apply Beep Tone within recorder**
- **Warn when available channels falls below**
- **Stop recording if the call drops to just one other party**
- **Ports Configured**

All of these are explained in [Common Settings](#) on page 146.

Ports Assigned

The table at the bottom of the page lets you assign specific recorder ports to this recording mode. Refer to [Assigning Ports](#) on page 147.

In most cases, you will want to place each of these ports in a hunt group and make your users aware of this hunt group number and/or set up a key on their phones to access it.

Confidential and Proprietary Information

Advanced Settings

Click on the **Advanced** link when entering or editing a port range to set:

- **Designated Recorder/Pool(s)**
- **Recording owner**
- **Warn when free port count falls below**

All of these are described under [Common Settings](#) on page 146.

Audix

To allow a user easy access to On Demand Recording from a station, combine On Demand Recording with the "One-Step Recording via Audix" Communication Manager feature. To do this, enter the hunt group used for some On Demand ports as the parameter for the **Audix-rec** feature button you assign to the user's station.

When using the **Audix-rec** feature, keep in mind:

- Recording beep tone can only be applied by the Communication Manager, not by the recorder
- The user pressing the button will not hear the beep tone.
- Calls recorded using this feature are only indexed with the party that pressed the button, not the other party on the call.

For more information, refer to the One-Step Recording via Audix topic, Feature Related System Parameters Section, in Chapter 19: *Screen Reference of the Administrator Guide for Avaya Communication Manager*.

Meeting Recording (Communication Manager only)

This type of recording uses a pool of ports on the recorder that you can access via one or more hunt groups.

Mode Setup

At the top of the page are the following settings:

- **Recording Owner**
- **Apply Beep Tone within recorder**
- **Warn when available channels falls BELOW**
- **Stop recording if the call drops to just one other party**
- **Prompt Users in** - sets the default language for spoken prompts

Confidential and Proprietary Information

- **Ports Configured**

All of these except for **Prompt Users in** are explained in [Common Settings](#) on page 146.

Note that all Meeting recordings are performed in G.711 to make the production of custom voice prompts simpler.

Ports Assigned

The table at the bottom of the page lets you assign specific recorder ports to this recording mode. Refer to [Assigning Ports](#) on page 147.

In most cases, you will want to place each of these ports in a hunt group and make your users aware of this hunt group number and/or set up a key on their phones to access it.

Advanced Port Settings

Click on the **Advanced** link when entering or editing a port range to set:

- **Designated Recorder/Pool(s)**
- **Recording owner.**

Tip:

On Meeting Recording ports, a user can enter a list of owners manually using the dial pad .

All of the above are described under [Common Settings](#) on page 146.

- **Prompt users in** - Sets the language for spoken prompts. If using multiple languages, you should configure a hunt group to correspond with each range of ports that uses a different language.

Custom Prompts

If the language you require is not offered, select **Customer defined prompts** and provide your own set of prompts. These files are located in `/wav` beneath the folder into which you installed the recorder and are called:

- `welcome_custom.wav`
- `owners_custom.wav`
- `recording_custom.wav`
- `help_custom.wav`

You can replace these four files with your own recordings. Listen to the corresponding file in a language you understand (for example, `welcome_english.wav`) and record the equivalent messages in your own language.



WARNING:

You **MUST** use the same G.711 μ -law encoding that the supplied files use.

(Telephone) Replay Ports (Communication Manager only)

The **Operatons > Replay** page is only available if you have purchased one or more telephone replay port licenses.

Mode Setup

The top of the page simply shows:

- **Warn when available channels falls BELOW**
- **Ports Configured**
- These are explained in [Common Settings](#) on page 146.

Ports Assigned

The table at the bottom of the page lets you assign specific recorder ports to this recording mode. Refer to [Assigning Ports](#) on page 147.

For this mode, you typically add a single range of ports - enough to handle the maximum concurrent number of replay users the recorder is to support.



Important:

Replay ports impose a significant load on the recorder. Be sure that you have specified a powerful enough server.

Confidential and Proprietary Information

Archive

This section explains how to configure the system to archive calls to DVD/Blu-ray drives (hereafter referred to simply as "DVD drives"), network file shares and/or EMC Centera file stores.. All configuration is performed on the Master recorder only. The information is disseminated to other recorders automatically.

The recorder archives recordings not as individual files but as "tar" files - each containing many megabytes of recordings. The recorder's database tracks which media each recording is on and will prompt you to insert the appropriate media if you try to play a call that is not present on the hard disk of a recorder or a file-share based archive location.

Completed archive DVDs/Blu-ray disks can be inserted into the recorder that produced them or a drive on the server holding the overall recording database (the Master, standby or, if you have one, the dedicated central replay server).

Overall Settings

The settings at the top of this page apply to all archiving on the recorders.

Wait before archiving (minutes): It is not uncommon for additional details to be added to call recordings shortly after the recording ends. This setting instructs the recorder to wait for the specified number of minutes before examining the call to see if it should be archived and if so, to where.

Downloading the EMC drivers

If you wish to archive recordings to one or more EMC Centera file stores, you must first download the appropriate driver files onto each Avaya Contact Recorder and then restart the recorder.

EMC provides drivers for Centera for Windows and Linux at their support website. The package is called Centera SDK. ACR is tested with version 3.2p5 of the Centera SDK.

For Linux choose the version for gcc 4.4.

For Windows choose the 64 bit version.

Installing the drivers on Linux

Download the Centera SDK.

Configuration

Perform the following steps as root (replacing the specific SDK version with the one you are installing if different):

```
cd /tmp
tar xvzf downloadedFile.tgz
cd Centera_SDK_Linux-gcc4/Centera_SDK-3.2.705/install/
./install
Accept the default installation location of /usr/local/Centera_SDK
cd /usr/local/Centera_SDK/lib
chmod 755 FPLibrary.jar
cd /usr/local/Centera_SDK/lib/64
chmod 755 *so.3.2.*
```

Perform the following step as witness

```
cp /usr/local/Centera_SDK/lib/FPLibrary.jar
/opt/witness/tomcat7/lib/
```

Installing the drivers on Windows

Download the Centera SDK.

Unzip the downloaded file to a temporary location.

Under the temporary location, locate the lib and lib64 folders.

Copy FPLibrary.jar from the lib folder to tomcat7\lib under the ACR installation.

Copy all the dll files (not the lib file) from the lib64 folder to the tomcat7\bin folder under the ACR installation.

Archive Destinations

The table at the bottom of the page lists the separate archival tasks that are configured. Each one is independent and is linked to one or more DVD drives folders on network attached storage (NAS) or EMC Centera storage systems. Never configure more than one active archive pointing to the same destination. If you wish to reuse a destination such as a DVD drive, first disable the old archive definition for that destination.

To add a new archive destination, click on either **Add DVD drive**, **Add NAS**, or **Add EMC** as appropriate. A pop-up window will let you enter the basic information about this archive task. If you simply specify the path of a drive or fileshare, or the pool access information for an EMC Centera, all recordings will be archived to that destination. If you need more precise control over the archive process, click on the **Advanced** button and alter any of the

Confidential and Proprietary Information

optional settings. These are described below. Note that some apply to DVD drives only and others to NAS folders or EMC Centera only.

Drive Paths (Linux) or Letters (Windows) - For a single drive, just enter its path. If you have multiple drives, enter their paths separated by semi-colons. In this case, you can put a blank disk in each drive and the recorder will use them in turn, wrapping back to the first one once the last has been used. This allows you to archive more than one disk per day without having to visit the recorder more than once a day.

UNC path(s) - Enter the path of the folder into which recordings are to be archived. This can be a local path (e.g. with SAN disks). You can also enter a sequence of paths, separated by semi-colons. In this case, files will be written to the first path until it is full (or inaccessible) at which point subsequent files will be written to the next path. This allows you to add NAS storage devices as the old ones fill and maintain a complete history of recordings online.

EMC Connection String - enter the pool access string for the EMC Centera server you want to use. You should include multiple IP addresses of the pool and the full path to the PEA file. A typical connection string takes the form
`10.10.10.10,11.11.11.11?/home/witness/atlantaemc.pea`

Comment (optional) - This field is provided for you to label the destination. For example "Gold and Silver Card calls, 90 days". It appears in the **Detail** column on the **Archive** tab.

The following settings are accessed by clicking the **Advanced** button.

Recorders (default all) - If you configure an archive destination, it will run identically on all Avaya Contact recorders - Master, Standby and Slaves and central replay server if present. If you need to override this - for example, if not all servers have the same DVD drive path, you can restrict it to one or more servers by listing their serial numbers here, separated by semi-colons. For example, if my Standby server (number 880002) has no DVD /dev/cdrom I would enter "890001;880003;880004" to have it run only on the master (890001) and slaves (880003 and 880004). Note that if you change this setting, it will only take effect the next time the servers are restarted.

Maximum minutes between batches (default 1440 minutes, or 24 hours) - Ideally, all tar archive files would be the same, large, size. However, on a quiet system it may take many hours or even days to record enough to completely "fill" such a file. It is important that recordings are archived in good time since, until they are, they are at risk of loss through fire, flood theft etc. of the server on which they are held. This setting determines how long the recorder will attempt to fill a tar file to the preferred size before giving up, closing it and copying it to the archive destination and starting a new

Configuration

one. This rule is only applied during the hours of operation of this archiver so may be exceeded if the archive is disabled for part of the day.

MB per file (default 100) - This determines the size of each tar archive file. When a file exceeds this size it is closed and copied to the appropriate drive or path as soon as possible.

Content to be archived - Determines whether audio recordings, screen recordings or both are copied to this destination.

Hours of operation - Normally the archiver will run continuously but by clearing one or more checkboxes here you can stop it from running during certain hours of the day. This may be needed if a DVD drive is used for other purposes; if network bandwidth to a NAS folder is limited or to stagger several recorders using the same NAS so only one operates at a time.

Layout file (default lacr.xml) - By default, all recordings will be archived. If you wish to select particular calls only, you can do so with the same flexibility and configuration approach that is used for search and replay. To use a different query or set of fields from the default replay layout, create a layout xml file as described in [Customizing Search and Replay with Layout Builder](#) on page 237 and enter its name here.

Disabled - check this box to disable an archive process. You cannot delete an archive destination once recordings have been archived to it but you can use this setting to stop any further recordings being sent there.

Days to retain (default 0 = indefinite) (NAS only) - By default, archived tar files are left indefinitely but on NAS drives, you can specify a retention period. As part of the recorder's overnight (normally 1:00am) tasks it will delete any tar files that were copied to the folder longer ago than this number of days.

Username and Password (NAS only) - If the path specified is on another server, you should specify the username (including domain) and password that the recorder should use to access this path. Ensure that this account has both read and write access to the folder(s) specified as the destination(s).

Media Volume Label starts with (default ACR) - Each DVD produced is labelled with a 10 character identifier. This setting defines the first one to three characters of this and should be set to a different value for each DVD archive destination (e.g. GLD and PLT for Gold and Platinum card caller archives respectively). The next three digits of the label are the least significant digits of the recorder's serial number (e.g. 001 for the Master normally). The final four digits are a sequential media number. You should label each disk as it is produced using the label shown in the **Operations > Archive** page.

Automatically Eject (default Yes) - This determines whether or not a DVD is ejected once it has been filled with archived recordings. Set it to "No" if the drive is behind a cabinet door.

Archive Recordings where... : By default, all recordings are archived to each destination. However, you can set one or more filter criteria here to limit the set of calls that are archived to this destination. The fields that are available are determined by the Layout file specified above. As these filter fields and layouts work exactly the same for

Confidential and Proprietary Information

archival as they do for search and replay, this allows you to test out any new layout file and corresponding filter settings on the search and replay form first. When it is selecting the calls you expect, simply transfer the settings that you have tested into these filter settings. Note that selection by Call Set is also supported as it is on the search and replay page. This allows users to manually select calls for archiving BUT note that the decision to archive or not is taken only once - typically a minute (see setting at top of page) after the recording completed. Hence unless you delay all archiving, it is unlikely that users will have had time to find calls and place them in the appropriate call set.

Note:

Although you can specify a date and time range for calls, this is seldom used as an archive destination is typically left running indefinitely. It would only be of use in selecting calls relating, for example, to a specific campaign to be run over a known time period.

If you specify a date/time range that extends into the past, the recorder will immediately run a query to identify existing recordings that meet the criteria. These will be added to the archive queue alongside new recordings.

When running such a query, you will see the number of recordings waiting to be archived increase. It is important not to stop or restart the recorder until this query has completed as the query will NOT be run when the recorder restarts. Only new recordings will be considered for archive. If you need to archive a large number of old recordings, this query can take some time. Consider specifying part of the time range (e.g. a month) at a time and when that has finished and the calls have subsequently been written to archive, move the timespan forwards to the next month.

When setting the timespan, you may notice that the SQL statement shown as a result of this appears to be one second out on the end date and time. This is deliberate - so as to avoid missing calls that you thought would be included. The start date and time displayed on screen is actually rounded to one second granularity so the stored time could be a fraction of a second later and would therefore not be included in the result of a query run to exactly that time.

The table of Archive Destinations at the foot of the page shows how you have configured archiving. The columns show:

No. - the unique reference for this Archive Destination within the recording system.

Detail - shows any comment you have added plus any of the Advanced settings that are not on their default values.

Path/Drive(s) - shows a line for each path or drive configured along with the current status and (where this can be determined) the free space remaining for archival on it. Check this column to ensure that each path or drive is correctly specified and is

Configuration

available. DVD drives show an **Eject** link here with which you can eject the media before it is full.

pending - shows the number of recordings awaiting archival to this destination. Each recording is tested after the wait time specified at the top of the page and those that pass any filtering rules associated with this destination (or all if no filter is set) are queued for archival. These recordings are appended to a "tar" file within a minute (assuming no backlog) but this file is not closed and copied to the destination until it has reached an appropriate size or age.

MB pending - shows the size, in Megabytes, of the recordings awaiting archival to this destination. If this exceeds the size of one tar file (100MB by default unless overridden with advanced settings) this implies that this archiver is backlogged. This could be because it is not scheduled to run till night-time; the DVD is full etc. Check the Path/Drives column and the Alarms page for problems.

Oldest pending - shows the age (to the nearest minute, hour or day as appropriate) of the oldest recording waiting to be archived to this destination. This is normally less than the interval set for archiving to occur (default 24 hours unless overridden under advanced settings). If this is greater than expected, check for reasons as described on the previous column.

To reconfigure an existing archive destination, click on the Edit link to its right. Do NOT remove folders from NAS locations as the recordings archived there will no longer be accessible.

To delete one or more existing archives, click the check-box(es) to the left of it/them and then click the Delete selected archive destination(s) button. You cannot delete a destination once recordings have been archived to it. You can only disable it from this point onwards or those archived recordings would no longer be accessible.

Note:

If your system contains a standby and/or slave recorders, you should NOT attempt to delete archive destinations as this requires manual intervention on the other recorders. Simply disable them.

Hard Disk Archiving

Location

You may archive recordings to locally attached, Storage Attached Network (SAN) or Network Attached Storage (NAS) (file-shares) or EMC Centera file stores. However, you are encouraged to use Network Attached Storage as this is typically physically distant from the recorder. A key goal of archiving should be to protect your recordings from physical damage or loss e.g. fire, flood, explosion, theft. Having them in a neighbouring rack to the recorder itself does not achieve this.

Confidential and Proprietary Information

A single folder can be specified for all recorders to use as each will create a sub-folder using its six digit serial number to ensure that each archives its calls into that sub-folder only.

Capacity

The recorder makes no attempt to manage the available storage space. You may use a Hierarchical File Storage (HFS) system to do so but you should test that the retrieval time is acceptable.

If instructed, the recorder will delete recordings that have passed the set retention period but it will not delete them merely to make room for new archives as the recorder's main circular buffer does.

Increasing Capacity

You may "top up" the available storage space by making additional directories available as the initial one(s) fill up. Add these paths to the end of the list of paths and the recorder will start using them as the earlier ones fill.

DVD+RW/Blu-ray Archiving

Device Access Rights

Ensure the recorder has access rights to the drive. Linux users should also note that access to the DVD+RW/Blu-ray drive is disrupted if the drive permissions change. To avoid this:

1. When logging on at the server console, always log on as root.
2. Do not start the RedHat windowing system on the console while the recorder is running.
3. Do not power down or unplug external USB connected drives while the recorder is running.

Media Must be "Fresh"

 **CAUTION:**

There are many variants of writeable DVD drives (+R, -R, +RW, -RW etc). The recorder **ONLY** supports truly blank DVD+RW or BD-R (on Linux) or BD-RE (on windows) media i.e. straight out of the wrapper. Do not attempt to reuse old media.

Media control and care

To find calls easily and reliably, ensure that all media are labelled, handled and stored correctly.

To ensure maximum reliability and consistent high quality recording and playback:

- Follow the drive manufacturer's guidelines for cleaning the drive's lens.
- Follow the media manufacturer's guidelines for storage and handling.
- Check that the maximum shelf-life of the disks is adequate for your purposes and, if not, plan to copy the contents to new media within this period.

Loading a disk

To load a new disk:

1. Insert a blank DVD+RW or BD-R (Linux) or BD-RE (Windows) disk in the drive.
2. Wait for it to spin up and be recognized. This can take up to one minute.

 **Important:**

Do not close the rack door as the tray will eject and automatically re-insert during the load process. If the tray does not eject and reload automatically for any reason, you must eject and reload manually.

3. In the recorder Administration application, click on the **Operations > Archive** tab to confirm that the recorder has recognized the disk and is reporting it as empty or has already started to label it and archive to it. A blank DVD+RW disk will show 4GB available for recordings.

Drive Status

This is shown on the **Operations > Archive** page next to the drive's name. Use this entry to confirm that the drive has sensed, and is using, a valid disk. It will show one of the following values:

- **active** if it is able to record to the disk
- **foreign** if it cannot use or recognize the inserted disk

Confidential and Proprietary Information

- **old** if a previously closed disk has been reinserted
- **empty** if there is no disk in the drive
- **unknown** if the recorder is still starting up or the archive device has not been specified correctly

One drive in each archive destination's set of drives should be showing Active unless you are replaying from a previous disk. If it is not, you should insert a new or the latest partially filled disk so that archiving can continue.

Changing disks

A warning level alarm is raised as the disk in an archive drive is filled and a further, higher priority alarm is raised if more recordings are ready to be archived to it.

To eject a disk that is still being recorded in order to retrieve calls from another disk:

1. Click on the appropriate Eject link on the **Operations > Archive** page.
2. Insert the required archive disk.
3. When you have finished retrieving calls, replace the partially full disk so recording can continue.

Note:

The archival process never writes to disks out of sequence. For example, if you eject a partially full disk, then insert a blank disk onto which the next set of calls is then written, you cannot then reinsert the previous disk.

Labeling disks

As you eject each disk, label the disk itself using an approved indelible marker. Your label should indicate:

- The disk's volume label as shown on the **Operations > Archive** page
- The date that the disk became full.

Verifying recorded disks

While a disk is being recorded, the files on it are not visible to the operating system. They only show once the disk has been ejected and reinserted.

To verify that the contents of a disk are valid, reinsert it then view the drive's contents. If the contents of the disk are valid, there will be a set of large tar files that contain the wav and xml files of the original recordings.

Be sure to:

- Place the disk back in its protective container.
- Store the disk in a logical order with the other recorded disks.

Confidential and Proprietary Information

Configuration

A standalone media verification tool is also available on request.

Central Replay Server(s) with Archive

As “tar” files are written to archive destinations, the Central Replay Server automatically tracks which archive destination this set of calls has been copied to. Because a single replay server can be uploading calls from more than one recording system, it cannot simply use the same archive id (normally starting at 1) that is used on the corresponding Master recorder. These could clash across systems. Instead it creates a new archive id consisting of the master’s six digit serial number followed by the archive identifier shown on that master. Hence archive 1 on 890001 becomes archive 890001001 on the Central Replay Server.

A Central Replay Server may therefore be aware of many different archive destinations, not all of which are necessarily accessible to it. This has several implications:

1. Unlike a normal recorder – which needs to actually archive its recordings – the Central Replay Server makes no recordings so will **ONLY** run an archive thread if that archive is explicitly set to run on it.
2. For NAS archives, the Central Replay Server may need to use a different path and/or credentials to access the share. For example, the share seen by the recorders may actually be a disk on the replay server and hence accessible to it via a local drive letter; the archive may be obsolete and has been moved to slower/cheaper storage on a different path.

The default mode of operation is that the Central Replay Server will forward all replay requests on to the recorder that made the recording. That recorder will then access an archive destination if necessary.

You can override this and have the replay server attempt to service requests for calls on this archive destination before forwarding the request on should it fail to find the required recording. To do this, use the administration pages on the Central Replay Server as follows:

- Click on the **Operations > Archive** tab.
- Click the **Edit** link to the right of the archive you wish to run on the Central Replay Server
- Click the **Advanced** button

Specify this Central Replay Server’s six digit serial number in the **Recorders** field to make it run there.

If the path is to a NAS, check the path and add username and password credentials to allow it to access the share.

Click **Enter** to save the new settings.

Confidential and Proprietary Information

Search and Replay

If you are deploying a centralized search and replay system using Viewer, you should see *Viewer Installation Guide* for instructions on how to customize, deploy and use the application. However, you should still prove that you can search for and replay calls directly from the recorder because:

- if you cannot, then Viewer will not be able to play calls either.
- in the event of server or network failure you may need to access recordings directly from the recorder.

The instructions below relate to the integral search and replay application that is part of the recorder itself. The accompanying User Guide provides end user instructions on this application. As the system administrator, however, you may wish to:

- control which users can search and replay recordings
- customize the search fields and/or display
- ensure that the ActiveX control used can be downloaded to your clients' PCs
- restrict access to certain replay layouts
- enable other security features
- allow users to "lock" and "unlock" recordings
- force some users to obtain authorization before they can replay recordings.
- modify default behavior via the properties file

The second of these is rarely required and is described with other advanced topics in [Customizing Search and Replay with Layout Builder](#) on page 237. The others are needed in most cases and are described below:

Search and Replay Access Rights

When a recording is made, the recorder assigns its "owner" or, in some cases "owners" as follows:

- If the **Recording owner** field is set for a recording mode as a whole, or on the **Advanced** settings for the address being recorded, the owner will be the number or name specified there.
- If an owner is not specified but the call was made by a logged in Agent, then the owner is that Agent's ID.
- If an owner is not specified and the call was not made by a logged on Agent, then the owner is the station that was recorded.

Confidential and Proprietary Information

Configuration

- (Communication Manager only) If **Add VDN as additional "owner" of calls** is set on the **General Setup > Contact Center Interface** page, then calls routed via a VDN will have a VDN as another owner. A further setting on that page determines whether this is the first or last VDN a call went through.

Meeting Recording however, does not follow the above rules. In this mode, the voice prompts advise the caller to enter one or more owners.

Tip:

Use dummy station identifiers to allocate owners to calls made in Meeting Recording mode. All members of a particular team can be configured with replay rights for a particular number, even though this is not a valid station number. When prompted at the start of the call, mark meetings recorded for and by a team with this "owner" so that all members of the team can access the recording.

You control which recordings your users can search for and replay by adding a user account for each person that needs to use the Replay page and specifying which range(s) of owner they are entitled to see.

To add a user account, follow the same procedure that you used in [Securing the System](#) on page 127 but do not select either of the Administrator roles. Other role options let you control whether the user can lock and/or unlock calls, must be authorized and/or be allowed to authorize others and whether or not the user is allowed to export recordings as files or email attachments.

In order to search for and replay a call, the user's replay rights must include at least one owner of that call. Each user's rights are shown on the **System > Manage Users** page and are set when adding the user account. You can change these by clicking on the **Edit** link next to them.

The initial administrator's account is automatically given access rights to all number ranges up to 10 digits. As you add other users you must specify which ranges of owners each user is entitled to replay. The number of digits is significant. A user with replay rights over 0000-9999 cannot replay calls made by and "owned by" agent 567 though they could play calls owned by agent 0567. In this example, you might grant the user replay rights over 0000-9999, 000-999.

Typical examples of how to use replay rights are:

- A user allowed to play calls made on his own station (1234) would be given replay rights 1234.
- An Agent who logs on as AgentID 5012 and is allowed to replay his own calls may be given replay rights 5012.
- A supervisor who logs on as AgentID 5050 and manages AgentIDs 5010-5019 and 5025-5028 may be given replay rights 5050 , 5010-5019 , 5025-5028.
- All recorded stations used by the HR staff have their **Recording Owner** set to HR on the Advanced settings. The Human Resources Manager, who uses station 5678 may be given replay rights **HR, 5678**

Confidential and Proprietary Information

ActiveX Control Download

The Replay page downloads a number of ActiveX controls, which it uses to decompress the audio for replay and export and to replay screen recordings. If your default browser security settings prohibit the downloading of such controls, you need to provide a means of getting the ActiveX control to your users' desktops.

Internet Explorer (IE) determines rights by putting web servers into zones and then granting those zones specific rights.

To access and use the Replay page with its ActiveX controls, the recorder must reside in a zone with the following rights:

- ActiveX controls and plug-ins
 - Download signed ActiveX controls
 - Run ActiveX controls and plug-ins
 - Script ActiveX controls marked safe for scripting
- Scripting
 - Active scripting

On Windows Vista and 7 you must also clear the **Enable Protected Mode** checkbox.

Your Intranet zone and/or the Trusted Site zone may already have these rights. If so, you need to verify that the Avaya Contact Recorder is in one of these zones. If the recorder is not in the local Intranet Zone or is not a Trusted Site, you can add it as follows:

1. In the **Control Panel**, open **Internet Options**.
2. Click the **Security** tab.
3. Click the **Trusted Sites** icon.
4. Click **Sites**.
5. Uncheck the **Require server verification (https:) for all sites in this zone** box (unless you are forcing users to use https)
6. Enter the URL of the Avaya Contact Recorder server and click **Add**.

Note:

Internet Explorer does not recognize that a certain Fully Qualified Domain Name (FQDN) and IP address are the same; you must add the URL to the list exactly as your end users are expected to type it in the address bar.

Before you advise end users of the URL of the recorder, you should make sure that your users can access the Replay page through your network and that the ActiveX controls download successfully. To test this:

1. Create a user account without either administrator or restricted administrator role checked and assign it some replay rights

Confidential and Proprietary Information

Configuration

2. From a typical client machine, enter the URL for the recorder in the form:
`http://myservername:8080/` (using the recorder's IP address or hostname - assuming you have entered it in your DNS server). If using https, replace 8080 with 8443.
3. When prompted, enter the account's Username and the temporary password set in step 1 above.
4. Set a new password as directed.
5. Confirm that the Replay page displays correctly and that the ActiveX control is downloaded.

Tip:

You may wish to copy steps 2 to 4 above, fill in your URL and send them out as instructions to your end users.

Installing the ActiveX Controls Manually

The ActiveX controls needed for the Search and Replay application are typically downloaded and automatically installed the first time the application is accessed. In a closed environment where users may not be able to download and install programs on their computers, you need to manually set up the Active X controls.

To install the ActiveX controls:

1. Download the .cab files that contain the required files from

`http://mycsserver:8080/cabs/vxreplay.cab`

and

`http://mycsserver:8080/cabs/atxwitplayer2.cab`

Where mycsserver is the name of the server on which the Avaya Contact Recorder is installed).

2. Save the files to the drive.
3. Unzip the files to find:

`csreplay.ocx`

`csexport.ocx`

`dspapi.dll`

`csreplay.inf`

`atxwitplayer2.inf`

`setup.exe`

4. Copy the dll to a location in the Path (typically \windows\system32).

Confidential and Proprietary Information

5. Right-click the `csreplay.inf` file and select **Install**.
6. Click **Start** › **Run**
7. In the field displayed enter

```
regsvr32 path\csreplay.ocx
```

replacing `path` with the full path for the `csreplay.ocx` file.
8. Repeat the previous step to register the `csexport.ocx` file.
9. Run `setup.exe` to install the screen replay control.

Note:

The files will need to be updated whenever the server is updated.

A Note About Downloading the .cab files

Some browsers won't let you save a cab file; instead they open and read the file. (It is not in human readable form.) To work around this limitation:

1. Create a file that contains the following html:

```
<html>
  <body>
    <a href="http://mycssserver:8080/cabs/vxreplay.cab">
      Right Click Here
    </a>
    <a href="http://mycssserver:8080/cabs/atxwitplayer2.cab">
      Then Right Click Here
    </a>
  </body>
</html>
```

Where `mycssserver` is the host name of your Avaya Contact Recorder server

2. Save and close the file.
3. Use your browser to open the file.
4. Right-click the first link and select **Save target as**
5. Save it as `vxreplay.cab`.
6. Repeat with the second link, saving it as `atxwitplayer2.cab`

Restricting Access to Replay Layouts

Avaya Contact Recorder provides a single default layout of search filters and result columns. If you create additional layouts as described in [Customizing Search and Replay with Layout Builder](#) on page 237 you should also consider restricting access to these layouts on a per user basis.

Using the layout editor you can choose whether a layout is made available to all replay users or none initially. You can then see which users are able to access each layout - and refine this using the **System > Manage Users** page.

As you click **Add User** to create a new user account or **Edit** an existing one, you can set the **Search/Replay layout(s) available** to each user. Those they are entitled to use are listed and can be changed by clicking the **Edit** link and altering the checkbox next to a layout's name. Click **Enter** to save these changes.

Miscellaneous Security Features

Additional security features can be enabled by setting `viewerx.secure=true` in the properties file.

Locking Recordings

The recording system normally keeps recordings for a planned time-span or until disk space is required for new recordings - at which point old recordings are purged from the recorder's disk buffer and/or archive path. However, specific recordings may be of interest for longer periods and it is important that these are retained for as long as needed. For example, those required by a "legal hold" order must not be deleted. This is achieved by "locking" the required recordings.

Enabling Lock/Unlock

To use this feature, assign the **May lock recordings** and **May unlock recordings** roles to at least one user account. Add the roles from the **System > Manage Users** page as you add a new user account or **Edit** an existing one. Typically, only one or two users (often the System Administrator) are allowed to unlock recordings while more people (supervisors, investigators, compliance staff) are allowed to lock recordings.

A **Restricted Administrator** is allowed to assign the **May lock recordings** role to non-administrator user accounts but not the **May unlock recordings** role.

Confidential and Proprietary Information

How it Works

Three system-wide call sets are created automatically, and made visible to users with either of these roles assigned. Authorized users have lock and/or unlock icons on their search/replay screens with which they can select one or more recordings and give a reason why they are locking or unlocking the set of recordings. Recordings to be locked are placed in the **Lock Pending** call set.

A background process retrieves these recordings from disk buffer, archive or the recorder on which they are held and places a copy of the recording, (which may consist of multiple audio and screen files) and its XML file in a special sub-folder within the **Call Storage Path**. This folder is not purged like the normal recording folders so anything placed there remains there until the recording is unlocked.

Note:

You should NOT attempt to delete or otherwise manage the files in this path by hand. Use the Lock and Unlock features provided for you.

All lock and unlock requests and associated actions are audited as **Call Storage** actions.

The *Avaya Contact Recorder User Manual* includes instructions for end users on how to use the Lock and Unlock features.

Multiple Server Systems

You should enable and use the locking features only on the recorder(s) that hold the consolidated database of recordings from all your recorders. Where you have installed one, this will be on the Central Replay Server. Otherwise, this will be the Master recorder - which will be providing these centralized replay services. Do not enable it on any user accounts on slave recorders.

Each recorder will forward a lock or unlock request to any other recorder to which it is consolidating its own recordings. A master/standby pair (in the absence of dedicated Central Replay Server(s)) will update each other automatically. However, if you have a backup Central Replay Server, it is important that each Central Replay Server is configured with the address of the other Central Replay Server (on the General Setup > Recorder page) so that it knows to forward lock related requests to the other server.

Purging the Locked Folder

It is deliberately easier to lock a recording than it is to delete one - as the latter is irreversible. Calls can be locked and unlocked by appropriately authorized users but this does not actually delete them from the locked folder. This gives the System Administrator one last chance to reverse the unlock decision if that turns out to have been made in error. You should be absolutely certain that the unlock decision was correct before purging the locked folder as described below. If a mistake has been made, simply select the relevant calls and lock them again.

Configuration

Overnight, as part of the daily purging process, the recorder will raise a Warning level alarm if it finds one or more recordings in the locked folder that no longer need to be locked. To purge these unlocked recordings, use the maintenance page (at url `/servlet/acr?cmd=mtce`) and click the **Purge Unlocked Recordings** button. Where locked recordings are retained on multiple servers, you must purge each one in turn.

Replay Authorization Process

You can, optionally, require specific users to obtain explicit authorization before they are allowed to replay any recording. How this process impacts users is described in the *Avaya Contact Recorder User Guide*.

Email Server

The process relies on email to advise users of requests and responses. You must therefore configure and test valid settings on the **System > Email Server** page as described under [Email Configuration](#) on page 141 (CHRIS TODO is this correct?).

Configuring the Process

To enable and configure this process, on the **System > Manage Users** page, set **Replay authorization process** enabled to **Yes**. A number of additional settings will then become visible. These let you specify:

Replay authorization to be approved by

By default, a single user must authorize each replay request but, by setting this to a higher number you can require two or more users to accept a request before the recording can be played by the user requesting it. This setting applies to all users who require authorization.

Replay authorization falls back after (hours)

If those asked to authorize a request are absent or do not respond after this number of hours (default 72) then the request will be copied to those you define as "fallback" authorizers so that they can make a decision on it.

Replay authorization falls back to

You can select any of the users you have given the **May authorize replay** role to act as "fallback" authorizers. (See immediately above).

Confidential and Proprietary Information

Replay authorization expires in (hours)

Once authorization is granted, the requesting user has a certain time in which to play the recording (default 48 hours). After this period, the authorization expires and he would have to request it again if he needs to play the recording again.

Configuring Authorizers

To use this process, a full administrator must give at least one user account the **May authorize replay** role and enter an email address through which that user can be contacted and identified to other users. **Add** or **Edit** an existing user account to assign this role and set their email address.

You should also consider adding at least one such authorizer to the list of fallback authorizers.

Requiring Authorization

For each user account that you want to force to use this authorization process, first ensure that the user(s) you wish to handle their requests have already been configured as authorizers (see above) and that you know the user's email address.

Log in as either a full or restricted system administrator and use the **System > Manage Users** page to add or edit the user's account. Set their **Email address** and click the **Edit** link opposite **Replay must be authorized by**. Select one or more authorizers from the list of email addresses shown and click **Enter**.

The email addresses of the selected authorizers are shown in the table at the foot of the **System > Manage Users** page. All of the authorizers that you select here will be notified immediately of requests by this user. Any "fallback" authorizers configured will also be notified if requests are still pending after the configured fallback period.

Audit Trail

All steps in the authorization process are logged to the Audit Trail as Replay actions. Where a step involves both a requesting and an authorizing user, two entries are made, one for each. This allows you to search for all replay actions by requestor or by authorizing user.

Standby Server

Although user account settings are copied to a standby server, the actual replay authorization requests and responses are not maintained on the standby. Should the system fail over to the standby, new requests would have to be issued. Similarly, when the Master is forced to take over again, any requests made on the Standby will be lost and must be re-requested.

Backup Central Replay Server

Neither user configuration nor details of authorization requests are copied to a backup Central Replay Server. You should be backing up the contents of the postgres database on the main Central Replay Server so that these details (which include all authorization requests and their results) can be restored in the event of server failure or corruption.

Modify Default Behavior

You can add or modify lines in the properties file as described in [Properties File](#) on page 224 to change the behavior of the Replay page to:

- limit the number of results returned
- save filter settings from session to session

These settings affect all users and are only updated when the Avaya Contact Recorder Service starts.

Limit results returned

Add the following line to the properties file to set the maximum number of calls returned from a query:

```
viewerx.limit=nnnn
```

where **nnnn** is the maximum number of calls to return. Increasing this maximum over the default of 100 results in more CPU use and higher network traffic if users choose to view or accidentally request a large number of calls.

Save filter settings from session to session

Normally, the entries in the search filter pane are blank when you first access it. If you wish, the application can remember the last used settings and apply these instead. This feature is controlled by a setting in the properties file:

```
viewerx.savesettings=true
```

Bulk Export Options

As described in the search and replay manual, you can export not only the audio of the calls you are interested in but also the details stored about these recordings. The default method is to export an html file along with the audio files. This allows you to view the details of the calls and play them from within a browser. Previous versions of Avaya Contact Recorder exported the call details in a "comma separated variable" (".csv") file. You can re-enable this type of output by setting `viewerx.ollexport=true` in the properties file. The ".csv" file these are written to does not, by default, contain a header

Confidential and Proprietary Information

row. If you want the system to add a header row (in English only), set `export.csvheaders=true` in the properties file.

Backup/Restore

Due to the huge volume of new files created every day, a voice recorder is not backed up in the same way as most application servers. This section guides you through the issues around backing up the application, the call details database and the recordings.

Application

The recorder's configuration is stored in its database (using PostgreSQL), alongside the details of the call recordings. To preserve the configuration of the server, back up the database frequently as described below.

If you have not installed other applications on the server, there is no need to backup the operating system or the recorder software. It is faster to reinstall these server components in the event of disk failure. You should therefore retain the installation media and license key that you used.

Backing up the Database

You can back up your recorder's database using a command line procedure. The procedure uses the PostgreSQL `pg_dump` command to extract data from the database. It must be executed while the database is running. Do not stop the Avaya Contact Recorder service or the Postgresql service before proceeding.

Linux

To back up your postgres database:

1. Log on as root.
2. Become the database owner by typing `su - postgres`
3. Create a backup file by entering the command:

```
pg_dump --format=c --compress=5 eware > backupfile
```

You should specify a full path for the backupfile, and consider moving the resulting backup file to external media or another machine.

Please observe the following guidelines concerning the compression factor:

- 5 is a modest compression factor.
- using a higher number (maximum is 9) makes the backup slower and uses more resources. However, it results in a smaller backup file.

Confidential and Proprietary Information

- using a smaller number makes the backup faster and uses fewer resources. However, it results in a larger backup file.

Windows

To back up your postgres database:

1. Log on as an administrator and open a command window.
2. Change directory ("cd") to the \bin folder beneath the installation path.

```
(\Program files\Avaya>ContactRecorder\bin )
```

3. Create a backup file by entering the command:

```
winbackup backupfile
```

where backupfile includes the full path and filename of the backup to be created. Make sure there is enough space on the target drive for the backup file. Consider copying the backup file to another server, or external media.

Restoring data to a new PostgreSQL database

Important:

You can only restore data to the server from which you dumped it because the dump file stores the software serial number and license key information. These are tied to a MAC address on the recorder. Unless you can move the original NIC into the new server, you will need to obtain a new license key if you wish to restore to different hardware.

The following process erases the default database that exists after a complete re-installation and replaces it with the database that you have backed up. The previous database is renamed rather than deleted - so if you need to restore the database again, you must first rename, backup or delete the previously retained database.

Linux

To restore the database:

1. Re-install the operating system.
2. Log on as root and install the recorder as described in [Installing Avaya Contact Recorder](#) on page 110.
3. Stop the Avaya Contact Recorder service.
4. Become the database owner by typing `su - postgres`

Configuration

- Drop the existing database by entering the following command:

```
dropdb aware
```

- Create an empty copy of the postgresql database by entering the following command:

```
createdb aware
```

- Restore the data by entering the following command:

```
pg_restore --dbname=aware --use-set-session-authorization  
backupfile
```

- Start the Avaya Contact Recorder service
- Test to verify successful restore

Windows

To restore the database:

- Log into server as an administrator.
- Stop the Avaya Contact Recorder service.
- Open a command window
- Change Directory ("cd") to the \bin directory beneath the install path.
- Enter the command:

```
winbackup <backupfile> restore
```

where <backupfile> is the full path name of the backup file.

- Ignore all warnings stating that functions 'already exist'.
- Start the Avaya Contact Recorder service.
- Test to verify successful restore

Backing up Voice Recordings

The Avaya Contact Recorder stores voice recordings in a single partition (/calls on Linux, selectable on Windows). This partition quickly fills up with thousands of directories and millions of files. When the partition is nearly full, the recorder maintains only a tiny amount of free space on the partition by deleting batches of 100 recordings (and the directory that catalogued them) at a time, as it requires space for new recordings. This causes a huge churn of files every day.

Limitations of full and incremental backup procedures

On a Avaya Contact Recorder server, two issues make it difficult to back up voice files:

Confidential and Proprietary Information

- the file size
- the rate of change of the voice recording files

Together these issues make most traditional backup strategies for the voice recordings ineffective. Traditional full backups are required more frequently than normal, which wastes backup media, and incremental backups are larger than expected because of the large churn of creations and deletions. For a backup strategy to be successful, it must be easy to restore the data if necessary.

Traditional "full plus incremental" backup solutions are ineffective because these backup solutions cannot complete fully. In the event of a complete disk failure, the process restores the full backup, then the increments in chronological order. This procedure immediately overflows the disk when the restore program tries to create the increments because the partition holding the call is almost at capacity to begin with. The full plus incremental backup will fail because it runs out of disk space before it has processed the "removals" part of the procedure.

Traditional restore procedures are also ineffective. If you use this solution to review a recording that has been deleted because of age, the recorder immediately deletes any restored file as part of its disk maintenance.

Finally, traditional backup solutions often require locks on the disk while they work. This can seriously disrupt the working of the recorder.

Backing Up Recordings

This simplest and cheapest strategy is to use the built in archive mechanism. This is not only fully integrated with the workings of the recorder and its search and replay mechanism, but also is well suited to the incremental recording required for a recorder. As recordings are added to the calls path they are copied to one or more archive destinations in an efficient manner. Even when they have been deleted from the hard disk, the recorder is still able to play them because it knows which media or folder they are on and can replay directly from there, without an intervening 'restoration' step. Each DVD holds about 4GB, which means it can hold about 150 channel-days worth of recordings from a busy system. For less than dollar a day, even a busy system can have limitless backup. Blu-ray disks hold much more (25GB) but are somewhat more expensive. They are suitable for larger systems and can be used on Linux based systems.

If you use NAS storage to archive your recordings, the data on these centralized disks is

- organized in a more permanent way
- subject to less "churn"

It is possible to schedule gaps in the archiving process (e.g. 1am-4am), so, if a backup process requires a disk lock, the downtime does not cause a problem with the server's operation. This scheduling feature, together with the way the archive process organizes the audio on disk, makes this data much more appropriate for traditional full/incremental backup solutions.

Distributing User Instructions

Once you have configured the recorder, you should ensure that the end users know how to use it. Some users may need to know how to use and control the recording modes. Some will need to know how to search for and replay recordings.

Confidential and Proprietary Information

Those Using Recording

You will need to advise users of some or all of the following:

Mode	If you...	You should tell...	This information
On Demand Recording	Use this mode at all	All potential users of On Demand recording	The station and/or hunt group number(s) to dial to reach an appropriate On Demand recording port. How to use this mode.
	Configured any Audix-rec buttons	Users of these stations	How to use the Audix-rec button
Meeting Recording	Configured any Meeting Recording ports	All potential users of Meeting recording	The station and/or hunt group number(s) to dial to reach a Meeting recording port (with prompts in the appropriate language)
Bulk Recording	Enabled the delete command	Users who may need to delete recordings during a call	The digits to dial during a call to have a recording deleted
	Enabled the retain command	Users whose stations are configured with this setting	The digits to dial during a call to have a recording retained
	Have configured delayed retention	Users who may need to retain a call after the call has ended	The number of the retain port and explain that only the previous call will be retained. They must retain the call before making another call from the same station.
	Use Record on Demand (ROD) or Save (SAV) buttons on CS1000 phones	Users of those phones	How to use these buttons and how to interpret the lamp conditions
	Use Contact Recording Desktop (CRD)	Users of workstations where it is installed	How you expect them to control and/or tag recordings.

Confidential and Proprietary Information

Those entitled to replay calls

The integral search and replay application is very straightforward and the online help within it is rarely needed. If you do not distribute the manual to all users you should still advise them of the following:

- The url (http or https) they should use to access search and replay
- Their username and how to log in for the first time (unless you are using Windows authentication)
- Any tips on which data fields would be particularly useful for them to search on (especially if you have populated any user defined fields).

Confidential and Proprietary Information

Configuring Avaya Support Remote Access

Refer to the instructions in the document RemoteAccess.pdf provided in the docs folder of the installation CD.

Configuration

Confidential and Proprietary Information



Chapter 5: Operations, Administration & Maintenance

This chapter provides details of regular maintenance required for an Avaya Contact Recorder system.

The main sections in this chapter are:

- [Introduction](#) on page 192
- [Status Monitoring](#) on page 193
- [Preventative Maintenance](#) on page 201
- [Restarting the System](#) on page 205

Introduction

In addition to initial configuration, there are a number of tasks that need to be performed on an ongoing basis. This section discusses

- the use of the Status monitoring pages
- the Audit Trail
- preventative maintenance tasks that should be carried out on a regular basis

Confidential and Proprietary Information

Status Monitoring

Recorder status is shown over four pages that are accessed under the **Recorder Status** tab at the top left of the Administration web interface. These show the current:

- **System** status - (On the Master and Standby only) the overall status of each recorder in the system and a table showing the overall loading across the whole system.
- **Server** status - shows the status of network links between this server and the others in the system plus an overview of what has been recorded.
- **CTI Monitors** - (On the Master and Standby only) the devices that are being observed via the CTI link(s).
- **Ports'** status - (On the Master and Standby only) - the state of each recording port in the system.

System

This page shows summary information about the current state of the system and is therefore the default page shown when you first log in as an administrator to a Master or Standby recorder. Each server is shown at the top of the page - with Master and Standby first, then any slave servers. The slaves are ranked according to their status. Any server with problems will show red or amber and, in the case of slaves, will be brought to the top of the (potentially long) list of slaves. Click on the buttons to jump to the administration interface for each server to drill down into any problems that are showing. You can also clear the accumulated alarm counts if necessary.

The recorder's own entry on this page will show whether it is "Active", "Standing By" (could go active if needed) or "Not Viable" (a major problem is preventing it from recording). Note that when a Master or Standby recorder makes contact with another recorder, only "persistent" alarms (ones that are still an issue) are refreshed. Any transient alarms that occurred while the recorder was disconnected will only be visible on that recorder's Alarms page.

Load

On the Master (or Standby if it is in control), the table at the bottom of this page shows the current and peak loading levels of the recorder. For each recording mode configured, it shows

- how many ports have been allocated
- how many are currently active

Confidential and Proprietary Information

- the maximum number that have been active concurrently since midnight
- the maximum number that have been active concurrently since the date and time shown above the right-hand column

To reset the monitoring period, select the **Restart Peak Activity Count** button. For example, if your business has a weekly cycle, you may want to reset the monitoring period at the start of each week. Use this page to predict when to expand your recording capacity.

For more detail of contention and "busy" events on the hunt groups associated with the pooled recording modes, use the Communication Manager's call detail recording tools. These tools might be useful if, for example, you are required to provide 98% availability of Meeting Recording ports.

Server

This page shows the status of the server displaying it. It includes a row for each network link that the server requires to function as well as basic counts of calls recorded.

See [Recorder Interfaces](#) on page 264 for a comprehensive list of interfaces.

Note:

Due to a problem in the RSA Key Management Service client software, the link to KMS may show "UP" even if the recorder is having to use a previously cached key. This problem may only become apparent when you next attempt to decrypt an old file. You should check for Alarms as well as look at this item.

The following items are not relevant to and hence are not shown on Central Replay Servers.

Total calls observed via CTI since startup

Shows how many calls have been tracked via CTI information (whether recorded or not) since the recorder was last started. Where overlay CTI feeds are used, the same underlying phone call may be advised to the recorder more than once (e.g. from TSAPI and via CCT). In such cases each appears as a separate "call" in this count.

Total Media Files recorded to date

This value shows the total number of files ever recorded by the system. Note that each recording may result in more than one file.

Confidential and Proprietary Information

Total calls observed via CTI today

Shows how many calls have been tracked via CTI information (whether recorded or not) since midnight (or since the recorder was last started if that was today). (As with the "to date" figure, multiple CTI feeds can make one underlying call appear as multiple calls).

Total Media Files recorded today

Use this value to confirm that recordings are being made today. If you have restarted the server today, this will show the number of media files recorded since that restart. As above, there may be more than one media file per recording.

Date of oldest call held on disk

Until your disk has filled for the first time, you should monitor the available space on the drive. Check that the rate at which space is being consumed is in line with your predictions. You should be able to estimate when the disk will reach capacity and when the first calls recorded will be deleted to make way for new calls. This occurs when the free space drops below 1GB.

Once the disk has started to "wrap" and calls are being deleted daily, use this figure to monitor the online retrieval capacity. If the figure starts to fall, recordings are using up your disk space more rapidly than before. The recording volumes are increasing, so you may need to expand the disk capacity before the duration of calls it can hold falls below your minimum requirement.

CTI Monitors

This page is only populated on Master and Standby recorders (not Slaves or Central Replay Servers). It shows each of the phone numbers that the recorder needs to monitor via the main CTI link. Note that not all recording modes use this CTI link so it may not be populated.

The detail shown and terminology used varies slightly from one telephone system to another.

Device

Shows each device that needs to be observed via the main CTI link.

Observing

Shows whether or not the device is being observed successfully. In the case of a CS1000, there may be multiple rows showing against a single DN or position ID. Each row shows the DN or positionID and the physical TN on which the number occurs.

Part of Range

This field shows which number or number range that has been configured for recording has resulted in this particular phone number being monitored. Any advanced settings that apply to this range will determine how calls on this phone number are recorded.

Agent

If an agent has logged on to this device, this field shows that agent's ID.

Active Calls

For all calls that this station is connected to, this column shows:

- the call type and ID
- whether the call is considered to be incoming or outgoing
- whether the call is considered to be internal or external
- the Automatic Number Identification (ANI - also known as Calling Line Identifier, CLI) if present.

Each party on the call is then listed - showing

- the state of the connection (held, ringing etc.)
- whether this party is an internal or external party

If a call is shown in bold typeface, it implies that the recorder believes that this particular call is active and therefore may need to be recorded.

Note:

The details about each call are not translated. The detail within this information is of most value to second and third line support staff who will be familiar with the terse English abbreviations used to convey a lot of information in a small space on this screen.

Port

When a call is active and needs to be recorded, a port on a recorder is assigned to it. The name includes both recorder and port identifiers.

Confidential and Proprietary Information

Desktop

(CS1000 only) Shows the computer (if any) controlling recording via the Contact Recording Desktop (CRD) interface.

Rec

This column shows whether or not the channel assigned is recording the call at the moment. In the case of external controller or dialer integrations, a channel may still be assigned but not actually recording all the time. If the recording includes screen content, this is shown by a screen icon for each recording that is being made. Hover your mouse cursor over the icon to see the IP address being recorded.

Events

This column shows how many CTI events have been observed on this CTI monitor. To update the page, click the Refresh button.

Ports

This page shows the current state and configuration of each port in the system that is visible to this server. It therefore includes the server's own ports plus the ports on any slave to which it is connected. Note that channels are dynamically assigned and released as calls come and go. The columns show:

Recorder/Port

Identifies each port in the system.

Assigned To

Shows the recording target(s) that the port is being used to record.

Recording

Shows whether or not the port has been told to record active calls. If the recording is being deliberately masked this will also show here. If the recording includes screen content, this is shown by one or more screen icons. Hover your mouse cursor over the icon to see the IP address(es) being recorded.

State

Shows the current state of the port. Possible states are:

Faulty (DMCC ports only)

These ports are incorrectly configured or have experienced an error. They will be reregistered two seconds after the initial problem, in an attempt to recover them. If the problem persists, they will back-off, doubling the time between retries until this reaches 1 minute. They attempt to reregister every minute thereafter.

Starting (DMCC ports only)

These ports are registering or queuing to register with the Device, Media and Call Control API.

Idle

These ports have registered successfully, but are not in use.

Setup

These ports are:

- Placing or answering a call
- Receiving instructions from the caller, for example, with Meeting Recording

Connected

These ports are in one of the following states:

- Have established a connection but are not actively recording
- Are replay ports that have placed a call but are not currently playing a file

Active

These ports are:

- Recording ports that are recording a call
- Replay ports that are actively playing a file

Stopped

A recording port may be in this state if it has stopped recording but has not hung up yet.

Resetting Ports (DMCC ports only)

To reset an individual port, select the **Reset** link to the right of the port. This action stops any current recording on that port.

Confidential and Proprietary Information

To force a reset on all ports in quick succession, select the **Reset All** button at the bottom left.

Alarms

The Alarms page shows system warnings, alarms and events. The recorder stores alarms in its database. It deletes them when they are more than a month old.

Check the box at the top of the page if you want to see all Alarms, including those that have been "cleared". The default is to show only those alarms that have not yet been cleared.

The radio buttons at the top of the page let you select the minimum severity of alarms that are shown. The Alarms page will only show the most recent 1000 alarms (in 100 pages of 10 alarms each). If there are Informational or Warning level messages, you may need to restrict your view to Minor or Major alarms if you want to see further back in time.

Use the buttons above or below the table to refresh the page and to clear some or all alarms.

Note:

As long as you have set up mail account information on the **System > Email Server** page, an email message detailing alarms and events will be sent to the address(es) listed there.

Refer to [Alarms](#) on page 301, for a list of alarms and events that may be generated and what to do about them.

Viewing alarms and events

The default on the page is to show all alarms and events that are uncleared. You can see any new or outstanding issues on first viewing the page. To change the set of events shown:

1. Click on the check box and/or radio button to specify your preferences.
2. Click on the **Refresh** button above or below the table.

Clearing specific events

New alarms and events are initially "active". To "clear" an individual alarm or event so that it no longer shows:

1. Click the check box to the left of the event.
2. Click the **Clear selected events** button.

Clearing all events

Be careful using the **Clear All Events** button. Clearing an alarm without fixing the problem may lead to system problems being "hidden" without your knowledge.

Audit Trail

The **System > Audit Trail** page shows administrator and user actions over a specific period. The default reporting period is the current day. You can also filter this report according to Event Type and Username. To generate a report for a different period, enter the date range in the calendar controls, and click the **Refresh** button.

The Audit Trail functions track the following user actions:

- Successful user logins
- Failed user logins
- Password changes (although, for security reasons, the actual password is not stored)
- End user searches on the database
- Replay requests (including steps in the replay authorization process)
- Call storage actions (lock, unlock, purge and delete).

It also tracks all administrator actions that affect recording, such as configuration changes, manual port resets and creation or deletion of user accounts.

Note:

Editing a station range is logged as a deletion followed by an addition.

The Detail column includes the SQL statement used in searching for calls. It also uses the internal name of a setting rather than the user-friendly, localized name. This avoids any change of meaning that could occur in internationalization.

Each report is restricted to a maximum of 1000 audit records. To report on more, break your reporting period into a number of smaller date ranges.

You can either click the **Export** button to obtain a file in comma separate variable (".csv") format or use your browser's print, save, or email features to provide a permanent record of the details. To create a summary that presents all results on a single page, click the **Show All** link at the top. The **Show All** and **Page at a Time** links are not shown if the list of audit entries is less than one page long.

Configuration records (which include the audit trail) are retained for three months by default. Each night after that period has elapsed, a background job deletes any records older than the retention period. If you want to retain the records longer, back up the database as described in [Backing up the Database](#) on page 182. You can change this default value of three months using the audit.purgemonths property as described in [Properties File](#) on page 224.

Confidential and Proprietary Information

Preventative Maintenance

This section highlights a number of administrative tasks that should be performed on a regular basis to ensure the system continues to operate smoothly.

Daily

Unless you have fully automated alerting of these conditions, you should carry out the following procedures at the start of each day:

Alarms

Check the Alarms page for new problems.

Disk capacity

Check the available disk space. The disk where recordings are stored will appear to be at or near capacity. However, the system consistently maintains a level of 1 GB of free space by deleting older files. This maximizes the number of recordings that are available online to you. The Avaya Contact Recorder's disk manager thread deletes files on a FIFO (First In First Out) basis.

System Status

It is difficult to detect some problems automatically. Check the system status regularly via the **Recorder Status > System and Server** pages and verify that all figures are in line with expectations as described in [Status Monitoring](#) on page 193.

Check the contents of the log files as described in [Troubleshooting](#) on page 291 and examine any errors logged since the previous check. Look at all error and warning messages, not just those generated by the Avaya Contact Recorder services.

Confirm port status

Use the **Recorder Status** pages of the Administration application to confirm that the recording ports are in the appropriate states.

Confirm recording and replay

To confirm recording and replay:

- Verify that calls are being uploaded into the database.

Confidential and Proprietary Information

Operations, Administration & Maintenance

- Use the **Replay** page to select the most recent calls to verify that calls are accessible.
- Confirm that the start time of these calls matches expectations. Verify that the start time corresponds to the most recent calls made on the extensions being recorded.
- Confirm that these calls are playable and that audio quality is good.

Archive

If using DVD+RW or Blu-ray archive, check the current disk's available capacity. Change the disk when it fills. If using NAS folders, check the available space and increase it or add additional folders as needed.

Weekly

As you become comfortable with the normal operation of your recorder, you can reduce the frequency of the daily tasks. For example, if you know that the rate at which your disk is filling is not going to fill the available space for several months, you can check it weekly.

Perform the following tasks each week:

Disk capacity: main recording store

When your recorder is first installed, the disk is almost empty. As it gradually fills, you should note the rate at which it is being used (at least weekly) and extrapolate to estimate when the disk will be full. At this point, the Avaya Contact Recorder will begin deleting the oldest calls to make room for new ones. If this happens to calls that are younger than planned, check the configuration of the recorder to ensure that only the anticipated calls only are being recorded. Add additional disk capacity to the partition before it fills.

Disk capacity: other partitions

Check the available space on any other disk partitions. Verify that these other drives have sufficient space. The recorder will warn you if they fall below 500MB of free space. Accumulated temporary files or log files can account for this drop in available space. You may need to purge them manually.

Confidential and Proprietary Information

⚠ CAUTION:

When you are purging files on Windows, remember that files you delete go to the Recycle Bin and that the space they occupy is not freed until you empty it.

Call detail database purging

If you have enabled automatic purging of aged call detail records, you should still monitor the size of the calls database during the first few months of use. You can then predict how large the database will get by the time old records begin to be purged. Many customers plan never to purge call detail records, but choose instead to add disk capacity every year or two as the database grows. If you do this, you should upgrade your server every few years to compensate for the increasing size of the database and the reduction in search and update speed.

Configuration Backup

Changes to system configuration that affect user access rights are stored in the PostgreSQL database. This means that the system configuration is backed up whenever the call detail records are. See [Backing up the Database](#) on page 182.

Monthly

Check the following aspects of the system on a monthly basis:

Loading trends

Note the total call volumes recorded every month to be aware of gradually increasing traffic trends. To do this:

- Note the number of calls recorded at the end of each month and compare with previous month's accumulated total.
- Note the age of the oldest call on the disk (only applicable once the disk has filled for the first time)
- Note the CPU load during busy hour

If it appears that the load is increasing, consider purchasing extra licenses if required and/or increasing server specification or disk space.

Every Six Months

The recorder must perform a full vacuum of the database approximately once every six months. As this interval is reached, the recorder issues a daily warning message. This tells you that it will do a full vacuum on next restart - unless you postpone it by clearing the checkbox on the **General Setup > Recorder** page. This setting only defers the maintenance once. To defer again, reset the option. However you must allow the recorder to perform this essential maintenance task within 30 days.

Confidential and Proprietary Information

Restarting the System

Occasionally, you will need to restart your Avaya Contact Recorders.

Linux

To start, stop, restart and monitor the Avaya Contact Recorder service use the linux `service` command. You must switch user (`su`) to root to use the service command.

To start, stop, restart and monitor the ACR service use the following commands:

```
service cscm start
service cscm stop
service cscm restart
service cscm status
```

You can combine the `su` and `service` command on the same line to save time:

```
su - -c "service cscm restart"
```

Windows

To start, stop, restart and monitor the Avaya Contact Recorder service use the Services Microsoft Management Console. The service name is `ACRService`.

Be patient

You should always make some test calls following a restart. However, it can take many minutes for a large system to register all its CTI observers. Use the Status pages to confirm that ports are available and that the appropriate CTI monitors have been created before attempting to place test calls.

Do not just keep restarting the system. Check the status pages to see if registrations are progressing and wait for them to complete.

CS1000 Agents

Remember that, in CC 6.0, Call Center agents must log out and log back in again before their status can be determined. If an agent logs out while the system is restarting, the system will not recognize that they logged out; it will still show them as logged in and as a result, may continue to try and record against that agent.

Confidential and Proprietary Information

Confidential and Proprietary Information



Chapter 6: System Security

Security of customer recordings is very important. This Chapter discusses the various features - some optional - that you can use to ensure the safety and integrity of recordings. This chapter assumes that you have suitable firewall, antivirus software and physical access procedures in place.

The main sections in this chapter are:

- [Access to the Recorder](#) on page 208
- [Server Hardening](#) on page 212
- [Single Login](#) on page 214
- [Dual Sign-in](#) on page 215
- [Changing Passwords](#) on page 217
- [Encrypted File Storage](#) on page 219
- [PCI Compliance](#) on page 220

Access to the Recorder

When the system is installed, it enforces a strong set of password criteria. This and a number of other settings can be changed at the top of the **System > Manage Users** page. These are discussed below.

Windows Domain Authentication

You can create local user accounts within the recorder application itself. However, it is more secure to use Windows domain accounts and you may wish to enable this feature - or even restrict access so that *only* windows domain accounts have access to the system.

To ENABLE Windows Domain Authentication:

1. Create a user in the Active Directory for ACR. If you have multiple ACRs they can share the same username. Set the password on the account, setting it to never expire, and making sure that the account is enabled.
2. Use the `setspn` command to create Service Principal Names (SPNs) for each recorder.

```
setspn -A HTTP/RecorderFQDN username
```

3. Patch the recorder's encryption policy files as described in [Installing Unlimited Strength Encryption](#) on page 386.
4. Encrypt the recorder account password as described in [Encrypting Properties File entries](#) on page 392.
5. Ensure that the recorder and Active Directory are time synchronized.
6. Edit the properties file of each recorder and add:

```
krb5.enabled=true  
krb5.username=RecorderUsername  
krb5.password=EncryptedPassword  
krb5.domain=KerberosDomain  
krb5.kdc=ADAddress
```

7. Create user accounts (as described in [Securing the System](#) on page 127) like `USERNAME@DOMAIN` (i.e. all in uppercase) - for example, `JSMITH@BIGCORP.COM`. By default the recorder forces usernames it receives to uppercase before comparing them with those you have entered. To change this, set `krb5.exact=true` in the properties file - but you must then enter usernames and domains with exactly the same cases as stored in the Active Directory.

Confidential and Proprietary Information

8. From a workstation logged into the domain as one of the users, access the recorder using its Fully Qualified Domain Name - `http://RecorderFQDN:8080/`

You should get straight to the recorder main page. If you see the recorder login page, something has gone wrong. Check the recorder log for errors.

To ENFORCE Windows Domain Authentication only:

1. Enable Windows Domain Authentication as above.
2. Log in as an Administrator using a domain account
3. On the **System > Manage Users** page, set **Allow local user accounts?** to **No**.

Tip:

If users are prompted for their domain passwords when they access the web interface, make sure that the recorder is either part of the intranet zone, or make it a trusted site and configure Internet Explorer to automatically log on to trusted sites.

Use of SSL

You should consider whether you wish to enforce the use of Secure Sockets Layer (SSL). By default, users can access the recorder via HTTP (on port 8080) or by encrypted HTTPS (on port 8443). You can force users to use the secure https port, by setting **Allow unencrypted (http) access?** to **No**. When you do this, any user who attempts to access the recorder through the unsecured (HTTP) route is automatically redirected to the secure (HTTPS) address.

Note:

If you have more than one server and you enforce https, the **View Alarms** button on the **Recorder Status > System** page must be changed to use the fully qualified domain name of the other server(s). To do this, add a property to the properties file as follows: `fqdn.nnnnnn=<fqdn>` - where `nnnnnn` is the serial number of a server and `<fqdn>` is the fully qualified domain name that it uses.

The application is distributed with an SSL certificate that is valid for 3 years from the date it was issued. The certificate makes it possible to give users secure access to the server. When users access it through this secure HTTPS port, the traffic between their browser and the recorder is automatically encrypted.

However, Internet Explorer will warn your users that the name on the certificate does not match the name of the server using it. You can either advise your users that this is acceptable and should be ignored or, for greater security, you may acquire and install your own SSL certificate as explained in [Installing a Signed SSL Certificate](#) on page 387.

Allow search and replay from this server?

If the details of the recordings made on a particular server are consolidated into the database on another server (Master, Standby or Central Replay Server) you may want to block users from replaying calls directly from this server - forcing them to access a server that has access to recordings from all servers. To do this, set **Allow search and replay from this server** to **No**.

Session Inactivity Timeout

You can specify how long a browser session will remain active before the user is asked to log in again. The effect of this is only noticed with local account access as when using Windows Domain authentication, the recorder simply requests authentication from the domain again.

Minimum Password Length

This applies to local accounts only - not windows domain accounts. This defaults to 8 characters but can be increased or reduced to match your corporate standards.

Force strong password

This applies to local accounts only - not windows domain accounts. By default, the recorder forces all passwords to be "strong" - which means that they must contain at least one of each of:

- Uppercase characters
- Lowercase characters
- Digits
- Special characters (#,@,%,! or \$)

Changing this setting is not advised.

Confidential and Proprietary Information

Password expires after (days)

This applies to local accounts only - not windows domain accounts. By default, passwords expire and must be changed on the next login that is 90 days after they were set. You can change this period to match your corporate standards.

Password cannot be reused within (days)

This applies to local accounts only - not windows domain accounts. By default, you cannot change your password to one that was originally set (rather than expired) less than 180 days ago. You can change this period to match your corporate standards.

Minimum changes between reuse of same password

This applies to local accounts only - not windows domain accounts. By default, you cannot change your password to one that is the same as any of your previous four passwords. You can change this count to match your corporate standards.

Replay Authorization Process

If you enable this setting, you can force some or all users to request authorization before they are allowed to replay calls. See [Replay Authorization Process](#) on page 178 for a full description of this feature and its parameters.

Server Hardening

The approach to server hardening for ACR is similar for Linux and Windows and consists of:

- running with minimal account privileges
- removing and/or disabling unused software to reduce the attack surface
- (optionally) blocking access to unused IP networking ports

The following sections provide recommendations for Linux and Windows.

Linux

ACR runs as an unprivileged user. The start-up script runs as root, but launches the recorder application under the 'witness' user. Almost all maintenance (e.g. gathering log files, editing properties files, patching, etc.) of the recorder should be carried out logged on at the witness user. Root access should only be needed for:

- initial installation of the RPMs
- starting and stopping the service

Never log on as root unless needed. Do not install patches as root.

Tip:

To start the recorder when logged on as witness type:

```
su - -c "service cscm start"
```

and enter the root password. This correctly makes use of root privileges only on a per use basis.

You should disable or remove any services that are not used. The recommended starting point for this is a kickstart installation with the minimum package selection. Even this will install some RPM packages that are not needed and may increase the attack surface.

You may optionally enable the RedHat firewall. ACR requires several ports to be open to operate correctly. See [ACR Firewall ports](#) on page 213 for a table of ports that must be opened depending on your configuration.

Windows

You should consider using Windows Specialized Security - Limited Functionality (SSLF). This disables most optional services on the server. SSLF is typically used by organisations

Confidential and Proprietary Information

where security is more important than functionality. When using SSLF you should make an exception for Remote Desktop connectivity.

Use the group policy editor to design a template for your ACR servers based on the SSLF template. You will need to open ports in the Windows Firewall (See [ACR Firewall ports on page xxx] for a table of ports that must be opened depending on your configuration). Unfortunately the group policy editor does not allow for port ranges. You will probably find it necessary to "allow local port exceptions" in the group policy editor and then use the Windows Firewall configuration screen on each ACR to open the ports required for that server. (The local configuration screens allow for port ranges to be entered.)

ACR Firewall ports

You should ensure that a firewall is enabled and block all ports bar those below.

Port	Protocol	Use
8443	TCP	HTTPS admin access
123	UDP	NTP
1209	TCP	Inter-server TLS. Open on Master and Standby
10000-19999	UDP	RTP

Other ports are needed if your Avaya Contact Recorder is connected to other system components. These are described in [Summary](#) on page 270.

Single Login

When using local accounts, you can restrict users to a single session if required. To do this, add the following line to the Properties file as described in Properties File on p224.

```
acr.singlelogin=true
```

Confidential and Proprietary Information

Dual Sign-in

Security can be enhanced by forcing some (or even all) users to sign in with the aid of an additional user. This is sometimes known as a "four eyes" approach.

How it Works

This works by presenting users with a second log-in screen asking them to have an "authorizing user" enter their username and password to validate their attempt to log in. Only after the second set of credentials has been checked can the user access the application.

 **CAUTION:**

The secondary or "authorizing" user account must be a local (not Windows Domain) account and must have replaced their original (temporary) password with one of their own choosing before they can authorize others.

Applying this Mode

To require a user to have a second, authorizing user help to log them in:

Check the **Login must be authorized** role when entering a new user record or editing an existing one.

You must also then assign one or more user accounts as who can provide these secondary credentials. Do this by checking the **May Authorize logins** role when adding or editing a user's record.

Making this the Default

This "four eyes" approach can be made the default for new user accounts that are created. To do this, set the following entry in the properties file:

```
foureyes.default=true
```

Audit Trail

The normal audit entry that records a user login now also includes the name of the authorizing user. Audit records relating to subsequent actions of that user do not explicitly mention the other user.

Using this Mode

You can use this mode in two ways:

- a. If an authorizing user signs someone in and then leaves them alone, you have improved the security of login (access) but not restricted or deterred the user from accessing areas of the application and/or recordings that they do not need to see.
- b. If the authorizing user signs someone in and then observes their actions up to and including a deliberate "Log Out" you can deter users from doing or replaying more than their job requires them to do.

The second approach can be particularly effective with administrator accounts - as it is difficult to restrict their actions (someone has to be able to change things). As long as the observer is vigilant - ensuring, in particular, that the administrator has not removed the requirement for a second login on their own account - security can be significantly enhanced as a rogue individual can no longer do as they wish. This obviously makes option (a) inappropriate for administrator accounts

Changing Passwords

The recorder and related applications use a number of user account settings that are installed with a hard-coded default. You may change these as described below but be sure to note the new passwords securely as remote support staff will need these to maintain your system. Should you lose these passwords, your system will become completely unmaintainable.

User Accounts

Linux

The root and witness user accounts are installed with default passwords. Change these by logging on to the server and typing `passwd`.

Windows

The installation process creates a local user account for the postgres database service to use. This account does not have administrator privileges. By default, the account name is "postgres" and the installer chooses the password for you. You may change this password later but if you do, you must also configure the Postgresql Database service with the new password to allow it to run under this account.

Postgres Database Owner

You may wish to change the password used by the recorder to access its local postgres database. Before doing so, you must first enable 256 bit encryption as described in [Installing Unlimited Strength Encryption](#) on page 386 and obtain the Avaya encryption tool as described in [Encrypting Properties File entries](#) on page 392. You can then configure the recorder to use an alternative password as follows:

1. Choose a new password
2. Encrypt the new password using the WitsBSUserCredentials tool.
3. Add the new password (in encrypted form) to the `acr.properties` file as

```
db.password=encryptednewpassword
```

Then follow the appropriate procedure below to set that password within postgres before restarting the recorder to have the above setting take effect.

System Security

Linux

Follow the steps below:

1. Log in as root
2. Switch to the postgres user account by typing
`su - postgres`
3. Access the database by entering
`psql`
4. Change the password by entering
`alter user eware with encrypted password 'newpassword';`
5. Quit the database by entering
`\q`

Windows

Follow the steps below:

1. Log in as an Administrator.
2. Open a command window and "cd" to the \postgresql\bin directory beneath the recorder's install path.
3. Access the database as the recorder would by entering
`psql -U eware`
4. Enter the default password (must be obtained on request from Avaya at the time and not written down)
5. Change the password on the account that the recorder uses by entering
`alter user eware with encrypted password 'newpassword';`
6. Quit the database by entering
`\q`

Confidential and Proprietary Information

Encrypted File Storage

Recordings (WAV files) and their associated XML data files are not normally encrypted but can be - using the AES256 algorithm and RSA Security's Enterprise Key Manager. Encrypted files are also "fingerprinted" to avoid tampering.

See the manual *Avaya WFO Security Configuration Guide* for details of how to deploy an RSA Key Management Server (KMS). To then enable encryption on the recorder:

1. Install the Unlimited Strength policy files as described in [Installing Unlimited Strength Encryption](#) on page 386.
2. Create a KMS client certificate (a PKCS#12 file) for the recorder. This will be protected by a passphrase to preserve the confidentiality of the private key.
3. Install this certificate on the recorder by logging in as witness and copying the file to the `/keystore` directory beneath the recorder's install path (`/opt/witness` on Linux systems).
4. Back at the KMS, convert the client certificate into a PEM file. The PEM file must be imported into the KMS to identify the recorder as a valid client. To convert the PKCS#12 file to PEM format use the command:

```
openssl pkcs12 -in svr_cert_key.p12 -out svr_cert_key.pem
```

5. On the **General Setup > Recorder** page of the recorder, enter the IP address of the Key Management Server and the passphrase for the certificate. You must restart the recorder after making any changes to the KMS settings, certificate or passphrase.

Note:

You must also configure WFO (if used) with the same Key Management Server.

PCI Compliance

To make your system compliant with PCI recommendations, you should adopt *all* of the above features. In addition:

1. Do not store sensitive data in the User Defined Fields of recordings.
2. Use the PAUSE and RESUME recorder control features to avoid recording sensitive information. This will require integration with your other systems.
3. Increase the default 3 months for which audit records are kept to 13 months.
4. Use encrypted audio to and from your phone system (setting on **General Setup > Contact Center Interface** page).
5. Force users to use the Master, central replay server or WFO rather than replaying calls from each recorder server.
6. Ensure all other components of your system (e.g. WFO) are configured in accordance with the *Avaya WFO Security Administration Guide*.
7. PCI dictates a session timeout of 15 minutes. When using Windows Domain Authentication (as required to meet other PCI requirements) the recorder will accept a valid Windows logon (on an appropriate account) as sufficient to gain access to the recorder's administration pages. You should therefore ensure that all users' PCs are configured to launch a screen saver after 15 minutes of idle time and have Password Protection on Resume enabled. To ensure this, domain administrators should lock down these settings in the group policies of the domain controller.
8. Review and adjust your Windows Domain policies for user accounts if required. For instance, the PCI specification mandates the following rules:
 - Immediately revoke access for terminated users.
 - Remove inactive user accounts every 90 days.
 - Do not use group, shared or generic accounts and passwords.
 - Change user passwords at least every 90 days.
 - Passwords should be at least 7 characters long and should include both numeric and alphabetic characters.
 - Do not allow individuals to submit a new password that is the same as any of the last 6 they have used.
 - Lock out the user account after not more than six unsuccessful access attempts (have a lockout duration of 30 minutes or until admin enables the account).
9. To ensure no recorded data is stored anywhere in an unencrypted format, including on the supervisor's PCs, Internet Explorer's Advanced Security **Do not save encrypted pages to disk** and **Empty Temporary Internet Files folder when browser is closed**

Confidential and Proprietary Information

settings on the supervisors' PC must be enabled and locked down. (**Internet Options > Advanced > Security**).

10. To ensure proper authentication when SSL is enabled in a recording system, the following advanced Internet Explorer security settings on Supervisor PCs must be enabled
 - Check for the publisher's certificate revocation.
 - Check for server certificate revocation.
 - Warn about invalid site certificates.
 - Use SSL 2.0.
 - Use SSL 3.0.
 - Use TLS 1.0

Confidential and Proprietary Information



Chapter 7: Advanced Configuration

This chapter provides an overview of the more complex and rarely used options for an Avaya Contact Recorder system.

The main sections in this chapter are:

- [Properties File](#) on page 224
- [Slave Server](#) on page 233
- [Standby Server](#) on page 234
- [Central Replay Server](#) on page 235
- [Customizing Search and Replay with Layout Builder](#) on page 237
- [Usage Report](#) on page 243
- [Selective Record Barring](#) on page 245
- [Contact Recording Desktop \(CRD\)](#) on page 246
- [Altering Translations](#) on page 257
- [Migrating from Central Archive Manager \(CAM\)](#) on page 258

Properties File

A number of system settings can be changed from their default values by placing entries in the properties file as described below:

- This is a plain text file, located in the installation path (which is /opt/witness on Linux) and with filename: `/properties/acr.properties`
- You should edit this file using notepad on Windows servers or, on Linux, using the "vi" text editor. On Linux you MUST be logged on as witness - NOT root.
- The Avaya Contact Recorder service reads this file as it starts, so any changes made to the file will not take effect until you next restart the service. Some properties are cached at startup but others are consulted as required. These can be changed temporarily at run time using the Maintenance page (`/servlet/acr?cmd=mtce`). You should only use this option under the direct guidance of Avaya support staff.
- The file is normally empty as all settings default as shown in the table below.

Most of these entries are discussed elsewhere in this manual, in the appropriate context. The table below provides a summary of the available settings.

Entry (case sensitive)	Default	Meaning
acr.disablecompress	false	Normally, recordings made in G.711 will be compressed to G.729 8kbps. Set this to true to disable compression.
acr.diskmanager	true	Whether to delete oldest calls when needed to create space for new recordings.
acr.localport	8080	The http port used by the recorder. Must match the entry in server.xml.
acr.logkeepdays	30	Number of days log files to retain before purging.
activitycode.fieldname	activitycode	(CS1000 only) The name of the user defined field to store (last) activity code in. Set blank to disable storage of activity code.
audioserver.inactivitytimeout	30	The number of seconds of inactivity before an audioserver port is released back to the pool of available ports.

Confidential and Proprietary Information

Entry (case sensitive)	Default	Meaning
audioserver.viewerbase64	not disclosed	Use this setting to specify the base64 encoded name that should be included in requests to Audio Server. You only need to set this if you have changed Audio Server from its default.
audit.purgemonths	3	The number of months to keep audit trail entries in the database.
call.tracing	false	Set true to provide additional tracing of call and connection states.
cc.v6	false	A number of changes have been made in the way the recorder interacts with the Avaya CCMS. The recorder assumes that you will be running it against CC 7.0 or higher AND CS1000 release 6 or higher. If your call center is earlier than release 7.0, or your switch release is earlier than CS1000 release 6.0, you must set cc.v6=true until you upgrade to both CC 7.0 AND CS1000 6.0.
conferenced.ignore	null	Set to one or more ranges of phones that should be ignored if present on calls. Use this to stop the recorder interpreting other recorders' softphones as additional parties on the call.
controllerlistener.localport	8232	TCP Port number the master listens on for connections from Contact Recording Desktop applications.
cs1k.showacddn	false	Set to true to stop the ACDDN to which an agent logs on showing alongside the agent's identifier.
cti.logfile	NULL	The filename (within the /logs folder) to read CS1000 CTI input from or write it to
cti.mssettling	250	How many milliseconds to wait after a CTI event before considering recording actions. Allows transient intermediate states to be ignored.
cti.offline	false	If true, read MLS or ICM input from the file specified in cti.logfile. Otherwise connect to live CTI feed(s).
db.password	Not disclosed	Encrypted password for recorder's normal postgres user account

Advanced Configuration

Entry (case sensitive)	Default	Meaning
<i>dddddd.field.ffff</i>	NULL	For dialer named <i>dddddd</i> , store field <i>ffff</i> as User Defined field specified.
disk.stopatMB	10	Stop writing to disk if free space is less than this many MB
disk.warnAtMB	500	Raise warning if free disk space falls below this many MB
diskmanager.mingb	1	The number of GB that diskmanager will attempt to keep free on the calls partition.
dmcc.port	4722	The port number on the AES for DMCC.
dmcc.secure	true	Whether to connect to DMCC using SSL.
dmcc.tracing	false	Set true to provide additional tracing of DMCC interactions.
dmcc.trustall	false	Allows different SSL certificates to be installed on the AES.
dn.regpersec	10	How many DNs/Position IDs to attempt to Associate per second on MLS or ICM links. Increasing this number speeds up initial startup but will impact the switch more during this period.
dtls.nonstandard	3	Change to 2 to use recorder with CS1K phones using Unistim 5.3 firmware or later.
email.minalarmlevel	0	Alarm level at or above which, emails will be sent . Default, 0 is INFO level. Set to 1, 2 or 3 to restrict emails to Warnings, Minor and Major Alarms respectively.
execmode.deletedelaymins	0	Minutes to wait after a recording ends for a "retain" command before deleting a call on a DN or Position ID requiring manual retention.
execmode.deletedelaysecs	0	Number of seconds to wait before deleting recordings.
execmode.retainnumber	no default value	The station number of the recorder port to be used as the "Retain" port.

Confidential and Proprietary Information

Entry (case sensitive)	Default	Meaning
farendcapacity. <i>nnnnnn</i>	1000	(where <i>nnnnnn</i> is the serial number of an ACR server). Sets the maximum concurrent recording capacity of the server.
farendscale. <i>nnnnnn</i>	1	(where <i>nnnnnn</i> is the serial number of an ACR server). Sets the load impact of an active channel e.g. setting to 2 makes this server appear to be twice as busy per active channel.
https.socket	8443	socket to use for https access. Must match that defined in server.xml
krb5.domain	No default value	The Active Directory Domain Name
krb5.enabled	False	Enables Kerberos Single Sign on
krb5.exact	False	If false, change incoming Windows domain/usernames to uppercase and compare with the configured user accounts. If true, require a case sensitive match between the received domain/username and a configured user account.
krb5.kdc	No default value	The address of the Active Directory
krb5.password	No default value	The encrypted password for the recorder account in Active Directory
krb5.tracing	false	Enables additional output to the log file
krb5.username	No default value	The username assigned to the recorder in Active Directory
log.annotate	false	Set true to have each administration web page display an annotation field and buttons allowing the user to submit entries for insertion into the log file(s) from their browser.
loop.ignore.nn	false	Ignore calls on CS1000 loop number nn (1-255). Add one entry for each loop that is not recorded on a partially equipped trunk-side recording system. Otherwise alarms will be generated as the recorder attempts to record calls on these loops.

Advanced Configuration

Entry (case sensitive)	Default	Meaning
meeting.defaultrecord	true	Whether or not Meeting recording ports will start recording automatically at the start of a call or wait for a START command from an external controller.
meeting.ocpneeded	true	Whether or not Meeting recordings should detect other call parties using the conference display feature. Set false if an external controller is to provide this information instead.
mls.acceptabledelay	200	Report warning if MLS response takes longer than this (in milliseconds)
mls.pollinginterval	20	Time (in seconds) between poll messages with MLS.
ocp.alwaysrefresh	false	In recording modes where the conference display button is used to determine who is on the call, this process will be restarted if the display indicates that a party has joined the call. In some cases, however, an existing party may be updated e.g. a trunk name/number may be replaced by a (late arriving) ANI. Set this property true to have ANY change to the display trigger a refresh of all parties on the call.
ocp.strictparsing	false	When forwarding via coverage answer groups, the conference display may not contain a single numeric field in the end of the display. Previously this would lead to the recorder continually pressed the Conf Disp button - resulting in the party being removed from the call. Now default is not to check for spaces or valid number in this string. To restore previous behaviour if this causes problems, set this property = true.
oemcomms.connecttimeout	120	Seconds a recorder will wait on startup before reporting that a previously connected recorder has failed to connect.
oemcomms.inactivitytimeout	60	Seconds the Master will wait between polling messages before reporting another server as having failed.
oemcomms.tracing	false	Enable tracing of messages between recorders

Confidential and Proprietary Information

Entry (case sensitive)	Default	Meaning
ondemand.defaultrecord	true	Whether or not On Demand recording ports will start recording automatically at the start of a call or wait for a START command from an external controller.
ondemand.ocpblocked	false	If enabled, prevents OCP with On Demand recording.
ondemand.ocpneeded	true	Whether or not On Demand recordings should detect other call parties using the conference display feature. Set false if an external controller is to provide this information instead.
postgres.password	not disclosed	Encrypted password to use for database vacuum.
purge.hourofday	1	Hour at which database and log file purges will take place. Default is 1am. Valid range 0 - 23
queue.xxx.threads	1	Number of threads to use for job queue xxx.
rec.maskallowed	false	You must set this to true to enable the "pause/resume" features of the Recorder Control Protocol.
rec.mincallduration	250	Calls shorter than this many milliseconds are deleted. In hybrid AACC systems, set this to 1000 to avoid short recordings that can result from the difference in arrival times of CTI events over the two CTI feeds being used. Deleting such sub-second recordings avoids confusion when searching and playing recordings.
record.persistmode	device	Use this setting to choose between "call", "device" and "segment" persistence of recording commands. See Persistence of Commands on page 247 for further details.
recorder.pool	NULL	Use this to have this recorder form part of a "named pool" of recorders - which will load share and/or provide fault tolerance. Set this property to a short string that is the same on all recorders in this "pool". Once set, you can specify this name in the "Designated Recorder/Pool(s)" Advanced setting.

Confidential and Proprietary Information

Advanced Configuration

Entry (case sensitive)	Default	Meaning
rtp.highport	20000	Upper limit on ports user for SIP and Duplicate Media Stream IP recording. Ports up to but not including this port will be used. Note: each recording uses up to FOUR ports.
rtp.lowport	12000	Lowest port number used for SIP and Duplicate Media Stream IP recording. Note each recording uses up to FOUR ports.
rtp.packetlog	false	If true, log details of every RTP packet received
rtplegacy.highport	12000	Highest port number used for On Demand, Meeting and Phone Replay ports.
rtplegacy.lowport	10000	Lowest port number used for On Demand, Meeting and Phone Replay ports.
screen.ieport	29522	The port number on which the recorder listens for connections from agent desktop screen capture client connections.
sip.tracing	false	Set true to provide additional tracing of SIP interactions.
smtp.port	25	The port used for emailing
snmp.authtype	SHA	Set to "MD5" to override the default SHA authorization type with MD5.
snmp.mainusername	acrsnmpuser	The main username the Network Management System will use to connect to the recorder.
snmp.password.nn	no default value	Encrypted password to be used in conjunction with the corresponding snmp.username.nn entry. This requires the java unlimited strength patch as described in Installing Unlimited Strength Encryption on page 386
snmp.port	2161	The port number to use for SNMP

Confidential and Proprietary Information

Entry (case sensitive)	Default	Meaning
snmp.privtype	AES128	Set to "DES", "3DES" or "AES256" to change the privacy type from AES128. Note that AES256 requires the java unlimited strength patch as described in Installing Unlimited Strength Encryption on page 386.
snmp.username. <i>nn</i>	no default value	Additional usernames can be entered. Replace <i>nn</i> with 1, 2, 3 etc.
standby.localconfig	false	Whether the standby is locally configured. If not, it copies config from the Master.
standby.stayactive	true	See Standby Recorder Options on page 346.
system.forcertl	false	Set true to have number ranges in audit entries and other database entries use right-to-left order (e.g. 200-100 instead of 100-200)
trunkgroup.ignore. <i>nnn</i> (Communication Manager only)	false	Set to "true" to suppress warnings about not being able to record calls on trunk group <i>nnn</i> . Add one entry for each trunkgroup that is not recorded on a partially equipped trunk-side recording system.
tsapi.retries	300	Number of times to keep trying to establish single-step conference.
tsapi.retrydelayms	1000	Interval in milliseconds between single-step conference attempts.
tsapi.timeout	65	How long (in seconds) the recorder will tolerate TSAPI failure to respond to heartbeats.
tsapi.tracing	false	Set true to provide additional tracing of TSAPI interactions.
unify.required	false	Whether a link to Unify is required for the recorder to be viable.
unify.xmlonstart	true	Set to false to restore behavior of STARTED message to that of 10.0 and earlier (where XML is not sent in the STARTED message but, rather, in an UPDATE message immediately after the STARTED).

Advanced Configuration

Entry (case sensitive)	Default	Meaning
usage.reporting	false	Whether to track actual usage to the ConfigHistory table and show the Usage report
uui.fieldname	no default value	User defined field name to store Avaya User to User data. If NULL, this data is not stored. Applies to Conferenced mode recording only.
vacuum.interval	180	Number of days between full database vacuums.
viewerx.limit	100	Maximum number of recordings returned for each search
viewerx.oldexport	false	Set to true to have bulk export use csv file output rather than the new html embedded player.
viewerx.savesettings	false	Whether to save and reuse users' previous entries in search filter pane.
activitycode.fieldname	activitycode	The name of the user defined field to store (last) activity code in. Set blank to disable storage of activity code.
<i>dddddd.field.ffff</i>	NULL	For dialer named <i>dddddd</i> , store field <i>ffff</i> as User Defined field specified.
viewerx.secure	false	Set to true for enhanced security features at the expense of usability.

Confidential and Proprietary Information

Slave Server

Installation

(IP) Slave servers are installed in the same way as a standalone recorder (see [Installing Avaya Contact Recorder](#) on page 110).

Licensing

Instead of entering a license key, follow the instructions on the lower half of the license entry page. Allocate the recorder a unique number (2 to 9999) and specify the IP address of the Master to which it is to connect.

If you also have a standby recorder, add its address too - separated from that of the master by a semi-colon. The slave will then connect to both.

Restart the Avaya Contact Recorder service.

Configuration

Work through Chapter 4: [Configuration](#) on page 119 configuring just those fields with **Edit** links next to them. Then configure the user accounts and replay rights for those entitled to use this server directly. In most cases, replay will be via a central replay server rather than directly from the slave server so you need only configure administrators' accounts.

 **Important:**

Note that a slave on a remote site may be better configured as a Standby server so that it can attempt to record calls locally should connection to the central master and standby be lost.

Standby Server

First, determine the number and type of standby servers required using the Topology tables in [Standby Recorder Options](#) on page 346.

Standby servers are installed in the same way as a standalone recorder (see [Installing Avaya Contact Recorder](#) on page 110 - steps 1-7). Instead of entering a license key, follow the instructions on the lower half of the license entry page. Allocate the recorder a unique number (2 to 9999) and specify the IP address of the Master to which it is to connect.

Follow the configuration guidance given in the appropriate table:

- Where a Standby is to copy the configuration of the Master recorder (the default) then you need to configure very few other details. In particular, all user account details are copied from the master. You are only able to edit these on the standby when it is active - and even then, you should only do so when really necessary as any changes you make on the standby will be overwritten when the master takes over again. Work through the Configuration chapter of this manual configuring just those fields with **Edit** links next to them.
- Where specific standby recorders need to be specified, ensure you have set the **Designated Recorder/Pool(s)** for each set of recording targets on the **Operations > Bulk Recording** page.
- Where a standby recorder is to be locally configured,
 1. Add the following line to the properties file (See [Properties File](#) on page 224 for detailed instructions)

```
standby.localconfig=true
```
 2. Restart the Avaya Contact Recorder service
 3. Configure all settings as you would on a standalone recorder.

Confidential and Proprietary Information

Central Replay Server

You can deploy the recorder application onto an additional server which collects details of recordings made on one or more other servers and therefore can act as a dedicated search and replay server. Users can then search for recordings from any of the recorders feeding it with a single url and a single search.

Installation

Install a Central Replay server in the same way as the Master recorder (see [Installing Avaya Contact Recorder](#) on page 110 - steps 1-7).

Configuration

Work through [Chapter 4: Configuration](#) configuring just those fields with **Edit** links next to them. Then configure the user accounts and replay rights for those entitled to use the application.

Telephone Replay (Communication Manager only)

You can also configure ports for telephone replay. As this is the only possible use for ports on a Central Replay Server, simply configure the softphones on the **General Setup > Contact Center Interface** Interface tab. All softphones placed there will automatically be used for telephone Replay.

Configuring other Recorders

On each of the other IP recorders (master, standby and slaves) enter this replay server's IP address including port number (e.g. **myreplayserver:8080**) as the **Replay Server(s)** on the **General Setup > Recorder** page. This will override their default configuration (which is to use Master and Standby as central replay servers).

Installing Multiple Central Replay Servers

Each recorder may upload recordings to more than one central replay server (in fact, in a master + standby configuration, this is the default). This can be used to create a regional and global hierarchy and/or to provide fault tolerant search and replay.

To configure this, set up each central replay server as above and then add both addresses - separated by a semi-colon (;) - to the **Replay server(s)** setting on the **General Setup > Recorder** page.

Confidential and Proprietary Information

Customizing Search and Replay with Layout Builder

The Replay page in Avaya Contact Recorder provides users with features to search through all the recordings made by the recorder (or recorders in a multi-recorder system). Replay users are able to find the recordings that they are interested in playing by filtering the selection of recordings based on criteria like date and time, length of recording, skill groups, phone numbers, agent names, etc.

The formatting (or *layout*) of the Replay page is normally fixed by ACR. This means that the selection criteria, the order of the display columns, the labels used to describe filters, etc. are pre-determined. The panel at the left of the replay screen is a list of *filters* that select a subset of the available recordings based on the selection criteria. The results are shown in tabular form in the right panel. The *columns* of the table show a subset of the full information available about each recording, some of which is grouped for ease of display. For example, the 'agents' column shows Communication Manager agents, Proactive Contact agents and Proactive Outreach Manager agents all merged into one column.

"Layout Builder" provides a mechanism to create multiple layouts each customized for a particular purpose. Some typical uses for customized layouts are:

- Changing the names of columns or filters (e.g. 'associates' instead of 'agents')
- Changing the order of columns or filters
- Pre-setting (and, optionally, locking) one or more filters to specific values (e.g. duration longer than 30 seconds)
- Hiding certain columns, which may contain confidential or irrelevant information
- Adding columns to display information that is not normally of interest (e.g. a customer-specific user-defined field)

Each replay user can be restricted to seeing just a subset of customized layouts. This means, for example, that managers may be given access to a layout showing certain confidential information, while other users may only be able to see a layout that has been customized to hide that confidential information.

Only users with full **System Administrator** role may use the Layout Builder and assign layouts to users.

Layouts

Each layout consists of these elements:

- An internal name, which allows administrators to differentiate between layouts. (The default layout that is provided with the system is called 'Avaya'.)
- A set of filters that select from the database just those recordings that match the filter. (By default, each filter selects all recordings, but replay users may use them to select just a subset.) Some filters may be hidden from users.

Confidential and Proprietary Information

Advanced Configuration

- A set of columns that define which information from each recording is displayed in the results table and how that information is grouped and ordered. Some columns may be hidden from users.
- Internationalized names (in whichever languages you actively use) for the layout itself, each filter and each column.
- A setting that controls whether the layout is hidden from all users (typically used during construction or if a layout is no longer in use).
- A setting that controls whether, by default, all replay users are automatically given access to the layout.

Administrators can use Layout Builder to change each of the elements of a layout, as well as creating new layouts and deleting layouts.

Note:

Only the two control settings may be changed in the system-provided layout. The internal name, filters, columns and internationalized text are fixed. If you want to change the system-provided layout you should copy it, change the copy, make the copy visible and available and then hide the system-provided layout.

Using Layout Builder

Note:

Layout Builder is designed for use in 'standards' mode of Internet Explorer 8 and 9 only. Make sure IE is not set in 'compatibility' mode.

On the **System > Manage Users** page, click the **Edit Layouts** button. Layout Builder launches in a new window.

Title Bar

The title bar shows a list of the layouts defined in the system. On a new install this is just the system-provided 'Avaya' layout. Use the drop-down list to select a layout to work on.

Save

When you have made changes to a layout, you must click save to commit the changes. If you try to move away from a layout that you have changed without saving you will be asked if you wish to discard those changes.

Copy

Click copy to make a new layout. The new layout is a copy of the currently selected layout, except that the internal name is changed to 'New Layout'. You should change the internal name to something meaningful to you before saving.

Confidential and Proprietary Information

Delete

Click delete to delete the currently selected layout. You may not delete the system-provided layout; if you do not want users to see it, you may simply hide it.

Close

Click close or close the popup window when you have finished using Layout Builder.

Left and Top Panels

The top and left panels show the columns and filters respectively. They are shown in the order that they are displayed in the Replay page.

Note:

Filters and columns are always paired, because, in the majority of cases, if you want to see a column with a certain piece of data you may want to filter that data, and vice versa. This pair is called a field. There will be times when you do not want to see one or other of the filter and the column (see examples below). In this case you can disable the filter or the column so that it will not be shown.

To change the order of the filters, drag the filters in the left panel into the correct order. To change the order of the columns, drag the columns in the top panel into the correct order.

Disabled filters and columns are shown faded. Disabled filters and columns are always shown at the end. To disable a filter or column clear the check box. To enable it, set the checkbox.

To change the settings of a field (filter-column pair) click the pencil in either the filter or column. This shows the field editor.

Field Editor

Clicking the pencil of either the filter or column of a field brings up the field editor for that field.

First Row

Use the drop list in the first row to select the field type. Refer to [Search and Replay Attributes](#) on page 278 for a full description of each field type. If the field type you select requires a parameter (e.g. UDF), enter it in the second box on the first row.

Second Row

Use the second row to set defaults for the filter, if required.

If you wish to default the search criterion of the filter, set the first drop list to:

Advanced Configuration

- **Normal** - sets the default search criterion, but allows the Replay user to change it
- **Fixed** - sets the default search criterion, but does not allow the Replay user to change it
- **Hidden** - same as fixed, but does not even show the filter in the Replay page

Select the search operator in the second drop list.

Enter the search criterion in the third box.

Examples

Normal < 5 - searches for recordings where this field is less than 5, but lets the user change both "less than" and "5" to other values

Fixed Contains 12345 - searches for recordings where this field contains 12345, and does not let the user change this selection

Internationalization Rows

Enter the display name of the filter in the left box and the display name of the column in the right box. Fill these in for your own language (highlighted in yellow) together with any other languages used by your replay users. Often the display names of the filter and the column are the same. However, since space is typically limited in the column display, it often makes sense to make this display name shorter.

Buttons

Save - saves your changes

Cancel - abandons your changes

Delete - removes the field (both filter and column) altogether

Middle Panel

Use the middle panel to:

- **Change the internal name of the layout.** You should make sure that all internal names are unique so that you can differentiate between layouts as you edit them.
- **Hide a layout.** Replay users will not see this layout, even if they are given rights to access it. This is useful while you are building and testing a layout.
- **Make a layout available by default.** If the layout is not hidden, all users will be able to see and use the layout without you having to assign them rights to it individually.
- **Create a new field.** As noted above, a field is a filter-column pair. The new field is added to both the filter panel and the column panel. After you create a new field, you should set its type and give it a name by clicking the pencil in either the filter or column panel.

Confidential and Proprietary Information

Right Panel

The right panel shows the internationalized name for the layout that users of each language will see. You should fill in the name for your own language (highlighted in yellow) together with any other languages used by your replay users. Unlike the internal name, there is no particular requirement for these names to be unique.

Examples

Removing Irrelevant Information

If your call center does not use agents, you will notice that the system-provided layout always contains a blank column. You could save that space by deleting the **Agents** field.

Copy the **Avaya** layout, rename it, click the pencil on the **Agent** filter or column, click delete. Uncheck the **hidden** box so your Replay users will see your new layout. Finally **Save** the layout. Select the **Avaya** layout, check the **hidden** box and **Save** that too.

You have created a new layout without Agents, made it visible and hidden the system-provided layout. Your users will now just see your new layout.

Changing Display Names

You may prefer to refer to your Agents as "Associates". To change the display name follow the instructions for removing irrelevant information, but do not delete the **Agent** field. Instead, in the **Field Editor**, change the two yellow highlighted names from **Agent** to **Associate**. Continue with the instructions above.

Fixing a search criterion

You may want to create a layout that only ever displays recordings that were tagged with a particular Vector Directory Number (VDN). This could be as a convenience to Replay users who make this search frequently (saving them from filtering Service Starts With xxxxx), or it could be a security measure to ensure that a particular set of users may only see recordings tagged with VDN xxxxx.

Create a new layout and name it. Choose a name that reflects that this layout only ever selects recordings tagged with VDN xxxxx. Edit the **Service** field. On the second row select: **Fixed, Starts with** and enter the VDN number. (If you don't want your users to see that the VDN in question is xxxxx, changed **fixed** to **hidden**.)

Since the column called **Service** will now always contain the value xxxxx it becomes largely irrelevant. Disable the column by clicking off the checkbox on the column called **Service**. It will be greyed out, and move to the end of the list of columns.

Displaying a User Defined Field

If you have an external integration you may be tagging your recordings with User Defined information. For example you may be tagging recordings with a customer id (as UDF 'custnum').

Create a new layout by copying the system-provided default.

Click the **Add Field** button to create a new field. Click the pencil on the newly added field to edit that field. In the first row, change the **Field Type** to **User Defined Field** and enter `custnum` to the right.

Fill in the relevant language translations (particularly the yellow highlighted ones). You might choose "Cust ID" for the column (where space is tight) and "Customer ID" for the filter.

If you want to display the UDF, but not allow Replay users to search by it, click the check box off on the Customer ID filter.

Usage Report

The recorder is occasionally sold to service providers with a "per use" license. Charges are levied based on the actual usage made of a recorder each month. This report can be enabled in such cases to provide the necessary billing information.

Enabling the Report

To enable this feature, you must add the following line to the properties file:

```
usage.reporting=true
```

Content

The Usage Report page shows a summary of the licenses that have been used over a specific period. The default reporting period is the previous calendar month.

To generate a report for a different period, enter the date range in the calendar controls, and click **Refresh**.

The report shows

- The maximum number of concurrent recordings
- The maximum number of telephone replay ports (if any) configured at any time during the reporting period.

Configuration records are retained for 3 months by default. Each night after that period has elapsed, a background job deletes any records older than this.

Accessing through URL:

This report can be accessed directly, without having to use the normal system administration pages.

To access the report by way of its URL, enter the following line in the navigation bar of your browser:

```
http://myservername:8080/servlet/report?from=t1&to=t2
```

Where $t1$ is the start time in UTC seconds and $t2$ is the end time in UTC seconds.

Note:

These times are in seconds not milliseconds and do not attempt to correct for leap-seconds. Unless an administrator made configuration changes within a few seconds of midnight, this will not affect reporting on monthly boundaries.

The names of recording modes and other information that can be localized are returned according to the language preferences established for the interface. If localized terms are not available, the returned values are in English.

Accessing the Usage report in a log file

If you request the usage report by way of its URL and the request is successful, the recorder writes the usage data to a log file called `usage.log` in the `/logs` directory beneath the install path (which is typically `/opt/witness` on Linux and `D:\Program Files\Avaya>ContactRecorder` on Windows).

You can access and view this log file in any text viewer. Its content is the same as the report returned for the URL request. Each time you request a usage report, a new log is created that overwrites the previous one.

If a request for the Usage report is not successful, no log file is written for it. You should examine the return value of the URL request for an indication of the error conditions (bad time parameters, configuration has been tampered with).

Selective Record Barring

Recent legislation changes mean that some customers may need to block recording of calls to or from specific area codes (e.g. California).

Configuration

It is possible to bar recording of calls to or from certain numbers. To configure such a “recording bar”, add the property file entry:

```
recording.barred=<regular expression>
```

Where <regular expression> is a regular expression that will match the digit strings to be barred from recording.

Tip:

See <http://java.sun.com/docs/books/tutorial/essential/regex/index.html> for instructions on how to form a regular expression.

Example

The following example shows how to bar calls to or from area codes 234, 567 and 890 – where the recorder is situated in area code 234 (which therefore does not have a 1 in front of it, unlike the others which may or may not). The trailing periods (there are seven of them) are important – as this forces the pattern to match only numbers with 7 digits following the area code.

```
recording.barred=((234)|(1?567)|(1?890)).....
```

Any recording that is barred due to matching the digit pattern specified will cause an INFO level message to appear in the log file.

Limitations

1. This feature does not apply to On Demand or Meeting Modes.
2. To bar incoming only or outgoing only, first determine the digit patterns that are used. You may be able to change the outbound dial plan to always prefix with a '1'. The "1?" matches calls with or without a preceding '1'. Remove the '?' to require a '1' before the pattern is matched.

Contact Recording Desktop (CRD)

This optional application is currently supported on CS1000 systems only.

Overview

Step by step installation instructions for this component are provided in [Installing Avaya Contact Recording Desktop \(CRD\)](#) on page 113.

This section provides a more detailed review of the capabilities and features of this component.

The Contact Recording Desktop (CRD) application is a simple application that normally resides as an icon in the tool tray of agents' desktop PCs. You determine which of the following features are available to each user by editing an XML file as described later in this Section.

- Start recording button
- Stop recording button
- Submit/Update button to "tag" call with details the user has entered into the customizable fields shown to him on the form. These can be text fields, selection lists or checkboxes.
- Delete recording button (IP recording only)
- Retain recording button (IP recording only)

The application can be configured to start when a user logs on to the PC. Each application that runs is associated with a single DN or Position ID using one of the following mechanisms:

- The user may log on by entering their AgentID
- The user may log on by entering the Position ID or DN that they wish to control

Note:

Recording Position ID and DN at the same time is not supported.

- The user's Windows account name can be entered in a central configuration file and matched to a particular agent ID.
- The PC name can be entered in the central configuration file and automatically matched to a DN or Position ID

Confidential and Proprietary Information

Status

The current status of the application and the DN or Position ID it controls is shown as follows:

- The left-hand status panel at the bottom of the main window shows whether or not the application is connected to the Avaya Contact Recording Master
- The third status panel shows whether or not the call is recording and provides feedback when commands have been issued to show whether or not they were successful.
- The right-hand status panel shows the DN or Position ID that the application is controlling.
- The icon in the tool tray also changes to show the current status of the application and the call in progress. Hold your mouse cursor over it to see the pop-up text that explains the current status.

The buttons and menu options will be enabled or disabled according to both the configuration file and the current state of the call in progress.

When the application is running and connected to the recorder, the context menu can be configured to show/hide the options available.

The application running in the tool tray lets the user control recording and tag recordings according to a configuration file that is set on the Avaya Contact Recording Master recorder. This determines which controls and fields are available to the user.

Persistence of Commands

When a user issues a command such as "start", "stop", "delete" or "retain" it is important that the user knows whether this relates to:

1. his interaction with this call ever - regardless of whether it is transferred to someone else and then back to him or not.
2. his interaction with this call until he disconnects from it - regardless of how many times he puts it on hold while doing something else
3. his interaction with this call now - and no longer applies if he puts it on hold and retrieves it again. (This latter mode allows him to deliberately return to the default behavior for the call.)

Use the properties file setting `record.persistmode=xxx` to choose between the three ("call", "device" and "segment" for (1),(2) and (3) respectively above). The default is "device".

CAUTION:

If using "call" persistence mode, it is the callid that is used to tie commands to calls. If callids wrap on your switch in less than 3 hours, you should adjust this setting on the **General Setup > Contact Center Interface** page to a value that is lower than the fastest time in which callids are reused. This will, however, limit the maximum duration over which commands can act.

Desktop Layout XML File on Avaya Contact Recorder Master/Standby

The configuration of the CRD is primarily controlled by an XML file in the \properties\desktops folder in the installation path on the master Avaya Contact Recorder. This determines what options are available to the user and how the user-defined fields are presented to them. A default file, dcs.xml, is provided.

You may change this to have all users configured the same way or you can create different XML files and use the Advanced settings for a particular DN or Position ID range to have those addresses use a particular XML file.

Any changes you make to the XML file will be picked up the next time the user logs in to CRD.

Operations › Bulk Recording

The desktop configuration file(s) determine which options show on the application but you must also configure the **Operations › Bulk Recording** mode to allow the users to perform the operations that you enable. This is necessary because such operations may also be performed directly from the phone rather than solely via the CRD application. As with the XML file, you can specify an overall set of rules (at the top of the **Operations › Bulk Recording** page) and then override this for specific DNs or Position ID ranges using their Advanced settings.

Client PCs

Either immediately after installation or ideally as part of the installation process, each client PC must be configured with the IP address of the master Avaya Contact Recorder (and any standby) that it is to use. These settings - and others (which you may wish to provide initial values for so as to avoid an inconsistent first logon) are held in the Windows Registry as follows under HKEY_LOCALMACHINE\Software\Avaya>ContactRecordingDesktop

Confidential and Proprietary Information

Registry Keys	Type	Default Value	Comment
ServerAddress	String	127.0.0.1	IP address of master Avaya Contact Recorder to connect to.
ServerPort	String	8232	IP port on master Avaya Contact Recorder to connect to.
BackupServerAddress	String		IP address of standby Avaya Contact Recorder to connect to.
BackupServerPort	String	8232	IP port on standby Avaya Contact Recorder to connect to.
LogonBypass	String	true	Whether or not to bypass the login dialog on startup. Will automatically be set to match XML configuration file after first login. ("true" or "false")
RecordingMode	String		Whether to ask for Extension or AgentID on login. Will automatically be set to match XML configuration file after first login. ("true" or "false")
HeartbeatEnable	String	True	Whether or not to send heartbeats to the server.
Extension	String	Last extension this user logged in as	Only used if logonmode= "agent" in XML file

Command Line Options

As an alternative to setting the registry entries, you can specify the following options from the command line that runs the application. These are more often used for diagnosing problems e.g. running as if located somewhere else or under a different user account

Advanced Configuration

Command	Explanation
-a	Log in with an agentID rather than extension number.
-a <nnnnnn>	Log in as agent ID nnnnnn.
-x	Log in with an extension number rather than an agentID.
-x <nnnnnn>	Log in as extension nnnnnn.
-i <ipaddress>	Use the NIC with this IP address to connect to the server.
-u <ipaddress>	Connect to server at IP address ipaddress.
-p <port>	Connect to server using port specified.
-h <hostname>	Login as running on host name specified.
-w <account>	Login as running under windows account specified.
-l d	Login bypass disabled.
-l e	Login bypass enabled.
-h e	Heartbeat enabled.
-h d	Heartbeat disabled.
-e e	Login using extension rather than agent number.
-e d	Login using agent number rather than extension.

Delayed Delete/Retain

By default, the recorder decides whether to delete or retain a recording segment 10s after the segment is completed e.g. when the Hold key is pressed or when the call terminates. If you wish to delay this decision so that users can click the "Retain" button on their CRD application after the call has completed, you must set the properties file entry "record.deletedelaysecs". The decision to delete a recording segment is then delayed by however many seconds is specified.

Note that a recording that has been "retained" after the above period can still be deleted at any time up to the call id wrap time. After this time a callid may have been reused and hence it is not safe to perform a deletion using the callid alone to identify the recordings associated with a particular call. The default period in which call ids are assumed to be unique is 3 hours but if your switch is busy, call ids may be reused more frequently than this. Use the setting on the **General Setup > Contact Center Interface** page to reduce this time period. You should set it to less than the time in which call ids are reused but longer than the longest call that you need to tag, delete or retain. Note that delete and retain commands use the "owner" field of a recording. A delete command issued by a desktop application will delete the previous recording "owned" by that DN/PositionID. If you

Confidential and Proprietary Information

override the owner field with the advanced settings, the delete and retain functions will effectively be disabled.

Fault Tolerant Configurations

When using a Standby recorder:

- Set its address in the Configure dialog.
- Copy the configuration files from your \properties\desktops folder to the standby any time you change them on the master.

XML Configuration File Format

The default file provided (dcs.xml) shows all possible options for user defined field entry.

CAUTION:

dcs.xml must not be modified. It is overwritten during upgrades. Copy the file and make your changes in files with different filenames (of your choice).

This default is shown below:

```
<?xml version="1.0" encoding="UTF-8"?>
<desktop>
  <logon mode="extension" bypass="false" />
  <pcs>
    <pc name="cbacer" extension="4114" />
    <pc name="another" extension="1234" />
  </pcs>
  <users>
    <user name="chrisx blair" agentid="6001" />
    <user name="john doe" agentid="2100" />
  </users>
  <udfs>
    <udf name="spare1" label="First Field" type="fixed">
      <entry>Fixed Text Entry</entry>
    </udf>
    <udf name="spare2" label="Second Field" type="text">
      <mask>##/##/####</mask>
      <mask>[abcd]</mask>
      <mask>[!xyz]</mask>
      <mask>##/##/####</mask>
    </udf>
    <udf name="spare3" label="Third Field" type="list">
      <filename>spare3entries.txt</filename>
    </udf>
    <udf name="spare4" label="Fourth Field" type="list"
      extensible="false">
      <entry>First Choice</entry>
      <entry>Second Choice</entry>
```

Confidential and Proprietary Information

```

    <entry>Third Choice</entry>
    <entry>Fourth Choice</entry>
</udf>
<udf name="spare5" label="Fifth Field" type="list"
      extensible="true">
    <entry>First Choice</entry>
    <entry>Second Choice</entry>
    <entry>Third Choice</entry>
    <entry>Fourth Choice</entry>
</udf>
<udf name="spare6" label="Sixth Field" type="checkbox">
<  entry>Checkbox label</entry>
</udf>
<udf name="spare7" label="Seventh Field"
      type="checkbox">
    <entry>First Checkbox label</entry>
    <entry>Second Checkbox label</entry>
</udf>
</udfs>
<buttons>
  <button name="start" mode="enabled" />
  <button name="stop" mode="enabled" />
  <button name="update" mode="enabled" />
  <button name="delete" mode="enabled" />
  <button name="retain" mode="disabled" />
</buttons>
<menu>
  <menuitem name="configure" visible="true" />
  <menuitem name="logoff" visible="true" />
  <menuitem name="exit" visible="true" />
</menu>
</desktop>

```

Confidential and Proprietary Information

Advanced Configuration

The individual fields within the XML file are defined as follows:

Logon

The <logon> field determines:

- whether the logon form is presented or not (bypass="false" and bypass="true" respectively)
- whether the identifier used in the logon form is treated as a DN or Position ID (mode="extension") or anAgent Identifier (mode="agent")

PCs

If calls are taken on DNs or Position IDs that are fixed and hence are located next to a specific PC, you can list these physical relationships in the <pcs> field. Rather than have each user specify a particular extension when they log in, simply set the logon bypass option as above and the system will identify the appropriate extension that corresponds to the PC from which the application is run.

Users

If, on the other hand, users log in to position IDs using a particular AgentID, this is often linked to their PC Windows Logon name and this too can be specified in the XML file. If the user's logon name is found when they start the application, the Avaya Contact Recorder will automatically tie the application to the Agent ID specified in the XML file.

User Defined Fields

As shown above, each user defined field ("udf") is defined inside the outer <desktop> and <udfs> tags. Each such field has:

Name

This is how it will be stored in the XML file associated with the call recording. Do not include spaces within these names as this is not valid XML.

Label

This is the text that will show on the desktop application to the left of the data entry field. This does not have to be in English but must only contain 8-bit characters.

Type

This will be one of the following:

Confidential and Proprietary Information

Fixed - A single "entry" field determines the (fixed) text that will be tagged with the call should the user perform any tagging.

Text - The user may enter a text string to be tagged against the call. Optionally, you may include up to 6 "masks". These follow the syntax for the Visual Basic "like" command and hence can be any of:

Mask	Meaning
?	Any single character
*	Zero or more characters
#	Any single digit (0-9)
[charlist]	Any single character in charlist
[!charlist]	Any single character not in charlist

List - This results in the user seeing a drop-down list. You can either specify up to seven individual <entry> fields or specify a file from which the entries in the drop-down list will be read. The <filename> specified is assumed to be in the same directory as the desktop application's executable file.

When using <entry> fields, you can also specify whether or not the user is allowed to enter their own text or is restricted to the available list.

Checkbox - One or more checkboxes will be shown, each labeled according to the "<entry>" fields.

Control Buttons

The application provides five command buttons, each of which can be enabled, disabled or completely hidden as shown in the XML file above. Any button not specified in the XML file will be hidden.

Note:

The "Update" button is labelled "Submit" until it has been used on each call.

Menu Items

A menu can be brought up by right-clicking over the CRD's icon in the tool tray. Several of the options on this menu reflect the configuration of the buttons as defined above and perform the same functions as clicking on the corresponding button.

Three additional menu items can be shown if required on this menu. These are:

Configure - If this is made visible, the user can bring up a dialog box allowing them to enter the IP address of the Avaya Contact Recorder Master and Standby that the

Advanced Configuration

application will connect to. These details are subsequently stored in the Windows registry. If you can configure these details as part of your deployment, there is no need to let the user have access to this dialog. If you do enable the option, the user must still know the password (default is 'admin' but can be changed in the registry as shown in the tables in [Client PCs](#) on page 248).

Logoff - If this is made visible, the user can log off. Use this where desks are shared and it is important that a user logs off at the end of a shift or where Agent ID is used to tie the CRD to a specific position.

Exit - If this is made visible, the user can shut the application down. Otherwise it will be running permanently (unless stopped via Task Manager or similar).

Restarting a Recorder

If you restart the Avaya Contact Recorder, any Contact Recording Desktop users that are connected to it must exit and log in again.

Confidential and Proprietary Information

Altering Translations

The Avaya Contact Recorder supports a number of different languages. The string displayed to a user is determined by looking up a "resource" in a particular language. The translations that the recorder ships with can be corrected without needing to wait for a subsequent release. To do this, log in as a System Administrator and access the **Maintenance** page (at `/servlet/acr?cmd=mtce`)

On this page you can enter the name of the resource to be changed, the string to be displayed instead of the one shipped with the program and the language to which this translation relates. Translations entered are stored in the database and are permanent. You should only use these fields under direct instruction from Avaya support staff who will advise you of the resource name to enter.

Migrating from Central Archive Manager (CAM)

Avaya Contact Recorder no longer supports Viewer or Central Archive Manager (CAM). If you have used these components to archive recordings to one or more NAS folders then you can import the details of these archives into the Avaya Contact Recorder's own database - allowing you to replay these recordings from their archive location without Viewer or CAM being present.

Limitations

1. This feature only supports import from CAM populated NAS shares, not EMC Centera, removable optical or tape drives.
2. CAM must be moth-balled prior to importing the tar files. The recorder does a one-time pass of the directory contents (assuming no errors).
3. Automated purging of these CAM tars is not included, even if the CAM had been configured to purge them automatically.

Replace Viewer with Central Replay Server

If you have previously been using Viewer to replay recordings, then unless your system is small and has plenty of database storage space, you should replace Viewer with an Avaya Contact Recorder configured as a Central Replay Server. You will need to upload the details of existing recordings from each Avaya Contact Recorder into this server. Contact Avaya services for assistance with this.

Note:

You can only configure CAM import on the central replay server(s) in your system - whether those are dedicated Central Replay Servers or a Master and (optionally) Standby server. Any Avaya Contact Recorder that has been configured (on **General Setup > Recorder** page) to upload its recordings' details to one or more specific servers will NOT import CAM data.

Preparation

Assuming you now have an appropriate Avaya Contact Recorder into which you can import the archived call details, you must configure it as follows.

Confidential and Proprietary Information

Call Detail Retention Period

Whether using a dedicated server or your Master Avaya Contact Recorder as your central replay server, it is important that the archived recordings are not immediately purged after you import them. Determine the age of the oldest recordings that you wish to have access to and, if necessary, increase the setting **General Setup > Recorder > Retain call details for (months)**.

Database Storage

Determine the number of recordings that will be imported and ensure that your database partition has adequate space for these additional records. If necessary, increase the available space. See [Central Database Storage](#) on page 58 for further details.

Log File Storage

Check that you have ample space on the log file partition.

Replace CAM

The import process does a single pass over the content of a folder. You must therefore configure a new NAS archive to replace CAM and stop CAM from archiving any further calls.

Network Load

Although the recorder skips over the audio content within the archived tar files, the rate at which the recorder is able to import their details depends primarily on the network throughput between it and the folder on which they are stored. You may wish to do this out of hours but it may take several days to import a large archive.

Multiple Replay Servers

Where a Master and Standby are acting as central replay servers, the archive configuration will be copied automatically to the Standby - which will automatically import the same recordings as have been configured on the master. If network bandwidth is limited, you should consider stopping the Standby server until after the Master has completed its import.

Where a pair of Central Replay Servers are used, you must configure each one separately to have it import the CAM information. Let the first finish before configuring the second.

Import a CAM Folder

For each NAS folder that contains archived recordings you wish to retain access to:

1. Determine the fileshare name and access credentials that Avaya Contact Recorder can use to access these tar files. Read-only access is acceptable.
2. On the **Operations > Archive** page, click **Add NAS**.
3. Enter the fileshare's **Path** and add a **Comment** such as **Imported from CAM**
4. Click the **Advanced** button to add additional settings.
5. You **MUST** set the **Recorders** setting to **CAM** to indicate that this archive was generated by CAM and should not be added to by any Avaya Contact Recorder.
6. Enter the username and password that the recorder can use to access the fileshare.
7. All other settings are ignored and should be left on their defaults.
8. Click **Enter and Close**.
9. The recorder will start to import the recordings automatically.
10. The process has finished when the log file includes
CAM Import from XXXXXXXX marked as completed.
where XXXXXXXX is the fileshare being imported.
11. Test that you can search for and replay calls that only exist in that archive folder.

After the import has completed you must leave the archive folder defined so that subsequent replay requests can use it.

Troubleshooting

1. Additional logging detail can be seen if you set the property value `cam.tracing=true` (can be done without stopping the recorder, via the maintenance page).
2. It is advisable to tail the log file for messages containing `CAM` to spot any problems and to see how rapidly the import is progressing.
3. If import is interrupted or retries following failure to import one or more files, it will be attempted again automatically. Successfully imported tar files are skipped over so that the problematic ones can be tried again.
4. If the recorder uses too much bandwidth, you can throttle it by setting the property value `cam.intervalms=nnn` where `nnn` is the number of milliseconds the recorder will wait between successive recordings. This can be adjusted at run-time from the **Maintenance** page.

Confidential and Proprietary Information



Appendix A: Technical Reference

This appendix provides technical details about the Avaya Contact Recorder system.

The main sections in this appendix are:

- [Recording files](#) on page 262
- [Internal Database](#) on page 263
- [Recorder Interfaces](#) on page 264

Recording files

Voice recordings are stored in an industry standard **wav** file. Screen recordings are stored in a proprietary format in files with extension **scn**. When each call is completed and as each recorded call segment becomes available, the recorder updates its local database with a record of the call segment. These files are stored in a hierarchy of folders beneath **/calls** on a Linux system or the path specified by the administrator on a Windows system.

Every recording results in an XML file and zero or more media files (.wav, .scn etc.).

WAV files

The **wav** files contain the actual audio of the recording. You can double-click some **wav** files to play them directly. Others are in audio formats that are not directly supported by Microsoft's Media Player. This applies to most recordings made by this recorder. These must be converted into a supported format before they can be played. Since the recorder's Search and Replay application does this conversion automatically, you do not need to access these files directly.

XML files

The **xml** files contain details about the recorded call segments. Although most users typically search against the recorder's database of calls, you can view these files directly in a browser if required.

Within each **xml** file there is:

- All the details known about this recording. Most of the information, but not all, is inserted into the calls database. Some of the information is only of interest for diagnostic and maintenance purposes.
- Start and end time in ISO format giving local time and offset from GMT.

SCN files

The **scn** files store the recorded screen content in a proprietary format. These can only be played using the search and replay tools provided with Avaya Contact Recorder.

Confidential and Proprietary Information

Internal Database

If you have retained all of the `xml`, `wav` and `scn` files as described above, then you have kept all of the details about the recordings you have made. However, the system uses an industry standard database (PostgreSQL) to hold this information in more readily accessible forms. This database is located on the recorder itself. The database stores details of the recordings as well as details of the recorder's configuration.

Recording details

The call details database uses approximately 2KB per recording (in the absence of user defined fields). Each voice segment counts as one recording regardless of whether it is in mono or stereo or has any associated screen recordings or not.

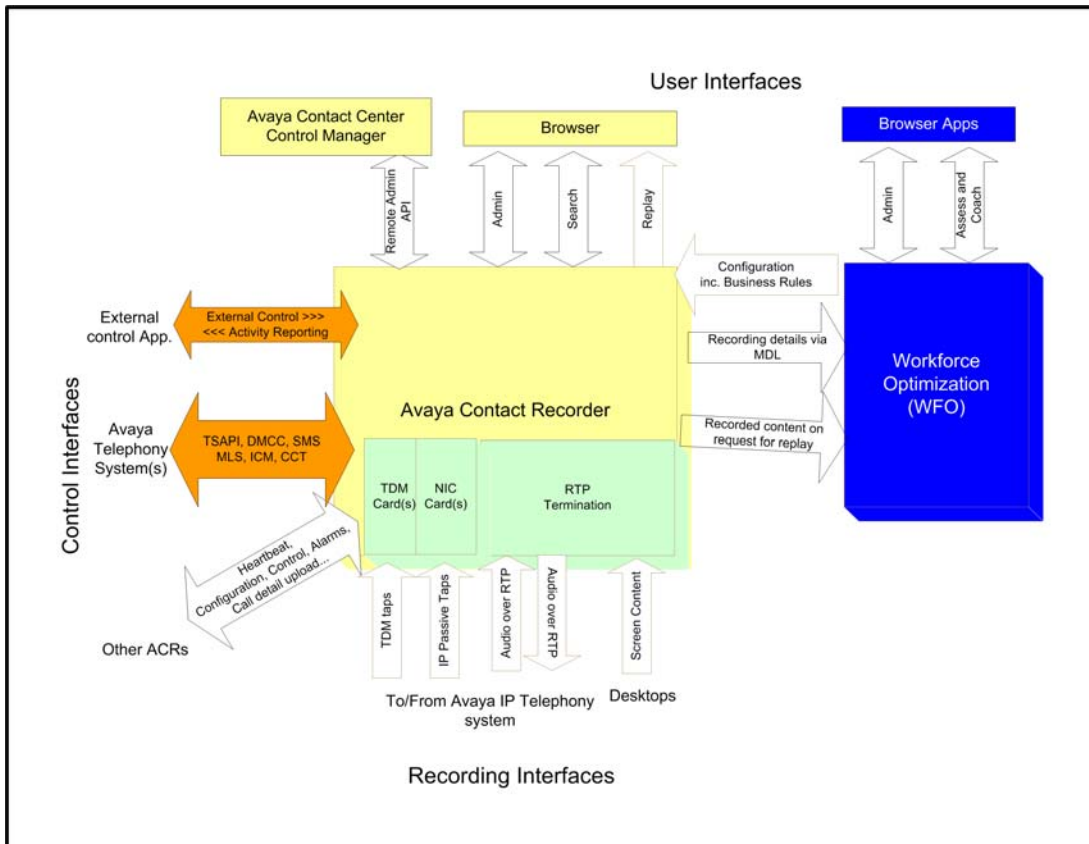
To allow you to search for calls easily, the details of recordings are inserted into this database. It contains one record for each call segment recorded and additional records for each party on the call and each owner of the call. The information stored for each call is described in detail under [Recording Attributes](#) on page 272.

Configuration details

Several tables hold details of system configuration, such as port assignments, file paths, timeouts and user authorization rights.

Recorder Interfaces

The interfaces supported by the recorder are described below (working clockwise round the diagram, starting at top left).



HTTP/HTTPS Interfaces Offered

The recorder uses the tomcat (see www.apache.org) web servlet container to offer a number of services via HTTP and/or HTTPS (on ports 8080 and 8443 respectively). These provide:

Remote Administration API

This SOAP interface allows administrators to configure many recorder features through Avaya Control Manager. These include:

- settings on the **General Setup > Contact Center Interface** page

Confidential and Proprietary Information

- user accounts
- stations to be recorded in Bulk recording mode

This interface is located at `/remoteadmin`

The service definition is available from the service itself at `/remoteadmin?wsdl`

Administration Interface

This provides administrators with access to configuration and status monitoring pages.

Search Interface

End users access this to search for call recordings that match specific criteria.

Replay (Retriever) Interface

End users and other applications (such as WFO) use this interface to retrieve the content of a specific recording.

Call Details Interface

The details about a recording can be provided on request. This is used by the bulk export feature of the integral search and replay application and the Central Replay Server to populate its database.

Search and Replay API

External applications may search for and retrieve the content of recordings using this interface. Full details are available on request.

Communication Manager

The recorder interfaces to the Avaya components via several mechanisms:

DMCC

DMCC runs on an AE Server and provides softphone registration and signalling services.

TSAPI

The Avaya Contact Recorder software exchanges TSAPI messages with an AE Server if Bulk recording is used or if an external controller asks the recorder to establish single-step conferences.

SMS Web Services

If using CoR based recording, the recorder uses this interface to determine which stations are in which CoR.

Audio over RTP

The softphones on the recorder terminate RTP streams over which the audio to be recorded flows. These sockets are connected to whichever VoIP resource (for example, Media Processor) is providing the conferencing bridge through which the call is recorded.

The recorder uses ports in the range 10000-20000 (by default) using two ports per channel.

IP Passive Tap

Ethernet packets can be picked up from a "SPAN" or "Mirror" port on an ethernet switch and connected to one or more NICs for recording.

TDM Taps

One or more trunks and/or phones can be tapped and connected to the appropriate Ai-Logix card(s) to allow recording directly from these devices.

CS1000

The recorder interfaces to these Avaya components via several mechanisms:

Meridian Link Services (MLS)

Master and Standby recorders connect using TCP/IP to the MLS feed from the Avaya Contact Center Manager Server. These recorders interpret the telephony events occurring in real-time and whichever is active instructs the server to forward call data from the required IP phones to the required ports on the recorder(s) when calls are to be recorded.

Confidential and Proprietary Information

Audio over RTP or DTLS

When the recorder instructs IP phonesets (via MLS) to perform Duplicate Media Streaming, the voice packets are sent using RTP to the recorder. If licensed for encryption, these streams will use DTLS.

The recorder uses ports 12000 upwards, allocating two ports per recording channel.

TDM Taps

One or more trunks and/or phones can be tapped and connected to the appropriate Ai-Logix card(s) to allow recording directly from these devices.

Avaya Aura Contact Center

The recorder interfaces to the Avaya components via several mechanisms:

CCT

The recorder uses the CCT web services to track activity on the switch and to ask for recorder ports to be invited into calls that need to be recorded. The recorder listens on port 9010 and sends to port 9080.

Session Initiation Protocol

The AMS interacts with a SIP proxy running on each recorder. It invites the recorder ports to join the calls as per the instructions passed over CCT. The SIP proxy on each recorder listens on port 5060.

Audio over RTP

Once the AMS has included the recorder port in the call to be recorded, the voice packets are sent using RTP to the recorder. The recorder uses ports 12000 upwards, allocating one RTP port per recording channel.

Screen Recordings

If licensed for screen recording, the system will also use this interface.

Screen Content

Each recorder communicates with the workstations whose screen it is recording. This is a TCP connection to port 4001 (by default) on the client workstation (or, in the case of thin client recording, with the server hosting the Windows session).

Windows Account Logon/off

Workstations that have been configured to track logons will send details of account logon/off to port 29522 on the recorder.

Workforce Optimization ("WFO")

In addition to the Replay (Retriever) Interface already described on page 280, Avaya Contact Recorder interacts with a WFO system over the following interfaces:

EMA Interface

System configuration information is transferred via TCP/IP ports 7001 and 7002 on the WFO server hosting the "EM" component. It uses ports 8080 or (with SSL) 8443 on the Avaya Contact Recorder to do this.

MDL Interface

Details of recordings made are passed to WFO via HTTPS on port 43 or HTTP on port 80 of the WFO server configured with the "APP" role.

Other Recorders

Recorders establish links between master, standby and slave recorders. Configuration, alarms and recording instructions are passed over these links. These are TCP/IP socket interfaces.

Master and Standby recorders listen for connections from other recorders on TCP/IP port 1209 by default and communication over these links is encrypted.

Confidential and Proprietary Information

External Control Interface

The recorder supports a simple TCP/IP command interface. This allows other applications to control recording directly and/or add further user defined data fields to recordings. This protocol supports START, STOP, TAG and BREAK (seamless stop and start) commands.

AET/DPA Interface

The recorder listens for incoming HTTP commands on port 3020.

Database Upload Interface

When configured with either a Central Replay Server or (defaulting to) a master and/or standby server performing this role, the recorder uploads details of calls into a database on the appropriate server.

To Central Replay Server

To upload call details to the Central Replay Server (CRS) a recorder uses a web service on the CRS, to inform it that a new recording is available. The CRS in turn uses a web service on the recorder to retrieve the details. Both of these interactions use port 8080.

Summary

System	Interface	Protocol	Local	Remote	Direction
All	HTTP - Admin and Replay etc.	TCP	8080		Inbound
	HTTPS - Admin and Replay etc.	TCP	8443		Inbound
	RTP Audio	UDP	10000-20000		Bidirectional (CM) Inbound (CS1000, AACC)
	Between Avaya Contact Recorders	TCP		1209	Towards master and standby
If installed and configured	Screen Capture	TCP		4001, 29522 (default)	Inbound
	Central Replay Server	TCP		8080	Bidirectional
	Dialers, External controllers	See relevant Appendices			
If WFO present	EMA	TCP		7001, 7002	Outbound
	MDL	TCP		80 or 43	Outbound
When recording Communication Manager	DMCC	TCP		4722	Outbound
	TSAPI	TCP		450, 1050	Outbound
	SMS web services	TCP		80	Outbound
When recording CS2x00	ICM or Linkplexer	TCP		2500	Outbound

Confidential and Proprietary Information

System	Interface	Protocol	Local	Remote	Direction
When recording Avaya Aura Contact Center	CCT web services (client)	TCP		9080	Outbound
	CCT web services (server)	TCP	9010		Inbound
	SIP proxy	UDP		5060	Inbound
When controlled by AET/DPA	EQConnect	TCP	3020		Inbound

Recording Attributes

The Avaya Contact Recorder stores some "tagging" information against each recording that it makes. Other information pertains to the overall telephone call or to one parties' involvement with that call. This section:

- Explains where and how data is stored
- Defines the terms "Call", "Contact", "Session", "Segment" and "Party"
- Explains how calls are identified by the recorder and how this relates to the underlying switches own call identifier
- Describes the available attributes; how they can be added to a search and replay layout and, where appropriate, consolidated into an associated WFO database.

Overview

Avaya Contact Recorder tracks the phone calls that are made on a switch in real-time. This results in one or more recordings. These in turn result in entries being made in the recorder's database and (optionally) in the database of one or more other Avaya Contact Recorders acting as "Central Replay Servers".

Real-time Tracking

Avaya Contact Recorder:

- Tracks CTI events from one or more data feeds in real-time.
- Builds a CSTA-like in-memory model of the state of each **CALL**.
- Models each call as a current (and historical) set of connections ("**CONN**"s).

Each connection (CONN) identifies a specific DEVICE which is linked to the CALL for a certain period of time in a specific connection STATE.

Some connections are **TRANSIENT** while others PERSIST.

A call is **SEGMENT**ed into time periods during which the set of (implicitly persistent) CONNectiions is constant i.e. any change to the connections results in a new SEGMENT starting. Some segments are recordable and others are not.

XML Files

For each recording, a snapshot of some of the call information is taken at the start of the recording. Some fields may be added during and at the end of the recording segments.

Confidential and Proprietary Information

This information is stored in an XML file alongside the content (audio and/or screen capture) of that recording - and is copied along with the content should that be archived. This gives a fallback record of the data associated with the recording allowing the retrieved files to be of use even in the absence of any associated database records.

Recorder's Database

The recorder's (Postgres) database is updated at the end of a recording with most - but not all - of the information present in the XML file.

Implicit in the above are the facts that

- **nothing** is stored in the database during a call segment
- **nothing** is stored for call segments that did not result in a recording.

Central Replay Server(s) Database(s)

In a system with more than one Avaya Contact Recorder, it is normal practice for all other servers to upload details of their recordings to one or more servers that fulfil the role of "Central Replay Server". Such servers allow a user to search against their database to find recordings made on any of the recorders that feed this server with copies of their recordings' details.

In many systems, the Master (and Standby if present) act as Central Replay Servers for each other and for their population of connected slave servers. In very large systems, dedicated Central Replay Server(s) may be provided to reduce the load on the Master and Standby.

The other reason for having a dedicated Central Replay Server is if custom integration is required into the Postgres database. (e.g. additional tables or data feeds populating it). This is NOT supported on a live recorder as the load is indeterminate and out of Avaya's control.

The information uploaded to the Central Replay Server is always the same as is stored on the Avaya Contact Recorder that is feeding it - but is typically delayed by at least several seconds (10 second batch job interval by default) and may be much further behind if the CRS or path to it is unavailable.

Definitions

Before listing the attributes stored against each recording, it is important to understand the concepts of "Calls", "Contacts", "Sessions", "Segments" and "Parties".

Call

Each telephone call that is active on an Avaya switch has a call identifier and this is stored as an attribute of a recording - its Call ID. The format of this identifier varies from switch to

Confidential and Proprietary Information

Technical Reference

switch. In the case of Communication Manager, this Identifier is extended to form a UCID (Unique Call ID). Other switches may reuse call identifiers over and over again. In this case, such an identifier is not sufficient to uniquely identify a call unless it is combined with some form of timestamp information to distinguish it from previous and subsequent uses of the same identifier. This combined, globally unique identifier is also stored but is kept internal to the recorder.

Contact

Note:

Contact related information is only stored for calls recorded using Bulk recording mode. Recordings made in other modes will not display this information.

When the first party on a call (the "calling party") starts to make a call, this is treated as a new "contact". A contact extends into other calls made while connected to this original call. Only when all such connected calls are over does the contact end. The total duration of this contact is tracked. Each recording is marked as being part of one and only one contact - with its Contact ID.

Session

Note:

Session related information is only stored for calls recorded using Bulk recording mode. Recordings made in other modes will not display this information.

Within a contact, several other parties may be involved with the call(s) made. Each of them cares about how they were treated during the contact. Did the other parties leave them listening to ringing tone; did they get put on hold many times or for an excessive period; were they transferred many times etc. Within the search and replay application, the user can search for fields that reflect the first session within the contact i.e. how the calling party was treated. (All sessions with appropriately configured internal parties are available to the optional Quality Monitoring application).

Segment

Each "call" is recorded as one or more recordings - each of which normally extends for only one "segment" of the overall call. A segment ends whenever the parties on the call change. This is because the recording rules typically operate on the basis of which parties are on the call and the security mechanisms that determine who will be allowed to replay a recording also operate on the basis of who was on the call - hence any change to these forces a new segment and, if appropriate, a new recording to start.

Confidential and Proprietary Information

Party

Many of the fields available refer to the parties or devices involved with the phone call - or, more specifically, with a particular recording - hence call segment. These range from agents to VDNs to public phone numbers. The table below shows the types of party that may be associated with a recording in the database; which type of switch each relates to and the numerical "party type" identifier that is used in the recorder's database to indicate this sort of party.

Each party has:

- an "address" (previously referred to as its "number") which is normally, but not always numeric
- and *may* also have an alphanumeric "description" (previously referred to as its "name"). Not all switch CTI feeds provide this.

Switch	PartyTypeID	Party Type	Notes
All	50	DNIS	Some switches (e.g. AACC) provide DNIS for all calls, others only for incoming calls. ACR follows the switches definition of "DNIS" (whereas WFO treats "DNIS" as synonymous with "called party")
	51	External Number	
	52	Unknown	
CM	100	Agent	Alphanumeric description or "name" as configured on the switch is usually provided via TSAPI and stored along with the (normally) numeric "address"
	102	Split	
	103	Station	
	104	VDN	
	108	Dynamic	
	109	Other	
	111	Announcement	

Switch	PartyTypeID	Party Type	Notes
CS1K	201	CDN	Name information not available via MLS. Numeric address only stored.
	230	DN	
	232	Position ID	
	234	Line appearance	
	235	Agent	
	236	Skillset	Skillset name provided and should be used in preference to the numerical Skillset identifier.
	240	Activity Code	May be overwritten during a segment. Only the last code is stored.
AACC	301	AACC Agent	
	302	AACC Skillset	
	303	AACC CDN	
	304	Unknown party	
Dialers	401	Dialer Agent	
	402	Dialer Skill	
	403	Campaign	

Call Identifiers

Each switch identifies its calls differently. The recording system must have a way of uniquely identifying each call that it has recorded - and not be confused by the same id being used again by the switch - which really only needs to distinguish each live call from all other live calls.

The Avaya Contact Recorder uses a single pool of Call objects so must ensure that the ids used to look calls up are unique across all call types that may be present (underlying switch, overlay switch such as AACC plus any number of heterogeneous dialers).

For each type of switch, the Avaya Contact Recorder derives its own variant of a CallID and how it maps the ID provided by its CTI feed(s) to this object - but each call identifier has:

Confidential and Proprietary Information

- a 64-bit (signed) **long** value which must be unique over the lifetime of the recording system - and is used internally but never normally shown to the end user.
- a "**native**" string representation which is shown to the user on the replay screen and may be searched for as a string. This is in the form used by the switch itself e.g. a Communication Manager UCID such as 00001012341212345457

In many cases the native call identifier is itself a representation of an underlying long (64-bit) value - and in such cases the Avaya Contact Recorder will use this value where it can. The various types of callID are summarised in the table below and discussed in more detail thereafter.

Call on	Type ID	64-bit callid			"Native" Callid
		Bits 48-63	Bits 32-47	Bits 0-31	
CM or POM	1	Switch(S)	Callid (C)	UTC (T)	SSSSCCCCCTTTTTTTTTT (standard Avaya UCID style)
		=Original CM provided UCID			
CS1K	2	HLOC	Callid (C)	UTC (T)	HHHHCCCC See MLS spec for HLOC encoding. Not direct map of hex digits and may be fewer than 4 chars.
		= Original NetworkCallid provided by MLS		ACR's Time	
AACC	5	ACR assigned switch ID	Cyclic identifier assigned by ACR	ACR's Time	May be a GUID, a UCID or other identifier passed in by originating switch.
Dialer (except POM)	4	ACR assigned switch ID	Low 48 bits of dialer's callid		Varies

User Defined Fields

In its internal PostgreSQL database, Avaya Contact Recorder can store:

- any number of user-defined fields (UDFs)
- each with a name of up to 50 characters
- each of arbitrary length (all are stored as TEXT fields)

Some of these fields can be populated by the Avaya Contact Recorder itself while others can be provided by external applications via the External Control Interfaces described in Appendix D.

Built-in User Defined Fields

In addition to the basic CTI information stored with every call, other CTI fields may be accessible to the recorder as it processes events from the switch. These are not of interest

Confidential and Proprietary Information

Technical Reference

to all users but can be stored in user-defined fields. Only the more commonly used ones default to being stored, are immediately available through the default search and replay layouts and are passed to WFO. Other, less useful ones default to not being stored but can be assigned to a user defined field using property file settings. Similarly, those that are on by default can be forced off (by placing nothing after the equals sign in the property file entry) or into differently named user defined fields with the property file settings shown below.

Attribute	Property Setting	Default	Notes
Activity Code	activitycode.fieldname	activitycode	CS1000 only. Last activity code set on each call segment.
Dialer call attributes	<i>dddddd</i> .field. <i>ffffff</i> (where <i>dddddd</i> is the dialer name and <i>ffffff</i> the field name).	Null	Available fields vary according to dialer type and how it is configured.
User to User Information (UI)	uui.fieldname	Null	Communication Manager, text (not binary) UUI only.

Externally Provided User Defined Fields

The Avaya Contact Recorder automatically stores new user defined fields under whatever name is provided in the simple XML tags passed via the External Control Interface.

Search and Replay Attributes

The table below describes the various CTI fields that are stored within the recorder's database and hence can be easily added to a search and replay layout. The description also explains how to use the field selection box and its neighboring parameter field at to the top of the **Field Editor**. The fields are grouped logically below rather than alphabetically and follow the order shown in the drop-down list presented by the **Field Editor**.

Confidential and Proprietary Information

Where attributes vary according to the switch type or CTI available, this is also described.

Field	Parameter	Description
Start Time	N/A	The start date and time of a recorded segment. As the search criteria for this field is normally a time range relative to the date the search is being done, it does not make sense to enter a fixed or pre-selected date/time range. Instead, enter the (integer) number of days back from today in the default search criteria box. So "0" sets the timespan to "today"; "1" to Yesterday through to today; "28" today and the previous four weeks etc.
Duration	N/A	The duration in seconds or minutes and seconds of the recording i.e. the call segment to which the recording relates.
Direction	N/A	This field is determined from the overall Contact. If there were NO external parties (types 51 or 108) on the call, it is "Internal". Otherwise, if the first session on the contact was from an external party (type 51 or 108) then the call was "incoming" otherwise it was "outgoing".
Call ID	N/A	The native identifier assigned by the switch. There may be several recordings sharing the same Call ID. Internally, this id is supplemented with timestamp information to derive a unique identifier for the call.
Inum	N/A	The unique 15 digit reference number assigned to the recording. The actual audio, screen and data files stored use this as their filename. Note that one recording may be stored as several consecutively numbered files (e.g. for stereo audio and/or one or more screen capture files). This number is always the lowest of the set.
Contact ID	N/A	Which contact this recording forms a part of. Search for other recordings with the same Contact ID to find related recordings.
All Parties	N/A	Displays all types of parties that have been stored in the database as being associated with the recording. Can be used to make a very simple set of search results with a single column showing all the phone numbers, agents etc that were on the call segment that has been recorded. However, this can be confusing as not everyone recognizes which numbers are skills, agents, VDNs, stations etc. Normally the parties are spread across several columns using the fields immediately below.

Technical Reference

Field	Parameter	Description
Agents	N/A.	Parties of types that represent logged on agents (100, 235, 263, 301, 401) that were connected to this call segment.
Skills	N/A	The most recent party of a type that represents a skill or split (102, 236, 302, 402) that the call segment was routed via.
Services	N/A	The first or last (according to preferences on the Settings > Contact Center Interface page) party of type VDN or CDN (104, 201, 303, 403) through which the call was routed.
DNIS	N/A	The first party of type DNIS (50) that the call was directed towards. (Technically, DNIS should only be present for an incoming call from the public network. Some switches treat the "called number" as the DNIS for internal calls).
Other Parties	N/A	This field automatically displays all parties connected to a segment that are not explicitly selected by any other field. So if you remove the Skills field, for example, this column will include those party types automatically. It is a useful catch-all to ensure that any party tagging not shown by your other columns is presented to the user.
Specific Parties	xxx or xxx,yyy,zzz	You can select one or more explicit party types to display in a column of this type. Enter the party type identifier(s) you want to include, separated by commas.
Hold Count	N/A	How many times the calling party (first session) on the overall contact was placed on hold by (all) the other parties and hence unable to continue talking.
Transfer Count	N/A	How many times the calling party (first session) on the overall contact was transferred to another party (i.e. the second party has left the call and been replaced by another).
Conference Count	N/A	How many times the calling party (first session) on the overall contact was involved in a conference with more than one party. Dropping from three to two parties and returning to three counts as a new conference regardless of who the parties were.
Agent Count	N/A	How many different agents were involved with the contact as a whole.
Ring Duration	N/A	How long the calling party spent unable to talk because the only other party on the call had not answered.

Confidential and Proprietary Information

Field	Parameter	Description
Total Duration	N/A	The total duration of the contact.
Call History	N/A	A text string describing the progress of the this session. For example: "Ring, Talk, Held, Conf, Talk, Disconnected"
Bulk Trigger	N/A	True if this recording was made because of configuration under Operations > Bulk recording mode.
Rule Trigger	N/A	True if this recording was made because of a WFO Business Rule.
Call Sets	N/A	When used as a filter, this allows the user to select calls that are in a Call set - from a drop-down list of existing call sets (including, if the user is permitted, the lock related call sets). When shown as a column, this shows the names of any call sets into which the recording segment has been placed.
All UDFs	N/A	Places all populated user defined fields into a single string of the form <i>udfname1:udfvalue1 udfname2:udfvalue2</i> - i.e. a colon between udf name and value and a space between successive udfs. This allows a single filter to be used to search for any udf e.g searching for "Incl. custid:1" would find all recordings with a udf "custid" starting with digit 1.
User Defined Field	<i>udfname</i>	Shows the value of the User Defined Field with name <i>udfname</i> for this recording/call segment.
Custom Field (String)	SQL	Allows additional text fields to be derived from the data held within the database. Please contact Avaya if you need to use this feature.
Custom Field (Number)	SQL	As for Custom Field (String) above - but in this case the result is treated as a number for filtering purposes and in the column sort order.

WFO Integration

Where the details of recordings are to be consolidated into a WFO system, a number of attributes are automatically provided, with fixed definitions, while other, user configurable fields can be added as required. See WFO documentation for procedures, limitations and

Confidential and Proprietary Information

Technical Reference

definitions of these. The tables below describes how Avaya Contact Recorder supports the standard attributes defined in WFO.

Contacts

The following fields are always provided as part of the Contact data. These fields are used in a standard way within WFO but the **Notes** column highlights any known issues or differences in how Avaya Contact Recorder determines their content.

Field	Meaning	Notes
ID	Unique identifier for this contact	19 decimal digits, starting with "92" and ending with "1"
Start	Contact start date/time	
End	Contact end date/time	
Holds	Number of times all other parties on the call placed the call on hold.	Calculated with respect to the original (calling) party on the call.
HoldDuration	Time spent with all other parties holding	Calculated with respect to the original (calling) party on the call.
Transfers	Number of times transferred	Calculated with respect to the original (calling) party on the call.
Conferences	Number of times call went from 2 parties talking to more than 2 parties.	Calculated with respect to the original (calling) party on the call. If one party on a conference holds the call then retrieves, this counts as dropping to 2-way then back to 3-way again, hence adds to the number of conferences.
IsException	Whether or not marked as an exception	Only Business Rules configured to do so will mark a contact as being an exception.
ExceptionReason	0 unless IsException is true, in which case 1	
ANI	Calling party address	WFO treats ANI as synonymous with "calling party" so this is provided, even on internal calls which, strictly speaking do not have an ANI.

Confidential and Proprietary Information

Field	Meaning	Notes
DNIS	Called party address	WFO treats DNIS as synonymous with "answering party" so this is provided, even on internal calls which, strictly speaking do not have a DNIS.
PauseDuration	Not supported	
WrapupTime	Not supported	

Sessions

Within Avaya Contact Recorder, every party that joins a call is assigned a Session. That party will have a device and may also be associated with an Agent.

Sessions Visible to WFO

By default, all sessions involving an internal party are passed to WFO but this can be overridden by setting set the property value

`core.consolidateall=false`

Once this has been set, a session will only be sent to WFO if the logical device (station or DN) associated with the session is appropriately configured in WFO. This is summarized in the table below, where the right-hand columns show whether or not a session will be sent to WFO.

Session's Device	RecordingType configured in WFO for this device	Type of recording made	Sent to WFO if <code>core.consolidateall=</code>	
			true (default)	false
External	N/A	Any	No	No
Internal	Device Not configured	Any	Yes	No
	Record Always, Application Controlled, Override or TAG	Any		Yes
	Start at Business Rule	Bulk Recording		No
		Business Rule		Yes
Any other recording type	Any	No		

Confidential and Proprietary Information

Standard Session Attributes

The following fields are always provided as part of the Session data. These fields are used in a standard way within WFO but the notes column highlights any known issues or differences in how Avaya Contact Recorder determines their content.

Field	Meaning	Notes
Telephony Contact Fields		
ID	The unique identifier of the contact of which this session is a part	Links this session to the appropriate contact.
User Fields		
StringExtension	The (normally numerical) address of the telephone device to which this session relates	Either a Station (CM) , DN or Position ID (CS1K).
PbxLoginName	The agent identifier used to log in to the switch (if any).	Normally numeric but may be alphanumeric on e.g. dialers.
ID	The unique reference within EMA configuration for this employee (if known)	Found by looking up the PbxLoginName within the appropriate DataSource file.
NetworkLoginName	The computer (normally Windows) account name associated with this employee.	Found by looking up the Employee's details in EMA files.
DisplayName	Same as StringExtension	
Telephony Session Fields		
SwitchCallID	The identifier used by the telephone switch and passed in CTI messages.	As the string was received from the switch. May be Avaya UCID, CS1K NetworkCallID, GUID or other. May not be unique.
SwitchID	The datasourceid for the switch on which the call was received.	As defined in XML files received from EMA.
ANI	The number of the calling party (with respect to this session).	Supplied even on internal and outgoing calls where there is no "real" ANI.
DNIS	The number of the called party (with respect to this session).	Supplied even on internal and outgoing calls where there is no real "DNIS".

Confidential and Proprietary Information

Field	Meaning	Notes
Direction	1 (Inbound), 2 (Outbound) or 3 (Internal).	Based on the direction of the call that initiated the session.
Holds	The number of times this party has placed the call on hold.	Includes hold implicit in transfer and conference setups.
HoldDuration	The total duration for which this party has left a call on hold.	Not the same as how long the other party has been kept on hold (for which, see the contact attribute). This timer stops when the party speaks on a consult call even though the original call is still on hold.
Audio Acquisition Fields		
Start	The timestamp of the start of the session.	Same as INumStart below i.e. does not include ringing or call setup period.
End	The timestamp of the end of the last recorded segment in the session.	Does not include e.g. wrap-up time or time on hold at end of session if session abandoned while on hold.
ParentInum (in Module and Channel fields)	The unique reference of the first recorded segment within this session.	Passed via AudioAcquisition Channel (9 least significant decimal digits) and Module (6 most significant decimal digits) parameters. The Module is also the serial number of the recorder making the recording.
Compression	Always "G.729A" unless default compress/mix behavior has been overridden in properties file.	Subsequent INums need not be the same compression format. Can be overridden by property setting "mdl.compression" if necessary.
WrapUpTime	0	Not currently supported.
Type	0	Not currently supported.

Field	Meaning	Notes
Screen Acquisition Fields		
ScreenInum	The unique identifier of the session-level screen recording (if any).	This screen recording persists for the duration of the session, including hold periods. Passed via ScreenAcquisition Exists (9 least significant decimal digits) and Module (6 most significant decimal digits) parameters. The Module is also the serial number of the recorder making the recording.
Additional Recorded Segments		
Inum	The unique reference of a further recorded segment within this session	
InumStart	The timestamp of the start of this further recorded segment within this session.	
Private Data		
Up to 25 fields	See below for available fields.	
Custom Data		
	NOT SUPPORTED.	Use Private Data fields instead.

Private Data Fields

Note that User Defined Fields within Avaya Contact Recorder can also be mapped to WFO fields (subject to the overall limit of 25 such fields). These fields provide additional tagging of a session, over and above the standard data fields described above.

Agent Related Fields

The ExternalID (or "EmployeeID") is always provided as part of the standard session information for a logged on agent that is configured as an Employee in WFO. The fields below may also be configured into one or more Private Data fields. Most are read from the "organization-xxx.xml" files provided by EMA - so rely on

- ACR being able to match the (agent logon id + switch/datasource ID) against the information given in EMA XML files.

Confidential and Proprietary Information

- The information being configured in WFO and received in updated EMA XML cache files.

ID	Name	Type	Description
-919022	AgentID	String 32	The PBX logon id of the agent to whom this session relates. Empty string if no agent logged on to this device.
-919038	NetworkID	String 32	The agent's network logon id derived from EMA data in the same way that other Verint recorders do.
-919003	Skill	String 32	Comma separated list of: CM: The one or more agent skillsets to which the agent is logged on and which the ACR is observing. CS1K: The lead ACDDN to which the agent logged on. AACC: Not supported as not provided in CCT agent login event.
-919036	EmployeeGroup	String 64	Comma separated list of the EmployeeGroups of the agent to whom this session relates. Determined from EMA data in the same way that other Verint recorders do.
-919037	Organization	String 128	Organization of the agent to whom this session relates. Determined from EMA data in the same way that other Verint recorders do.
-919004	SupervisorName	String 128	The name of the Supervisor of the agent to whom this session relates. Determined from EMA data in the same way that other Verint recorders do.
-919001	AgentName	String 128	The name of the agent to whom this session relates. Determined from EMA data in the same way that other Verint recorders do.
-919002	LoggedOnDuration	Int	Not supported.
-919046	ScreenUnit	Int	Not supported.

User Defined Fields

Any User Defined Field stored in Avaya Contact Recorder can be configured as a private data field and sent to WFO. Define the field in EMA using the name of the User Defined Field.

Predefined CTI Derived Fields

The following fields are available where provided by the appropriate switch and relate to the specific session that has been recorded.

The data **Type** shown in the table below is the default that WFO uses. These fields will, however, be truncated according to the size of the private data field into which they are placed. The types shown are therefore a guide as to which of the 25 private data fields would be suitable for each rather than a strict limit on each. Where the data available in a field exceeds the length of the Private Data Field to which it has been assigned, the contents will be truncated.

The table below shows only those fields that are available, that are of value and are not already present in, or directly equivalent to the standard session or contact data fields shown above

ID	Name	Type	Description
-919032	CalledParty	String 32	The address (normally numeric) of the second party on the first call of this session.
-919031	CalledParty Name	String 32	The name of the second party on the first call of this session. Currently only provided on CM, for internal calls.
-919026	CallingParty	String 32	The address (normally numeric) of the second party on the first call of this session.
-919030	CallingParty Name	String 32	The name of the first party on the first call of this session. Currently only on CM, for internal calls.
-919008	DataSource Name	String 64	The name of the DataSource configured in EMA that provided the CTI for this session.
-919016	EventType	String 16	Limited support. One of: "Other", "Alerting", "Connected", "Held", "Retrieved", "Transferred", "Disconnected". Set at start of session only. Note that if you use this attribute in a business rule to control recording, the value stored when the recording is made may be different from what it was when the rule was triggered. For example, a rule set to trigger when EventType equals "Alerting" will recording incoming calls but by the time the recording starts, the EventType will typically have become "Connected".
-919035	Extended CallHistory	String 32	Comma separated string showing the progress of the session. Consists of one or more of "Ring", "Talk", "Held", "Transfer", "Disconnected", "Conf".

Confidential and Proprietary Information

ID	Name	Type	Description
-919053	Fired BusinessRules	String 128	Comma separated list of the names of the Business Rules (if any) that fired on this session. May end in ",..." if the list is longer than 100 characters.
-919051	GlobalCallID	String 64	Globally unique call identifier assigned by the Avaya Contact Recorder.
-919013	NumberDialed	String 32	Number of the answering (second) party on the call.
-919040	Parties	String 128	Comma separated list of all parties involved in the first call of the session.
-919007	Queue	String 32	The CDN (CS1K, AACC) or VDN (CM) if any through which the first call of the session was routed.
-919024	Thirdparty	String 32	The other party involved in a transfer or conference associated with this session.
-919014	Trunk	String 16	The trunk member carrying the call to/from the switch. Only populated for external calls on CM and CS1K. Not available on AACC.
-919015	TrunkGroup	String 16	The trunk group carrying the call to/from the switch. Only populated for external calls on CM and CS1K. Not available on AACC.
-919039	Workstation	String 32	The workstation name associated with the device or agent, as defined in EMA files or in screen capture client agent login data where available.
-919029	LastMessage	String 32	NOT SUPPORTED
-919028	FirstMessage	String 32	NOT SUPPORTED

Confidential and Proprietary Information



Appendix B: Troubleshooting

This appendix covers two areas: general troubleshooting tips and some specific common issues:

The main sections in this appendix are:

- [Hints and Tips](#) on page 292
- [Specific Problems](#) on page 293

Hints and Tips

Where to Look for Clues

When problems occur, check the following:

- **Emailed Alarms and Events.** If you have been using the email settings to have alarms and events forwarded to one or more email addresses, you should check these carefully. As well as checking the contents of messages that you have received, also check for days when the nightly log file purge message has not been received.
- **Alarms Page.** This page within the administration application provides a wealth of information on problems that the system has detected. Review the alarms carefully. If the problem is not immediately apparent, consider viewing all alarms, including those that have previously been cleared. It may be that someone has cleared an alarm without addressing it or realizing its significance.
- **Log Files.** Check for errors being reported in log files within the following directories beneath your installation directory: (/opt/witness on Linux; typically D:/Program Files/Avaya/ContactRecorder on Windows)
 - logs
 - /tomcat7/logs

Determining Current Version

When reporting problems you should state precisely which version of software you are running. To determine this, click on the **System > License** tab.

Note the precise version number shown.

Confidential and Proprietary Information

Specific Problems

System Administration page problems

You may encounter problems as you access and use the System Administration application. This section lists those problems and suggests steps to take to correct them.

Cannot access the System Administration pages

If you cannot access the System Administration pages, try the following:

- Ping the server to confirm that connectivity is possible. If not, trace the network connections between client and server and double-check the server's IP address, default gateway etc.
- Use the numeric dot notation IP address instead of the hostname. If this works, then the hostname is wrong or cannot be translated by your DNS services. You may need to use a fully qualified node name, such as `recorder.bigco.com`.
- Use the browser installed on the server itself to access the application at `http://localhost:8080`.

If this works, then the problem is in the network between server and client. If it does not work, then the problem may be with the Tomcat web server.

Cannot log in

If you have trouble logging in, double-check the state of Caps Lock and ensure the password is being entered with the correct case.

If you can log in under another account, set a new (temporary) password for the account having problems.

If nothing happens when you click the OK button, check that your Internet Explorer settings allow javascript to run. See [ActiveX Control Download](#) on page 173.

These symptoms have also been seen when trying to access a server with an underbar in its node name. Note that this is not a valid IP name and should be changed.

Connectivity

Email alarm problems

Invalid entries in any one of the parameters used to define the email settings will result in errors. To check this:

- Try the settings you are using in a standard mail client, such as Outlook. Send a message using the account specified to prove that the settings are valid.
- If email messages have been working and then stop without any of the settings changing, verify that nothing has changed on the mail server. This problem occurs, for example, if your password has been reset or changed on the mail server.
- If the recorder is not sending email messages, it may be because it is not able to access the SMTP server. Check the network connections to the recorder.

CTI Link Connection Problems

The recorder communicates constantly with your switches CTI feed. If this link fails, alarms are raised. If you suddenly get multiple alarms, including those with other components, then the problem is more likely to be with the recorder's network connection than with a specific link..

Search and Replay problems

For most problems with Search and Replay, consider the following diagnostic approaches to narrow down the cause of the problem:

1. Search for a different call, for example, one that is more recent or older, shorter or longer.
2. Log in as a different user with different replay restrictions

Cannot access the replay application

If you cannot get to the login page, try accessing the page from a different machine:

1. From the same side of any firewalls.
2. On the same LAN if you are having problems with WAN access
3. From the same sub-net, if having problems from a different sub-net
4. From the recorder itself, if having problems from the same sub-net.

Confidential and Proprietary Information

User replay restrictions do not work

If you have given a user account replay rights over a number of addresses but the calls from these stations are not listed when you enter a valid search that should include them, check the recording ownership. When an agent has logged on to a station that is being recorded, the calls recorded are "owned" by the agent number not the underlying station. Give the user replay rights to the range of agent IDs who have been using the stations in question. In fact, in most cases, you should restrict access to a set of Agent IDs rather than station numbers.

Problems downloading ActiveX control

If you see error messages relating to ActiveX controls being downloaded-or blocked from being downloaded, your security settings may be too restrictive. See [ActiveX Control Download](#) on page 173 for more information.

Problems displaying ActiveX control

If the ActiveX control downloads but displays a red cross on white background at top of page, upgrade to Internet Explorer 8.0 or later. These symptoms have been seen on Internet Explorer 5.0.

 **Important:**

You must run 32-bit Internet Explorer. The ActiveX control will not run in 64-bit IE.

Cannot log in

If you see the login page but cannot get past it:

1. Verify that Caps Lock is off and that you are entering the password with the correct case.
2. Log in as a different user
3. Confirm the spelling of your log in name with the system administrator and check that your account is still configured in the administration pages.
4. Ask the system administrator to reset your password. Log in with a blank password and change your password when redirected to the Change Password page.

Search returns no calls

If you get to the search page but no calls are returned when you perform a search:

1. Broaden your search criteria to confirm that you can at least find some calls. Start by requesting calls from any parties for today. If that shows no calls, extend the time period.

Confidential and Proprietary Information

Troubleshooting

2. Try setting the date range back to at least the time you know you have seen call records for in the past.
3. Check that the system administrator has given you access to the correct calls. Your search and replay restriction may be wrong or too narrow for the search you are attempting.
4. Confirm that calls are being recorded. Follow the troubleshooting guidelines for recording problems if you suspect that the system is not actually recording or processing any calls.

Calls listed but cannot play them

If you can see the list of calls that matched your search criteria, but cannot actually play them, look at the area at the top of the browser page where the "graph" of the audio normally shows and match your symptoms to one of the following:

No Audio "graph"

This means that the call has not been retrieved from the recorder or DVD disk or has not reached the client PC.

1. Check the server logs for errors.
2. Note the call's 15 digit reference number (shown if you hold the mouse pointer just to the right of the radio button that you click to retrieve the recording. Search for that wav file in the calls path to confirm that the recorded file exists.
3. Check connectivity and available bandwidth to the client PC.

Audio graph stops in mid call

This implies that the transfer of data from the Recorder to your client PC has been stopped or interrupted.

1. Request the same call again. There may have been a temporary network problem.
2. Request a different call. If the problem is only with one call, you may have a corrupt file on your hard disk.
3. Request the problem call from another PC on the same network. If the other PC can retrieve it successfully, assess the differences between the two client PCs; the problem is most likely at the client end.
4. Request the problem call from different sub-nets, ideally working closer to the recorder.
5. Request the call from the recorder server's own browser. If this works and the others don't, then the problem is likely to be in the network between server and clients.

Confidential and Proprietary Information

Audio graph appears but no sound

The audio file has reached the client PC successfully; the problem is most likely to be with the PC's multimedia setup or current settings.

1. Verify that the PC has a sound card.
2. Play a wav file through Media Player or similar application to verify that that the sound card is set up correctly.
3. Adjust any hardware volume and/or mute controls on the speakers/headphones.
4. Double-click on the icon in the system tray at the bottom right-hand corner of the screen to verify that the PC's software volume controls are not set to mute or very low.
5. Ensure you are not running any other programs that may be locking the sound card exclusively. If in doubt, shut down all other programs.
6. Try another similar PC. If that works, look for differences in the multimedia setup of the two PCs.

Replay Hangs Intermittently on Internet Explorer 8

Add the recorder to your Trusted Sites as described in [ActiveX Control Download](#) on page 173.

No New Recordings Playable

If you can replay old recordings but not newly made calls, there may be a problem with the recording and/or storage components of the system. Follow these steps:

1. On the **Recorder Status > Server** page of the Recorder's System Administration application, look at the counts for total calls recorded and calls recorded today.
2. Use Bulk recording mode to make a test recording.
3. Complete the recording and hang up.
4. Return to the **Recorder Status > Server** page and note the **Total media files recorded today** and **Total media files recorded to date**. These counts should have increased by at least one, the recording that you just made. If the counts have increased, the recorder is processing recordings. This is probably a search/replay problem. See earlier sections for help.

Note:

If these counts have not increased, the recording has not been successfully stored on the Recorder or inserted into the call details database. Do the following:

5. Look for alarm messages that indicate problems with the recording channel or with file read/write or rename functions. The error message should indicate whether disk space

Troubleshooting

or a directory access problem is the cause. Check that .wav files are appearing in the latest folder beneath the calls path as recordings are made.

6. Check disk space in all partitions. If any of these is 0 or less than 50MB, this may be the problem. Check for build up of log files. Check that the call details database hasn't exceeded the available space. Consider reducing the number of months of calls kept-use the purge settings on the **General Setup > Recorder** configuration page to adjust this.
7. Look for alarm messages that indicate licensing problems. The recorder will not process any new calls if you have changed the MAC address, tampered with license settings or are running on a time-expired license. In all cases, you should obtain a new license key.
8. Check that the Avaya Contact Recorder service is running.
9. Check for messages in the log files.
10. Reboot the server and watch for error messages on startup.

Poor Audio Quality on Telephone Replay

If the network configuration is correct and there are no problems with its function, the most likely cause of this problem is that the recorder or the network is overloaded.

To look for a problem on a managed network switch, you should look at the diagnostics and configuration details. You should see ZERO errors on all ports. Any port showing more than 1 packet error in 10,000 is suspect and must be looked at.

If the C-LAN, MedPro and/or recorder ports are failing to auto-sense full/half-duplex properly, you can force each port to either full or half duplex so as to reduce the error count to zero.

Note:

Even though a port may show an error rate of less than 1 in 100 packets, the error counts are deceptive. A single packet error can trigger a full/half duplex negotiation during which all packets are lost in the servers, but none of these show as errors on the switch.

If your error counts are zero on all ports, then we must also consider overload of the recorder as a possible cause. You should monitor the CPU load of the recorder during busy hours. Replay and live monitor are very sensitive to overload. Recording may be unaffected but if the CPU load is too high, audio quality on replay can suffer.

Similar problems have also been seen on multi-CPU AMD Opteron servers. This is caused by an unstable system clock, which is addressed in RedHat Version 5 update 4.

Confidential and Proprietary Information

Recording Problems

Partial recording problems

Since no hardware component in the system is dedicated to specific ports, any hardware problem is likely to affect all recordings equally. Therefore, if some calls are being recorded and are playable but others are not, the problem is probably in the configuration.

1. Recording Mode versus Recording Channel? Determine whether your problems relate to all channels of one or more recording modes or just to certain ports.
2. Check the configuration pages for the affected recording mode(s).
3. Calculate the range of stations carefully. For example, 11000 to 11010 is a range of 11 addresses, not 10.
4. Use the **Recorder Status > Ports** page to observe the ports on the recorder during your test calls. The ports should go from idle to active and back again.

Meeting Recording (Communication Manager only)

Cannot Enter Owners

The recorder requires **rtp-payload** signalling as described in [Configuring tone detection](#) on page 94 in order to interpret dialled digits. Check that both IP phones and Digital phones are configured for this signalling mode as IP phones will default to it whereas digital phones may not.

Bulk Recording (Communication Manager only)

Cannot Enter Delete or Retain Command

The recorder requires **rtp-payload** signalling as described in [Configuring tone detection](#) on page 94 in order to interpret dialled digits. Check that both IP phones and Digital phones are configured for this signalling mode as IP phones will default to it whereas digital phones may not.

Confidential and Proprietary Information

■ ■ ■ ■ ■ ■

Appendix C: Alarms

This appendix provides details of the alarms that can be raised by the system..

The main sections in this appendix are:

- [Alarms](#) on page 302
- [Alarms Table](#) on page 303

Alarms

The recorder may generate the following Alarm or Event notification messages. These events are:

- shown on the **Alarms > View Alarms** page
- sent in email messages as specified on the **System > Email Server** page
- reported via SNMP
- logged to the recorder's log file `acr.log`

Confidential and Proprietary Information

Alarms Table

Within messages, the strings XXX and YYY represent a specific parameter such as a station number, an IP address etc. The table shows both the English text of the message (that appears on the Alarms page) and the underlying resource string that appears in the log file.

Entries within the table are sorted according to the log file entry.

Severity	Log File Entry	English Alarm text	Comment	What to Do
Major	alarms.applyingconfig	Error applying configuration from master recorder: XXXX.		Note recent admin changes and submit details with log files from standby and master.
Major	alarms.archive.badlayout	Archive destination XXX cannot open layout YYY.	Layout name is set on Archive configuration.	Check this layout exists.
Major	alarms.archive.drive	Error accessing archive drive XXX. YYY.		Check the drive exists, is working and is not being used by any other application.
Major	alarms.archive.filter	Archive XXX filter incorrect. Can occur on upgrade. Check release notes and update layout details. Error: YYY.	Filter mechanism for archive changed in 12.0.	Bring this archive's Advanced settings in line with new Layout design.
Minor	alarms.archive.filterbad	One or more archive filters are invalid.		Check this Archive's advanced filter settings.
Minor	alarms.archive.filtererr	Error determining if recording XXX should be archived: YYY.	Probably SQL problems. Check log file for full detail.	Use search and replay to look at this call and apply same filter and layout as this archive destination has been told to use.
Major	alarms.archive.nolayout	Archive destination has no/bad layout.	Layout name is set on Archive configuration.	Check this layout exists.
Warning	alarms.archive.notreinserted	Newly initialized disk XXX has not been reinserted on YYY.	Deiced disk should automatically reinsert.	Push disk in manually. Replace drive with motorized one.

Alarms

Severity	Log File Entry	English Alarm text	Comment	What to Do
Warning	alarms.archive.old	Calls XXX hours old have not been archived (threshold is YYY hours).		Check archive and alarms pages for clues as to why the archive is backlogged.
Minor	alarms.autherr	Error processing authorization request for user XXX. Error: YYY.	Replay authorization request problem.	Depends on error shown.
Minor	alarms.call.notap	Cannot record call XXX. No suitable port available.		Provide additional capacity and/or tap points or (in the case of a deliberately partial trunk-side TDM recording system, suppress alarms on specific trunks using property file entries.
Major	alarms.callspath.invalid	Call storage path is invalid. Please change it under Settings > Server.	Separate partition preferred.	Set this to a valid path.
Major	alarms.cdb.blocked	Upload to XXX blocked due to YYY calls failing.	XXX is a central database (master or Standby or dedicated replay server).	Check that server's alarm pages.
Major	alarms.cdb.exception	Exception adding YYY to XXX.	YYY is a recording INum XXX is a central database (Master or Standby dedicated replay server).	Check the XML file for that recording for anything unusual about it.
Major	alarms.cdb.linkdown	link to central database at XXX DOWN. Reason: XXX.	XXX is IP address.	Check far end.
Info	alarms.cdb.linkup	Link to central database at XXX UP.	XXX is IP address.	Problem resolved.
Major	alarms.cdb.parse	Parsing xml file for XXX failed.	XXX is a recording INum.	Open the XML file for that recording in browser and notepad to determine error.
Major	alarms.cdb.unblocked	Upload to XXX resumed. Less than YYY calls failing.	XXX is a central database.	Problem resolved.
Minor	alarms.cdb.upload	Failed to upload call YYY to XXX.	Specific call YYY failed to upload to central database XXX.	Check the alarms pages on XXX and the log file on this server.

Confidential and Proprietary Information

Alarms Table

Severity	Log File Entry	English Alarm text	Comment	What to Do
Major	alarms.cmapi.down	Device, Media AND Call Control API not running on YYY. Reason: XXX.	Major failure of DMCC services.	Check connectivity to AE Server.
Major	alarms.cmapi.up	Device, Media AND Call Control API running on XXX.	DMCC services are restored.	No action required.
Major	alarms.core.nodatasource	No datasource configured for XXX.	WFO must be configured with datasources that match the name of the main switch and (if present) AACC.	Bring WFO datasource names in line with ACR.
Minor	alarms.crs.upload	Failed to upload details of recording XXX to central database. Response code YYY.	Applies to central replay server only not Viewer. YYY is standard HTTP response code.	Look up HTTP response code.
Major	alarms.cti.badinitialsend	IO Exception on initial transmission.	Could not transmit over the socket connection.	Check far end is listening. Check network connection is up.
Major	alarms.cti.cannotconnect	Cannot connect.	Could not establish a TCP/IP link.	Check address. Check server is up.
Major	alarms.cti.clientrelease	Link dropped by far end.		Check far end for problems or manual shutdown.
Warning	alarms.cti.configchanged	CTI Configuration changed. Dropping previous connection.	System is responding to change in configuration.	Nothing.
Major	alarms.cti.connfailed	Connection failed.	An established link has been dropped.	Check for neighboring events at each end of the connection.
Major	alarms.cti.error	Link to CTI on XXX reporting error: YYY.	A problem occurred between the recorder and the Avaya Contact Center server.	Depends on error YYY reported.
Major	alarms.cti.heartbeatfailed	CTI link failed. Heartbeat lost.	No activity on the link for an unacceptable period.	Check network connectivity. Check health of component at far end.
Minor	alarms.cti.invalidcallid	Invalid call id: XXX.		Check CTI link configuration. Check switch patch levels.

Confidential and Proprietary Information

Alarms

Severity	Log File Entry	English Alarm text	Comment	What to Do
Major	alarms.cti.invalidparams	Invalid CTI Address: XXX.	You have not specified an address for the Avaya Contact Center server. (CS 1000).	Enter a valid address on the General Setup > Contact Center Interface page.
Major	alarms.cti.ioexception	IO Exception.	A socket error occurred on the link.	Check network integrity.
Info	alarms.cti.providerok	CTI Services on XXX UP.	Connection to CTI link server has been established.	Check earlier error message to determine why link failed earlier.
Major	alarms.cti.shutdown	Service shut down.	The link has been shut down.	If not planned, check for reasons preceding this in the event log.
Warning	alarms.cti.slowresponse	Slow response from CTI link. CN XXX reg/unreg took YYYms.	Registration or unregistration of an address took longer than expected.	Check the recorder is not overloaded. Check the MLS link is not overloaded.
Major	alarms.cti.timeout	Connection timed out. Far end not responding.	The component specified has not responded; has not connected or reconnected within the expected time.	Check the network connectivity and the state of the component specified.
Major	alarms.dapi.aesvcsconfig	Cannot use CallInformationServices. Please check AES.	See AE Server manuals.	
Major	alarms.database.cannotinsert	Cannot insert details of recording XXX into database.		Check disk space on the partition holding the call details database.
Major or Minor	alarms.database.migration	Error migrating database: XXX YYY.	Severity varies according to nature of problem.	Retain backup of database made before upgrade. Take backup of database now. Contact Avaya.
Major	alarms.dialer.key	Dialer(s) configured but not licensed.		Obtain and enter valid license key.
Major	alarms.dialer.linkdown	Dialer XXX link DOWN. Reason: YYY.	XXX is name of dialer.	Check dialer end and network.
Major	alarms.dialer.linkup	Dialer XXX link UP.	XXX is name of dialer.	Problem resolved.
Major	alarms.dialer.noclassname	Class name not defined.		Correct dialer class name in properties file.

Confidential and Proprietary Information

Severity	Log File Entry	English Alarm text	Comment	What to Do
Major	alarms.disk.full	Disk full on partition 'XXX'.	'Check log files. If calls partition, check for files that cannot be purged.	Delete some files to make space.
Major	alarms.disk.notarchived	Recordings from XXX to YYY were purged from disk buffer but had not all been archived.		Provide more disk space. Check what is using up space.
Major	alarms.disk.purging	Disk buffer nearly full. Purging recordings regardless of required retention period.		Provide more disk space. Check what is using up space.
Warning	alarms.disknearlyfull	Disk nearly full on partition 'XXX'. Only YYY MB free.	Check log files. If calls partition, check for files that cannot be purged.	Delete some files to make space.
Minor	alarms.dn.notobservable	Cannot observe DN/Position ID XXX. CTI Cause Code YYY.	The recorder was not able to register for CTI events on the address shown.	CS 1000: Check the AST flag is set on the DN/Position ID. Check that the Meridian1 Machine name and number are correctly set. Check the MLS specification for specific cause codes.
Minor	alarms.dn.regdropped	Observation of DN/Position ID XXX dropped.	The recorder is no longer receiving CTI events for the position ID shown.	CS 1000: Check that the AST flag has not been removed. Check the MLS specification for meaning of each cause code.
Minor	alarms.dn.startrec	Recording Start failed on DN/TN XXX. Cause Code (hex): YYY.	Could not start Duplicate Media Streaming.	Check the specific cause code against MLS specifications.
Warning	alarms.dn.starttimeout	Timeout on recording start on DN XXX TN YYY.	Did not receive prompt confirmation of Duplicate Media Streaming stopping.	Check recorder is not overloaded. Check CTI is not overloaded. Check network connectivity.
Minor	alarms.dn.stopnotif	Recording stopped on DN/TN XXX. Reason Code (hex): YYY.	Duplicate Media Streaming stopped unexpectedly.	Check the specific cause code against the MLS specification.
Minor	alarms.dn.stoprec	Recording Stop failed on DN/TN XXX. Cause Code (hex): YYY.	Failed to stop Duplicate Media streaming.	Check the specific cause code against the MLS specifications.

Confidential and Proprietary Information

Alarms

Severity	Log File Entry	English Alarm text	Comment	What to Do
Warning	alarms.dn.stoptimeout	Timeout on recording stop on DN XXX TN YYY.		Check recorder is not overloaded. Check MLS is not overloaded. Check network connectivity.
Major	alarms.emc.notavailable	EMC Archive XXX not usable. Error: YYY.		Check configuration if it has never worked. Otherwise, check EMC Centera file store is available.
Minor	alarms.file.compressfailed	Failed to compress audio file for recording XXX. Reason YYY.		Depends on reason.
Major	alarms.file.copyfail	Failed to copy file XXX.		Check disk space, path, security.
Major	alarms.file.copyretry	Retrying file copy of XXX.		No action required.
Minor	alarms.file.deletefailed	Failed to delete file XXX. Reason: YYY.		Depends on reason.
Major	alarms.file.iocopyfail	Failed to copy file XXX. I/O Error: YYY.		Depends on reason.
Warning	alarms.file.notindb	XXX recordings up to and including YYY were not stored to database on last shutdown.	Implies last shutdown was not "clean".	Shut down service rather than kill.
Minor	alarms.file.wavwritefail	Failed to write file XXX.wav. I/O Error: YYY.		Depends on reason.
Major	alarms.file.xmlwritefail	Failed to write XML file XXX. Reason: YYY.		Depends on reason.
Major	alarms.jobthread.stalled	Job thread stalled. XXX.	XXX is the name of the job thread	Should be neighboring alarm giving more detail.
Major	alarms.license.channelcnt	Licensed bulk recording capacity reached. Cannot record call on XX.	Cannot record a call on the address shown. The recorder is already operating at its maximum licensed capacity.	Purchase and/or install additional capacity.
Minor	alarms.license.quality	Quality Monitoring agent station license exceeded. Cannot record XXX.	You have attempted to record more agent stations than your license permits.	Increase licensed capacity.

Confidential and Proprietary Information

Severity	Log File Entry	English Alarm text	Comment	What to Do
Minor	alarms.lockadvisor	Failed to advise server of XXX. Response code YYY.	Lock or unlock not passed to other server.	Check other server is available and network path is good.
Major	alarms.lockfailed	Failed to lock recording XXX. Reason: YYY.	A call has not been locked as requested.	Depends on reason.
Warning	alarms.lockinconsistency	Inconsistency in locked call information affecting XXX recordings.	May indicate attempts to tamper with recordings.	Report security concerns.
Warning	alarms.lockpurgeneeded	Lock directory contains XXX unlocked recording files. Use maintenance page to purge.	Nightly check of lock folder detects that calls are now unlocked and can be purged.	Purge as instructed.
Info	alarms.logpurge	Purged XXXKB of old log files. Now YYYMB free.	Nightly message.	No action required if received. If not received, check recorder is running.
Major	alarms.node.overflow	Call failed to record XXX due to overload on recorder YYY.		Rebalance load or add capacity.
Info	alarms.node.portsavailable	XXX or more ports available on recorder YYY.		Problem resolved.
Major	alarms.node.portslow	Less than XXX ports available on recorder YYY.		Rebalance load or add capacity.
Minor	alarms.props.obsolete	Properties file contains a setting for XXX. This is no longer set via the properties file. The value found when upgrading has been migrated to the administration settings. This item should now be removed from the properties file to avoid later confusion.		Remove this property.
Major	alarms.queue.acceptable	XXX Job Queue backlog reduced to acceptable level. Currently YYYms.		No action required.
Major	alarms.queue.copy	Failed to copy to XXX. Reason:YYY. NOTE: Further errors with the same root cause on the same path will only show here once every 24 hours. Check the log file if in doubt.	Will cache files until problem is resolved then copy all outstanding.	Determine why recorder cannot write to the share.

Confidential and Proprietary Information

Alarms

Severity	Log File Entry	English Alarm text	Comment	What to Do
Warning	alarms.queue.slowjob	XXX Job Queue individual slow job - took YYYms.	This activity took longer than expected.	May occur under startup conditions. If occurring later, check recorder is not overloaded.
Warning	alarms.queue.tooslow	XXX Job Queue backlogged. Delay currently YYYms but may go higher.	The recorder cannot process these jobs as quickly as it should.	May occur under startup conditions. If occurring later, check recorder is not overloaded.
Minor	alarms.recfailed	Recording XXX failed. Reason: YYY.		Depends on reason.
Major	alarms.remoteids.serversocket	Error on server socket port XXX. YYY.	YYY is another Avaya Contact Recorder.	Check alarms on server YYY.
Major	alarms.replayapi.redirect	HTTP not allowed. XXX should be configured to use HTTPS.		Use the https url instead.
Major	alarms.rtp.misc	Error on RTP: XXX Parameters: YYY.		Check network.
Major	alarms.rtp.nopackets	No audio packets received on call from XXX. Call failed or no network path to recorder.	See Avaya support site re PSN #345U - TN570C and TN570D Expansion Interface boards log chronic fiber alarms.	Check TN570 boards are correct vintage. (Communication Manager). Check network paths from phones to recorder (CS1000).
Major	alarms.sfi.certmissing	The Key Manager client side certificate file is missing.		Supply the file.
Major	alarms.sfi.initfailed	Key Manager initialization failed. Reason: XXX.		Depends on reason.
Major	alarms.sfi.kmsdown	Key Manager unreachable. Reason: XXX.		Check KMS server and network.
Major	alarms.sfi.needboth	Both Key Manager parameters must be specified.		Enter the missing parameter.
Major	alarms.sfi.needunlimited	Key Manager parameters are specified, but the Unlimited Strength Policy files are not installed.		Install unlimited strength policy files.
Major	alarms.softphone.beepstart	Port XXX. Failed to start beeptone. Reason: YYY.	Internal error.	Report problem.

Confidential and Proprietary Information

Severity	Log File Entry	English Alarm text	Comment	What to Do
Major	alarms.softphone.beepstop	Port XXX. Failed to stop beep tone. Reason: YYY.	Internal error.	Report problem.
Major	alarms.softphone.buttonlookup	Port XXX. Error looking up button Id. Reason: YYY.	Softphone misconfigured.	Check softphone configuration is as per installation section.
Major	alarms.softphone.buttonmissing	Port XXX. Unusable as button YYY is missing from softphone.	Softphone misconfigured.	Check softphone configuration is as per installation section.
Major	alarms.softphone.callstopped	Port XXX. Call dropped as it exceeded maximum permitted duration.	Recording port has been active for several hours.	Consider setting recording mode to release call on dropping to one other party.
Major	alarms.softphone.endrecfailed	Port XXX. Error ending recording. Reason: YYY.	Internal error.	Report Problem.
Major	alarms.softphone.hookswitch	Port XXX. Error setting hook switch. Reason: YYY.	Internal error.	Report Problem.
Major	alarms.softphone.inservice	Port XXX restored.		No action required.
Major	alarms.softphone.nullpointer	Port XXX. DMCC event 'YYY' fired with null pointer.	Internal DMCC error related to a particular recorder port.	Report occurrences with a copy of your log files.
Minor	alarms.softphone.outofservice	Port XXX out of service.	Should recover within a few seconds.	Depends on reason shown before this alarm.
Major	alarms.softphone.ownerreg	Port XXX. Error unregistering owner. Reason: YYY.	Internal error.	Report Problem.
Major	alarms.softphone.play	Port XXX. Error playing file. Reason: YYY.		Depends on reason shown.
Minor	alarms.softphone.processfailed	Error processing file XXX. Reason YYY.		Depends on reason shown.
Major	alarms.softphone.recordstartfailed	Port XXX. Failed to enable recording. Reason: YYY.		Depends on reason shown.
Major	alarms.softphone.recordtime out	Port XXX. Recording failed to start. Resetting port.		Depends on reason shown.
Major	alarms.softphone.registration failed	Port XXX Registration failed. Reason: YYY.		Depends on reason shown.
Major	alarms.softphone.regtimeout	Port XXX. Registration timed out.		Check connectivity to AE Server.

Confidential and Proprietary Information

Alarms

Severity	Log File Entry	English Alarm text	Comment	What to Do
Major	alarms.softphone.rtpthread	Port XXX. RTP handler failed. Reason: YYY.		Depends on reason shown.
Major	alarms.softphone.setuprecording	Port XXX. Error setting up recording. Reason YYY.		Depends on reason shown.
Warning	alarms.softphone.shortpacket	Port XXX. VoIP packet interval of YYYms less than recommended 60ms.	Default settings of 20 or 30ms are not efficient for recording.	Configure codec set and network region as per installation instructions.
Major	alarms.softphone.sscdropped	Port XXX. Single-step conference dropped unexpectedly while in state YYY.		Report problem if more than very occasional occurrences.
Major	alarms.softphone.sscfailed	Port XXX. Single-step conference failed despite multiple retries.		Consider increasing number of retries.
Major	alarms.softphone.ssctimeout	Port XXX. Single-step conference setup timed out. Trying to conference in to YYY.		Check system loading.
Major	alarms.softphone.startrecfailed	Port XXX. Recording failed to start. Reason: YYY.		Depends on reason shown.
Major	alarms.softphone.stopplaying	Port XXX. Error stopping file playing. Reason: YYY.		Depends on reason shown.
Major	alarms.softphone.stoprecordfailed	Port XXX. Error disabling recording. Reason: YYY.		Depends on reason shown.
Major	alarms.softphone.timedout	Port XXX. Timed out when in state YYY.		Report if more than very occasional occurrences.
Major	alarms.softphone.ttd	Port XXX. Failed to set up touch tone detect. Check you have OUT_BAND signalling configured. Failure Reason: YYY.		Configure signaling in accordance with installation instructions.
Warning	alarms.softphone.userreset	Port XXX. User 'YYY' reset the port.	Also logged to audit trail.	No action required.
Major	alarms.standby.invalidstns	Invalid Station list "YYY" received from master for station pool "XXX".	Internal error.	Report problem.
Major	alarms.standby.noswitch	No link to Communication Manager, All ports have failed.		Check AE server is up.

Confidential and Proprietary Information

Severity	Log File Entry	English Alarm text	Comment	What to Do
Major	alarms.standby.notlicensed	A Standby recorder is attempting to connect but this server is not licensed to support backup channels. Apply new license and restart server.		Enter a license allowing backup channels.
Major	alarms.standby.notviable	Recorder fatal error:XXXX.	The recorder has detected a major problem that means it cannot record.	Check the alarms preceding this one for the root cause of the problem
Major	alarms.standby.primarynotok	Master recorder requests that Standby(s) take over.	The master Avaya Contact Recorder has decided that it cannot record and requests that the standby recorder should take control.	Check the alarms preceding this one for the root cause of the problem. This may be that a disk partition is full or the recorder cannot communicate with the CTI link.
Major	alarms.switchchanged	Switch type changed to XXX. Restart required.	Master configuration has changed and been copied to standby.	Restart server
Major	alarms.syslog	Cannot create syslog appender to host XXX. Error: YYY.		Check configuration and/or route to host according to error shown.
Major	alarms.timesynch	Clock synchronization error. XXX is YYYYms adrift from this server.	Another ACR server's clock does not agree with this one's - by more than 5 seconds.	You MUST time synch all ACR servers (and any others they interact with) to real time via NTP.
Major	alarms.tsapi.backlogcleared	Single-step Conference Queue Backlogged. Flushing.	Queue of requests is too long.	Check system loading and increase capacity if needed.
Major	alarms.tsapi.backlogged	Single-step Conference Backlog Cleared.	Queue of requests now acceptable length.	No action required.
Warning	alarms.tsapi.conffailed	Single-step Conference Failed: XXX.	Very occasional failures are nothing to be concerned about. Regular failures should be reported.	Increase number of retries in properties file. Check for latest versions of AES TSAPI.
Major	alarms.tsapi.configchanged	AES TSAPI Configuration changed. Dropping previous connection.	User changed configuration details.	No action required.

Alarms

Severity	Log File Entry	English Alarm text	Comment	What to Do
Minor	alarms.tsapi.csta44	Single-step Conference failed on address XXX. CSTA Error 44. Check that no other AE Server is controlling this call.	Always means that another application is trying to control the call.	Stop using Follow the call options or stop the other application.
Major	alarms.tsapi.error	AES TSAPI Services on XXX reporting error: YYY.		Depends on error shown.
Major	alarms.tsapi.heartbeatfailed	AES TSAPI Services failed. Heartbeat lost.	System should attempt to restart TSAPI services automatically.	Report if recurring,
Major	alarms.tsapi.invalidparams	Invalid Service, username or password parameters for AES TSAPI: XXX.		Check all parameters.
Major	alarms.tsapi.invalidskill	Invalid Skill Group: XXX.		Check that this is a valid skill hunt group.
Major	alarms.tsapi.invalidvdn	Invalid VDN: XXX.		Check that this is a valid VDN.
Major	alarms.tsapi.notaskill	Not a valid skill group (or AES TSAPI cannot reach switch).		Check that this is a valid skill hunt group.
Major	alarms.tsapi.observationended	Observation ended.		Report problem.
Major	alarms.tsapi.observer	AES TSAPI Observation of XXX reports error:YYY.		Report problem.
Major	alarms.tsapi.outofservice	Out of Service.		Check AES TSAPI services.
Major	alarms.tsapi.overflow	Conferenced Recording Mode failed to record a call because all ports were busy.		Increase number of concurrent recordings allowed on Conferenced mode.
Major	alarms.tsapi.portsavailable	Conferenced Recording Mode now has XXX ports available.		No action required.
Warning	alarms.tsapi.portslow	Conferenced Recording Mode has less than XXX ports available.		Increase number of concurrent recordings allowed on Conferenced mode.
Major	alarms.tsapi.providerok	AES TSAPI Services on XXX UP.		No action required.

Confidential and Proprietary Information

Severity	Log File Entry	English Alarm text	Comment	What to Do
Major	alarms.tsapi.shutdown	Service shut down		Check AES TSAPI services.
Minor	alarms.unify.ioexception	File I/O error updating call details of XXX. Reason: YYY.		Depends on reason.
Minor	alarms.unify.parseexception	Parsing error updating call details of XXX. Reason: YYY.		Depends on reason.
Minor	alarms.unify.parseerror	Error parsing Unify/External control information. XXX is not a number.		Correct external controller command.
Major	alarms.url.badport	Invalid IP port number for recording mode: XXX, Set to: YYY.		No action required.
Major	alarms.url.general	Error on link to 'XXX': YYY.		Check connectivity.
Major	alarms.url.linkup	Link established with XXX server on 'YYY'		No action required.
Major	alarms.url.nourl	Ports are allocated to XXX recording but no url is set to communicate with the server.		Configure appropriate link's URL.
Major	alarms.url.socket	Error connecting to 'XXX'. YYY.	Problem connecting to other server.	Depends on reason shown. Typically network routing or security issues.
Major	alarms.url.unknownhost	Unknown host 'XXX' in url for YYY server.		Check network, address is correct; add to DNS or use numeric IP address.
Warning	alarms.vacuum	It is now XXX days since the last full database vacuum. The recorder will perform a full vacuum the next time it is restarted. This may take some time. To postpone this to the following reboot, clear the setting on the System Settings > Server page. You MUST restart the recorder and allow it to vacuum the database at least once every 240 days.		See text of message.
Major	err.alarmtag.exception	Error displaying alarm tag.	Internal error.	Report problem.

Alarms

Severity	Log File Entry	English Alarm text	Comment	What to Do
Major	err.alphas.invalidchar	Invalid character ('-') in a non-numeric string.		Correct the entry.
Major	err.alphas.toolong	Non-numeric list is too long. 10000 character maximum including commas.		Reduce the length of the entry.
Major	err.confighistory.recordsdeleted	One or more configuration history records have been deleted.		Do not trust config history or audit records.
Major	err.confighistory.tampered	One or more configuration history records have been altered.		Do not trust config history or audit records.
Major	err.cscmstatetag.exception	Error displaying state tag.	Internal error.	Report problem.
Major	err.database.purge	Error purging database. Reason: XXX.		Depends on reason shown.
Major	err.license.clocksetback	The system clock has been set back. Timed licence is invalid.		Obtain and enter a non-timed license.
Major	err.license.create	Error creating licence token object.	Internal error.	Report problem.
Major	err.mail.authentication	Authentication failed attempting to send e-mail.		Check email user and password entries.
Minor	err.mail.invalidaddress	Invalid email address: XXX.		Correct the address.
Minor	err.mail.send	Error sending e-mail.		Check all email account entries. Send a test email manually to verify settings.
Major	err.maxusagetag.exception	Error displaying peak usage details.	Internal error.	Report problem.
Major	err.mls.notconfigured	CTI Link not yet configured.	You have not yet provided the IP address of the Avaya Contact Center server.	Specify the address of the Avaya Contact Center server.
Major	err.portpool.nocurrent	No port pool specified.	Internal error.	Report problem.
Major	err.portpooltotaltag.exception	Error displaying port pool totals.	Internal error.	Report problem.
Major	err.settingstag.exception	Error in IterateSettingsTag.	Internal error.	Report problem.

Confidential and Proprietary Information

Severity	Log File Entry	English Alarm text	Comment	What to Do
Major	err.settingstag.invalid	Invalid settings group requested in IterateSettingsTag.	Internal error.	Report problem.
Major	err.settingstag.exception	Error in SettingTag.	Internal error.	Report problem.
Major	err.settingstag.invalidfield	Unrecognised field request in SettingTag.	Internal error.	Report problem.
Major	err.softphonestatetag.exception	Error showing port state details.	Internal error.	Report problem.
Major	err.stnpooltag.exception	Error in StnPoolTag.	Internal error.	Report problem.
Major	err.stnpooltag.invalid	Invalid station pool requested in StnPoolTag.	Internal error.	Report problem.
Major	err.stnrangetag.exception	Error displaying station range details.	Internal error.	Report problem.
Major	err.stnrangetag.invalidfield	Unrecognised field name in StnRangeTag.	Internal error	Report problem.
Warning	err.system.restart	System restarting.		No action required.
Info	err.system.shutdown	System shut down.		No action required.
Major	err.tags.license	Error displaying licence tag.	Internal error.	Report problem.
Major	err.tags.misc	Error displaying miscellaneous tag.	Internal error.	Report problem.
Major	err.tokenetag.exception	Error in TokenTag.	Internal error.	Report problem.
Major	err.tokenetag.invalid	No token set in TokenTag.	Internal error.	Report problem.
Major	err.tokenetag.invalidfield	Unrecognised field name in TokenTag.	Internal error.	Report problem.
Major	err.usertag.exception	Error in UserTag.	Internal error.	Report problem.
Major	errpage.label.badstuffhappened	An error has occurred:	Internal error.	Report problem.
Info	info.archive.errorcleared	Wrote to archive disk correctly.		No action required.
Info	info.archive.righdisk	Correct archive disk now inserted.	Now able to write to disk in drive.	No action required.
Info	info.core.datasources	Datasource XXX configured.	Configuration error has been corrected.	Nothing.
Info	info.dn.observed	CTI Monitor now established on XXX.		Problem resolved.
Info	info.emc.available	EMC Archive XXX available.	Previous error cleared.	Nothing.

Confidential and Proprietary Information

Alarms

Severity	Log File Entry	English Alarm text	Comment	What to Do
Info	info.jobthread.unstalled	Job thread XXX running OK.		Problem resolved.
Info	info.mail.sent	Mail sent successfully.		No action required.
Info	info.queue.copy	File copied successfully to XXX.		No action required.
Info	info.sfi.kmsup	Key Manager connection restored.		Problem resolved.
Info	info.standby.goingstandby	Standby recorder returning to idle.		No action required.
Info	info.standby.primaryok	Master recorder requests Standby(s) go idle.		No action required.
Info	info.standby.viable	Recorder fatal error resolved XXXX.		No action required unless another problem is highlighted.
Info	info.timesynch	Clock synchronization corrected. XXX is now YYYms adrift from this server.	Drift corrected.	Nothing.
Major	link.master.linkerr	Error on link to Slave recorder at XXX: YYY.		Check connectivity, check other node is up.
Major	link.primary.linkerr	Error on link to Standby recorder at XXX: YYY.		Check connectivity, check other node is up.
Major	standby.reason.connecttimeout	Initial connection timed out with XXX.		Check connectivity, check other node is up.
Major	standby.reason.inactivity	Heartbeat failure via XXX.		Check connectivity, check other node is up.
Major	standby.reason.noactivity	Heartbeat failure.		Check connectivity, check other node is up.
Major	standby.reason.primaryrequest	Instruction from Master Recorder.		No action required.
Major	standby.reason.reconnecttimeout	Connection dropped and reconnection timed out with XXX.		Check connectivity, check other node is up.
Major	standby.reason.timeout	Initial connection timed out.		Check connectivity, check other node is up.

Confidential and Proprietary Information

Alarms Table

Severity	Log File Entry	English Alarm text	Comment	What to Do
Info	stnrange.usage.nowarn	The pool of ports XXX has YYY or more port(s) available.		No action required.
Minor	stnrange.usage.warn	The pool of ports XXX has LESS THAN YYY port(s) available.		Consider allocating more ports to this mode.

Alarms

Confidential and Proprietary Information



Appendix D: External Control Interface

This appendix provides details of the external control protocol and associated Java class library.

The main sections in this appendix are:

- [Introduction](#) on page 322
- [Java API Toolkit](#) on page 324
- [TCP/IP Protocol Overview](#) on page 329
- [Examples](#) on page 333
- [TCP/IP Message Sequences](#) on page 335

Introduction

External applications can control or influence recording by using the Recorder Control Protocol. You may integrate directly to a TCP/IP socket interface using the protocol described or by using the Java package provided for this purpose. An example application that uses the Java interface is also provided for reference.

When to Use External Control

The recorder includes sophisticated CTI interfaces and recording control but there are still occasions when additional flexibility or further data tagging is required. You will require an "external controller" in the following cases:

Complex Recording Rules

If your "record/do not record" requirements are more complex than the administration interface supports. For example, if you wish to start and stop recording at specific points within a call.

Additional Tagging

If you need to "tag" recordings with details that are not normally provided by the recorder.

Hybrid Systems

If your telephone system is controlled by another application (e.g. Genesys) then it may be appropriate to control recording as a result of the events occurring on a CTI feed from that application. In such cases, you may need not only the external control protocol but also Verint's Integration Framework or Unify server. These can interpret a wide range of CTI feeds. This is beyond the scope of this document.

CAUTION

Note that CSAPI, along with the "Unify" or "NGA" interface on which it depends is deprecated as of ACR 12.0 and will not be supported beyond this release.

Confidential and Proprietary Information

This Appendix

The remaining sections of this appendix provide:

- a brief overview of the Java interface classes. For detailed information refer to the JavaDocs for this package
- an Overview of the underlying TCP/IP control protocol
- a reference guide for the message sequences exchanged between recorder and controller

Port Allocations (Communication Manager only)

On CS1000 systems, all interactions are with Bulk recording ports. When working with Communication Manager, you should use the external controller with ports in the following modes:

- Bulk - for single-step conference recording where the external controller needs to provide additional tagging or is splitting long recordings into segments (as needed with many auto-diallers). Do NOT use ports in this mode if you want to initiate recordings from the external controller. You must allow the ACR to establish conferences before sending TAG, STOP (and then subsequent START) commands. Do NOT send "START SSC:nnnn:" commands as these will conflict with the recorders allocation of ports to calls.
- On Demand - for single-step conference recording where the external controller is determining which calls are to be recorded. It can either instruct the recorder to establish a single-step conference; do so itself or support manual conferencing.

Master + Slave Systems (Communication Manager)

When used with Communication Manager, note that only bulk mode is supported on slave recorders. In this case, the only permitted uses of Unify/External controllers are:

- tagging calls
- splitting (and tagging) long calls (e.g. autodialler sessions) with STOP and subsequent START commands

You *cannot* use the external controller to initiate single-step conference recordings (e.g. by sending in **START STN:nnn: SSC:mmm:** commands) as this will conflict with the Master's port allocation algorithms.

Connect Unify/External controller to the Master (and Standby if present) only. Do *NOT* connect Unify to the Slaves.

Confidential and Proprietary Information

Java API Toolkit

Rather than write directly to the socket level interface described below, you may use the Java language API provided. This contains the following components:

Packages	
com.swhh.cti.csapi.lang	Provides a high-level API for controlling the recorder.
com.swhh.cti.csapi.msg	Provides Recorder Control Protocol message classes and interfaces as well as classes that implement the <code>java.io.Reader</code> interface for reading these messages from streams.
com.swhh.cti.csapi.service	Provides a low-level API for communication with the recorder.
com.swhh.cti.csapi.tools	Contains two debugging tools as well as examples of applications that use the low-level API.
com.swhh.cti.csapi.ui	Contains a test harness with a graphical user interface that also serves as an example application built on top of the high-level API classes.

These classes and associated JavaDoc are provided on the distribution DVD, in the `sdk` folder as `acr-csapi.zip`. To view the JavaDoc without a Java IDE, unzip the contents and double-click `index.html` for a top-down view. For a comprehensive reference index, double-click `indexall.html`.

The content of the XML files produced in Bulk recording (previously known as "Conferenced mode") changed significantly between ACR 10.1 and 10.1SP2. The `RecordingData` and `RecordingParty` objects provided within the CSAPI toolkit are created by parsing the XML received from the recorder and hence have been affected by this change.

RecordingParty

In 10.1 and earlier, each party on a call was represented by the `RecordingParty` object - which had a (typically) numerical "number", optional alphanumeric "address" and, if an agent was logged on at the station or position, it ALSO had a numerical "agentId" and, optionally, alphanumeric "agentName".

In 10.1SP2 and beyond, the concept of "parties" has been changed. The station or position is still considered a party but the "agent" is now also promoted to a full party on the call. So

Confidential and Proprietary Information

instead of one party with number, name, agentid and agentname, there would be two parties, each with a (typically) numerical "address" and optional alphanumeric "description". Different types of parties are distinguished by their "partytypeid" field.

This does not map easily back to the existing RecordingParty object - but, as the primary use of this is to determine which agent or station is on a call, the following approach has been taken:

Each party that represents an Agent (whether CM, CS1K, AACC or Dialer agents) is mapped to a RecordingParty - but only the AgentId and (if available) AgentName fields are populated.

Any other party is mapped to a RecordingParty with "number" and, if available, "name" fields completed - but agentId and AgentName blank.

Therefore you CAN still:

1. Iterate through the parties looking at the AgentId field (getAgentId()) of each to determine the agent(s) on a call - so long as you code to expect null values there as well.
2. Iterate through the parties looking at the number field (getNumber()) of each to determine the station(s)/positions/DNson a call.

However, you CANNOT infer the agent on a particular station by looking within a single RecordingParty object. If you need to do this, then take advantage of the fact that the agent's RecordingParty (if there is one) will be the NEXT RecordingParty.

Summary

The table below shows which getter functions are available in 10.1SP2 - 12.0.

Method	10.1 and earlier	10.1SP2 - 12.0	Notes
getNumber()	Y	partial	Only present on station parties, not present on agent parties
getName()	Y	Partial	
getAgentID()	Y	partial	Only present on agent parties, which, if present follow the station party on which the agent is logged on.
getAgentName()	Y	Y	
getStartTime()	N/A	N	Was never really used.
getEndTime()	N/A	N	Was never really used and not present till end of call anyway.

External Control Interface

Method	10.1 and earlier	10.1SP2 - 12.0	Notes
getDuration()	N/A	N	Was never really used and not present till end of call anyway.
getNameNumber()	Y	Y	Works where number and name are present (i.e. not in agent parties)
getAgentNameNumber()	Y	Y	Works where agentid and name are present (i.e. only in agent parties)
All setters, merge() and constructors			Could (and still can) be called but doesn't achieve anything as RecordingParty only ever read from, not written to recorder.

RecordingData

The table below shows which getter functions are available in 10.1SP2 - 12.0.

Method	To 10.1	10.1SP2 - 12.0	Notes
getINum()	N/A	N/A	No reason to call this as it is always the same as the INum parameter that is already provided with the event to which this RecordingData relates.
numOwners()	Y	Y	
getOwners()	Y	Y	
getFirstOwner()	Y	Y	
geetParties()	Y	Y	But see changes to RecordingParty
getStartTime()	N/A/	N/A	Should be same as real time anyway
getEndTime()	N/A	N/A	Not present during call anyway

Confidential and Proprietary Information

Method	To 10.1	10.1SP2 - 12.0	Notes
getDuration()	N/A	N/A	Not present during call anyway
isNoStart()	Y	Y	Very rarely used.
isNoEnd()	Y	Y	Very rarely used.
getRecordingType()	Y	N	Can only be "bulk" now unless CM recorder configured for OnDemand with Unify controlling recording - in which case it would only be "ondemand". If you really need to use a mixed system, configure it to know which STN or DN/TN is in which recording mode.
getRecordingTypeEnum()	Y	N	As above
getServiceName()	Y	Y	Mapped from VDN or CDN as before.
getServiceNumber()	Y	Y	
getserviceNameNumber()	Y	Y	
getUniversalcallid()	Y	Y	No change
getCallDirection()	Y	N	Reports "Incoming" or "Outgoing" as before.
getCallDirectionEnum()	Y	Y	
getFileName()	Y	Y	Can be deduced from INum anyway
getCallinfo()	Y	N	Rarely of use - only where another Unify is adding tagging as well.
getUnifyData()	Y	N	Rarely of use - only where another Unify is adding tagging as well.
formatUCID()	Y	Y	Static helper function still available
All Setters including add Owner, addBackupOwner, addUnify data and constructors	N	N	Could (and still can) be called but doesn't achieve anything as RecordingData only ever read from, not written to recorder.

Confidential and Proprietary Information

Reconnection

Previously, if the connection to the recorder failed for any reason, it was difficult to connect again as the server socket was not closed down properly.

Now, there is a new method that lets you create the serverSocket yourself once e.g.

You can then create a new RecorderClient, call its accept(ServerSocket serverSocket) method and when that exits, do the same again e.g.

```
ServerSocket myserversocket = new ServerSocket(port);
while (!exitrequested) {
    RecorderClient client = new RecorderClient(...);
    client.accept(myserversocket);
}
```

Confidential and Proprietary Information

TCP/IP Protocol Overview

Connection Method

An external controller can drive the recorder via a TCP/IP socket using the protocol described below.

You configure the Master recorder with the IP address and socket number of the controller(s) to which it should connect. Connection defaults to port 1415 but you can specify an alternate port.

The recorder creates a socket and attempts to connect to each specified address. If it fails to connect, it will try again every 60s.

You can use multiple, independent controllers connected to a single recorder.

The controlling application should open and bind a server socket and accept incoming connection requests.

Enabling Control

By default, recording is under the control of the recorder and NOT external applications. To allow an external application to control recordings you must explicitly enable this using the Recording Control settings as described under [Recording Control](#) on page 153.

Persistence of Commands

This can be set so that external commands only persist for the current recording segment; for that phone's interaction with a call or for the call as a whole. See [Persistence of Commands](#) on page 247 for further discussion.

For the external controller to assume full control (beyond a single call boundary) for recording, it must send a FALLBACK OFF command for the station(s) it wishes to control.

Channel Identification

Most messages refer to a specific recording channel or port. The field or fields used vary according to switch type as described below.

Confidential and Proprietary Information

CS1000

Each recorder port or channel is referred to by Directory Number ("DN:nnnnn:") and by Terminal Number ("TN:mmmm").

Where "nnnnn" can be 1 to 7 digits long and may include leading zeroes. The Directory Number passed is that of the DN (or Position ID) being monitored by the recorder. The TN (1-5 digits) is that of the specific terminal on which this DN is present. Note that the TN value must be in decimal even though the CTI Monitors page shows these in hex format.

 **Important:**

This scheme allows recording of MARP/MADN multiple appearance DN's on CS 1000 IP media streaming phonesets in knowledge worker environments. See [Limitations](#) on page 31.

Communication Manager

Each station that has been configured for Bulk Recording is referred to by "station" number in a STN parameter:

`STN:nnnnn:.`

Where *nnnnn* can be 1 to 16 digits long and may include leading zeroes. External control should only be attempted where recording is targeted by station.

General Protocol Specification

Messages take the form:

```
<protocol version number> <command> (<command specific data>)\x1b'
```

When sending messages, follow these rules:

3. Transmit messages in ASCII 8-bit encoding. Wrap any 16-bit XML content in CDATA blocks.
4. All messages and responses are terminated with an escape character (27 / 0x1b).
5. Separate fields with space characters.
6. Enclose field contents in double quotation marks where the field needs to contain a space - as, for example, with filenames. Always enclose filenames in double-quotes.
7. Delimit sub-fields with colon characters ":".
8. Apart from HELLO messages (see below) and responses, all messages must be responded to in the form:

```
<protocol version number> <error code> <channel identifier>\x1b' <error qualifier> <additional info> '\x1b'
```

Confidential and Proprietary Information

Where

```
<error qualifier> is typically "DESC:xxxxxxx:"
```

and

```
<additional info> may be 0 or more instances of  
"PARAM:pppppp:"
```

A typical response to a successful command is therefore:

```
1 0 STN:nnn: \x1b
```

and a typical error response is

```
1 -1 STN:1234: DESC:"Invalid Parameter": PARAM:STN:\x1b
```

9. Ignore unexpected or malformed responses.

10. Send commands in uppercase, but test for them case insensitively.

XML Tagging

All tagging information is passed straight through the recorder into the XML file associated with the recording. The recorder only looks for an escape character to delimit each command. The intention is that the controlling application will pass through valid XML tags which the recorder will insert into the body of the call's XML file. These may include valid expansions of control and other characters (e.g. %20 etc). The entire xml string will be inserted between opening and closing "taglist" tags. For example, the command

```
1 TAG STN:1234: INUM:800369000000009: <spare1>some  
data</spare1><spare4>John Doe</spare4>\x1b
```

will result in call reference 800369000000009, which is currently being recorded on STN 1234 being tagged with the additional fields:

```
<taglist><spare1>some data</spare1><spare4>John  
Doe</spare4></taglist>
```

Basic Call Tagging (Communication Manager only)

When used with Communication Manager, recorder uses DMCC's CallInformationServices interface to tag recordings in all modes except Bulk (for which it uses AES TSAPI derived information). This imposes a load on the switch. If the external controller has access to all details about the call, there may be no need for the recorder to request these details itself.

External Control Interface

You can choose whether or not the recorder collects these details itself by setting property file entries as specified in the table below:

Port Type	Default	Override with this in prop	Comment
On Demand	On	ondemand.ocpneeded=false	
Meeting		meeting.ocpneeded=false	
Bulk	Not Applicable		Uses AES TSAPI info.
Quality	Not Applicable		Uses CTI events forwarded by ACR from TSAPI and (where present) dialers.

If the recorder is collecting call details itself, the external controller can ask to be advised whenever these change. Use the REQUEST ACTIVITY ON command to do so.

Fallback Mode

When a recorder starts, it automatically runs in locally controlled mode - where call events it detects cause it to start/stop recording. This is also known as "fallback" mode.

If the external controller only wishes to TAG calls with additional data, it may be happy to leave the ports in this mode. On the other hand, if it wishes to take control of the recording decisions then it must instruct the recorder to relinquish control of the ports it wants to use. It does this with the FALLBACK OFF command - either for a specific recorder port (STN or DN+TN) or for all ports.

If the heartbeat to the external controller that turned FALLBACK off is subsequently lost, the channel(s) will revert to fallback mode and recording will continue as if the controller had never been present.

Use the station specific command to take control of specific channels if you want to allow other channels to continue to be controlled by the recorder or if you are using multiple controllers, each of which manages its own set of channels.

Confidential and Proprietary Information

Examples

Typical examples of how to use an external controller are given below. You should read these in order as later examples refer back to earlier ones.

Third-party CTI Control

A bank using Genesys to route calls through an Avaya switch and wishes to record certain calls according to user defined data and events occurring within their call routing application.

In this case:

1. Configure a pool of On Demand ports - large enough for worst case concurrent recording need.
2. The controller establishes contact with the recorder (exchanges HELLO messages)
3. The controller notes the pool of ports that are ONLINE (and may alarm if there are too few)
4. When a call is to be recorded, the controller picks an available port and sends it a START message with SSC parameter specifying the station that is already on that call.
5. When recording is no longer required, the controller sends that port a HANGUP message,
6. Ports can only be reused for another call after they have hung up. The controller can send a HANGUP message to make this happen. Alternatively, if the call to which the port is connected terminates before it is told to hang up, the recorder sends a HUNGUP message to the controller. Note that some recording modes include an option to automatically terminate if the call drops to just one other party.
7. The recorder performs basic tagging itself but the controller sends Genesys user data through as TAG commands.

Should the controller fail, no recording will happen. For fault tolerance, use a pair of controllers and have one or the other send messages to the recorder.

For large systems or to make the system tolerant to recorder failure, use a pool of N+1 independent recorders.

Additional Call Tagging

User wants to tag each call with a customer identifier that is known to an in-house application. This knows the station handling the call and the customer on the call in real-time i.e. during the call.

In this case, the recorder will be configured for bulk recording.

1. Configure Bulk recording for all stations to be recorded.
2. The controller establishes contact with the recorder (exchanges HELLO messages)
3. The controller notes the stations that are ONLINE (and may alarm if any are missing)
4. Any time the controller receives a STARTED message, it looks up its current map of stations v customers and sends a TAG command to apply the appropriate customer identifier to the call.

Should the controller fail, the recorder continues to record as normal in Bulk mode but calls will not be tagged with customer id. A fault tolerant pair of controllers can be used if required.

For a system that is tolerant of recorder failure, use a Standby recorder. This will contact the controller when it takes over from the master.

TCP/IP Message Sequences

The table below shows all supported message sequences using Communication Manager style channel identification, such as "STN:1234". If using CS1000, replace this STN parameter with DN and TN parameters instead. For example: "DN:1234: TN:1001:"

Controlling Application Sends	Dirn	Recorder Sends	Comments
On recorder first establishing connection with controller's socket (default 1415)			
	<<<	2 HELLO ACRCapture NNNNNN	The controller can determine which recorder is which from the port that it connects on, its IP address or its serial number NNNNNN. When using Unify, the former method is normally used and hence each recorder should be configured to contact a different port number.
2 HELLO XXXXX	>>>		Where XXXXX is the application's name or other identifier. The recorder does not parse beyond "HELLO". The recorder writes the full message to the log file but does not act on the name given.
	<<<	1 ONLINE STN:nnnnn:	For each softphone configured and available, the recorder sends this message. This allows the controller to build a table of available stations and respond with 1 FALLBACK OFF STN:nnnnn: if it wishes to take control of that port.
Heartbeat messages			
1 PING			Record sends heartbeat
1 PINGACK			External controller responds
To take control of recording on all ports			
2 FALLBACK OFF	>>>		External controller must now enable/disable recording on this station.
	<<<	1 0	Confirmed
To relinquish control of recording on all ports			

External Control Interface

Controlling Application Sends	Dirn	Recorder Sends	Comments
2 FALLBACK ON	>>>		Recorder now controls stop/start on all ports in all modes
	<<<	1 0	Confirmed
To take control of recording on a specified station			
2 FALLBACK OFF STN:nnnn:	>>>		External controller must now enable/disable recording on this station.
	<<<	1 0 STN:nnnnn:	Confirmed
To relinquish control of recording on a specified station			
2 FALLBACK ON STN:nnnn:	>>>		Recorder now controls stop/start on this station.
	<<<	1 0 STN:nnnnn:	Confirmed
To activate additional notifications			
1 REQUEST ACTIVITY ON STN:nnnn:	>>>		The controller can ask that it is advised of call details in addition to basic started/stopped messages.
	<<<	1 0 STN:nnnnn:	Confirmed
Start Recording (optionally, in Communication Manager systems only, set up single-step conference)			
1 START STN:nnnnn: SSC:mmmm: <xml data> Note: SSC parameter is optional and only supported on Communication Manager.	>>>		Start recording on station specified (nnnn) and tag with optional data supplied. If SSC parameter is provided, the recorder will use TSAPI to request that the recorder's softphone (nnnnn) be single-step conferenced onto the call currently active on station (not agent or VDN) mmmm. Use this parameter with OnDemand, Conferenced and Unify (Conferenced) ports only. Failure to attempt to establish a connection (e.g. because the call terminated before connection could be established) is indicated by an error message with "NOSSC" in the description. Parameter 1 repeats the target address and Parameter 2 gives the error message.
	<<<	1 0 STN:nnnnn:	Confirmed

Confidential and Proprietary Information

Controlling Application Sends	Dirn	Recorder Sends	Comments
Stop Recording			
1 STOP STN:nnnnn: <xml data>	>>>		Stop recording on station specified and tag with optional data supplied. Note: This command does not cause softphone to hang up.
	<<<	1 0 STN:nnnnn:	Confirmed
External controller wishes to terminate single-step conference recording on known softphone (Communication Manager only)			
1 HANGUP STN:NNNN: <optional XML data>	>>>		Note that the STOP command simply stops recording – it does not cause the port to hang up. Hence an additional command is required where a DMCC port is conferenced into a call. This command instructs the specified station to hang up – implicitly terminating any current recording and, optionally, tagging it with the XML data provided. However, the recording state (enabled/disabled) of the softphone is NOT changed.
	<<<	1 0 STN:nnnnn:	Confirmed
On recording starting			
	<<<	1 STARTED STN:nnnn: INUM:nnnnnnnnn nnnnnn: <xml data>	Unify can note the INum to ensure subsequent tag commands go to the right segment even if that call has finished. Unify can also parse out the station number if it wants to check for orphaned records hanging around from this station which are obviously now in error. If ACTIVITY ON has been requested, then the full XML for the call is sent at the end of this message. (This is different from 10.0 and earlier. For backwards compatibility, set unify.xmlonstart=false . This will send an UPDATE message with the XML immediately after the STARTED instead.)

External Control Interface

Controlling Application Sends	Dirn	Recorder Sends	Comments
On recording stopping			
	<<<	1 STOPPED STN:nnnn: INUM:nnnnnnnnn nnnnnn:	We could drop the call if told to but we can't be sure it won't stop before then so maybe best to always report when call drops. Don't see any need to include tagging as we will not normally be getting any additional tagging beyond stn number.
On recording port hanging up (Communication Manager only)			
	<<<	1 HUNGUP STN:nnnn:	
On recording getting new or changed info (only if ACTIVITY ON previously requested for this port). NOT sent if this Unify caused the change by sending in a TAG command.			
	<<<	1 UPDATE STN:nnnn: INUM:nnnnnnnnn nnnnnn: <xml data>	Info available for call specified on station specified. Unify may need to interpret some of the xml to determine recording action. Will send all call info on each update so Unify can cache single string.
On Unify wanting to tag call			
1 TAG STN:nnnn: INUM:nnnnnnnnnnnnnnnn: <xml data>	>>>		This allows tagging to be sent for the current and previous calls on a channel. The recorder will use nnnnnnnnnnnnnnnn to determine whether the tagging is for the current call or the previous one. In the latter case, it will open the XML file and append the details given.
	<<<	1 0 STN:nnnnn:	Confirmed
Call Break – Unify initiated			
1 BREAK STN:nnnn: <xml data>	>>>		Recorder breaks the call seamlessly. The optional tag data is applied to the stopped call. Send further TAG command to tag new call. Noend and nostart fields are set true on the old and new calls as per MediaStore.
	<<<	1 0 STN:nnnnn:	Confirmed

Confidential and Proprietary Information

Controlling Application Sends	Dirn	Recorder Sends	Comments
	<<<	1 STOPPED STN:nnnn: INUM:nnnnnnnnn nnnnnn:	
	<<<	1 STARTED STN:nnnn: INUM:nnnnnnnnn nnnnnn:	Same STN but different INum
Call Break at recorder due to max segment duration exceeded			
	<<<	1 STOPPED STN:nnnn: INUM:nnnnnnnnn nnnnnn:	
	<<<	1 STARTED STN:nnnn: INUM:nnnnnnnnn nnnnnn:	Same STN but different INum
	<<<	1 UPDATE STN:nnnn: INUM:nnnnnnnnn nnnnnn: <xml data>	Only sent if ACTIVITY ON previously requested. Unify can identify this as a broken call from the "nostart" field being "true". Unify tagged data will have been rolled over from previous call and included in this call's data already.
Call Masking			
<p>Note: The properties file setting rec.maskallowed must be set to true for this feature to be enabled. PAUSE remains in effect until RESUME is sent or the recorder automatically resumes. When this happens depends on the persistence mode being used. See Persistence of Commands on page 247 for more details.</p> <p>In addition to disconnects; STOP commands etc, a duplicate media stream recording segment always ends whenever a call is placed on hold by a recorded party (which may be either party on the call for internal calls).</p> <p>If a call is placed on hold by an internal party that is NOT being recorded:</p> <ul style="list-style-type: none"> - A TDM recording is not broken - so the masking will persist even in "segment" persistence mode. - An IP recording is broken but only if the call is placed on hold for more than 2 seconds. <p>If the CTI application sending PAUSE/RESUME is aware of far end hold via its CTI events, then it should send a PAUSE or RESUME command as required.</p>			

External Control Interface

Controlling Application Sends	Dirn	Recorder Sends	Comments
3 PAUSE STN:nnnn:	>>>		Instructs the recorder to begin 'masking'. The recorder continues to record, but replaces the real audio with a fixed tone pattern and blanks any screen recordings in progress. This is useful for portions of conversations that are confidential.
	<<<	1 0 STN:nnnn:	Confirmed
	<<<	3 PAUSED STN:nnnn:	
3 RESUME STN:nnnn:	>>>		Instructs the recorder to revert to normal recording of the real audio.
	<<<	1 0 STN:nnnn:	Confirmed
	<<<	3 RESUMED STN:nnnn:	
On shutdown			
1 BYE <reason>	>>>		<reason> can be 1. FALLBACK – recorder should continue to answer calls and record (though in most cases, no calls will appear unless Unify is sending them to the recorder's stations). Without knowing the mappings in Unify, it is not as easy to drop into a fallback mode – unless station numbers are also configured somewhere. 2. SHUTDOWN – recorder will stop recording on Unify controlled ports. Allows "busing out".
	<<<	1 BYE <extra info> message	
On channel error			
	<<<	1 ERROR STN:nnnn:	Softphone unusable e.g. cannot register. In AUTO-ANSWER mode, Unify should mark this port faulty and not attempt to use. Hopefully, an ONLINE message will follow shortly as the recorder re-registers the port. Unify should probably be written to recognise faulty behaviour too e.g. if it doesn't get STARTED from softphone it tried to place a recording on, it needs to report this and busy out the faulty one?

Confidential and Proprietary Information

Controlling Application Sends	Dirn	Recorder Sends	Comments
On channel being restored			
	<<<	1 ONLINE STN:nnnn:	Softphone available

Confidential and Proprietary Information

■ ■ ■ ■ ■ ■

Appendix E: Fault Tolerant Systems

In addition to using fault tolerant components within servers as described in [High Availability Systems](#) on page 83, recording systems can be made tolerant of many server and network failure conditions. This appendix details how such systems are designed and configured, how they handle failures and how to upgrade them. This Appendix assumes that the reader is already familiar with design, installation and operation of single server recording systems as described in the body of this manual.

The main sections in this appendix are:

- [Redundant SAN](#) on page 344
- [Duplicated recording \(Communication Manager only\)](#) on page 345
- [Standby Recorder Options](#) on page 346
- [Mode of operation](#) on page 356
- [Standby Recorder Configuration](#) on page 361

Redundant SAN

If you already have a fault tolerant storage network in place, you can assign the calls storage path to an area of this storage system. This is supported for locally connected drives - NOT for Network Attached Storage (NAS).

You are then reliant on the mirroring or other redundancy and standby mechanisms associated with the storage network. These mechanisms typically include a tape library backup and might include hierarchical file storage (HFS), in which older files are replaced by small tokens that allow the system to retrieve the original content from the tape library.

The recorder runs successfully with Tivoli Storage Manager and might also support other similar systems. However, Avaya does not proactively test against these systems. Connect to them at your own risk. If you want to use such a system, turn the recorder's own disk management function off. To do this, add the line `disk.manager=false` to the properties file. This stops the recorder from deleting the oldest files as the available disk capacity falls to 1GB. You must then ensure that the available space on the disk holding the calls directory does not fall below 1GB.

Confidential and Proprietary Information

Duplicated recording (Communication Manager only)

Where recording is controlled by an external application (such as Unify) establishing conference calls onto the recorder's ports, a fault tolerant system can be deployed by using two totally independent recorders and establishing 4-way, instead of 3-way conferences.

By conferencing in one port from each of the two recorders, a fully redundant recording system can be delivered. Alternatively, completely independent recorder systems can be installed using duplicated TDM taps or passive IP taps.

 **WARNING:**

Although the recorders are running in parallel, you must also ensure that the mechanism that is establishing the conferences is, itself, fault tolerant. This may imply duplicated Unify servers and/or duplicated CTI feeds. The default behavior of recorders is to fall back into basic recording mode (where possible) should connectivity to Unify be broken. This often suffices as an acceptable failure mode.

You must ensure that the mechanism that establishes the conferences can handle the error condition that occurs when one of the recorders fails. It must establish the other conference party to the remaining, good recorder rather than fail totally.

Note:

A parallel recording system inevitably requires twice the VoIP resources. This option is, therefore, an expensive one.

 **WARNING:**

The overall maximum of 6 parties on a conference might become a constraint if two of these are recording ports. Call scenarios in which two calls merge (transfer and conferencing) - and where each of these is already a 4 party call due to duplicated recording can exceed these limits and are not supported. To avoid this, recording ports are removed from a call as soon as it goes on hold. In this way there are less parties present on the call when it later merges with a consultation call. (Note that this cannot be done with the "Follow the call" recording option as otherwise the call may be lost from the recorder's sight.)

Standby Recorder Options

You can configure additional Avaya Contact Recorders to act as standby to a master recorder. The recording capacity provided by the standby is available and is used by the master in the same way as that of a slave recorder but these can also take over the control of recording should the master fail. These would normally be in "standby" mode and only become "active" when they detect the failure of the master they are shadowing. On Communication Manager systems (only), where you have multiple sites, you can use multiple standby recorders. Each standby can back up a specified master or a specific subset of a master recorder's configuration.

This section describes:

- Prerequisites for high availability
- Standby recorder licensing
- Known limitations
- Supported fall back scenarios
- Supported failure modes
- Mode of operation
- The impact of a switch-over
- Restoration of a master recorder once it has been repaired
- Upgrade procedures specific to master / standby topologies
- A summary comparison with hardware switch-over units
- Supported Master/Standby Topologies

Prerequisites for high availability

To get maximum benefit from a standby recorder topology, you must adopt the appropriate elements of an overall strategy for high availability:

Centralized database and replay

Although the standby unit(s) can work without a centralized database, you need one or more of these to provide a seamless, single point of access to all recordings. Without them, those recordings made on a standby recorder are only accessible by accessing the url of that recorder. With the central database, all recordings made on any of the recorders, including the standby(s), are consolidated into a single, searchable pool.

Confidential and Proprietary Information

Fault tolerant storage

Both master and standby recorders must be configured with RAID1 or (preferably) RAID 5 arrays or be using a fault tolerant SAN on which recordings are kept. Using standby recording provides fault tolerant recording. However, it does not itself provide for fault tolerant STORAGE of recordings.

Off-site archive

It is also assumed that, where DVD+RW or Blu-ray disks are written, that these will be stored away from the recorders, ideally in a separate building for maximum protection. Should these be needed for regular access, a copy should be made and kept off-site. Unless the fault tolerant disk system is spread across multiple buildings, off-site storage of archive media is essential.

Fault tolerant network connectivity

Where centrally located master and standby recorders are co-located or are in disaster recovery sites with fault tolerant connections between them, it is critical that the master and standby recorders are connected by way of a fully fault tolerant network topology. Failure of any one networking component (NIC, cable, Ethernet switch or router) between them must not result in connectivity being lost between them. Each standby recorder assumes that failure to communicate with the master indicates that the master has failed. It will therefore attempt to take over from it. If this is not the case, then the two recorders will clash as they attempt to use the same softphone numbers on the switch. You must provide a fault tolerant network path including bonded NICs with independent network paths between primary and standby as described in [Bonded or Teamed NICs](#) on page 109.

In the case of Communication Manager based systems, where remotely sited standby recorders are provided so as to record should the remote site lose connectivity with the center and fall back to ESS mode, you should ensure that the remote standby is connected to the master recorder over the same network path that the Avaya components use. This ensures that it will lose contact with the center - and hence become active - should the site fall into ESS mode.

Location of recorders

Where possible, you should locate the standby recorder(s) in a different building from the master recorders. You should also provide diverse network routing between the recorders and the Avaya switch components that they interact with.

One additional Media Processing Resource per Media Gateway

In Communication Manager based systems using DMCC recording, you must provide one additional media processor per Media Gateway to ensure that failure of a single card does not impact the ability of a recorder to record at its configured capacity.

Confidential and Proprietary Information

Standby recorder licensing

To use one or more Standby recorders, your master license key must include the appropriate number of backup channels. On the licensing page, a standby is assigned a recorder number and given the IP address of the Master recorder.

When you configure a recorder as a standby unit, you must subsequently stop and restart the recorder in order for it to take notice of this setting.

In laboratory conditions, when switching between master and standby licenses, a restart is required.

Configuration Options

When a standby recorder is asked to "go active" (or determines for itself that it should), it can act in one of three ways.

Automatic Full Shadowing

The default is to take over the entire role of the master it has been connected to. The configuration of the master is automatically downloaded to it.

Automatic Partitioned Shadowing

Against each set of recording targets, you can specify an **Advanced** setting that designates one or more recorders (by serial number) and/or pools of recorders (by poolname). Recordings of those targets will only occur on the recorders/pools specified.

Manual Partitioning

In other cases, you may wish to specify exactly what the standby should do when it takes over. See [Standby Server](#) on page 234 for instructions on how to specify this option.

Known limitations

Deploying standby recorders:

- Does not guarantee access to recordings made by the failed server. You must also use centralized replay server(s) and archiving to achieve this.
- Does not guarantee "no loss" of recording on failure. See [Mode of operation](#) on page 356.

Confidential and Proprietary Information

- Requires that the standby recorder can contact the master recorder when it is designated as a standby so that its licensing and/or configuration can be copied.
- Does not support the use of Telephone Replay ports on the master and standby recorder (unless you force local configuration). Place these on a central replay server (or pair of servers if fault tolerant replay is required).

Fault Tolerant Topologies

Note:

This section primarily relates to Communication Manager based systems. Fault tolerant support for CS1K and AACC is limited to ACR server failure.

To provide fault tolerant Bulk recording, first determine the design load (maximum concurrent recordings), "D" and the capacity of each server, "C" for the hardware and recording mode(s), codecs etc. that you intend to use. Then follow these design guidelines.

In all cases:

1. Load will be balanced across all viable servers - including standby servers. In the event of any server failing, calls being recorded on it will be reassigned to the remaining servers.
2. You must ensure that network paths between ACR servers use fault tolerant network connections (including NICs).
3. Connect each ACR to a single AES on the same site.
4. Connect only one master or standby recorder to any AE Server.
5. Spread slaves across multiple AE Servers.
6. Do NOT specify particular C-LANs when entering softphone ranges.
7. Configure the Master with enough softphones to support the total design load PLUS 20 softphones (headroom) per server.
8. Do NOT set the **Designated Recorder** setting on any softphone ranges. They will be assigned automatically to the servers that need them.
9. Consolidate recordings from all recorders into centralized databases at the master and (main) standby or dedicated Central Replay Servers.

The following sections describe how to protect against:

- failure of the Master server using a ("main") standby on the same site as it.
- failure of any server on a site by providing an additional server
- network failure, isolation or complete site destruction or shutdown using standby server(s) and (optionally) slaves on remote sites.

Confidential and Proprietary Information

"Main" Site

Each system will have one "main" site - where the Master ACR in the system resides. The table below shows how the total ("sunny day") and fault tolerant capacity vary according to the number of master, standby and slave recorders provided.

ACR Servers at Main Site				Main Site Recording Capacity	
Master	Standby	Slaves	Notes	Sunny Day	Fault Tolerant
1	0	0	1	C	0
1	1	0	2	2C	C
1	1	1	2,3	3C	2C
1	1	S	2,3	(2+S)C	(1+S)C

Notes:

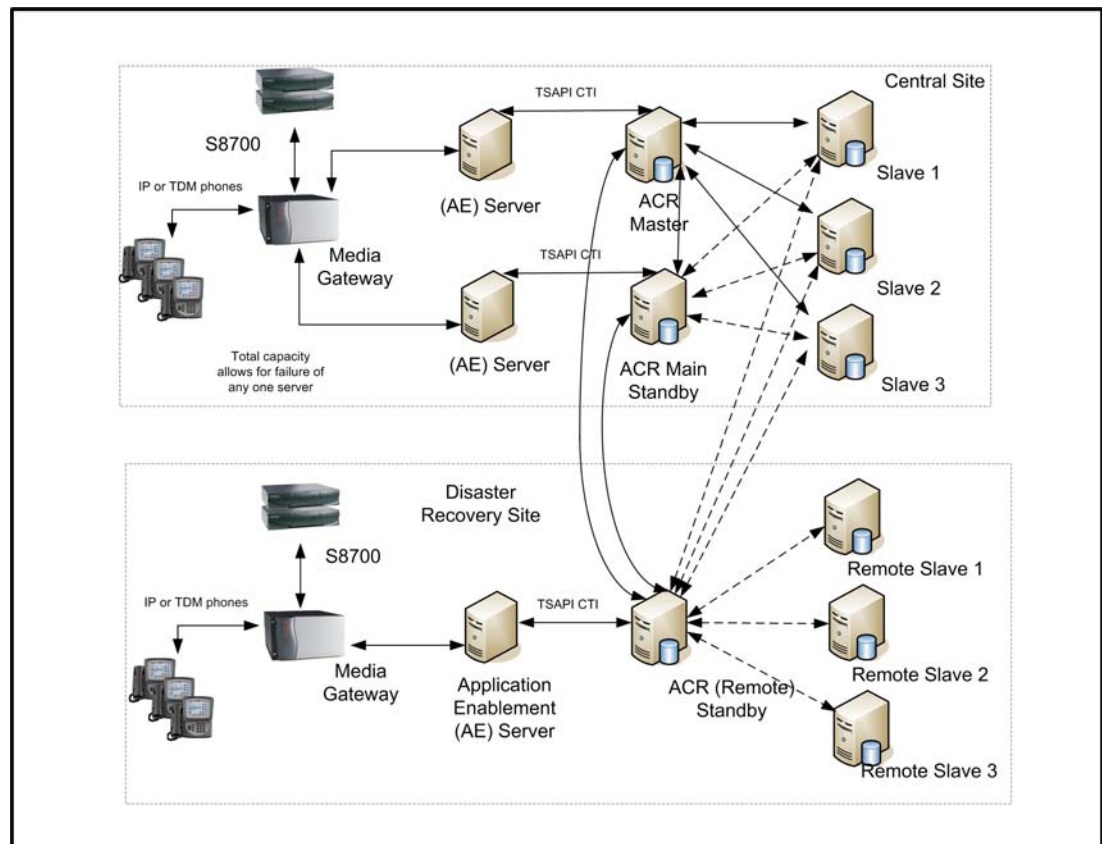
1. There will always be one "Master" recorder - into which you enter your overall system license and then configure your recording requirements.
2. Use the licensing page to configure a server as a Standby - giving the master's IP address. This server will provide additional capacity AND can take over control of recordings should the master fail.
3. Use the licensing page to configure each additional server as a Slave - giving both the master and standby IP addresses so that the slave can be controlled by whichever of these is active at any time.

This fault tolerance relates to the failure of any **one**

- ACR server.
- AES server (so long as the Master and Standby are connected to different AES servers)

Should the Standby take over, it will remain in control even if the master recovers. An administrator must deliberately force the master to take back control (using the **Go Active** button on url `/servlet/acr?cmd=mtce`) out of hours. This will interrupt recording briefly at that time.

Confidential and Proprietary Information



Disaster Recovery ("DR") Site

An increasingly common requirement is to provide a complete backup system at another site - to allow full capacity operation should the Main site fail, become isolated or be destroyed. To achieve this:

- Explicitly configure the standby on the Main Site to be a "main standby" by setting "standby.main=true"
- Provide an AES server at the DR site
- Provide one or more recorders at the DR site as per the table below
- If, in addition to continuing to record, you require uninterrupted replay access to all previous recordings while the main site is down, you must provide and configure a NAS archive destination (and associated bandwidth) at each site. For large systems, consider providing a dedicated Central Replay Server at each site (as this

Confidential and Proprietary Information

Fault Tolerant Systems

will impose less load on the other servers than having records uploaded to master and two standby servers).

ACR Servers at DR Site				DR Site Recording Capacity
Master	Standby	Slaves	Notes	
0	1	0	1,2	C
0	1	1	1,3,4	2C
0	1	S'	1,3,4	(1+S')C

Notes:

1. When switchover to a DR site occurs, the standby on the DR site will start to record calls that it hears about via CTI. It will not restart recording of calls that were in progress on the main site - but these will, in any case, have been interrupted as the trunks were switched over to the DR site.
2. Following a switchover, the standby on a remote site will stay active until it is reset. This is the appropriate behavior for ESS or LSP sites that are manually restored to normal operation. If, on the other hand, the site automatically reverts to normal mode you can change this behaviour with `standby.stayactive=false` - in which case the standby will drop back to idle should it make contact with the Master or main standby again.
3. When setting the license on the Standby server at the DR site, enter the IP addresses of both the Master and the Standby at the main site. This server will then only take charge if it loses contact with both of these (i.e. in the event of site failure, not single server failure).
4. The **standby at the DR site** will be given the same recording load as those at the main site unless you set property file entries on both the Master and Central Standby as follows.
 - a. Limit the maximum load to be applied to each server (regardless of site) by adding `farendcapacity.nnnnnn=C` where `nnnnnn` is the serial number of each recorder and C is the maximum capacity of a server.
 - b. Bias load balancing heavily away from the standby on the DR site by setting `farendscale.nnnnnn=100` where `nnnnnn` is the serial number of the Standby on the DR site. The standby server will only be given one recording for every 100 present on the other servers. If load never reaches 100 on each of the other servers, reduce this figure so that the remote standby is used at least occasionally and hence any problems with it are flagged before it needs to take the full load.
5. When setting the license on each **Slave server at the main site**, configure each with the IP addresses of the Master, the main Standby and the Standby on the DR site. These slaves will be visible to all three potential controlling servers.

Confidential and Proprietary Information

6. When setting the license on any **Slave server(s)** needed **at the DR site**, ONLY configure them with the IP address of the Standby on the DR site. These slaves should NOT be visible to servers on the main site and will be idle unless the standby on the DR site takes over. However, if you wish to archive calls from these remote slave servers, the archive settings need to be pushed down from the standby server to which the remote slave is connected. To enable this, you must set this property on the standby server that controls the remote slave.

`forceconfig.nnnnnn=true`

where *nnnnnn* is the serial number of a remote slave.

7. Unless using dedicated Central Replay Server(s), configure the IP addresses of the Master and Central Standby server as the Centralized Replay Servers for the Standby on the DR site. For the slaves on the DR site, configure the Master, Central Standby and DR site standby - so that recordings made on these slaves are uploaded to all three servers.

Tip:

If there is sufficient bandwidth between main and DR sites for one recorder's worth of recording to happen at the DR site should a server at the main site fail, the server count at the main site can be reduced by one as the Standby server at the DR site will take all remaining load once the servers at the main site reach their full capacity.

ESS or LSP Satellite Sites

Where one or more sites can continue to provide *partial* operation in the event of the main site being shut down, isolated or destroyed, backup systems can be provided at these satellite sites.

Follow the same guidance as for a full DR site but, in addition,

1. Place all the recorders at the central site into a named pool (by setting `recorder.pool=main`)
2. Place all the recorders at each satellite site into a named pool for each satellite site (by setting `recorder.pool=sitename`)
3. Use the Designated Recorder advanced setting to specify, for each range of recording targets, that they can be recorded on the main pool and the appropriate site specific pool.
4. On the master and central standby, use the `farendscale.nnnnnn=100` property (where *nnnnnn* is the serial number of each remote server) to bias recording towards the central site when available.
5. On LSP sites, ensure the "add/change survivable processor" setting is "i" or "o" or the AES will not be able to communicate with the CM.

Confidential and Proprietary Information

Distributed Recording System

Where the normal recording mode is to force at least some specific recording targets to be recorded at other sites, using the Designated Recorder settings on recorded targets, you can provide additional fault tolerance on any of those remote sites as follows:

To protect against failure of a ACR server on a remote site:

1. Provide one more server than is required to handle the load at that site.
2. Place all servers on that site in a single recording pool (by setting `recorder.pool=xxx`)
3. Use this poolname rather than a single recorder number in the Designated Recorder setting when configuring the Master.

Further, to protect against isolation of the remote site from the main site:

4. Explicitly configure the standby on the Main Site to be a "main standby" by setting `standby.main=true`
5. Provide an AES on each remote site
6. Configure the first server on each remote site to be a "Standby" and give it the IP addresses of both the Master and the Standby at the main site. This server will then only take charge if it loses contact with both of these (i.e. in the event of site failure, not single server failure).
7. Configure the remaining servers on the remote site as slaves, giving them the addresses of the Master, Central Standby and local Standby. If using WFO, you must also instruct the Master to include the serial numbers of these slaves in the roles that it reports to WFO. To do this, add a property to the master in the form `remoteslave.1=8xxxxx` where `8xxxxx` is the 6 digit serial number of the remote slave. For a second remote slave, use `remoteslave.2=8yyyyy` etc.

Supported failure modes

The Standby recorder is designed to become active within a few seconds of a complete system failure of the master recorder (and, optionally central standby recorder) it is configured to "shadow." These failure modes include:

- Catastrophic server failure
- Total network isolation
- Accidental power down or power failure
- Sustained failure of the main CTI link
- Disk full

Confidential and Proprietary Information

Standby recorders and Unify/External Control

Unify/External Controller connected to Master/Standby pair

When using Unify or an equivalent external controller with a master/standby recorder pair, it should send any START/STOP commands to the recorder that sent it port ONLINE messages.

Only the active recorder will send STARTED/STOPPED messages. Unify should only send TAG commands to this active recorder.

Unify/External Controller connected to Master only

If the external controller is essential to the operation of the Master (for example, if it is setting up single step conferences) then the master needs to recognize that it is not viable if it has no links to external controllers. Set the property `unify.required` in the properties file to indicate this. You can then provide either:

- a standby recorder, locally configured for an alternative recording mode (such as Station Bulk or Bulk Recording)
- a second Unify/External controller connected to the standby recorder

With this property set, the Unify/External controller can force a switchover to the standby by sending a `1 BYE SHUTDOWN` message and then not sending the `HELLO` response when the recorder re-establishes connection. When it is ready to take control again, it can send the `HELLO` message and the recorder will take over from the standby again.

CS1000 Master/Standby Topologies

A master and standby recorder can be connected to a single MLS to protect against failure of the master recorder.

A standby recorder may be configured against a secondary call server to protect against failure of the main call server.

Mode of operation

This section describes how the standby recorder is configured and how it monitors the health of its master recorder. It also explains how it takes over when needed and returns to standby mode when appropriate.

Standby configuration (automatic)

If you do not make alterations to the standby machine's properties file, it automatically copies the license details and settings from its master whenever the master recorder is "viable" (regardless of which recorder is actually active).

Standby configuration (manual)

You only have to configure a standby server manually if you have forced local configuration in the **acr.properties** file. A Standby recorder is configured manually in the following way:

- to match the master recorder it is to shadow in most respects, for example, system timeouts, maximum recording durations and so on.
 - with the IP addresses of the master recorder that it is to shadow.
-

Power-On

A common case is that all recorders are powered on within a second or two of each other. To avoid destabilizing the system, the standby unit will always wait for a pre-defined period after it starts trying to contact the master recorder before it assumes that it is dead. This period allows for slight variations in boot time and manual power-on of one unit after another.

The time-period is determined by the `oemcomms.connecttimeout=xxx` property in the properties file. (`xxx` is in seconds).

Standby mode

Once configured, the standby unit attempts to establish TCP/IP socket connections to the master recorder(s) over the one or more IP addresses it has been configured with. If it succeeds, it downloads the configuration details of the master recorder that are necessary

Confidential and Proprietary Information

for it to take over in the event of the master failing. It continues to refresh these details every minute, thus keeping up to date with configuration changes.

Heartbeat messages are exchanged every few seconds.

Failure Detection

The standby recorder will attempt to take over from the master recorder in the following circumstances:

- The master requests that the standby unit take over because it has detected a fatal error such as hard disk full, switch connectivity lost completely.
- On startup, if connection cannot be established with master after 120 seconds (default - and accurate only to within one minute).
- All TCP/IP sockets to the master(s) failing and attempts to re-establish them every second are still failing after 60 seconds.
- Either or both TCP/IP sockets to the Master are still active but the master does not respond to repeated heartbeat polls for 30 seconds.

The three timeout settings above may be overridden by setting the property values `oemcomms.connecttimeout`, `oemcomms.reconnecttimeout` and `oemcomms.inactivitytimeout` respectively in the properties file. Times are specified in seconds.

These same parameters are also used by the master recorder to report corresponding failures of the standby although it will not do anything other than raise an alarm if this occurs. The default values for these timeouts can be overridden on the master using the same property settings.

A master recorder is not aware of standby recorder(s) until it has established contact with a standby for the first time. Thereafter it will expect to establish contact with that standby recorder always. (This can only be reversed by editing the underlying configuration database).

Disk Space Monitoring

Once a minute, each recorder will monitor the available disk space on the partitions used for the operating system, call details storage and recording storage. If any of these drops below 500MB a warning will be raised.

To override this default; set `disk.warnAtMB=nnn` in the properties file.

Active mode

On inferring failure of or being instructed to by the master, the Standby unit will try to start recording as per the automatically copied configuration or its local configuration.

It will configure its recording channels in the same way that the failed recorder had been using them prior to failure (unless you have forced local configuration). In the case of Communication Manager recording modes, where softphones are marked with specific standby recorder numbers, only those designated for a given standby will be registered.

Recordings will be made and their details uploaded to the Central Replay Server (if present).

Return to Standby mode

A standby recorder will return to Standby mode:

- If the standby unit is shutdown before the failed master is restored. When the standby unit is rebooted, the master responds within the timeout mentioned above and the standby recorder remains in standby mode.
- If the failed unit recovers it may instruct the standby recorder to return to idle immediately - or not until the administrator forces this (see [Restoring the Master](#) on page 359). At this time, the standby unit will truncate all current recordings and un-register all softphones allowing the master to take over again. Note that this switch-back has the same impact on recordings as the initial switch-over. Hence you should only bring a failed unit back on-line out of hours.

Switchover Implications

It takes a few seconds to detect most of the failure modes. Although configurable using the properties file, this interval is a compromise between rapid detection of true failure versus risk of false alarms and/or "yo-yoing," a condition where the system goes unstable. The system defaults aim to detect failures within 10 seconds and should not normally be altered.

When a failure occurs and the standby recorder becomes active:

- Recordings in progress are interrupted. The partially completed .wav files for the recordings in progress might be manually recoverable (professional services chargeable). In G.729A mode, up to 1 minute of audio is buffered in memory and hence will not have been appended to the file. In G.711 mode, files are appended to every 30 seconds.

For On Demand and Meeting recording modes:

Confidential and Proprietary Information

- Recordings in progress are dropped. The standby recorder switches in within seconds, registers its softphones and awaits new calls arriving on these ports.

The worst case loss of recording on a port is therefore determined by the speed with which the switch can re-register the failed softphones. The more channels on the failed recorder, the longer this process takes.

Restoring the Master

The fault condition that caused the standby to become active can be removed in a number of ways, not all of which are ideal. These methods are:

- Power restored to master
- Network connectivity restored to master
- Connection to the switches CTI feed is restored
- Master repaired and reinstated.

If there is only one standby recorder, the master recorder will allow it to continue so as not to interrupt recordings unnecessarily. The administrator may force the master to take control again by logging into the administration web pages on the master and then entering the url `http://servername:8080/servlet/acr?cmd=mtce`. Click the **Go Active** button on this page.

This will cause the master to take over. It should be performed out of hours as there will be a brief interruption in recording as the system switches over.

In cases where multiple standby recorders are, between them, providing backup for a master, this is usually less desirable than having the (single) master regain control. It is also more difficult for the Master recorder to be confident that all recordings are being handled by the standbys. In this case, a recovering Master will retake control automatically - with a brief interruption to service as it does so.

The one exception to this is a remote standby configured as part of Communication Manager ESS or LSP site. Default behavior of the standby recorder is appropriate for sites that have to be manually restored when connection to the central site has been re-established. The standby recorder will continue to record until it is reset. If your ESS/LSP site is configured to restore automatically when the network has recovered, you should set `standby.stayactive=false` on the standby recorder. This tells it that it can drop back to fallback mode when the link to the master recorder has been re-established (and the master is viable).

Comparison with hardware switch-over units

Traditionally, high availability digital recording has been provided by inserting an "N+1 Switchover Unit" between the recorders and their audio sources. Although this provides a slightly faster switchover, it has several negatives in comparison to the software only approach used here:

- The cost of the switchover unit makes N+1 systems uneconomical for N=1 or 2
- The additional cabling required to and from the switchover unit introduces further cost, failure mechanisms and opportunities for mis-configuration (swapped cables) that might not be noticed until after a failure has occurred.
- The switchover unit itself introduces a significant single-point of failure into the system.

Confidential and Proprietary Information

Standby Recorder Configuration

Unless you specifically request otherwise, most configuration details of the master are copied automatically to the standby. This occurs once a minute and allows the standby to track the day-to-day adds, moves and changes that you will make.

If you make major changes to the system, such as changing the mode of recording or the codec in use, you should restart the standby recorder after your changes are complete to ensure that it has a clean configuration. You should always check for any alarms on the standby following configuration changes.

Configuration Differences

The following Administration pages differ on a Standby recorder:

- **General Setup > Contact Center Interface** - Some of the settings on this page are derived from the master and will not show an **Edit** link next to them. The others must be configured on the standby as these can (and in some cases should) differ from the Master. However, the settings that must be made here are ones that are unlikely to change once your system is running.
- **System > License** - When setting up the Standby server, assign the server a unique number in your enterprise and enter this on the licensing page.
 - An additional setting allows you to enter the IP addresses of the master recorder (and any central or "main" standby in the case of a remote standby) that this recorder is to shadow. You must use bonded (or "teamed") NICs. The default IP port number will be 1209 but you may override this by adding the port number to the IP address, separated by a colon, for example, **192.134.34.45:1419**. If you enter a port number, this must match the configuration of the master recorder, which also defaults to 1209. You can override this default by setting the `oemcomms.secureport` property in the `acr.properties` file. Unless you are confident that your DNS server is fault tolerant, you should specify numeric IP addresses to ensure that connectivity does not fail because of address translation problems.
- **System > Email Server**
 - You are strongly advised to create a separate email account, using a separate SMTP server from that used by the master. This way, failure of an SMTP server will be noticed as you continue to receive e-mails from the standby unit but not the nightly heartbeats from the master - or vice versa. It is critical that you ensure that the standby unit is ready to take over at any time.

Fault Tolerant Systems

- **System > Manage Users** - User accounts are copied automatically from the master. Details can only be edited here when the master is down - and changes made will be lost when the master is restored.
- **Operations** - These pages are provided but their contents are not editable as these are copied from the master recorder (once contact has been established with it).
- **Alarms > View Alarms** - This page is identical to that on the master recorder though some different alarms will be generated - when the standby establishes contact with the master and should it ever try to take over from the failed master. You should use the email settings on the **System > Email Server** page to ensure that you are advised of these alarms within 10 minutes of one occurring.
- **Recorder Status** pages are similar to those on the Master.

Confidential and Proprietary Information



Appendix F: Auto-Dialer Integrations

This appendix describes how the system can be connected to a number of popular auto-dialers.

[Introduction](#) on page 364

[Configuration](#) on page 366

[Avaya PCS/PDS Dialer](#) on page 369

[SER Dialer](#) on page 374

[Davox Dialer](#) on page 377

[Proactive Outreach Manager \(POM\) Dialer](#) on page 379

Introduction

When agents log in to dialers using "nailed up" sessions, the whole session of customer calls appears to the recorder as a single "call" and hence recordings are concatenated. These can be broken up and tagged with the outbound call details using CTI integration to the dialer.

One or more dialers can be supported. These may be of the same or mixed types.

Currently supported dialers are:

- Avaya PCS/PDS
- Davox/Concerto (on CS1000)
- SER (on CS1000)
- Proactive Outreach Manager

Functionality

Dialer integrations allow calls made over "nailed up" sessions to be split into individual customer calls. Without the dialer integration, such calls are recorded as a single recording for the duration of the session, tagged only with the identification of the dialer port - not the numbers of the customers actually called.

When an agent logs in to a dialer, the nailed up call is recognised as such and recording stops. This recording may include an initial greeting or login dialogue. If it is very short it may be automatically deleted but typically results in a 0 or 1s duration call. If the agent subsequently drops this call by releasing at the phone set or otherwise, the dialer will re-establish the nailup with a new call. This will be recorded unless the dialer sends an agent not ready event as it does this. In either case, when a customer is next connected to the nail-up, a new recording will begin.

When the agent is presented with a call, the dialer tells the recorder and it starts recording. Information provided by the dialer at this time is used to tag the call. This typically includes campaign information and identification of the party being called. At the end of a call, the dialer tells the recorder and it stops recording.

Optionally:

- Agent logon/logoff from the dialer can be used to determine the agent number and name (but the default is to use the underlying switch's login information).

The dialer integration normally provides details of the external party on the call. In addition, many of the other data or "tagging" fields provided by the dialer can be stored as User Defined Fields ("UDFs") against the call. Detailed functionality varies from dialer to dialer and from installation to installation. See below for more details.

Confidential and Proprietary Information

How it Works

The recorder starts an additional thread to monitor the CTI activity from each dialer. This picks up Agent Logon/logoff and start/stop events as the agent takes each call. The details vary from dialer to dialer. Each dialer is implemented as a specific Java "class" and can be configured via the normal acr.properties file.

Status Monitoring

The status of the CTI link to each dialer is shown on the **Recorder Status > Server** page alongside all the other interfaces.

Alarms are generated whenever a link fails or is restored.

Details of dialer calls in progress will be shown on the **Recorder Status > CTI Monitors** page above or below the details of the underlying "nailup" call.

Errors, warnings, informational and debug messages are written to the log file along with all other messages generated by the recorder.

Configuration

Dialer configuration is done via the `acr.properties` file.

Licensing

To interface to any dialer other than the SER dialer, you must purchase and install a license key containing this option.

Dialer List

First, specify how many dialers you have and what they are called by adding the following line to the properties file `acr.properties`:

```
acr.dialerlist=dialer1name,dialer2name,...
```

Choose each dialer's name to reflect not just the make of dialer but also its location or identity if you have more than one dialer of a given type.

For example:

A single, PCS dialer:

```
acr.dialerlist=PCS
```

Two PCS Dialers:

```
acr.dialerlist=PCS_London,PCS_NewYork
```

Generic Dialer Configuration

For every dialer name given in the `acr.dialerlist`, you should include the following lines in your properties file. Each begins with the name of the dialer to which it refers.

Mandatory Fields

You MUST include this for each dialer so the application knows which Java class to use:

```
dialer1name.class=java classname for the type of dialer
```

Confidential and Proprietary Information

Optional Fields

The following fields need only be added if you wish to override the default settings.

Block Agent IDs

By default, agent logon/logoff messages are not passed on to the recorder (i.e. it is assumed that the agent logon to the station is sufficient to tag the call). To change this, add

```
dialer1name.blockagentids=false
```

This will allow the dialer's view of agent ids and names to be included in call tagging.

Switch Number

Most dialers provide a reference number for each call they make. This is not in the same format as the UCID of a Communication Manager call but can normally be displayed in a similar fashion. Normal UCIDs start with a switch identifier of up to 5 digits (padded with leading zeroes in most places). Each dialer can be allocated a pseudo "switch number" as follows:

```
dialer1name.switchnumber=nnn
```

Where nnn is a 1 to 5 digit number (less than 32768) that does not conflict with that of any Communication Manager in your network. Calls from this dialer will be assigned a "UCID" as if they had come from a Communication Manager of this number.

If you do not set this value, it will default to switch number 9.

Trunk Range(s)

Where a dialer is physically connected to the switch over one or more trunk groups, you should identify the range(s) of trunks that are used for connections to headsets (as opposed to internal, outbound or transfer purposes) so that the recorder can recognize calls over them as being dialer calls.

```
dialer1name.trunkranges=n1:a1-b1,n2:a2-b2
```

Where the dialer uses trunkmembers a1 to b1 (inclusive) on trunk group n1; members a2 to b2 (inclusive) on trunk group n2 etc. If an entire trunk group is use, you do not need to specify the range of members.

Completion Code

Where this is supported, it will be stored in User Defined Field "comcode" unless overridden as described below with property setting

```
dialer1name.field.comcode=xxxx
```

Tagging of Calls

Recordings split by dialer instructions are:

1. tagged with details of the external (normally "called") party
2. tagged with the agent details that the user logged into the dialer with (unless blocked - see above)
3. tagged with other fields - the names of which vary from dialer to dialer

Should you need to change the name of a user-defined field from that provided as default, you can do so using the property file entry

dialer1name.field.originalfieldname=newfieldname

where

- *dialer1name* is the name of the dialer in question
- *originalfieldname* is the name of the user defined field being provided by the dialer integration
- *newfieldname* is the alternate fieldname that you want the recorder to store this as. (To suppress the field altogether, leave *newfieldname* empty). The fieldname will be used as an XML tag name so should only include a-z. You should not include spaces in the field name but if you do, these will be converted to underbars.

Confidential and Proprietary Information

Avaya PCS/PDS Dialer

This dialer is supported on systems based on Communication Manager and CS1000. Set the `.class` property to `com.swhh.cti.pcscon.PCSDialer`. For example,

```
PCS_Boston.class=com.swhh.cti.pcscon.PCSDialer
```

Versions Supported

The recorder interfaces to dialers running the following versions of software, each of which has a corresponding "personality file" as shown below:

Dialer Type and Version	Personality File	Notes
PDS V12	pds12_idl.jar	
PCS V3.0	pcs30_idl.jar	
PCS V4.0, V5.0	pcs40_id.jar	Secure connection can be enabled

Limitations

When using multiple PCS or PDS dialers, they must all be of the same major version as only one personality file can be loaded at a time.

Configuration

The various property file settings are discussed in detail below and are summarized in the table which follows.

1. All three personality files can be found in the folder beneath the install path. Copy the appropriate one into the `/tomcat7/lib` folder
2. Ensure you have a license key installed that includes the optional dialer license.
3. Edit the `properties/acr.properties` file as described below
4. Restart the recorder service to have your configuration take effect.

Confidential and Proprietary Information

Dialer Name

Specify the dialer name. This value is used to look up the address of the dialer, and to look up the dialer's Event Service in the Name Service. This is the name by which the dialer knows itself and is CASE SENSITIVE. Note that the recorder must be able to ping the dialer using this name. Add the name to the hosts file or to DNS to allow this. The setting in the property file is:

```
dialer1name.hostname=dialername
```

For example:

```
PDS_Boston.hostname=pdsboston
```

Credentials

Set the username and password that the recorder should use when registering as a client:

```
dialer1name.username=username  
dialer1name.password=password
```

For example:

```
PDS_Boston.username=ACR1  
PDS_Boston.password=secret
```

Return Path

The dialer needs to be able to connect to recorder (as well as vice versa). The dialer must be able to resolve the hostname of the recorder. If this is not possible you should set *dialername.replyip=ipaddressoftherecorder*. Unless the dialer can connect, you will get 'timeout' errors.

Encryption

When using PDS 4.0 you can force the recorder to use a secure connection to the dialer by setting:

```
dialer1name.secure=true
```

For example

```
PDS_Boston.secure=true
```

If you are using secure mode to connect to PCS 5 you need to change the certificate file that is used to verify the connection. In the keystore folder, overwrite the *avayapcs* file with the *avayapcs5* file.

Confidential and Proprietary Information

Name Service IOR (Optional)

This parameter is optional but if not provided, the recorder attempts to look up the Name Service using corbaloc.

```
dialer1name.NSIOR=name_service_ior
```

For example

```
PDS_Boston.NSIOR=IOR:010000003200000049444c3a61766179612e636.....
```

Multiple NICs

If the recorder has multiple NICs you must specify which one is to be used for communication with the dialer. Include the replyip setting. Specify the ip address of the recorder to be used for communications.

For example

```
PDS_Boston.replyip=10.10.11.12
```

Firewalls, multiple dialers

The Recorder initially connects to the dialer's name service. This uses port 23200 (or 23201 if secure). Subsequently it connects to the dialer's event service. This uses port 23120 (or 23121 if secure). Finally the dialer connects back to the Recorder on a randomly assigned port.

If the Recorder is communicating with the dialer through a firewall, or there is more than one dialer, the reply port must not be randomly assigned, but must be fixed.

For each PCS dialer choose a port number for the dialer to communicate back to the recorder. (Each dialer must use a different number.) Add the replyport setting for each dialer (or replysslport if using SSL).

For example

```
PDS_Boston.replyport=4999
```

Now make changes to the firewall to allow the communications.

The recorder must be able to connect to each dialer on TCP ports 23200 and 23120 (or 23201 and 23121). Each dialer must be able to connect to the recorder on the TCP port specified for that dialer.

PCS Dialer PODs

If there is more than one dialer and they are configured as a POD, you must use the Name Service IOR optional parameter. The name service runs on the master dialer, but can provide the location of the event service for all the dialers.

Create one set of entries for each dialer. You must include the hostname, username, password, NSIOR and replyport parameters. Populate the NSIOR parameter for each dialer in the POD with the value from the primary dialer.

FieldMappings

The dialer's "job name" and "job number" are stored as used defined fields "jobname" and "jobnumber" respectively. The "IDENT=" field may contain a list of (comma separated) tag/value pairs - each of which is stored by default. See [Tagging of Calls](#) on page 368 for how to change this.

Trunk Group(s)

If you have a HARD dialer, then you should set the trunkgroups property, otherwise Avaya Contract Recorder will record the initial greeting and may fail to record unrelated calls made while the nailed-up call is on hold.

PCS/PDS Settings Summary

Setting	Usage	Required	Comment
hostname	The dialer name	Required	Not the ip address
username	Credentials	Required	
password	Credentials	Required	
secure	Turns on SSL encryption	Optional	Applies to PC4.0 or later only
NSIOR	The Name Service IOR	Optional	Required for POD dialers
replyip	The IP address of the recorder used for communication	Not normally required	Required if the recorder has more than one NIC

Confidential and Proprietary Information

Setting	Usage	Required	Comment
replyport or (if using SSL) replysslport	The TCP port used by the dialer to contact the recorder	Not normally required	Required if the port must be fixed for firewalls. Required if there is more than one PCS dialer. (Each must use a separate port.).
trunkranges	The trunk group and member number(s) through which the dialer is connected to the switch.	"Hard" dialer only.	See Optional Fields on page 367

SER Dialer

This dialer is supported with the CS1000 switch only.

Configuration

Set the `.class` property to `com.swhh.cti.sercon.SERDialer`. For example:

```
SER_Chicago.class=com.swhh.cti.sercon.SERDialer
```

HostName

Specify the IP host name of the dialer to which the recorder should connect:

```
dialername.hostname=hostname
```

For example:

```
SER_Chicago.hostname=10.100.205.23
```

Use a numeric IP address if the host name cannot be resolved or is not known.

Port

Specify the port number to which the recorder should connect:

```
dialername.port=portnumber
```

The default is set to port 40000 but you may need to change this to suit your dialer. For example,

```
SER_Chicago.port=9000
```

SwitchName

An SER dialer can be connected to more than one switch. You must specify the name that has been set in SER for the Avaya switch that this recorder is recording. In most cases, the default of "switch1" will be correct.

```
dialername.switchname=switchname
```

For example:

```
SER_Chicago.switchname=switch2
```

Confidential and Proprietary Information

FieldMappings

A standardized set of mappings is provided from the SER fields to the recording tagging fields as described in the table below:

SER Field Name	Notes	Mapping to Recording XML and Database Field	Example Value
Campaign	Dial plan and strategy. Can be alphanumeric.	User defined field "campaign"	Nd400k
Group	The skill set from which agents are selected to service the campaign	Agent name of the dialer agent party on the call (unless blocked)	PR_Test SKT
UserName	SHOULD match the CS1000 logged on Agent ID	AgentID of the dialer agent party on the call (unless blocked)	3508
Extid	The extension that the recorder has been asked to observe. Actually the secondary DN on the position.	A party on the call.	8900
Telnum	Dialed number	The number of the external party on the call	07767123456
RetKey	Unique reference for this record in the dialling list or "portfolio". Often is customer identifier e.g. a/c number.	The name of the external party on the call hence customer will show with this in parentheses after their number e.g. 07767123456 (000012234)	

Auto-Dialer Integrations

SER Field Name	Notes	Mapping to Recording XML and Database Field	Example Value
Portfolio	Set of numbers i.e. customer list and their phone numbers. Mapping of fields, import file, which wrapup codes etc.	Stored as user defined field "portfolio"	ND400k
RE_segnum	A numeric identifier that uniquely identifies the contact. Reused upon system restart - i.e. starts at 1 again.	Extended to form a unique call id using a switch number that should not overlap with any other Avaya switch number in the system.	16

Note:

Fields shown in search pane are derivatives of these not 1:1 mappings

Confidential and Proprietary Information

Davox Dialer

This dialer is supported with the CS1000 switch only.

Configuration

Set the .class property to `com.swhh.cti.davcon.DavoxDialer`. For example,

```
Davox_Dublin.class=com.swhh.cti.davcon.DavoxDialer
```

HostName

Specify the IP host name of the dialer to which the recorder should connect:

```
dialer1name.hostname=hostname
```

For example:

```
Davox_Dublin.hostname=10.100.205.23
```

Use a numeric IP address if the host name cannot be resolved or is not known.

Port

Specify the port number to which the recorder should connect:

```
dialer1name.port=portnumber
```

The specification uses an example of 4252 so try this if in doubt. For example,

```
Davox_Dublin.port=4252
```

FieldMappings

The standard Davox integration for Avaya Contact Recording recorders can be used. This provides user defined fields in the CTI output as DATA1 through DATA16. You can choose how to map these into the partynumber, partyname, servicenumber and service name fields as described below.

These fields are passed on from the various campaign files - and hence there may be more than one mapping required if campaigns' fields are not uniformly labelled. You can specify multiple strings for cases where only one of each is present in any given campaign

Auto-Dialer Integrations

or where you want to store multiple fields in one e.g. title, firstname and surname. Individual fields will be separated by a space character.

In each case below, start with n=1 and do not skip any.

`dialer1name.partynumber.n=fieldname`

(Normally used to hold the phone number dialled. Maximum length = 50 characters).

`dialer1name.partyname.n=fieldname`

(Normally used to hold the name or other identifier of the customer dialled e.g. account number. Maximum length = 50 characters).

`dialer1name.campaign.n=fieldname`

`dialer1name.list.n=fieldname`

Normally used to store the name of the database list being used on the campaign.

For example:

`Davox.partynumber.1=DATA1`

`Davox.partyname.1=DATA2`

`Davox.partyname.2=DATA3`

`Davox.partyname.3=DATA4`

`Davox.partyname.4=DATA5`

`Davox.campaign.1=DATA6`

`Davox.list.1=DATA7`

You can check that all fields have been specified correctly by looking for the corresponding INFO level messages in the log file after startup e.g.:

```
2008-10-30 17:04:29,896 [Dialer Manager thread] INFO
com.swhh.cti.davcon.DavoxDialer - starting davox dialer: Davox
2008-10-30 17:04:29,896 [Dialer Manager thread] INFO
com.swhh.cti.davcon.DavoxDialer - Found keyword [DATA1] for
partyname
Etc.
```

Agent IDs

Note that the Agent IDs sent from the Davox dialer are normally alphanumeric names rather than numbers. These can be entered into QM as if they were additional CS1000 agent IDs.

Confidential and Proprietary Information

Proactive Outreach Manager (POM) Dialer

Configuration

Set the `.class` property to `com.swhh.cti.popdialer.POMDialer`. For example,

```
POM1.class= com.swhh.cti.popdialer.POMDialer
```

HostName

Specify the IP address or hostname of the dialer:

```
dialername.hostname=hostname
```

For example:

```
POM1.dialer=pom1.bigcorp.com
```

Use a numeric IP address if the hostname cannot be resolved or is unknown.

Port

Specify the port number to which the recorder should connect:

```
dialername.port=portnumber
```

The port defaults to 7999. You only need to specify this if it is different.

Credentials

Specify the username and password needed to access POM.

```
dialername.username=username
```

```
dialername.password=password
```

For example:

```
POM1.username=BIGCORP\acrpomuser
```

```
POM1.password=H0t1ant@
```

Limitations

This dialer is supported with the Avaya Aura Contact Center only.

Versions Supported

Version 3.0 is currently supported.

Configuration

Set the .class property to `com.swhh.cti.xxx.xxx`. For example,

```
POM_Boston.class=com.swhh.cti.xxx.xxx
```

Confidential and Proprietary Information



Appendix G: Non-standard Hardware

This appendix discusses considerations for non-standard hardware such as blade servers. It covers the following topics:

- [Overview](#) on page 382

Overview

This manual and the automated installation processes assume a "typical" rack-mounted server as the server hardware. However, Avaya Contact Recorder has been installed on other hardware successfully, including blade servers. This appendix covers the considerations for such non-standard hardware.

Disks

SAN

Blade servers are normally equipped with locally attached SAN which is ideal for Avaya Contact Recorder. See [Storage at Each Recorder](#) on page 56 for further details.

Partitioning

The standard installation assumes either one or two physical disks, or one RAID array. In a more complex environment there could be separate arrays for different partitions. For example, a RAID 0 mirror for everything except call storage and a RAID 5 array for call storage. For Linux systems, you must edit the kickstart script to specify the appropriate disk device for each partition by changing the "on" parameter. See [Expert kickstart options](#) on page 105.

NICS

Blade servers often have redundant network configurations. It is therefore more likely that Avaya Contact Recorder should be installed with just one IP address (eth0 on Linux) instead of two (eth0 and eth1).

DVD

As a blade will not normally have dedicated access to a DVD/Blu-ray drive, NAS archive is the preferred solution in this environment.

Confidential and Proprietary Information

Kickstart (Linux only)

If no floppy disk is available for kickstart installation, use the network-based kickstart instructions in [Performing a kickstart install without a floppy](#) on page 105.

Non-standard Hardware

Confidential and Proprietary Information

■ ■ ■ ■ ■ ■

Appendix H: Advanced Security Settings

This appendix discusses some features and prerequisites for advanced security. It includes:

- [Server Hardening](#) on page 212
- [Installing Unlimited Strength Encryption](#) on page 386
- [Installing a Signed SSL Certificate](#) on page 387
- [Changing Tomcat Port Numbers](#) on page 391
- [Encrypting Properties File entries](#) on page 392

Installing Unlimited Strength Encryption

To support key sizes larger than 128 bits, you will need to replace the standard Java Jurisdiction Policy Files using the following instructions:

1. Using your browser, go to the following link:

<http://www.oracle.com/technetwork/java/javase/downloads/index.html>

2. Follow the link entitled:

Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6 at the foot of the page.

3. Download and unzip the files.

4. Follow the instructions in the `readme.txt`. The path for installation on Linux is `/usr/java/jre1.6.0_37/lib/security`. On Windows, it is in your install path, under `jre\lib\security`.

5. You should note the instruction to back up the existing jars that will be replaced

Confidential and Proprietary Information

Installing a Signed SSL Certificate

If you want to install your own SSL certificate, you must replace the certificate distributed with the application. Your replacement certificate must be specific to your installed server.

Selecting a Certificate Authority (CA)

If you do not already use a certificate authority, you can use:

- <http://www.freessl.com/startersssl/startersssl.html> - FreeSSL requires that the web server has a fully qualified domain name (e.g. contactrecorder.bigcorp.com or contactrecorder.division.bigcorp.com) and needs to be able to send an email to an address like ssladmin@bigcorp.com or administrator@division.bigcorp.com. The list of addresses can be found on their website, and it includes admin, ssladmin, root, and administrator. This provides a free 30 day trial after which you will have to purchase RapidSSL.
- <http://www.instantssl.com> - InstantSSL is more flexible and allows intranet addresses (such as WINS names and IP addresses) as well as fully qualified domain names.

Backing up the Keystore file

In the instructions which follow, replace *installdir* with the location into which you installed Avaya Contact Recorder (always /opt/witness on Linux, typically D:\Program Files Avaya>ContactRecorder on Windows).

The certificates and keys are stored beneath your installation folder in the file:

```
installdir/keystore/keystore.jks
```

Because this file contains the original, distributed certificate, it is important to make a backup of it. You will delete this file during the remaining steps. Should it be necessary to restore the original certificate, you can copy the backup to the original filename.

Creating the new Certificate

If you would like to test this implementation, you can practice this procedure with a certificate authority's 30-day trial certificate. Then, to implement real certificates, you can start over from this point.

Advanced Security Settings

To create a certificate:

1. Create a new certificate with the real URL of the Avaya Contact Recorder.
2. Log onto the server and change directory as follows:

```
cd installdir/keystore
```

3. Remove the original keystore file

```
(Linux) rm keystore.jks
```

```
(Windows) del keystore.jks
```

4. Run the java keytool utility with

```
(Linux)/javadirectory/bin/keytool -genkey -keystore keystore.jks  
-alias tomcat -keyalg RSA -keysize 1024
```

```
(Windows) ..\..\jre\bin\keytool -genkey -keystore keystore.jks  
-alias tomcat -keyalg RSA -keysize 1024
```

5. Fill in the Keytool prompts with the following:

```
Password: Contact5tor3
```

Note:

You must type this password, exactly as shown. It is case sensitive.

- a. **First & Last Name:** enter the FQDN, IP address or intranet name
 - b. **Organizational Unit:** enter your division
 - c. **Organization:** enter your company name
 - d. **City/Location:** enter your location
 - e. **State/Province:** enter your state
 - f. **Country Code:** enter the ISO 2 letter code for your country (for example, GB is the code for United Kingdom)
6. Enter **yes** if the information is correct.
 7. Hit **enter** when prompted for the second password.
 8. Restart the Avaya Contact Recorder service.
 9. Access the Administration pages via **HTTPS**.
 10. Check that the certificate matches the information entered.
 11. Double click the padlock icon. Internet Explorer should warn you that the certificate is unsigned. However, it should no longer display a message that indicates the certificate does not match the web server name.

Tip:

If you do get a warning that the certificate does not match, check that the Common Name matches the URL. Double click the padlock, select the details tab, and click the Subject line. This displays the Common Name.

Confidential and Proprietary Information

Generating a Certificate Signing Request

You need a Certificate Signing Request (CSR) as the first step of the signing process. When you have it, paste it into the Certificate Authority's web page. To generate a CSR:

1. Re-run the keytool command (still in the keystore directory as above)


```
(Linux) /javadirectory/bin/keytool -certreq -keystore keystore.jks
      -alias tomcat
      (Windows) ..\..\jre\bin\keytool -certreq -keystore keystore.jks
      -alias tomcat
```
2. Enter the password - which is `Contact5tor3`.
3. Copy and paste the output into the CA's web page. (Include the BEGIN and END lines.)
4. Complete the verification process
5. Reply to the verification emails and other verification steps until you obtain a signed certificate back from the CA.

Importing the CA's certificates

Before you can import your certificate reply, you need to import the certificate authority's root certificate and any intermediate certificates between their root and your certificate.

To acquire these certificates:

1. Download these certificates from the certificate authority's website.
2. Save the root as `rcert.crt` and any intermediate as `icert.crt`.
If you have more than one intermediate certificate, give them separate filenames.

To import all your certificates:

1. Import the root certificate by running keytool:


```
/javadirectory/bin/keytool -import -keystore keystore.jks
      -alias root -file rcert.crt
```
2. Enter the password - which is `Contact5tor3`.
3. Import the intermediate (if required).


```
(Linux) /javadirectory/bin/keytool -import -keystore keystore.jks
      -alias inter -file icert.crt
      (Windows) ..\..\jre\bin\keytool -import -keystore keystore.jks
      -alias inter -file icert.crt
```

If you have more than one intermediate certificate, import them as `inter1`, etc.

Advanced Security Settings

4. Import your signed certificate.
5. Save the file the CA sent as cert.crt.
6. Import with the keytool.

```
(Linux) /javadirectory/bin/keytool -import -keystore keystore.jks
      -alias tomcat -file cert.crt
(Windows) ..\..\jre\bin\keytool -import -keystore keystore.jks
      -alias tomcat -file cert.crt
```

7. Restart the Avaya Contact Recorder service.
8. Access the administration pages using https.
9. Double click the padlock icon and ensure that Internet Explorer no longer displays a message that the certificate is unsigned.

Backing up the keystore file

The keystore file now contains:

- the random private key that is unique to this web server
- the signed certificate you just paid for

These two are linked and cannot be regenerated, so it is important to back up the keystore file. If either one of these components is lost, you must regenerate the certificate and pay again to get it signed.

Adding Additional AES CA Root Certificates to ACR

Go to the AES Server and navigate to **Security>Certificate Management>CA Trusted Certificates**.

Select the new CA Root Certificate via the associated tick box. .

Now click on the **Export** button and you will be presented with a window that contains the CA Root cert in a textual format

Copy the entire contents of this text (including the -----BEGIN CERTIFICATE and END CERTIFICATE lines) and paste it into a filename of your choosing - a sensible choice would be the name of the CA cert

Save this file in *installdir/keystore/cacerts*

Confidential and Proprietary Information

Changing Tomcat Port Numbers

You can change the default http and https ports (8080 and 8443 respectively) by editing *install_dir/tomcat7/server.xml*.

Locate the two **Connector** elements on roughly lines 20 and 30 and change 8080 to the chosen plain port number and 8443 to the chosen secure port number.

You must also set the following property in the properties file:

```
acr.localport=nnnn
```

specifying the replacement for 8080.

Note:

If you are using Central Replay Server you must change all the recorders and the Central Replay Server. The port numbers must be consistent across all of these servers for upload to the Central Replay Server to work. You must provide an http port if using Central Replay Server.

Note:

If you change the **HTTPS** port from the default of 8443 *and* you do not allow HTTP access, you must also set the following line in the properties file so that attempts to use HTTP are redirected to the correct HTTPS socket.

```
https.socket=nnnn
```

The server.xml may be overwritten on subsequent upgrades. You should keep a copy of the file after editing it so that this can be compared with any changed version and the appropriate set of merged changes determined after the upgrade.

Encrypting Properties File entries

Avaya provides a tool to encrypt your passwords so that they can safely be placed in properties files. You will need this tool if you want to, for example, change the postgresql password.

Obtain the WitsBSUserCredentials tool from Avaya support and install it following the instructions provided with it.

To encrypt a password for use in the properties file:

1. Launch the tool.
2. Select Other for the application type.
3. Enter a dummy username (it is not used) together with the password to be encrypted.
4. Use the encrypted password in the properties file.

Confidential and Proprietary Information

Glossary

ACD	Automatic Call Distribution. This is a feature offered by the Avaya Communication Manager that queues and distributes incoming calls to waiting agents. Calls are queued until an agent is available. If multiple agents are available, calls are distributed on an equitable basis.
ACD DN	The DN associated with an ACD group. Calls made to an automatic call distribution directory number are distributed to agents belonging to the group, based on the ACD routing table on the switch.
AE Services	Avaya's Application Enablement Services are APIs to services such as telecoms, database, and so on. They include DMCC and TSAPI.
AGENT Logon ID	An unique identification number assigned to a particular agent. The agent uses this number when logging on. The agent ID is not associated with any particular phoneset
AMS	Avaya Media Server - a component of the Avaya Aura Contact Center through which SIP calls are routed.
ANI	Automatic Number Identification (Service). The provision of calling party information (typically, telephone number or billing/account number) to the called party.
Avaya CT	Now known as AES TSAPI services. See TSAPI below.
BHCA	Busy Hour Call Attempts. The number of calls that are attempted during the switches busy hour. Typically slightly higher than, but often used interchangeably with BHCC
BHCC	Busy Hour Call Completions. The number of calls that are completed during the switches busy hour. Typically slightly lower than, but often used interchangeably with BHCA

Glossary

CDN	Controlled DN (CS1000 and AACC systems only). A CDN is similar to an ACD queue with no agents, a "holding place" for calls. Calls are queued in a CDN, and while in the queue, calls can receive treatment commands from a controlling application (for example, host application giving treatments such as music, ringback, or silence, or routing the call). CDNs can operate in controlled or default (uncontrolled) mode. An active application controls calls in a CDN when the CDN is in controlled mode. In default mode, calls entering a CDN are immediately given the default treatment (for example, routed to an ACD DN and receive RAN, music, and so on), as specified in the default configuration in Overlay 23).
Codec	An abbreviation of COder/DECoder. A device or program that converts signals from one form to another. In this context, between different digital audio compression standards.
Communication Manager API (CMAPI)	Now known as Device, Media and Call Control (DMCC)
CRD	Contact Recording Desktop
CTI	Computer Telephony Integration - typically an interface through which a computer system can be advised of events occurring within a telephony system and/or control the telephony system. TSAPI is an example of such a link.
CUSTOMER	The CS1000 supports multitenant operations. The PBX can be partitioned into multiple, independent systems known as customers. Within each customer, DNs are unique and routes are private. Meridian Link is a system feature: that is, it covers all customers in the Meridian 1 PBX. However, when an application registers over Meridian Link (Application Registration message), it selects the customer it wants to work with.
Device, Media and Call Control (DMCC)	A software platform (part of AE Services, previously known as Communication Manager API or CMAPI) that applications such as the recorder use to create softphones that can participate in calls made on Avaya Communication Manager-based systems.
DID	Direct Inward Dialing. An attribute of a trunk. The CO passes the extension number of the called party over a DID trunk to the PBX when offering a call to the PBX. The PBX is then able to automatically route the call to that extension without requiring operator/attendant assistance. In this way, a single trunk can terminate calls for many different extensions (but not simultaneously).

Confidential and Proprietary Information

DN	Directory number (CS1000 only). The number that identifies a phoneset on a PBX or in the public network. It is the number that a caller dials to establish a connection to the addressed party. The DN can be a local PBX extension (local DN), a public network telephone number, or an ACD-DN-the pilot or group number for an ACD queue.
Duplicate Media Streaming	A means of recording telephone calls by having the phoneset duplicate the packet streams that make up the real phone call - sending the copies to a specified IP address (the recorder).
DVD+RW	Digital Versatile Disk + Read/Write. One of several competing optical storage standards, supported by a wide range of manufacturers.
HFS	Hierarchical File Storage system. Typically a combination of hard disk and tape drives plus controlling software that automatically migrates little used files to cheaper storage media.
IDN	Individual DN (CS1000). ACD agents using BCS sets can have additional DN's (in addition to their ACD key) configured on their phonesets. Key 0 is used to receive incoming ACD calls; other keys can support other DN's. IDN's are treated just like any other DN. 500/2500 set ACD agents can also have a (single) IDN configured.
IP	Internet Protocol. IP specifies the format of packets and the addressing scheme for internet data. The IP, like the postal system, allows you to address a package and drop it in the system. The packet may traverse multiple networks on the way to its ultimate destination.
IVR	Interactive Voice Response. A system/facility that plays voice menus to callers, and acts upon user input (typically, DTMF digits from a touch tone phone). It is sometimes called VRU (Voice Response Unit).
MADN	Multi-Appearance Directory Number (CS1000).
Master Controller	An Avaya Contact Recorder that is being shadowed by one or more Standby Controllers. The Master will default to "Active" on startup unless configured for a single standby recorder and this is already "Active" but will ask a Standby to take over its role if it determines that it cannot record e.g. a disk fills.
Meridian Link (ML)	Meridian 1's host interface. Meridian Link supports X.25 and LAPB communication protocols for host connectivity to CS1000.

Glossary

NAS	Network Attached Storage. A term used for RAID, tape and other mass storage systems which have an integral network connection such as Ethernet or fiber-channel.
NIC	Network Interface Card. An expansion board that you insert into a computer so the computer can connect to a network. Most NICs are designed for a particular type of network, protocol, and media, although some can serve multiple networks.
Position ID	A unique identifier for a CS1000 phone set, used by the switch to route calls to the phones
QoS	Quality of Service
RAID	Redundant Array of Inexpensive Disks. RAID controllers use two or more hard disk drives together for fault tolerance and enhanced performance. RAID disk drives are used frequently on servers.
SAN	Storage Attached Network. A high-speed network that is typically part of an overall network of computing resources for an enterprise, in which the software knows the characteristics of storage devices and the quantity and value of the data stored in those devices.
Skill Hunt Group	A telephone number that is used to route calls to agents on the basis of the skills needed to handle the call. Agents are assigned to one or more such skill groups according to their expertise and appropriate calls are routed to them when they are available.
Slave Recorder	An Avaya Contact Recorder being controlled by the active Controlling Recorder. i.e. recording what it is told to record.
Softphone	(SOFTware PHONE) In this context, a software-based emulation of an Avaya VoIP phone. Multiple such emulations run on the Avaya Contact Recorder and each can participate in a telephone call in order to record it.
Standby Controller	An Avaya Contact Recorder that shadows a Master Controller and takes over its role ("goes active") should the master fail or appear to fail (e.g. the standby loses contact with it).
Tagging	Adding details to the database of call recordings so that recordings can later be retrieved by searching through the available data fields.
TDM	Time Division Multiplexing. The traditional means of transmitting large numbers of voice calls over circuit switched networks - as distinct from VoIP.

Confidential and Proprietary Information

TN	Terminal Number (CS1000 only). The physical address of a device (for example, a phone set, a trunk, an attendant) on the Meridian 1 PBX. The TN is composed of the loop, shelf, card, and unit IDs.
Trunk	A communications link between a PBX and the public central office (CO), or between PBXs, or between COs.
TSAPI	Telephony Services Application Program Interface. A CTI interface standard to which AES TSAPI conforms.
UTC	Universal Time Coordinated. A time scale that couples Greenwich Mean Time, which is based solely on the Earth's inconsistent rotation rate, with highly accurate atomic time. When atomic time and Earth time approach a one second difference, a leap second is calculated into UTC. UTC, like Greenwich Mean Time, is set at 0 degrees longitude on the prime meridian.
VDN	Vector Directory Number. An extension number used in Avaya's ACD software to connect calls to a vector for processing. The VDN by itself can be dialed to access the vector from any extension connected to the switch. (See also Vector.)
Vector	A list of steps that processes calls in a user-defined manner. The steps in a vector can send calls to splits, play announcements and music, disconnect calls, give calls a busy signal, or route calls to other destinations. (See also VDN.)
VoIP	Voice over Internet Protocol. A means of transmitting telephone calls over the packet-switched IP network - as distinct from TDM.
VPN	Virtual Private Network. Private, or restricted, communications networks which use encryption and other security measures to transmit information through a public network such as the Internet and avoid unauthorized use.
VRU	Voice Response Unit. A device that plays voice menus to a caller and responds to caller instructions entered on a touch tone phone. Also known as Interactive Voice Response (IVR).

Confidential and Proprietary Information