Arc Pro

Design Guide

Version 6.3.1

arc solutions

Terms of use

Any software ("Software") that is made available by Enghouse Interactive Inc. ("Enghouse"), together with any User Documentation ("User Documentation") is the copyrighted work of Enghouse. Use of the Software is governed by the terms of a Master Purchase Agreement, End User License Agreement, or similar software license agreement ("License Agreement"). End users are not legally authorized to install any Software that is accompanied by or includes a License Agreement unless he or she first agrees to the License Agreement terms.

The Software is made available for installation solely for use by users according to the License Agreement. Any reproduction or redistribution of the Software not in accordance with the License Agreement is expressly prohibited by law and may result in severe civil and criminal penalties. Violators will be prosecuted to the maximum extent possible.

WITHOUT LIMITING THE FOREGOING, COPYING OR REPRODUCTION OF THE SOFTWARE TO ANY OTHER SERVER OR LOCATION FOR FURTHER REPRODUCTION OR REDISTRIBUTION IS EXPRESSLY PROHIBITED, UNLESS SUCH REPRODUCTION OR REDISTRIBUTION IS EXPRESSLY PERMITTED BY THE LICENSE AGREEMENT ACCOMPANYING SUCH SOFTWARE.

THE SOFTWARE IS WARRANTED, IF AT ALL, ONLY ACCORDING TO THE TERMS OF THE LICENSE AGREEMENT. ENGHOUSE HEREBY DISCLAIMS ALL OTHER NON-EXPRESS WARRANTIES AND CONDITIONS WITH REGARD TO THE SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT.

Enghouse grants a nonexclusive license to customer for use of the User Documentation. The User Documentation contains copyrighted and other proprietary materials. By accepting the User Documentation, recipients agree that they will not transmit, reproduce, or make available to any external third-party this User Documentation or any information contained herein. Copying, reverse-engineering, or reselling any part of the Software or User Documentation is strictly prohibited.

The information contained in the User Documentation furnished by Enghouse is based on the most accurate information available at the time of printing. No representation or warranty is made by Enghouse as to the accuracy or completeness of such information or any ongoing obligation to update such information. Enghouse reserves the right to change the information contained in this document without notice.

Registered trademarks

Syntellect®, Voiyager®, Continuum ®, MediaVoice®, Apropos®, Envox®, Envox® Activecall, Envox CT ADE®, Envox CT Connect®, Dynamic Application Discovery®, Interaction Vault® CT Impact®, SmartDialer®, SmartVoice®, SmartCollect®, SmartSupport®, Zeacom®

Enghouse Global End User License Agreement (EULA)

THIS END USER LICENSE AGREEMENT ("AGREEMENT") GOVERNS THE USE OF PROPRIETARY SOFTWARE AND THIRD PARTY PROPRIETARY SOFTWARE LICENSED THROUGH ENGHOUSE. READ THIS AGREEMENT CAREFULLY, IN ITS ENTIRETY, BEFORE INSTALLING, DOWNLOADING OR USING THE SOFTWARE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER INTERCHANGEABLY REFERRED TO AS "YOU", "YOUR" OR "CUSTOMER"), AGREE TO THIS AGREEMENT AND CREATE A BINDING CONTRACT BETWEEN YOU AND ENGHOUSE INTERACTIVE, INC. OR THE APPLICABLE ENGHOUSE AFFILIATE THROUGH WHICH THE SOFTWARE WAS DISTRIBUTED TO YOU ("ENGHOUSE"). IF YOU ARE ACCEPTING THIS AGREEMENT 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. IF YOU DO NOT HAVE SUCH AUTHORITY OR DO NOT WISH TO BE BOUND BY THESE SOFTWARE LICENSE TERMS, SELECT THE "DECLINE" BUTTON AT THE END OF THIS AGREEMENT AND/OR RETURN THE SOFTWARE TO ENGHOUSE IMMEDIATELY UPON REJECTION, WITHOUT INSTALLING, COPYING, OR USING THE SOFTWARE FOR A REFUND THEREOF. A REFUND MAY ONLY BE GIVEN WITHIN 30 DAYS FOLLOWING DELIVERY OF THE SOFTWARE. YOUR USE OF THE SOFTWARE, EVEN IF OBTAINED IN CONTRAVENTION OF THIS LICENSE AGREEMENT OR OBTAINED OTHERWISE THAN THROUGH ENGHOUSE OR AN ENGHOUSE RESELLER, INDICATES YOUR AGREEMENT TO ALL OF THESE TERMS.

1. DEFINITIONS

"**Affiliate**" – means any entity that is, directly or indirectly, controlling, controlled by, or under common control with Enghouse Interactive, Inc. or is a subsidiary of Enghouse Systems Limited. For the 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.

"**Enghouse Reseller**" – a reseller, distributor, direct partner, service provider or other partner authorized by Enghouse to provide Software to end users in applicable territory.

"**Software**" – shall mean the collective reference to Enghouse's proprietary software and any third party proprietary software which Enghouse or Enghouse Reseller may distribute to Customer on the basis of resell or other transfer. Such Software includes any product documentation and any upgrades, updates, new releases or other modification thereto made generally available by Enghouse in its discretion from time to time. Software shall not include custom development.

2. SCOPE

This Agreement is applicable to anyone, who installs, downloads, and/or uses Software, obtained from Enghouse or an Enghouse Reseller. Customer is not authorized to use the Software if the Software was obtained from anyone other than Enghouse or an Enghouse Reseller authorized to distribute the Software.

3. SOFTWARE LICENSE TERMS AND CONDITIONS

3.1 **Rights Granted to Customer**: The rights granted to Customer shall be subject to Customer's compliance with the terms of this Agreement including, without limitation payment for the Software. If Customer has purchased the Software, Enghouse grants to Customer a non-exclusive, non-transferable license (on a perpetual or subscription basis depending on purchase) to install, use and execute the Software in object code form on a per-license basis at the location specified ("Software License"). The location of the Software use may be changed by Customer from time to time with written notice to Enghouse. Software License is limited to the site(s), number of seats, concurrent users, agents, servers, ports, devices, managed applications, and/or copies as applicable to the Software obtained, not to exceed the number of licenses set forth on applicable orders. The Software License shall become effective upon delivery of the Software and shall remain in force unless terminated due to expiration or breach of these license grant terms or confidentiality. This right does not include permission to grant sub-licenses or otherwise transfer such rights. Customer may make copies of the Software for archival purposes only, provided that it retains or affixes the equivalent of Enghouse's proprietary legend and copyrights to the copy. Additionally, the Customer may make several copies of the system documentation, excluding training manuals and materials, provided that they are for internal use only. Customer may not reverse engineer, disassemble or otherwise translate the Software License provided pursuant to this Agreement. Enghouse, or any third party that owns the Software License, retains exclusive title to and all rights to the Software. The Customer acknowledges that the Software and documentation are the property of Enghouse and that the only right that the Customer obtains to the Software is the right of use in accordance with the terms of this Agreement.

3.2 **Governmental Use**: All Software Licenses and documentation furnished pursuant to this Agreement were developed at private expense and are provided with RESTRICTED RIGHTS. Any use, duplication or disclosure by or for any governmental agency of the United States Government or any other jurisdiction shall be subject to the restricted rights applicable to commercial computer software including under FAR Clauses 12.211, 12.212, 52.227-19 or DFARS 227.7202, 252.227-7013 as applicable or any successor provision or any other legal provisions respective of restricted rights for commercial software. Consistent with the above, all Software and third party software as well as commercial computer documentation are licensed to governmental end users only as commercial items and only with those rights as are granted to all other end users under the terms and conditions set forth in this Agreement. Customer may not use or export the Software, third party licensed software, or documentation except as authorized by law and under this Agreement. In particular, but without limitation, the Software may not be exported to any U.S. embargoed country.

3.3 **Software Title**: No title to or ownership of the Software or any of its parts, the information it contains or in any applicable rights therein, such as patents, copyrights and trade secrets, is transferred to Customer. Any reference to "sale", "purchase" or "subscription" of the Software shall be deemed to mean, "License on the terms contained in this Agreement." Enghouse considers the information contained in the Enghouse Software owned or created by Enghouse to be trade secrets of Enghouse and any third-party software licenses which Enghouse may resell to Customer to be trade secrets of such third-party licensor. Customer agrees to treat Software as Confidential Information and shall use the same degree of care used by Customer to protect its own Confidential Information. Except as set forth herein, or as may be permitted in writing by Enghouse, Customer will not provide, transmit or otherwise make available, the Software or any part or copy thereof to any third party, reverse engineer, reverse compile or reverse assemble the Software in whole or in part, or attempt to derive the source code, modify, adapt, translate, or create derivative works of the Software or any updates or any part thereof. Notwithstanding the previous sentence, Customer may configure Software to meet Customer's needs and user preferences.

3.4 **Restrictions**: Customer may not publish, display, disclose, sell, rent, lease, loan, or distribute the Software, or any part thereof. Customer may not assign, sublicense, convey or otherwise transfer, pledge as security or otherwise encumber the rights and licenses granted hereunder with respect to the Software. Customer may not market, co-brand, private label or otherwise permit third parties to link to the Software, or any part thereof. Customer may not use the Software, or any part thereof, in the operation of a service bureau or for the benefit of any other person or entity. Customer may not cause, assist or permit any third party to do any of the foregoing.

3.5 **Third Party Software**: Some third party software (including some imbedded software) are exclusively licensed pursuant to express end user license terms made available at http://www.enghouse.com/legal/agreements.html ("Third Party EULA"). To the extent applicable, Customer agrees to be bound by these end-user terms respective of the applicable Third Party EULA provisions. Third party software licenses provided to Customer which are not expressly provided for in the Third Party EULA provisions are provided to Customer pursuant to the terms of this agreement including without limitation this Section 3. All third party software are restricted for use solely in conjunction with the particular Software intended by Licensor to be used therewith or with which Enghouse provides the third party software, and may not be used with any other products, or on a stand-alone basis.

4. WARRANTIES

4.1 **Limited Warranty**: Enghouse warrants, for a period of thirty (30) days from date of delivery, that the Software will substantially conform to the published specifications prevailing at the time of purchase or delivery. Enghouse's sole obligation and liability hereunder will be to use reasonable efforts to remedy any such non-conformance which is reported to Enghouse in writing within the warranty period. The exclusive remedy for any breach of the foregoing warranties is for Enghouse to repair, modify, replace or re-perform (as applicable). Notwithstanding the foregoing, if longer warranty periods are mandated under applicable law those periods shall apply for that location only.

4.2 **Disclaimer of Warranty**: EXCEPT AS OTHERWISE SPECIFICALLY PROVIDED IN THIS SECTION 4, SOFTWARE IS PROVIDED BY ENGHOUSE AND ACCEPTED BY THE CUSTOMER "AS IS" AND ENGHOUSE GIVES TO THE CUSTOMER NO OTHER REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH RESPECT TO SOFTWARE OR THE PERFORMANCE OR RESULTS OF USE THEREOF. WITHOUT LIMITING THE FOREGOING, ENGHOUSE DOES NOT WARRANT THAT THE SOFTWARE OR THE OPERATION THEREOF IS OR WILL BE ERROR-FREE OR UNINTERRUPTED OR MEETS OR WILL MEET THE CUSTOMER'S REQUIREMENTS, AND ENGHOUSE GIVES NO IMPLIED WARRANTY OF ANY KIND, INCLUDING, WITHOUT LIMITATION, WITH REGARD TO MERCHANTABILITY, NONINFRINGEMENT OR FITNESS FOR ANY PARTICULAR PURPOSE AND WHETHER ARISING BY USAGE OF TRADE, COURSE OF DEALING OR COURSE OF PERFORMANCE.
ENGHOUSE DOES NOT MAKE ANY WARRANTIES OR REPRESENTATIONS TO THE ADEQUACY OR SUFFICIENCY IN COMPLYING WITH THE TELEPHONE CONSUMER PROTECTION ACT ("TCPA"), ANY DECISIONS, DIRECTIONS OR GUIDANCE GIVEN BY OFCOM OR ANY COMMUNICATIONS REGULATORY AUTHORITY IN ANY OTHER APPLICABLE JURISDICTION. THE CUSTOMER ACKNOWLEDGES THAT IT IS CUSTOMER'S EXCLUSIVE LIABILITY TO COMPLY WITH ANY REGULATORY AUTHORITY AND ALL APPLICABLE COMMUNICATIONS LAWS INCLUDING OUTBOUND COMMUNICATIONS AND DO-NOT-CONTACT OBLIGATIONS. IF CUSTOMER PURCHASES OUTBOUND DIALLER SOFTWARE OR SERVICES, THE PARTIES ACKNOWLEDGE THAT CELL PHONE DATA CONSTANTLY CHANGES AND AS A RESULT MAY NOT BE ERROR FREE.

5. MAINTENANCE AND SUPPORT

Enghouse has no obligation under this Agreement to provide maintenance/support for the Software. Any maintenance/support purchased for the Software is subject to Enghouse's then-current maintenance/support policies.

6. LIMITATION OF LIABILITY

6.1 IN NO EVENT SHALL ENGHOUSE BE LIABLE FOR ANY DAMAGES RESULTING FROM LOSS OF USE, DATA, PROFIT OR BUSINESS OR FOR ANY PUNITIVE, EXEMPLARY, SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES, WHETHER ARISING IN CONTRACT, TORT OR OTHER LEGAL THEORY. ENGHOUSE AND THIRD PARTY SOFTWARE SUPPLIERS' LIABILITY FOR DAMAGES FOR ANY CAUSE WHATSOEVER, AND REGARDLESS OF THE FORM OF ACTION, SHALL BE LIMITED TO THE LESSER OF THE PURCHASE PRICE PAID BY THE CUSTOMER FOR THE PRODUCTS OR SERVICES UNDER THE SPECIFIC ORDER RELATING TO THE CLAIM IN THE PRIOR TWELVE (12) MONTH PERIOD OR ANY OTHER LIMITATION PROVIDED IN ANY SPECIFIC THIRD PARTY EULA AVAILABLE AT HTTP://WWW.ENGHOUSE.COM/LEGAL/AGREEMENTS.HTML. ENGHOUSE SHALL HAVE NO LIABILITY FOR ANY CUSTOM APPLICATION PROGRAMS. NO ACTION ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT OR ANY TRANSACTION HEREUNDER MAY BE BROUGHT BY EITHER PARTY MORE THAN TWELVE (12) MONTHS AFTER THE CAUSE OF ACTION HAS ARISEN, EXCEPT FOR AN ACTION FOR NON-PAYMENT.

7. CONFIDENTIAL INFORMATION

Each party acknowledges that, in the course of performing its duties under this Agreement, it may obtain information relating to the other party, which is of a confidential and proprietary nature ("Confidential Information"). Such Confidential Information may include, but is not limited to, this Agreement, pricing and proposals, computer software, trade secrets, know-how, inventions, techniques, processes, programs, schematics, data, customer lists, financial information and sales and marketing plans. Each party shall at all times maintain in the strictest confidence and trust all such Confidential Information, which shall not be less than those measures employed by each party in protecting its own Confidential Information of equivalent value. Customer and its employees agree not to disclose such information to any third party.

The commitments set forth above shall not apply to any Confidential Information which:

A. is now generally known or available or which hereafter through no act or failure on the part of the receiving party becomes generally known or available;

B. is legally known to the receiving party at the time of receiving such information;

C. is hereafter furnished to the receiving party by a third party without restriction on disclosure, where such third party legally obtained such information and the right to disclose it to the receiving party; or

D. is independently developed by the receiving party without violation of any legal rights which the disclosing party may have in such information.

Both parties agree that all Confidential Information disclosed hereunder shall remain the property of the disclosing party and may only be copied or reproduced as expressly permitted herein. Upon expiration or termination of this Agreement, the receiving party shall return all Confidential Information to the disclosing party along with all copies and portions thereof, or certify in writing that all such Confidential Information has been destroyed. No license, express or implied, in the Confidential Information is granted other than to use the Confidential Information in the manner and to the extent authorized by this Agreement. All Confidential Information disclosed hereunder is provided by the disclosing party without representation or warranty of any kind.

Where the parties have entered into a separate, confidential non-disclosure agreement ("NDA") and the terms of the NDA are inconsistent with the terms contained herein, the terms of the NDA shall take precedence.

8. JURISDICTION

A. If the Software is going to be used in the United States, South and Central America, or the Caribbean, the Agreement is controlled by and construed under the laws of the State of Arizona, United States of America, notwithstanding any conflicts of law provisions; and the state and federal courts of Arizona shall have exclusive jurisdiction over any claim arising under the Agreement.

B. If the Software is going to be used in Canada, unless expressly prohibited by local law, the Agreement are controlled by and construed under the laws of the Province of Ontario, Canada, notwithstanding any conflicts of law provisions; and the courts of the Province of Ontario shall have exclusive jurisdiction over any claim arising under the Agreement.

C. If the Software is going to be used in Europe, the Middle East, Africa, Asia or Oceania (excluding Australia and New Zealand), unless expressly prohibited by local law, the Agreement is controlled by and construed under the laws of England and Wales, notwithstanding any conflicts of law provisions; and the English courts shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. In addition, if the Agreement is controlled by the laws of England and Wales, no person who is not a party to the Agreement shall be entitled to enforce or take the benefit of any of its terms under the Contracts (Rights of Third Parties) Act 1999.

D. If the Software is to be used in Australia, unless expressly prohibited by local law, the Agreement is controlled by and construed under the laws of the State of New South Wales, Australia, notwithstanding any conflicts of law provisions; and the State and federal courts of New South Wales shall have exclusive jurisdiction over any claim arising under the Agreement.

E. If the Software is to be used in New Zealand, unless expressly prohibited by local law, the Agreement is controlled by and construed under the laws of New Zealand, notwithstanding any conflicts of law provisions; and the courts of New Zealand shall have exclusive jurisdiction over any claim arising under the Agreement.

F. If the Software is to be used in any other country, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of the State of Arizona, United States of America, notwithstanding any conflicts of law provisions; and the state and federal courts of Arizona shall have exclusive jurisdiction over any claim arising under the Agreement.

9. GENERAL

9.1 **Assignment**: The interests of Customer in this Agreement are personal and shall not be assigned, transferred, shared or divided in any manner by Customer without the prior written consent of Enghouse. Enghouse shall be entitled to assign this Agreement and the rights granted hereunder to any affiliate, subsidiary or successor in interest to Enghouse's business.

9.2 **Injunctive Relief**: Customer acknowledges that remedies at law may be inadequate to provide Enghouse with full compensation in the event of Customer's material breach of any: (i) license grant hereunder, (ii) confidentiality and nondisclosure obligations herein, or (iii) intellectual property rights of Enghouse, and that Enghouse shall therefore be entitled, without bond or other security obligation, to seek injunctive relief in the event of any such material breach.

9.3 **Verification**: At the request of Enghouse, Customer shall furnish Enghouse with a signed statement that the Software is being used pursuant to the terms and conditions of this Agreement. If Enghouse has reason to believe that the Software is not being used in accordance with the terms and conditions of this Agreement, Customer shall permit Enghouse to review your relevant records and inspect your facilities to verify compliance with this Agreement. Enghouse will conduct such inspection during normal business hours in a manner that does not unreasonably interfere with your business operations. In the event such inspection results in fees due to Enghouse, Customer shall immediately pay those fees to Enghouse, and any reasonable inspection costs.

9.4 **Exports**: This Agreement is expressly made subject to applicable laws, regulations, orders or other restrictions on the export of the Software or information about such Software which may be imposed from time to time. Customer shall not export the Software, documentation or information about the Software and documentation without complying with such laws, regulations orders or other restrictions. Customer agrees to indemnify Supplier and its licensors against all claims, losses, damages, liabilities, costs and expenses, including reasonable legal fees, to the extent such claims arise out of any breach of this section.

9.5 **Severability**: If any provision of this Agreement is determined to be void or unenforceable, in whole or in part, it shall be severable from all other provisions hereof and shall not be deemed to affect or impair the validity of any other provisions, and each such provision is deemed to be separate and distinct.

9.6 **Termination**: This Agreement is effective until it is terminated. Customer may terminate this Agreement at any time by destroying or returning all copies of the Software and documentation in your possession or under your control. Upon termination, Customer agrees to destroy or return all copies of the Software and documentation and to certify in writing that all known copies, including archived copies, have been destroyed. All provisions relating to confidentiality, proprietary rights and limitation of liability shall survive the termination of this Agreement.

9.7 **Full Agreement**: This Agreement supersedes any and all agreements, either oral or written, between the parties hereto with respect to Enghouse licensing the Software to Customer and contains all the covenants and agreements between the parties with respect to the licensing of such Software. Each party to this Agreement acknowledges that no representations, inducements, promises or agreements, orally or otherwise, have been made by any party, or anyone acting on behalf of any party, that are not embodied herein, and that no other agreement, statement or promise not contained in this Agreement shall be valid or binding.

Contents

About this document

This chapter contains the following information:

Audience

This document should be used in conjunction with the *Arc Pro Installation Guide* to assist you in the successful planning and implementation of an Arc Pro system. This document assumes basic knowledge of the Arc Pro system and discusses possible implementation scenarios, taking into account topologies and environmental issues.

It is intended for the following audiences:

- Those involved in the planning and implementation of an Arc Pro Solution.
- Arc Pro Administrators.

Contents

This document contains the following sections:

- About this document explains who should use this document, what is new in this release, and where to find additional resources and support. It also explains the conventions used in this document.
- 1: Architecture gives an overview of the system architecture.
- 2: CUCM Interoperability describes important considerations that must be made when configuring Arc Pro Server to interoperate with the CUCM platform.
- 3: CTI integration explains how to select and monitor devices for Arc.
- 4: SQL database overview explains how to install the Microsoft SQL Server for database operations.
- 5: Arc Directory describes LDAP synchronization.
- 6: Multi-Tenant including Multiple Cluster Support explains what Multi-Tenant Operation is and which options are available.
- 7: Arc features focuses on PCP, Serial Calling, SMS, Voice Connect and Enhanced Directory View.
- 8: Dial plans and expression handling describes the Dial Plan feature.
- 9: Arc Pro Server environment explains all other components of the Arc Pro Server environment.

- 10: Third party integration describes Unity voicemail integration and Call recording integration.
- 11: AXL/Database Field Mappings describes AXL to CUCM DB Field Mappings used for device synchronization.

Reference materials

This document should be read in conjunction with the information and procedures in the following documents or Help:

- Arc Pro documentation:
  - http://enghouseinteractive.co.uk/services/support/console-for-cisco-enterprise-edition-arc-pro-technical-documentation/
- Cisco documentation:
  - Cisco SRND 7.x
  - Cisco SRND 8.x
  - Cisco SRND 9.x
  - Cisco SRND 10.x

Document conventions

This document uses the following text formats and notation conventions.

Text format

Bold text indicates a button, field, link, option name, or similar function requiring an action.

Italicized text indicates new terms, directory paths, or references to external documents.

`Text in this font` indicates code.

Notes and cautions

Icons used throughout this document identify additional details or special conditions.

> **Note**
> Provides additional information or describes special circumstances.

> **Caution**
> Warns of user actions that may cause system failure or irreversible conditions.

> **Stop**
> Describes actions that you should only perform under the supervision of Enghouse Customer Support.

Contact information

To submit comments or questions about the content in this document, please open a case in Support.

1: Architecture

This chapter contains the following information:

System architecture overview

The engine of the Arc Pro system is several services that run on a single Windows server, that can be physical or a VMWare image. Two servers can be run together to provide a resilient solution with one server acting as a hot standby for the other. The system requirements are contained in a separate document that can be found here:

http://enghouseinteractive.co.uk/console-cisco-enterprise-edition-technical-documentation

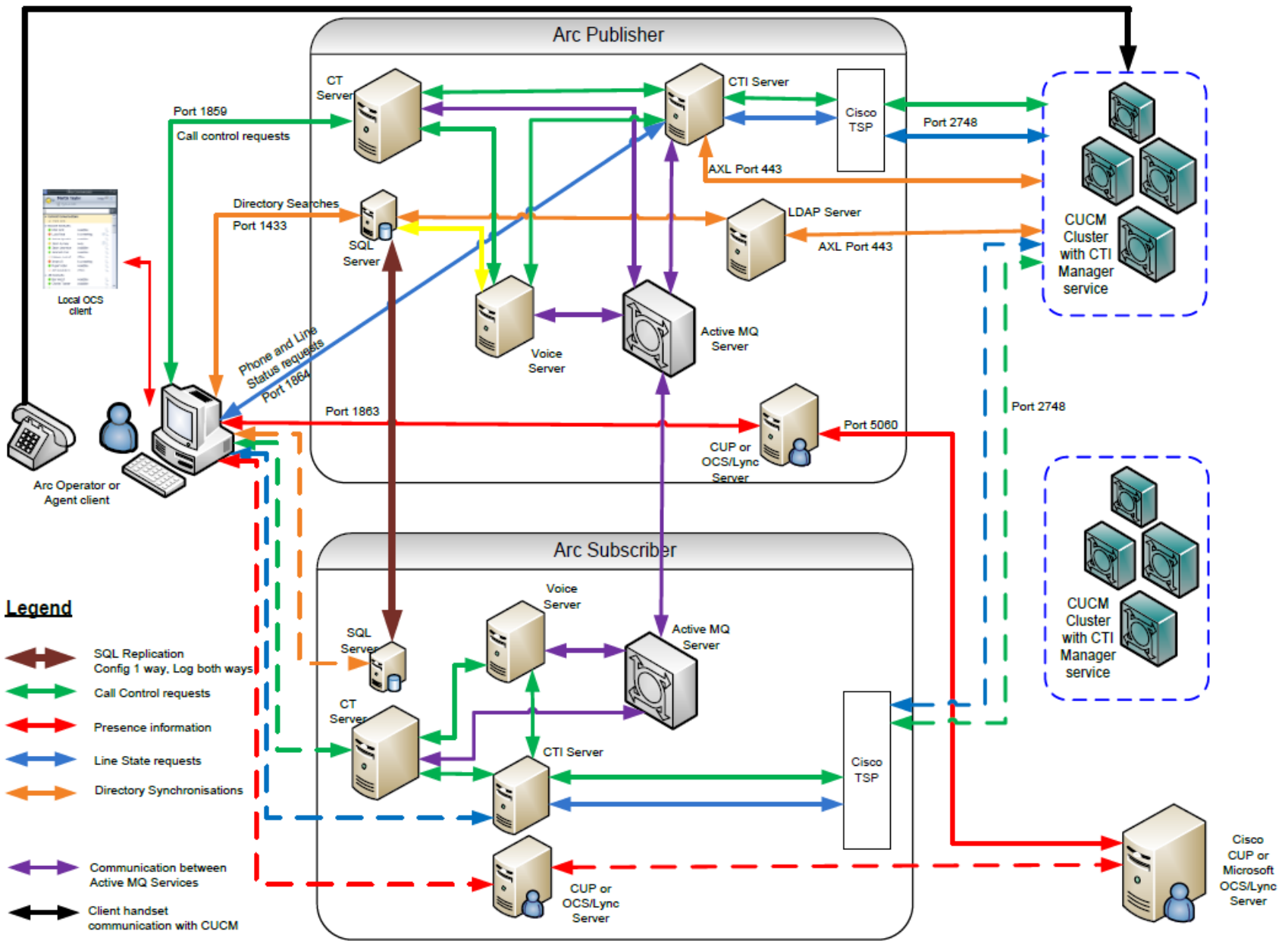
All the relevant Arc Pro services are installed by a single installation script ensuring that they will be in place when needed. These services are:

Arc Pro CT Server	This is the engine of the system and runs the configuration of the system. It is also the service that the clients (agents, operators, supervisors, wallboards) connect to.
Arc Pro CTI Server	The CTI Server handles all communications requests between the Arc Pro system and the CUCM system. This includes communication to the Cisco TSPs installed on the Arc Pro Server and handles all CTI requests, and AXL communications allowing the system to request information on the correct CUCM devices.
Arc Pro LDAP Server	This service handles all directory synchronization requests via LDAP including to the CUCMs being used.
Arc Pro Voice Server	The Voice server provides both a basic IVR system and in-queue messaging for call held in Arc queues. It streams the relevant messages at the correct point in a call. It connects to both the CT and CTI Servers.
Arc Presence Server	Allows a direct connection to a Cisco IM&P, WebEx Connect and Skype for Business Server to obtain relevant presence information for contacts.

In addition Arc makes use of a Microsoft service called Active MQ. This allows communication between the two Arc Pro Servers if a resilient solution is installed. This service is also installed by Arc during the main installation.

Also required on the Arc Pro Server are SQL Server, and Cisco TSP(s). More details of the requirements of these are given in 4: SQL database overview and 3: CTI integration respectively.

The diagram below shows the basic elements of an Arc Pro system. The server components all reside on the machine known as the Arc Pro Server. The clients connect to the Arc Pro CT Server over port 1859 for all of the call control communications. Other ports are used for additional elements, and are shown on the diagram. For a full list of IP ports used by Arc, refer to TCP Ports reserved for Arc use.


Arc Publisher
CT Server
CTI Server
Cisco TSP
Port 1859
Call control requests
Port 2748
AXL Port 443
Directory Searches
Port 1433
SQL Server
LDAP Server
AXL Port 443
CUCM Cluster with CTI Manager service
Local OCS client
Voice Server
Active MQ Server
Phone and Line Status requests Port 1864
Port 1863
Port 5060
CUP or OCS/Lync Server
Port 2748
Arc Operator or Agent client
Arc Subscriber
Voice Server
SQL Server
Active MQ Server
CT Server
CTI Server
Cisco TSP
CUCM Cluster with CTI Manager service
CUP or OCS/Lync Server
Cisco CUP or Microsoft OCS/Lync Server
Legend
SQL Replication Config 1 way, Log both ways
Call Control requests
Presence information
Line State requests
Directory Synchronisations
Communication between Active MQ Services
Client handset communication with CUCM

Bandwidth and Latency

As with any client/server software architecture there are many items of communication that pass across the network layers in order to function correctly. In terms of Arc the area that is critical is the messages between the Clients (Operator and agents). Arc will support a maximum latency of 150m/s Round Trip Time (RTT) between any client and the server.

In addition care should be taken to ensure that the RTT between the Cisco TSP on the Server and the CUCM. Details on this are available in the *Cisco SRND*.

CTI architecture

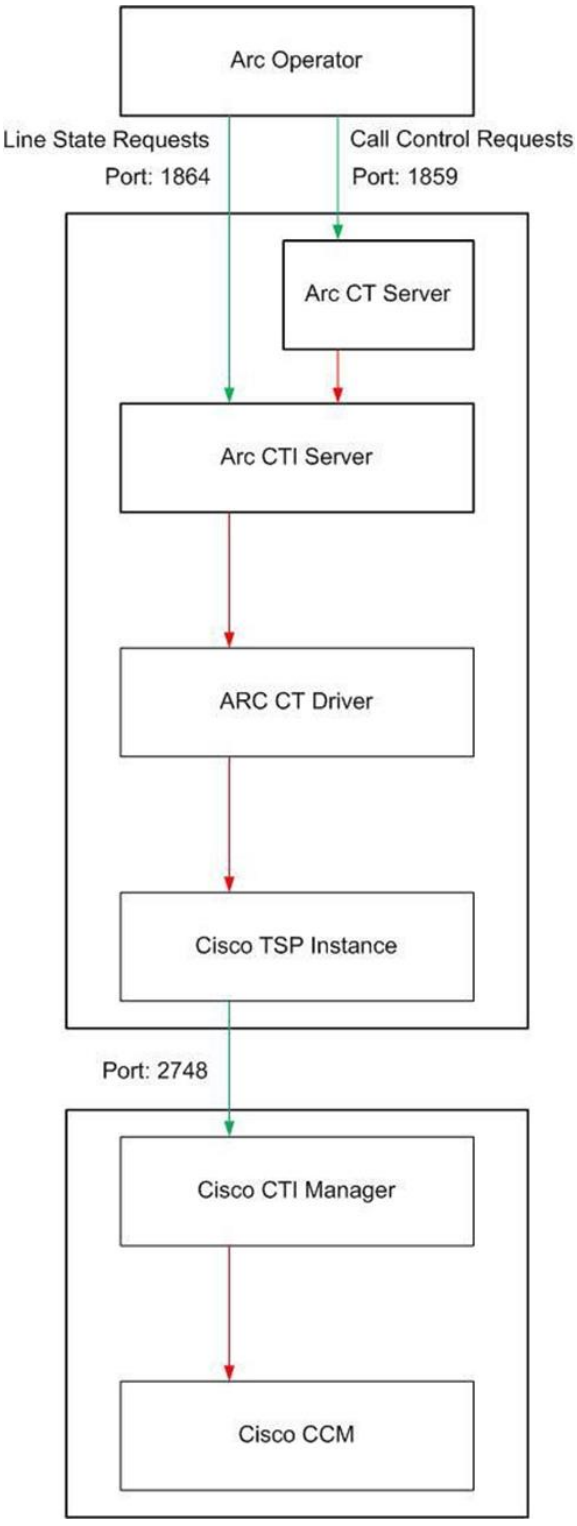
The diagram above shows the basic connectivity between the Arc Pro Server(s) and the CUCM clusters. The system provides call control and device monitoring via CTI connections between the Arc Pro Server and the CUCM cluster(s). In essence the Arc Pro Server must request every element of call control to be made via this interface, and the CUCM will act upon that request, sending back a confirmation message when the action is complete. This requires software to be installed on the Arc Pro Server, the Cisco TSP. The TSP communicates with a service on the CUCM - the CTI Manager. It is possible to install up to 10 TSP instances on a single server to increase scalability of CTI resources or allow connections to multiple CUCM clusters.

Only one TAPI application can be installed on the server, with up to 10 separate instances. The TSP instances can be pointed to different nodes, which can be on the same or different clusters. It is recommended that the TSP version is kept fully up to date with the latest version from the most up to date cluster in the system. Cisco have backwards compatibility within their TSP to allow support for different versions during an upgrade cycle. Ultimately it is recommended that all CUCM cluster being used by the Arc Pro Server are running the same version.

The CTI Manager is a service that can be activated on each CUCM node in the cluster if required, however this is on request only. It is therefore important to design the CTI requirements into the overall CUCM design. It must be ensured that at least one node has CTI Manager enabled as a minimum.

CTI Request Information Flow

The diagram below illustrates how the information flows from the Arc Pro Client right through to the CUCM, which actually moves the calls. The green arrows indicate requests made across the network, the red arrows indicate requests made within a single environment, that is the Arc Pro Server or the CUCM node.

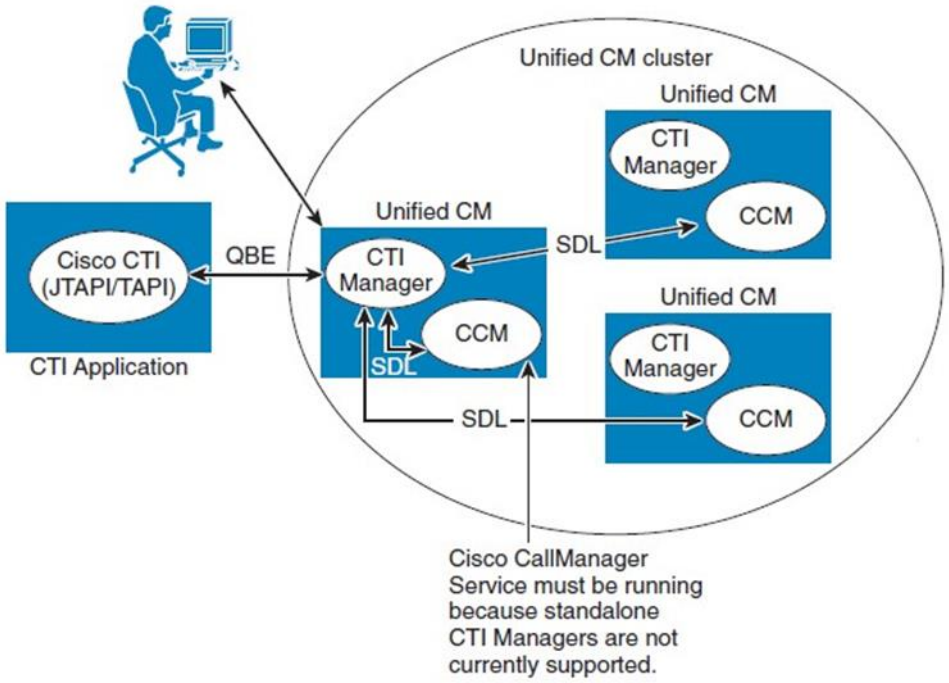


For CTI applications that require redundancy, each TSP instance can be configured with two IP addresses, thereby allowing an alternate CTI Manager to be used in the event of a failure. It should be noted that this redundancy is not stateful in that no information is shared and/or made available between the two CTI Managers, and therefore the CTI application will have some degree of re-initialization to go through, depending on the exact nature of the failover.

When a CTI Manager fails-over, just the CTI application login process is repeated on the now-active CTI Manager. Whereas, if the Unified CM server itself fails, then the re-initialization process is longer due to the re-registration of all the devices from the failed Unified CM to the now-active Unified CM, followed by the CTI application login process.

Cisco CTI consists of the following components (see Figure below), which interact to enable applications to take advantage of the telephony feature set available in Cisco Unified CM:

- CTI-enabled application — Cisco or third-party application written to provide specific telephony features and/or functionality.
- JTAPI and TAPI — Two standard interfaces supported by Cisco CTI. Developers can choose to write applications using their preferred method library.
- Unified JTAPI and Unified TSP Client — Converts external messages to internal Quick Buffer Encoding (QBE) messages used by Cisco Unified CM.
- Quick Buffer Encoding (QBE) — Unified CM internal communication messages.
- Provider — A logical representation of a connection between the application and CTI Manager, used to facilitate communication. The provider sends device and call events to the application while accepting control instructions that allow the application to control the device remotely.
- Signalling Distribution Layer (SDL) — Unified CM internal communication messages.
- Publisher and subscriber — Cisco Unified Communications Manager (Unified CM) servers.
- CCM — the Cisco Call Manager Service, the telephony processing engine.
- CTI Manager (CTIM) — A service that runs on one or more Unified CM subscribers operating in primary/secondary mode and that authenticates and authorizes telephony applications to control and/or monitor Cisco IP devices.

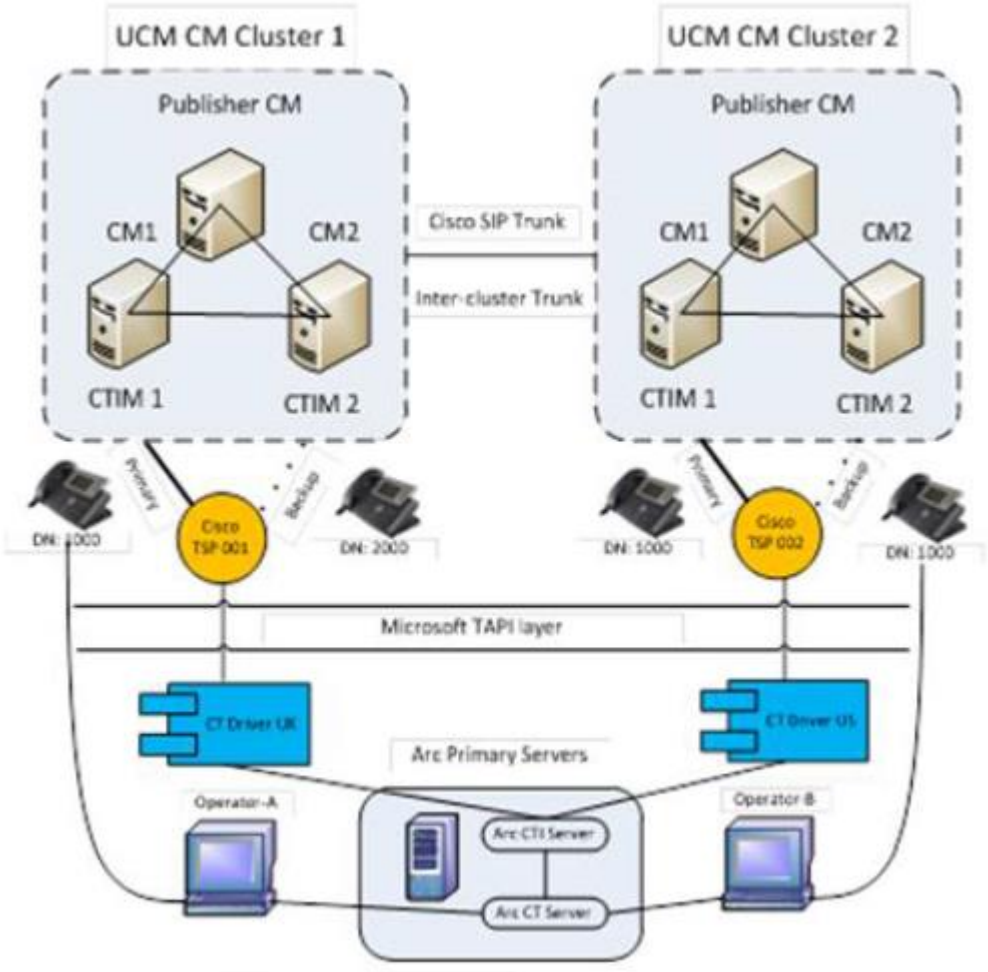


Arc Pro CTI setup

With a basic understanding of the Cisco CTI setup, this section looks at the options for setting up the CTI for Arc to function correctly. The table below gives a brief explanation of the terms used in this section:

Term	Definition
Cisco TSP Instance	The Cisco TSP is installed on the Arc Pro Server machine, and can run up to 10 separate instances. Each instance is configured separately with regards to its Primary and Secondary CTI Manager Connections allowing multiple clusters to be connected to from the same server. Each instance also requires a unique Application User profile which gives the instance its roles and permissions.
Cisco CTI Manager	See Section above.
CT Driver	Configured internally within Arc and linked to a TSP Instance. Allows the Arc Pro CTI Server to knowingly communicate with a specific CUCM node or cluster.
Resource Group	Allows the Arc controlled CTI Devices to be grouped together for specific tenants allowing multiple tenants to be supported on a single Arc Pro system. These are assigned to a Resource Repository Group. See below.
Resource Repository Group	A logical grouping of items within Arc. Associated to a RRG are Resource Group(s), contacts, CT Drivers, Dial Plans and clients (operators/agents). Via the link to a CT Driver > TSP Instance these items are linked to a particular CUCM cluster.

Each Arc Pro Server requires a minimum of one TSP instance to be configured and active before it can start. The diagram below shows an example of an Arc Pro Server setup configured to connect to two CUCM clusters.



Within Arc is a requirement to set up CT Drivers. These are used internally to determine which TSP Instance is used when a device is to be monitored. If 10 TSP Instances are being used then 10 CT Drivers within Arc need to be configured, and through configuration these are then linked together. TSP Instances can be configured to connect to the same cluster if required, or can be used to provide control of devices across multiple clusters. The diagram below shows a simple example of a two cluster set up, which could be expanded as required.

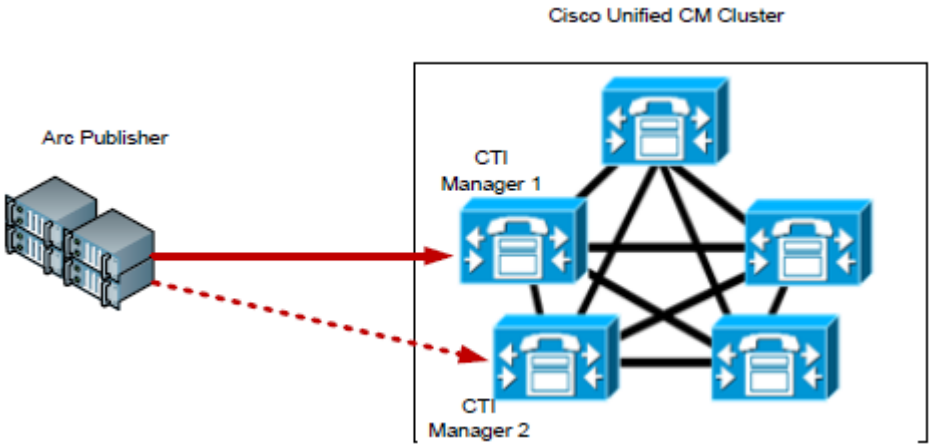
In this case two CT Drivers have been configured within Arc, one linked to TSP Instance 001 and the other with TSP 002. Each of these instances in connected to a different cluster allowing the single Arc Pro Server to monitor devices on both clusters.

To complete the link a CT Driver within Arc is linked to a Resource Repository Group, to which Contacts are linked, and also to a Resource Group, meaning that the controlled Arc Pro system Devices are also linked to a CT Driver. For more details see CT drivers.

CTI Resilience

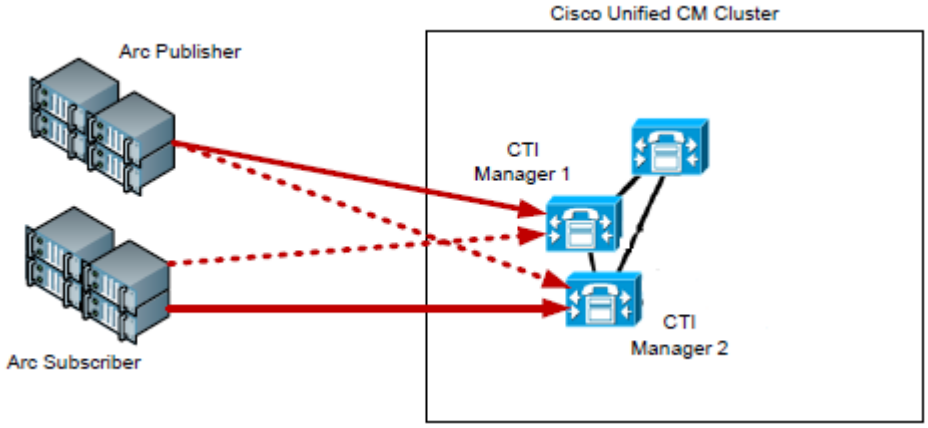
The Arc Pro Server(s) can be configured to use resilient TSP setups to provide resilience in the event of a CTI Manager Service failing for whatever reason. This is configured in the TSP itself and allows a Backup CTI Manager to be used when the Primary fails. The diagrams below show the options for this.

Single server



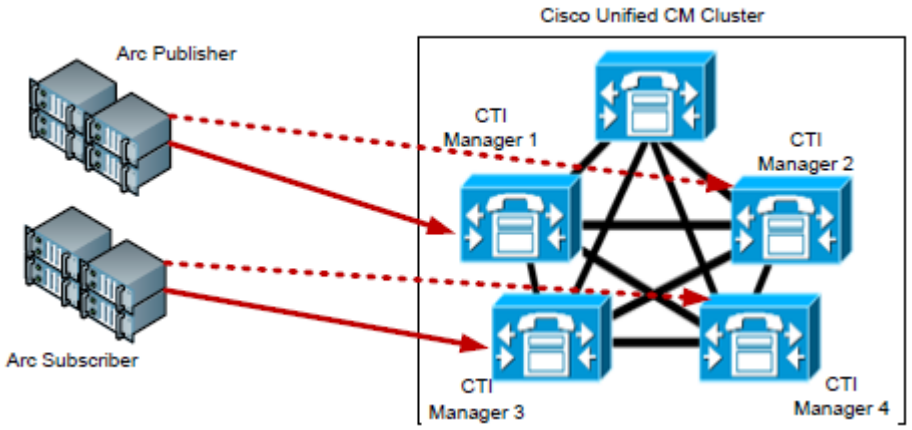
In this example there is a single Arc Pro Server, the Publisher and a five node cluster. There are two nodes running the CTI Manager Service. The Arc Pro Server is running a single TSP instance with a Primary connection to CTI Manager 1 and a Backup connection to CTI Manager 2.

Resilient Arc Pro Servers on a small cluster



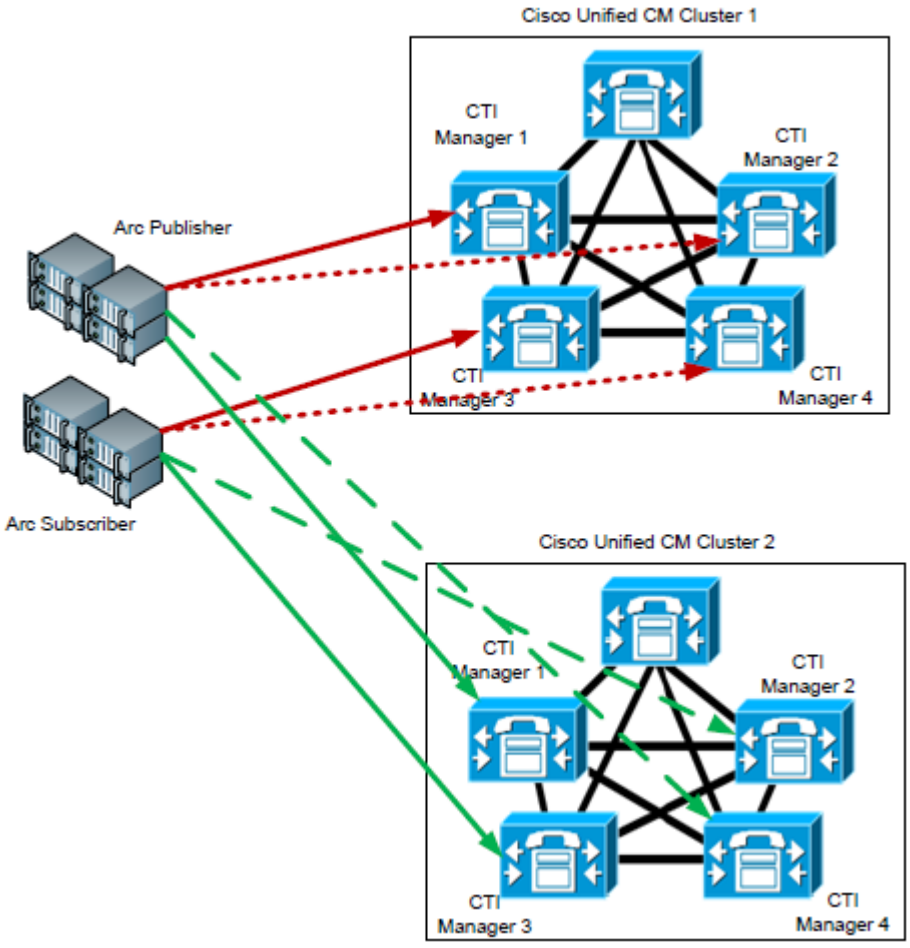
In this example there are only three nodes in the cluster. It is not recommended to use the CTI Manager on the Publisher node, therefore both servers should use the CTI Managers on the two subscribers, while trying the balance the load as best they can. Each server should use a different CTI Manager as the primary connection, and fail over to the other node on failure.

Resilient Arc Pro Servers on a single large cluster



This setup aims to provide complete CTI redundancy. Each Arc Pro Server is configured with a single TSP instance with Primary and Backup connections. To spread the load completely the setup uses 4 CTI Managers on the cluster, with neither server relying on the same CTI Manager as the other server.

Multi Cluster with resilient Arc Pro Servers



In the a Multi cluster environment each Arc Pro Server requires a minimum of two TSP instances – one per cluster, with Primary and Backup connections for each. Using this method allows the solution to scale to a maximum of 10 clusters.

2: CUCM Interoperability

This chapter contains the following information:

Cisco UCM compatibility matrix

The Arc Pro system relies on the CUCM being a fully supported and tested version.

To confirm that your CUCM version is supported check the *Arc Pro Compatibility Matrix*.

The compatibility matrix shows Arc versions currently 'in life' and the CUCM platforms they support. It also describes specific TSP versions that Arc has tested.

Cisco Phone compatibility

The Arc Pro suite needs to be compatible with Cisco handsets for a large number of reasons to provide comprehensive functionality. These reasons are:

- User Handsets (operator/agent).
- End Point, that is, whether we can get Line State information.

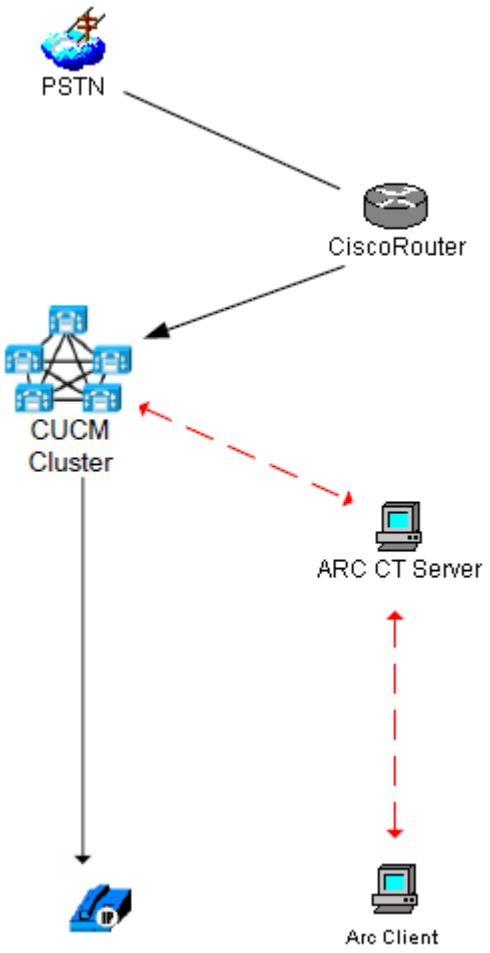
A full list of handsets and their compatibility is presented in the *Arc Pro Compatibility and Performance Guide*.

Arc Call Flow

The Arc Pro system is designed to provide comprehensive call queuing capabilities to allow the right calls to reach the right people. It is also designed with flexibility in mind to manage peaks and troughs in call traffic across the call queues within the system.

Basic System Call Flow

The below diagram explains the standard call flow and describes how a call is delivered into the Arc Pro system.



Calls are delivered from the PSTN to the Cisco CallManager (PBX) via the Gateway Router. A transcoder may be in place for Compression and Decompression of Calls (see Bandwidth and Latency).

The call is routed to a CTI Route Point (Pre CT Gateway) controlled by the Arc Pro Server, the CallManager is then informed how to route the call according to the configuration of the Arc Pro system.

The call is delivered by the Cisco CallManager to the Arc Pro Client via the IP Phone. The ARC PRO CT Server communicates with the Arc Pro Client via IP with status messages.

Call Route

IP Communication

The CUCM needs to be configured for the call from the PSTN to be routed to a Pre CT Gateway device.

Arc-controlled system devices

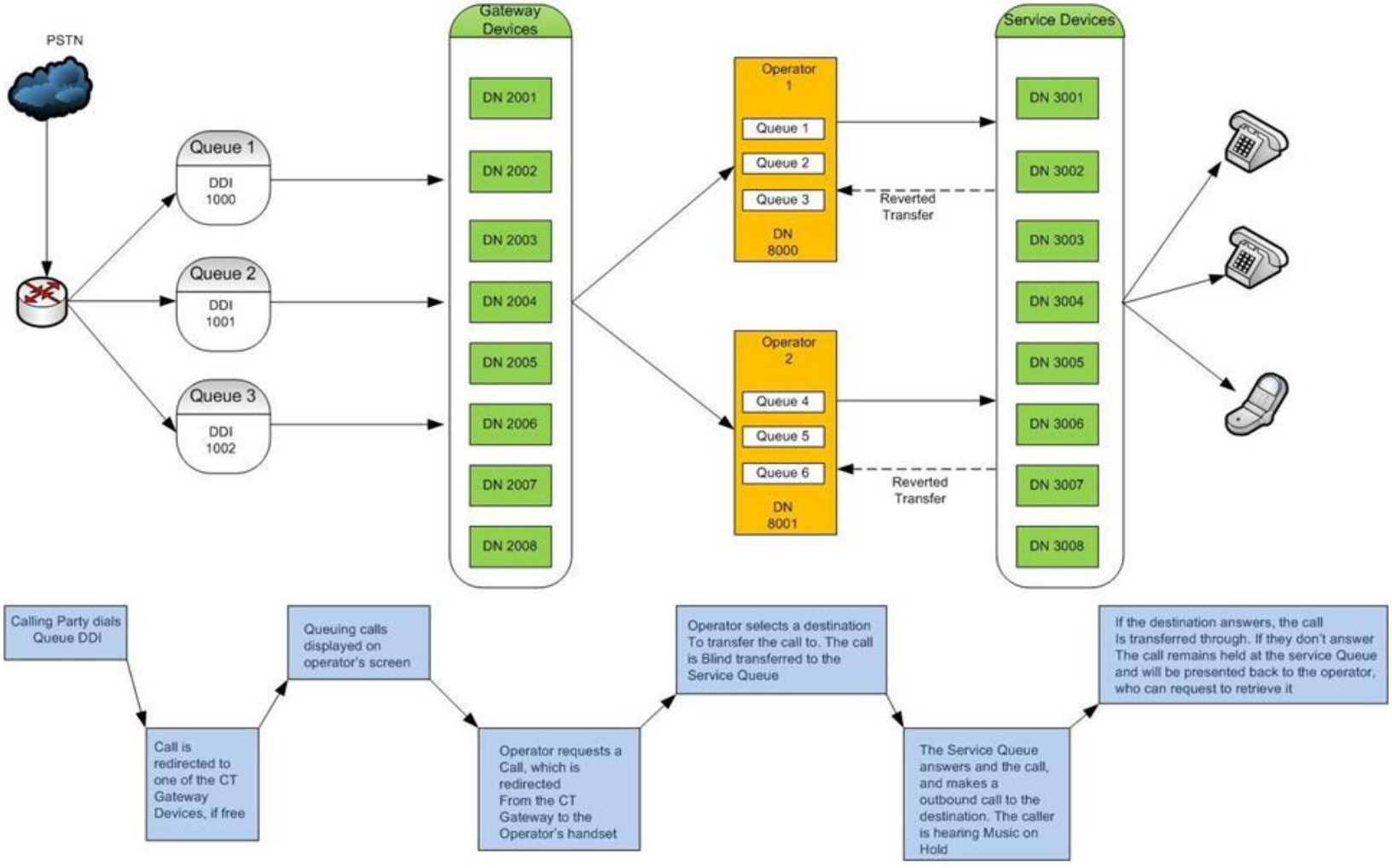
Arc requires virtual CTI devices to be configured on the relevant CUCM to allow the call to flow correctly. The table below describes important considerations when defining system resources.

Item	CUCM device type	Consideration
Pre CT Gateway	CTI Route Point	For EVERY DDI/DID that is to be routed into the Arc Pro Server, a Pre CT Gateway needs to be configured.
Queue Location	CTI Route Point	For each Console and Voice queue configured in the Arc Pro system, a queue location is required.

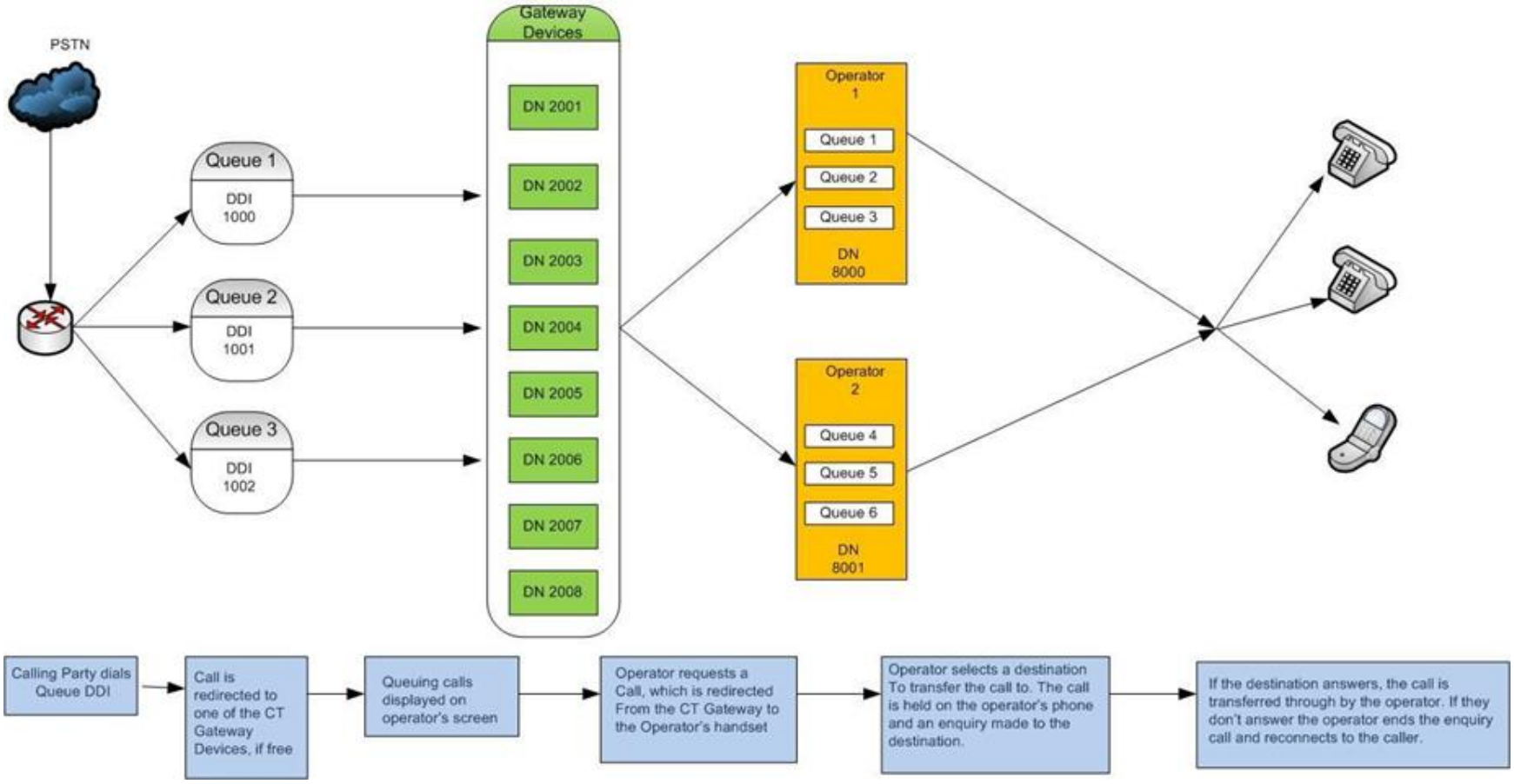
Item	CUCM device type	Consideration
Host PBX Gateway	CTI Port	These devices are used for queuing calls that have not yet been answered. The recommendation is that there is the same amount of Host PBX Gateway Devices as there are PSTN lines coming into the Arc Pro system. Once a call has been answered by an Arc Pro Client app this Port will be freed up to receive another call. Example: If there will be a 30 line PRI coming into the Arc Pro system, then create 30 Host PBX Gateway devices. This will mean that the Arc Pro Server will be able to queue as many calls as there are physical phone calls.
Service Queue	CTI Port	The Service Queue is used by the attendant console to Hold, Transfer and Camp On calls. The recommendation is 4 – 6 Service Queue devices are configured per attendant console user. These devices are only used with the attendant console. If the attendant console is not going to be installed, then these devices need not be created. Once a call is taken by the desired end point, or the Arc Console Operator if needed, it frees up the CTI Port to take another call.
Call Park Devices	CTI Port	The Call Park Devices are used for the Operators to park calls. It is recommended that 3 Call Park devices are configured per attendant console user. These devices are only used with the attendant console. If the attendant console is not going to be installed, then these devices need not be created. Once a call is taken by the desired end point, or the Arc Console Operator if needed, it frees up the CTI Port to take another call.
Static Voice Ports	CTI Port	These devices are used to record messages via the Voice Connect configuration. It is recommended that two Static Voice Ports are configured. These devices are only used with the Voice Connect product. If Voice Connect is not going to be installed, then these devices need not be created.
CTI Reference Device	CTI Port or CTI Route Point	A standalone CTI Port or CTI Route Point must be created for use by the CTI Server to ensure that it can function. This is very important and requires a unique CTI Ref device per Application user/TSP Instance.

Detailed Call Flow

The following two diagrams illustrate the call flow followed in the case of both an operator blind and consultation transfer. Call Connect calls follow the same methodology as the console calls to reach an agent.



Blind Transfer: outlines the way that calls will flow through the Arc Pro system when a blind transfer is performed.



Consultation Transfer: the above diagram outlines the way that calls will flow through the Arc Pro system when a consultation transfer is performed.

Calling Search Spaces and Partitions

Calling Search Spaces (CSS) and Partitions are used within a CUCM system to control the calling abilities of the devices in the system. Due to the architecture of the Arc Pro system it is essential that incoming calls to Arc can be transferred to all devices that could possibly be required. This will include potential external to external transfers as well as internal transfers.

Arc v6 introduces a new method of moving the calls from one devices to the next. Technically this is called a lineBlindTransfer which replaces the previous lineRedirect. Although this changes nothing on the surface, behind the scenes it means that the CSS of the call changes as it progress and is based on the transferring device. It is therefore important to understand the call flow explained above,

Arc Pro CTI Route Points and CTI Ports therefore need to have the relevant Calling Search Spaces and Partitions assigned to allow them to receive and then transfer the call. Under the default installation Service Queue Ports must be able to call any destination which any operator may wish to transfer a call to. If the operators use Direct Transfer then it is the operator's line that needs to be able to call any individual destination.

Arc recommends that a separate Partition and CSS be created for the System Devices.

The Arc operator or agent client IP Phones do not need to have the same Calling Search Space and Partition as the controlled CTI devices, however it must be ensured that they can receive incoming calls from the Host PBX Gateways devices, and the Service Queue devices where calls return unanswered. They also need to be able to dial both the Service Queue and any other destinations to which they may transfer calls. The Service Queue devices must be able to dial the operator's handset and all other destinations for transfers.

CSS/PTN and their effect on Arc

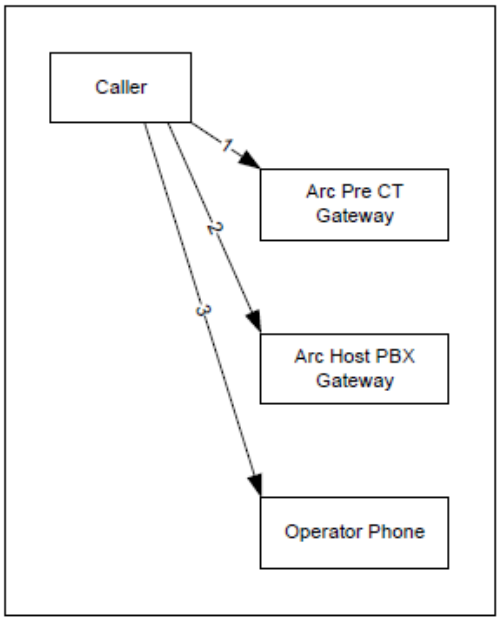
This section outlines the detail of calling search spaces and the requirements of these to allow Arc to function correctly in many of the most common call routing scenarios.

Key to all elements of operation is that whenever a call is moved through the Arc Pro system, it is done using lineblindtransfers. In doing this, the Calling Search Space of the call is changed at each point as the call moves through the system.

The sections below outline the CSS impacts in each of the main stages of Arc operation.

Answering Calls

The scenario below outlines a call being answered on the operator console.



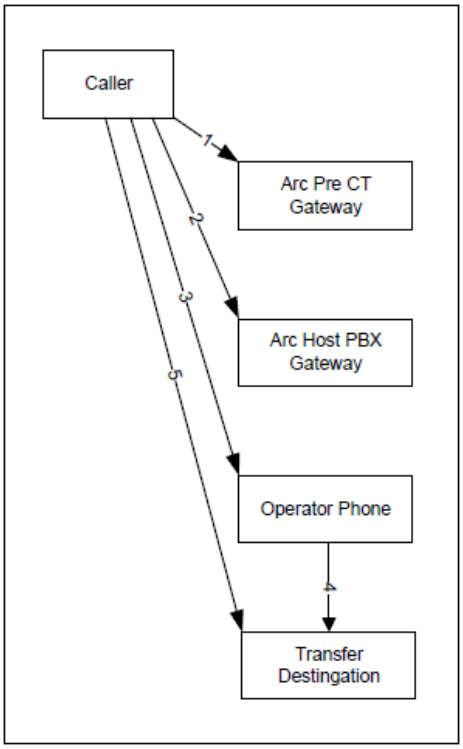
1. Call arrives to the Arc Pre CT Gateway device, this notifies Arc that the call has arrived for the specified queue, and allows for CLI filter checking. The CSS of the CTI Route Point is now being used.
2. Call is routed to the pool of Host PBX Gateway devices, based on the resource group of the Pre CT Gateway. Call now being made from the originating point to the Host PBX. The CSS changes from that of the originating point to that of the Host PBX port.
3. Operator selects to answer the call or the call is delivered by forced delivery. Call is routed from the CTI Port to the Operators Phone. The operator is now connected to the original caller.

Note

If a call can be seen within the operator console (F8) but when selected to answer the call does not move to the operators phone, check the CSS for the Host PBX port. Does it contain the partition that the operator's phone is in?

Consult Transfer

The scenario below explains a call being answered and then consult transferred to a destination.



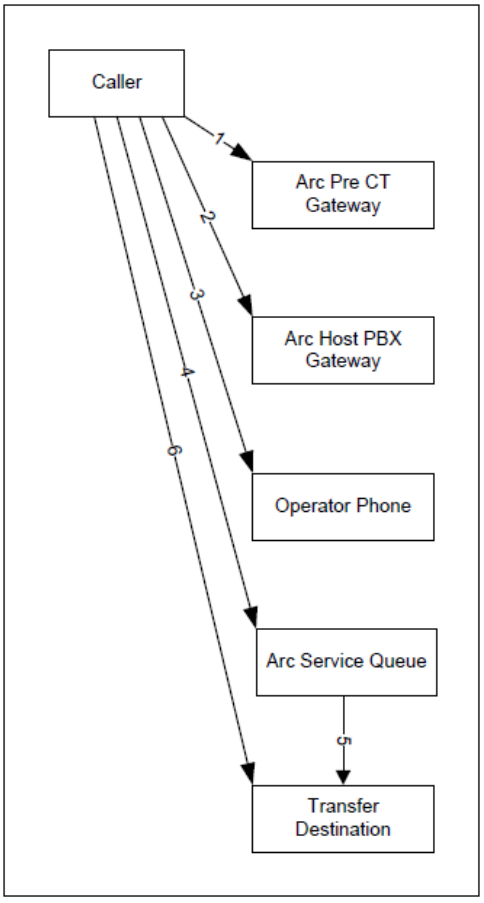
1. Call arrives to the Arc Pre CT Gateway device, this notifies Arc that the call has arrived for the specified queue, and allows for CLI filter checking. The CSS of the CTI Route Point is now being used.
2. Call is routed to the pool of Host PBX Gateway devices, based on the resource group of the Pre CT Gateway. Call now being made from the originating point to the Host PBX. The CSS changes from that of the originating point to that of the Host PBX port.
3. Operator selects to answer the call or the call is delivered by forced delivery. Call is routed from the CTI Port to the Operators Phone. The operator is now connected to the original caller. The call now takes the CSS of the Operator's Line/phone.
4. The Operator dials the destination for the consult transfer, this will use the CSS of the operators line/phone, as per any other call / transfer made just using the IP handset.
5. With the end party having answered the call, completing the transfer will connect the original caller, with the transfer destination.

Note

If a user waits for the phone to start ringing and then completes the transfer this will cancel the consult transfer, and initiate a blind transfer to the end destination.

Blind Transfer (Standard functionality)

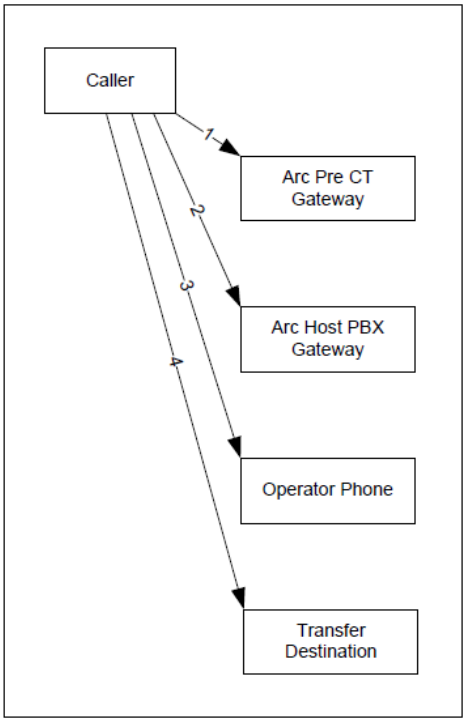
The scenario below explains the steps involved in a blind transfer, without using the direct transfer feature of Arc.



1. Call arrives to the Arc Pre CT Gateway device, this notifies Arc that the call has arrived for the specified queue, and allows for CLI filter checking. The CSS of the CTI Route Point is now being used.
2. Call is routed to the pool of Host PBX Gateway devices, based on the resource group of the Pre CT Gateway. Call now being made from the originating point to the Host PBX. The CSS changes from that of the originating point to that of the Host PBX port.
3. Operator selects to answer the call or the call is delivered by forced delivery. Call is routed from the CTI Port to the Operators Phone. The operator is now connected to the original caller. The call now takes the CSS of the Operator's Line/phone.
4. The Operator dials the destination for the blind transfer at which point the call is transferred to one of the pool of service queue devices, based on the resource group it originally arrived at. The CSS changes from that of the Operator's line to that of the Service Queue port.
5. The Service Queue answers and puts the call on hold and will then make an enquiry call from the to the end destination.
6. Once the call has been answered by the destination the call is connected.

Blind Transfer (Direct transfer)

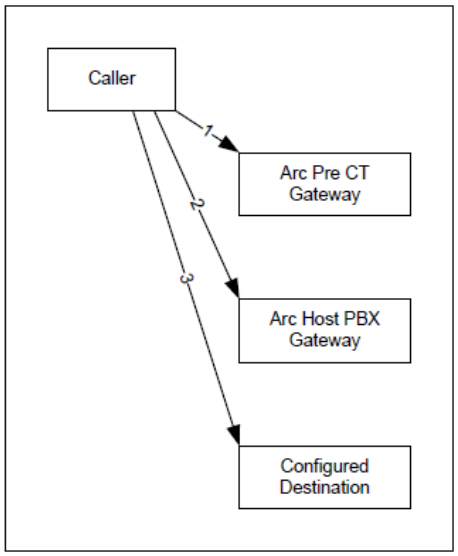
The scenario below explains the steps involved in a blind transfer, using the direct transfer feature of Arc, thereby when the call is blind transferred it is seen as from the original caller, not the Arc Pro Service Queue devices.



1. Call arrives to the Arc Pre CT Gateway device, this notifies Arc that the call has arrived for the specified queue, and allows for CLI filter checking. The CSS of the CTI Route Point is now being used.
2. Call is routed to the pool of Host PBX Gateway devices, based on the resource group of the Pre CT Gateway. Call now being made from the originating point to the Host PBX. The CSS changes from that of the originating point to that of the Host PBX port.
3. Operator selects to answer the call or the call is delivered by forced delivery. Call is routed from the CTI Port to the Operators Phone. The operator is now connected to the original caller. The call now takes the CSS of the Operator's Line/phone.
4. The Operator dials the destination for the blind transfer, the call will be transferred from the operators extension to the transfer destination, using the operator's line CSS.

Night Service / Overflows / Out of Service

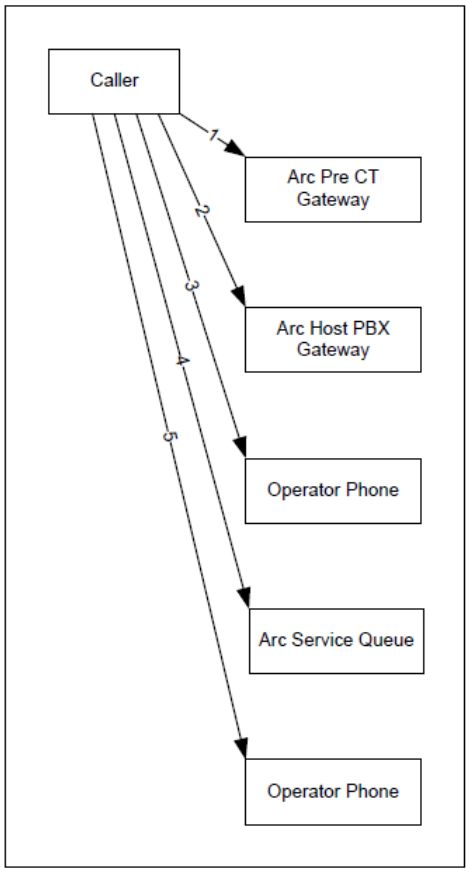
This scenario describes the effects of the calls where the calls are in night service, set to over flow based on an overflow condition or set to out of service, and the destination number entered is a DN not an internal queue within Arc.



1. Call arrives to the Arc Pre CT Gateway device, this notifies Arc that the call has arrived for the specified queue, and allows for CLI filter checking.
2. Call is routed to the pool of Host PBX Gateway devices, based on the resource group of the Pre CT Gateway. Call now being made from the originating point to the Host PBX. The CSS changes from that of the originating point to that of the Host PBX port.
3. Based on the night service / overflow / out of service forwarding the call is forwarded to the DN configured as the destination.

Holding Calls

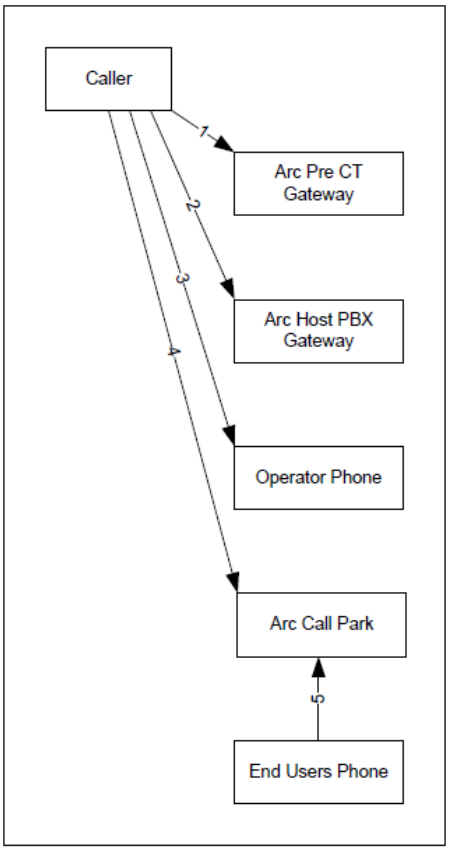
The scenario below describes the process undertaken when a call is answered and then held, and then retrieved.



1. Call arrives to the Arc Pre CT Gateway device, this notifies Arc that the call has arrived for the specified queue, and allows for CLI filter checking. The CSS of the CTI Route Point is now being used.
2. Call is routed to the pool of Host PBX Gateway devices, based on the resource group of the Pre CT Gateway. Call now being made from the originating point to the Host PBX. The CSS changes from that of the originating point to that of the Host PBX port.
3. Operator selects to answer the call or the call is delivered by forced delivery. Call is routed from the CTI Port to the Operators Phone. The operator is now connected to the original caller. The call now takes the CSS of the Operator's Line/phone.
4. Operator places the call on hold, the call is routed to one of the service queue devices, based on the resource group of the original queue the call entered through. The call now has the CSS of the Service Queue port.
5. If the Operator choses to retrieve the call, then the call is redirected back to the operators phone. The call reverts back to the CSS of the operator's line/phone.

Parking Calls

The scenario describes the situation where a call is parked and the call is picked up from that park location by the intended recipient.

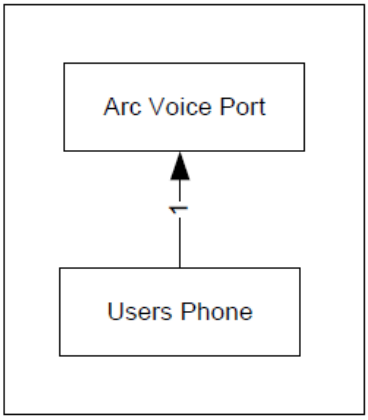


1. Call arrives to the Arc Pre CT Gateway device, this notifies Arc that the call has arrived for the specified queue, and allows for CLI filter checking.
2. Call is redirected to the pool of Host PBX Gateway devices, based on the resource group of the Pre CT Gateway. Call now being made from the originating point to the Host PBX. The CSS changes from that of the originating point to that of the Host PBX port.
3. Operator selects to answer the call or the call is delivered by forced delivery. Call is routed to the Operators Phone. Call now takes the CSS of the Operator's line/handset.
4. The Operator parks the call for a user, the call is redirected to one of the call park devices, based on the original resource group of the call. The Call then takes the CSS of the CTI Port where the call is parked.
5. An End user dials to the Arc Call Park device, therefore their CSS must have access to the Call Park Devices, once connected, the two calls are joined together.

Note

If the call is not picked up by the intended recipient, and is in fact retrieved by the operator, then the call flow is as that of a held call.

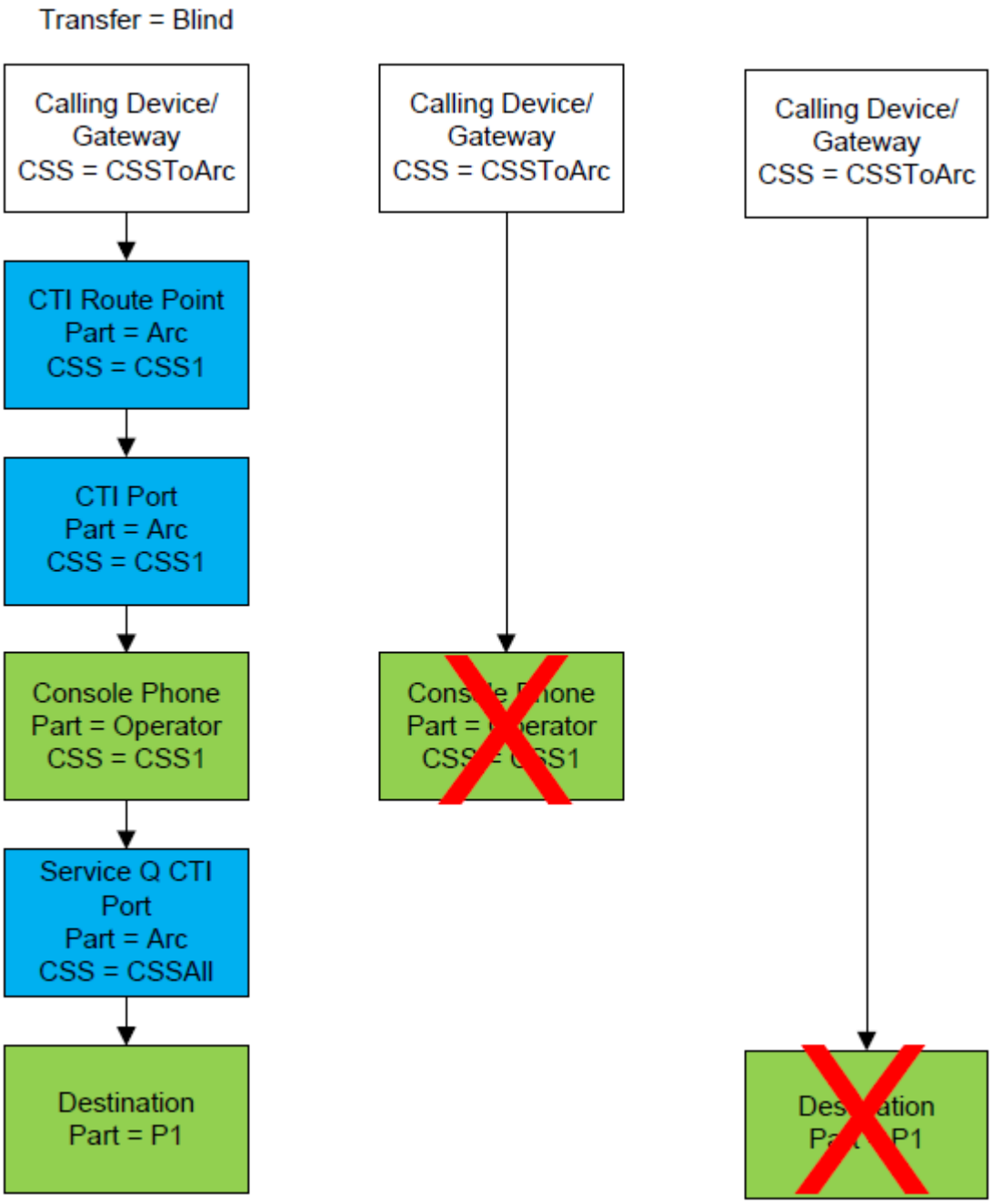
Voice Port – Recording a message



When the user selects Connect to a controlled phone from Arc Pro Admin / Supervisor then a call is made from the Users phone, to the Arc Pro Voice Port. Therefore the CSS of the user's phone, needs to be able to dial the Arc Pro Voice Port directly.

Call Flow example with Partition/CSS

The example below can be used to explain how the theory above can be used:



In this example, a call is made into the system via a gateway, The Gateway has a CSS assigned called "CSSToArc" which includes the partition of "Arc" only. The devices coloured blue are the Arc Pro system Devices and are in the partition "Arc", meaning that the call on the Gateway can dial any of the controlled devices if required. The operator phone is in a different partition "Operator", which is not in the CSS of the Gateway, therefore as per the second item above a call cannot be routed from the Gateway directly to the operator. In the same way the final destination that the caller requires is in partition "P1" and again this could not be routed directly from the Gateway.

In the working example these destinations can be reached when using Arc. Firstly the call can be routed from the Gateway to the CTI Route Point, where the CSS is changed to "CSS1" which includes the Partition "Arc". This allows the call to be routed onto the Host PBX Gateway port, which has the same partition and CSS as the CTI Route Point. Now the call needs to be routed to the operator's handset in Partition "Operator". This partition is also included in "CSS1", which allows the call to reach the operator.

The end result is that using the routing within Arc a call can be connected between the Gateway and the operator, whereas if the routing was to be made directly the call would fail. Similarly, the CSSToArc CSS does not include the partition of P1, in which the notional destination handset is located in the example. This means that a direct call via the gateway would not be delivered but as a blind transfer from Arc, via a Service Queue CTI Port, will be delivered successfully.

Music on Hold

Arc Pro does not provide Music on Hold, Instead it relies on CUCM MOH to provide the media streams when a call is being held on one of the Arc controlled CTI Ports. The Arc Ports in the Host PBX Gateway and the Service Queue are allocated randomly, and you cannot guarantee that specific calls will use specific ports, however this can be controlled in multi-tenant situations, see below. It is therefore recommended that you use a standard MOH source across all the Arc Pro CTI Ports. This should be set up as a Unicast broadcast due to issues being seen in certain when transferring calls to other applications such as UCCX when using multicast MOH.

Callers are likely to hear MOH when they are being held by the operator, when being blind transferred, when they are awaiting a consultation transfer or conference to be completed or when they have been parked.

Multi-Tenant scenarios

It is possible to use Resource Groups to group the relevant Arc Controlled devices together, effectively making several mini Arc Pro systems running off the same server. This means that as a call goes through the system it will be kept within one resource group or another. This could be made relevant to multi tenants on the same system, or could be configured per queue if desired. There are limits on the number of CTI Ports that can be used – 255 when using the TAPI Wave Driver or 1000 when using the New Media Driver (default). This would allow different MOH sources to be used for each resource group, which could be made relevant to each. More details on Multi Tenancy can be found in 6: Multi-Tenant including Multiple Cluster Support.

CODECs

It is imperative that this section is understood fully before an Arc Pro implementation commences.

G711

G711 is a supported codec for any Arc installation, whether the TAPI Wave or New Media Driver is deployed.

G729

The Cisco New Media Drivers allows us to support the codec natively for the first time.

G729 Native Support

Where the New Media Driver is available Arc will also support G729 without any need for transcoding resource between clusters. In order to support G729 the codec must be advertised as available, which is not done by default.

Applications which natively support G.729 can change the default codec advertisement by setting the G729PassThrough registry option to ON (1). This should be set on the Arc Pro Server, or both Servers in a resilient solution.

The Registry key can be found at:

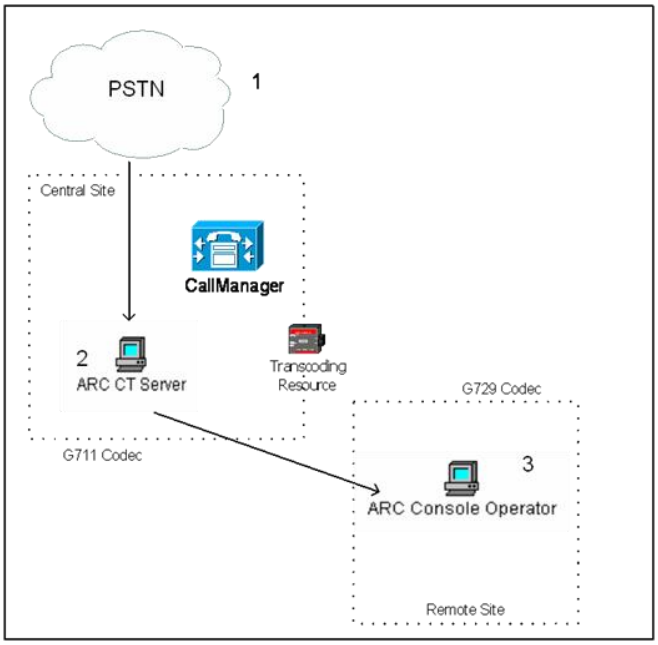
- Windows Server 2003: *HKEY_Local_Machine/Software/Cisco Systems, Inc./RtpLib/G729PassThrough*
- Windows Server 2008: *HKEY_USERS\S-1-5-20\Software\Cisco Systems, Inc.\RtpLib\G729PassThrough*

Example

1. G729PassThrough set to ON.
2. TSP application registers CTI port 1.
3. CTI port 1 advertises G.711 and G.729 support.
4. Unified CM is not configured with MTPs for transcoding.
5. CTI port 1 calls Device 1000.
6. Device 1000 only supports G.729, so the application plays the appropriate G.729 media file.

The figures below illustrate a typical call flow:

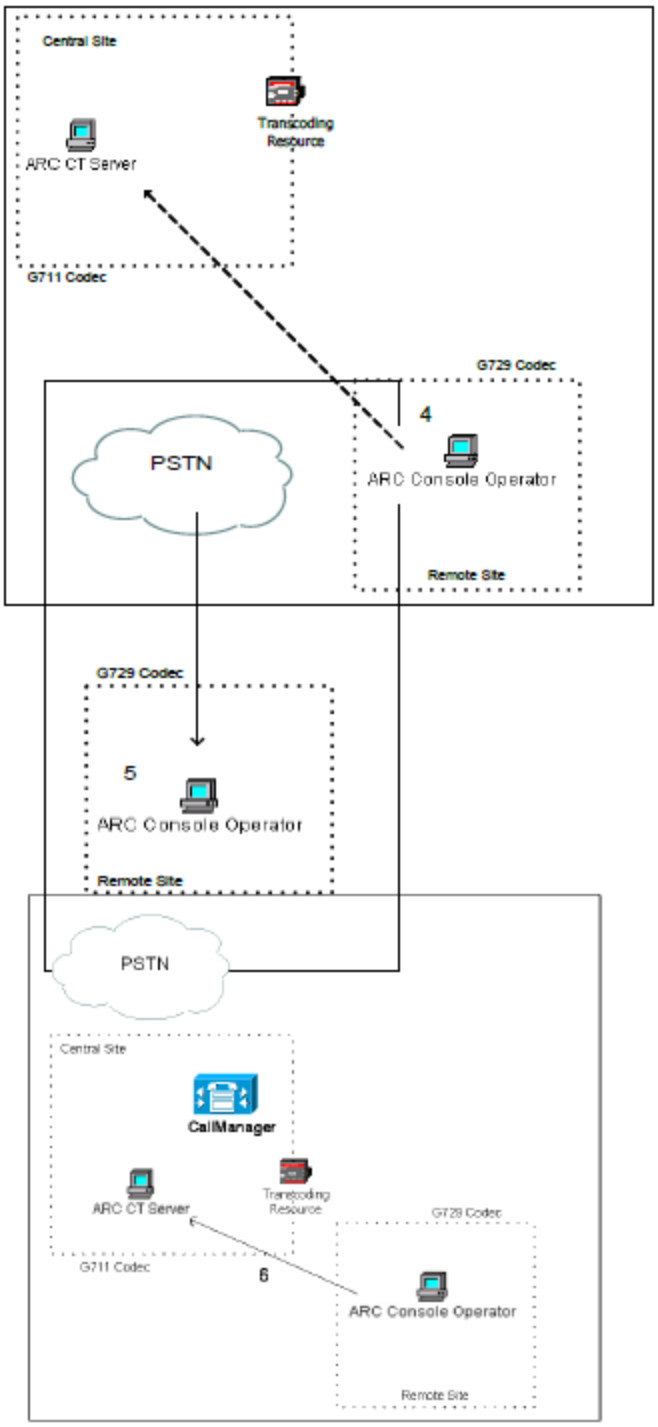
Figure 1: Call enters the system



1. Call is received from PSTN
2. Call is routed from the Pre CT Gateway to the Host PBX Gateway.
3. The attendant console client now has visibility of the call in the queue.

At this point, the call is ringing on the Host PBX Gateway and is in the queue waiting to be answered. The Host PBX Gateway devices are registered to the CUCM in the local site. Therefore the call has a codec of G711 at this point.

Figure 2: Remote Operator Requests the call



4. The attendant console requests the call.

Once the attendant console requests the call, the call will be delivered to the Operator extension.

Figure 3: The attendant console answers the call

5. The attendant console is talking to the caller.

Now that the Operator is talking to the caller, and the Operator is on the remote site, the call has will be established with the G729 codec.

Figure 4: The attendant console puts the call on hold

6. The attendant console requests the call to be put on hold.

When the attendant console requests to put the call on hold, the call is redirected back to the Arc Pro Server, to be put on hold on a Service Queue Device (CTI Port).

At this point, the transcoder will be required to convert the call back to the G711 codec so that the Wave enabled CTI Port can accept the call.

If the call is still G729 when it reaches the Service Queue, the CUCM will disconnect the call. The same theory applies if the call is being transferred, parked, or camped on.

3: CTI integration

This chapter contains the following information:

Arc v6 uses the CTI Server element to monitor all required devices, whether for Line State or the Arc Pro system Devices, and manage all CTI Interactions with the Cisco TSP Instance(s).

Multiple TSP instances are supported and, by using configured CT Drivers within the Arc Pro system, these can be linked to different types of devices and communicate with different CUCM CTI Managers, including on different clusters. This section covers all aspects of the CTI integration for Arc.

CTI overview

The CTI Server runs as a service on the Arc Pro Server. It is installed as part of the default installation of the Arc Pro Server elements, and because it is essential to the running of the Arc Pro system it is mandatory and cannot be unchecked from the installation. The Arc Pro Clients do not connect to the CTI Server at any point, instead they connect to the main Arc Pro CT Server, and all their requests for call control and Line State information are routed through the CT Server to the CTI Server for onward processing.

TSP instances

The Cisco TSP must be manually installed on the Arc Pro Server. The TSP can be configured with up to 10 instances, allowing each instance to communicate with a different CTI Manager (CUCM Node), including nodes on multiple CUCM clusters. If running across clusters it is a requirement that all the clusters being used are running the same CUCM version.

CT drivers

Arc requires internally recognized CT Drivers to communicate with the correct Cisco TSP Instance to obtain the correct information about a device. As a rule there should be one CT Driver configured for each active TSP instance that is being used on the Arc Pro Server.

A Default CT Driver must be configured for both the Publisher and Subscriber Arc Pro Servers. The default driver is very important to the system and its name cannot be changed. This driver will be used in lieu of other configured drivers if they become unavailable for whatever reason. Each server requires a working Default Driver before the CT Server will be able to be activated.

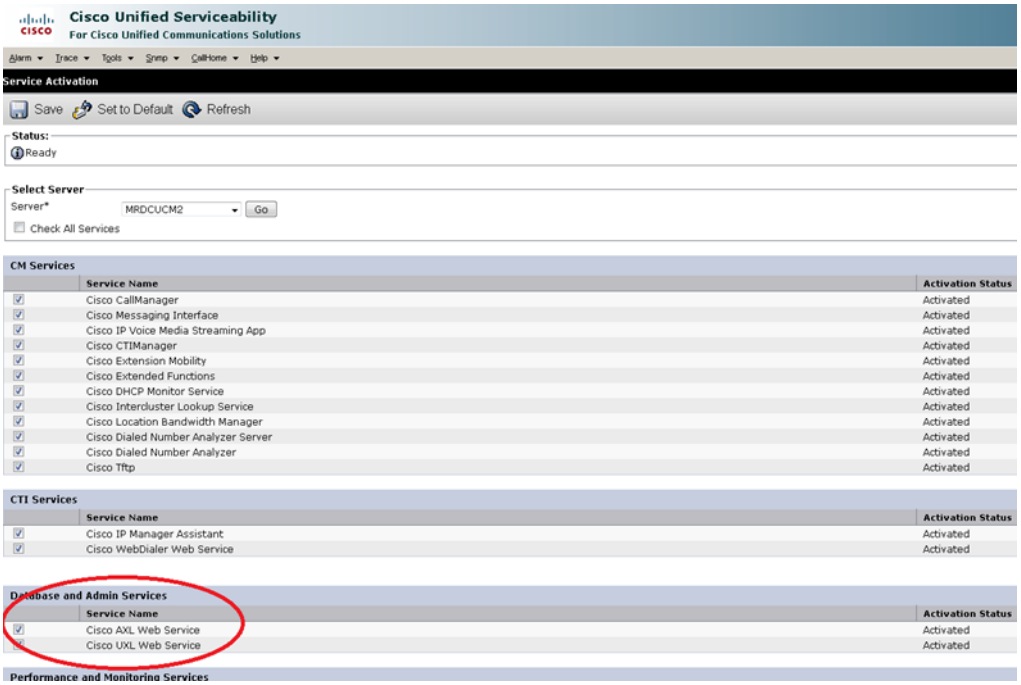
It is possible to assign more than 1 TSP instance to a CT Driver, via the  button. This lists all the TSP instances configured on the Publisher server. When configuring subsequent CT

Drivers for the Publisher TSP Instances that are already assigned to Drivers will not be available for selection.

The Admin does not read in the instances when configuring against the Subscriber server. The same list is used. For this reason it is recommended that the Pub and Sub are both configured with the same number of TSP's, and the selection list is effectively a name only, like *CiscoTSP001.tst*, *CiscoTSP002.tsp*. If the Subscriber has more TSP instances that the Publisher the workaround is to create dummy instances on the Publisher so that the selected instance can be selected.

Device Resolution Manager (DRM)

This is the CUCM connection that is required for the CTI Server to know where it needs to connect to when it needs to resolve a device for call control or line state. This is done using the AXL SOAP protocol and this can be any CUCM node on the relevant cluster, but the chosen node(s) must have the Cisco AXL Web Service running, as below:



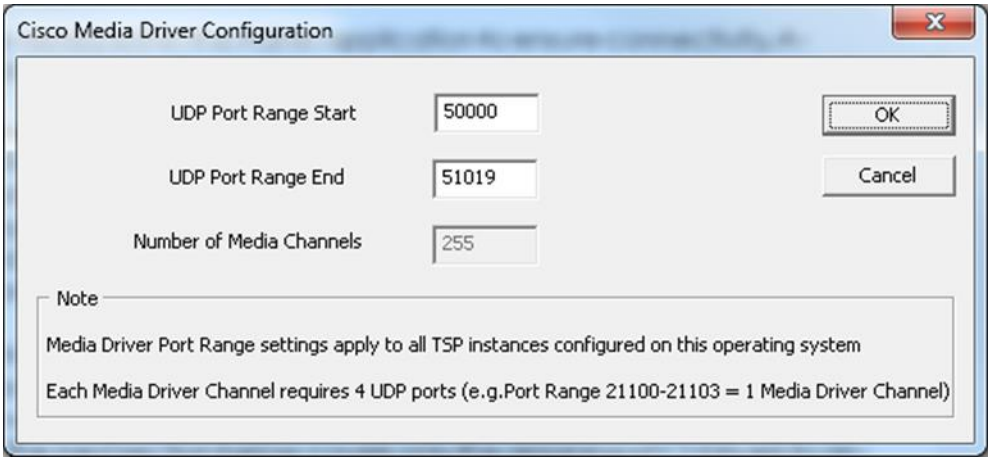
These should be tested within the Admin application to ensure connectivity. A secondary DRM can be configured for each CT Driver for system redundancy purposes. The DRM configured within Admin does not have to match the CTI Manager configured against the TSP instance, therefore you can balance the load of CTI and DRM requests across multiple nodes in a cluster.

Media details

Both the Cisco TAPI Wave Driver and the New Media Driver are supported by Arc, however the installation defaults to the New Media Driver. Among the benefits of this are increased system scalability and codec support and ease of installation. Which driver is required depends on the CUCM version being used, but where there is an option Arc recommends using the New Media Driver.

Once the CT Drivers are configured and tested within the configuration, they are then added to a Resource Repository Group (RRG). Without this additional configuration they will not be used. More information on RRGs is shown in the Multi Cluster section of this document. The next section below covers only the assigning of CT Drivers to an RRG.

The CTI Ports to be used by Arc require a media driver to be available in order for them to activate. The two driver types have different scalability limits. The default New Media Driver support is scalable and determined on the Call manager CTI Node and is documented under Multi-cluster support, the Cisco TAPI Wave Driver will support 255 CTI Devices. When configuring the New Media Driver during the installation is a requirement to enter a range of UDP Ports to allow for these device. There must be 4 ports available for each CTI Port being used. This can be changed after installation via the Cisco TSP Media Driver configuration in Programs>Cisco TSP:

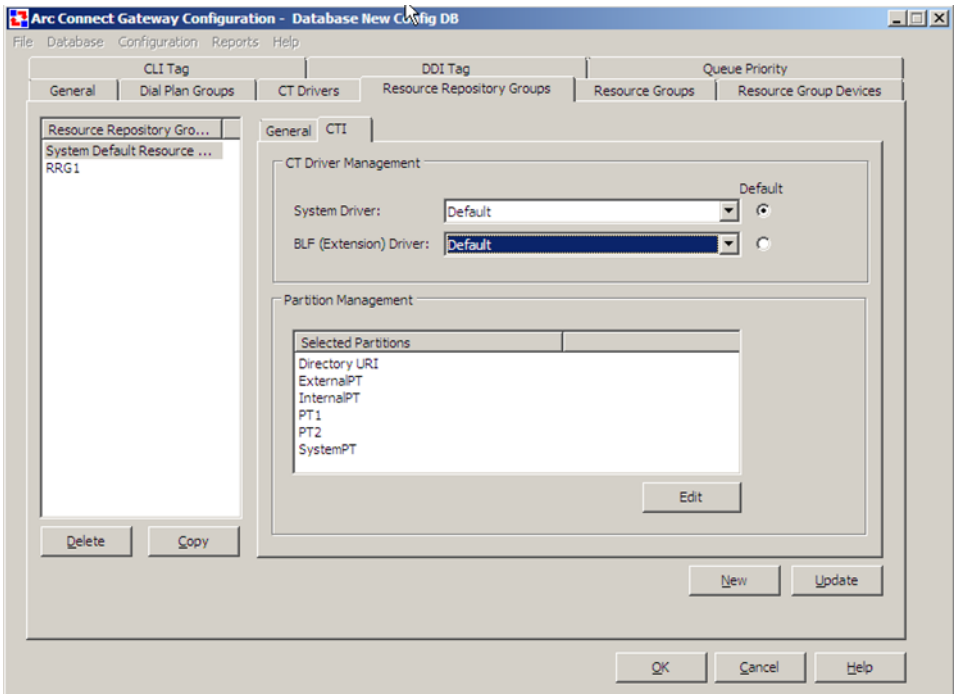


Assigning Drivers to TSP Instances

Resource Repository Groups (RRGs)

RRGs are a concept that brings together several elements and concepts of the Arc Pro system, allowing them to be aligned with different CUCM clusters. Within their configuration the main elements are the applicable Dial Plans to be used and the CTI Drivers to be used for System Devices and Busy Lamp monitoring.

A separate CT Driver can be used for System Devices and BLF within the same RRG, as seen below:



By having separate drivers available for each RRG it becomes possible to load balance between the System Devices and the ones being monitored for line state. As each TSP instance can use different CUCM nodes to connect to the CTI Manager Service this allows the CTI load to be spread, where possible. We do recommend where possible that a separate BLF Driver be created which can be shared amongst other RRG's connecting to the same cluster but in other CT Drivers.

Determining the correct device to be monitored relies on as much information being passed to the DRM as possible, and one of the key pieces of that information is the partition that a device belongs to. In this section the partitions to be used when resolving devices in this RRG are selected and ordered.

Using the Edit button a table is shown with all the available Partitions read in from the CUCM to which the assigned CT Drivers are connected, based on the Primary DRM of the System Driver. Once the partitions are selected they can be ordered in terms of preference, so where devices have the same DN and different partitions, the actual device returned is based on the one with the highest preference. It is possible to create separate RRG's using the same CT Driver with different order of partitions to allow different devices to be returned where contacts are put into a different RRG. This would allow, for example, for different offices to have identical number plans with the point of differentiation being the partition, and get the right device state returned.

Due to the preference system, the more partitions selected within an RRG the slower the DRM system will be in returning the DN/Device resolution as it has more queries to run. It is recommended that where possible the Partitions are limited to an absolute minimum.

For more details on RRGs see 6: Multi-Tenant including Multiple Cluster Support.

Device association

Application User

Each TSP Instance requires an Application User to be configured on the CUCM with the relevant Roles assigned. These are:

- Standard AXL API Access
- Standard CTI Allow Control of all Devices
- Standard CTI Allow Control of Phones supporting Connected Xfer and conf
- Standard CTI Allow Control of Phones supporting Rollover Mode
- Standard CTI Enabled

CTI Template Device

Arc can now provision the entire CTI range of devices via the Provisioning Wizard/Administrator. In order to do this it is highly recommended that you create a template device on the Call Manager for all CTI device configuration to be based on.

The purpose of this is to ensure that all CTI devices have the relevant configuration to function correctly such as CSS, Partition and Device Pool amongst many others. Without a template device the call manager will select its own 'defaults' or a 'Null' value will be used where default options are not available.

It is strongly recommended that the template device be a CTI Port as default settings for maximum number of calls and busy trigger (5000 / 4500 respectively) is not supported for a CTI port and will cause a failure. However this will in turn create all route points with the maximum setting of the CTI port so it is recommended that you up the default on the CTI port to its maximum (Max Calls 200).

Cisco System Sizing Tool

CUCM device weightings are calculated depending on the device type, number of lines, number of applications per line and the BHCA (Busy Hour Call Attempts) that can be expected. To assist in planning your system there is information on system sizing in the *Cisco SRND*.

Monitoring of devices for Arc

There are a number of imposed restrictions placed upon the limits of device numbers that can be monitored concurrently. Recent improvements in the CTI scalability within CUCM mean that Arc is capable of scaling as well in terms of the number of devices that can be monitored. The Cisco Unified Communication Manager Design Guidelines advise that there are device association limits dependent on the types of servers hosting the CUCM.

It should be noted that figures used throughout this section refer to CUCM clusters running on 7845 servers. For clusters running 7825/7835 servers the figures should be reduced, however with the ability for the devices to be monitored only as and when they are needed Arc will be able to run and manage the system to stay within any set limits without affecting the system reliability.

Refer to the relevant *Cisco SRND* for more details on these scalabilities.

It is recommended that you create at least one CT Driver for BLF users per cluster. This will ensure that requests for BLF are treated separately to call control requests and ensure efficiency.

System Device monitoring

Arc 6.1.1 and above exploits the extended CTI scalability of the latest CUCM versions, and requires all system devices to be assigned to appropriate application users.

Previously, CUCM limitations prevented the Arc Pro system from achieving the desired scalability unless system devices were monitored dynamically - as described in TAPI Super provider (dynamic) monitoring. Devices are assigned automatically when either using the Provisioning Wizard, or performing a CUCM synch through the Admin application.

TAPI Super provider (dynamic) monitoring

All devices within Arc used for Line State, are monitored dynamically, irrespective of the CUCM version being used. This utilizes functionality within CUCM known as Super provider, which allows any device in the cluster to be monitored on demand, subject to the CUCM load limitations.

The functionality requires that the Roles of “Standard CTI Allow Control of All Devices” and “Standard AXL API Access” be associated with the User Profile, in addition to the other CTI roles assigned previously. All devices used by Arc are based on the device selection algorithm.

The CTI Server application is used to monitor all devices. Once started it waits to receive requests before doing anything else.

The BLF devices are opened based on requests from the Operators only when they need to view their state. The devices are monitored dynamically and will be managed automatically. The CTI Server will keep a number of devices monitored in a cached list per CT Driver, set to 2000 by default. At this point the CTI Server will start de-monitoring (close) opened lines as new ones are requested. There is also a maximum number of opened lines allowed which is set to 2500 by default per CT Driver but can be increased.

These figures are on a Line basis. When monitoring a device every line on that device is monitored to provide the device state that is displayed on the Operator’s screen. If a device has 4 lines configured then this gives a count of 4 towards the 2000 total.

Device and Line monitoring

With Attendant Console applications of old there has traditionally only been one Busy Lamp 'slot' per person in the directory. This would generally show whether just that individual line was busy. If the user has other lines on that device this status was generally unknown unless all the lines were being individually monitored.

Device centric monitoring is used as default within Arc. This CTI feature allows Arc to not only monitor the user's whole device, but also to see the line usage detail against that device. This is important because many Cisco phones support 2, 6 or 8 or more lines.

The operator directory view displays the 'summary' device (phone) status without the operator having to do anything, so it's immediately obvious that the user is busy or not. Paging up and down the directory will update the phone status for all contacts shown. Pressing the F2 key pops up a window that shows all lines configured on a contact's device with their status, as well as the CLID of the caller if they are connected (and their name if there is a match to their CLID in the Arc directory). This powerful feature means the operator can be fully informed of all call activity against any telephone user in the Arc directory, as well as being able to perform group pickup of any of the calls visible on that phone (in ringing state only) should they so wish to do so.

Call Forward Display

Call forwarding information is limited to Call Forward All's that are set. The information is shown in the main directory view when using Device Centric monitoring but only if the Line is the primary line on its monitored device, due to the fact that forwards are set on Lines and NOT devices. The forwarding information will be shown in this mode when the operator opens up the device in F2 to view each individual line, and will be able to see each line which may have a forward set on it.

Note that this ability to see call/caller information against a device can be turned off for those countries where privacy of information is sensitive.

Line States explained

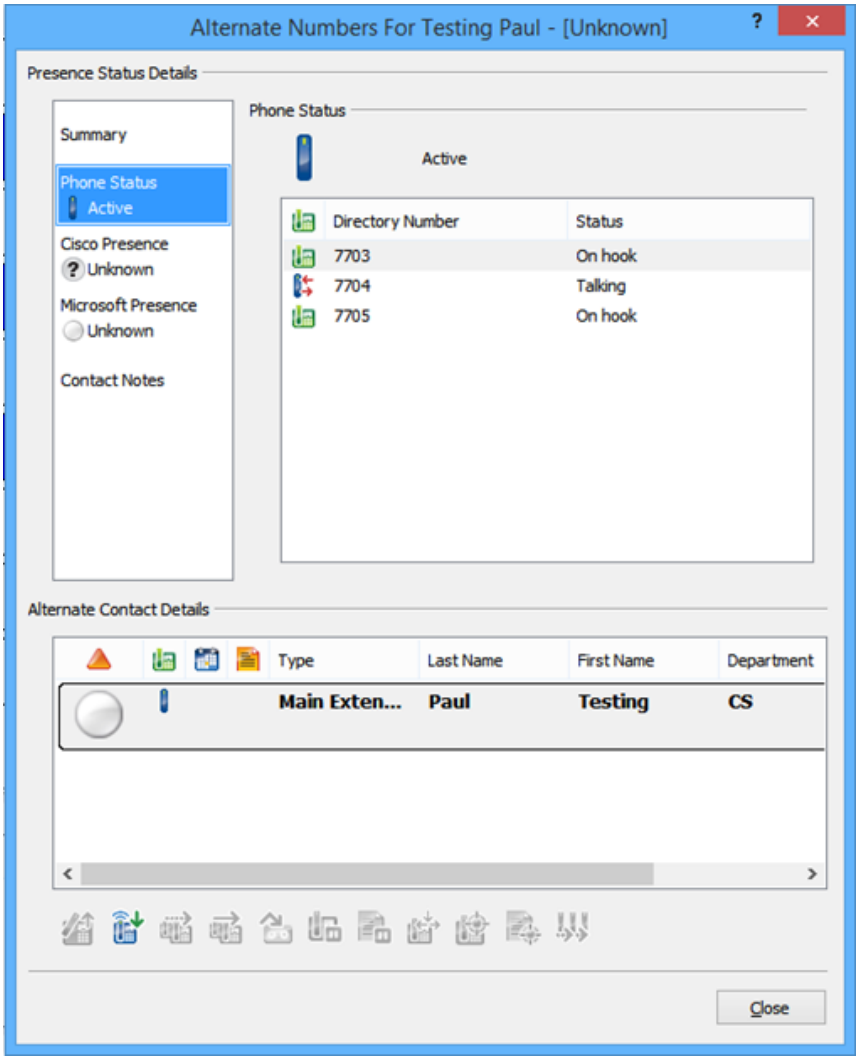
Shared Lines

The term 'Shared Lines' refers to DN that share the same number and partition on the CUCM. This gives the user the ability to monitor and answer calls for those colleague(s). This might be because they are part of a team or are working as a fall back answer point for another person. So the lines are 'shared' in their appearance.

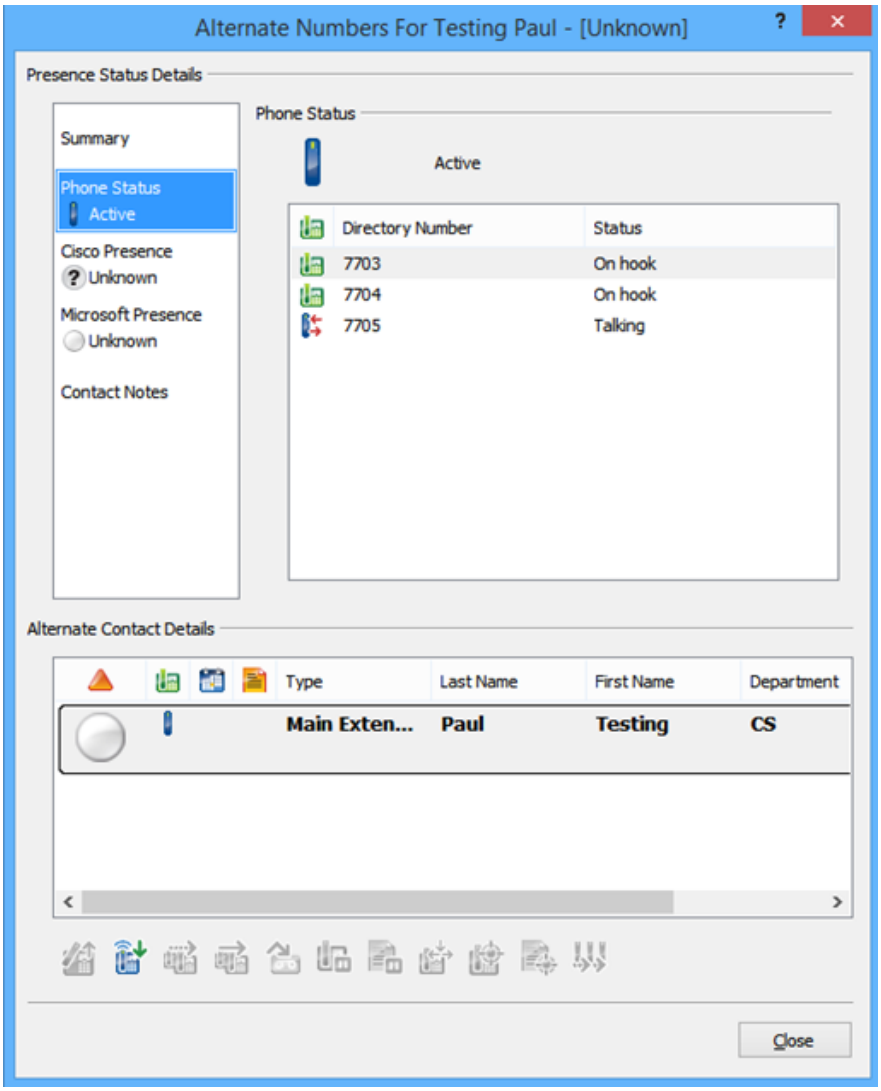
Actual shared line example based on the following lines configured on 2 devices:

Device	**Device 2**
Line 1 = 7703	Line 1 = 6051
Line 2 = 7704	Line 2 = 7704
Line 3 = 7705	

This provides a device view (Phone Status) for each contact on the main directory window of the Attendant Console. This means that no matter which line appearance (shared or not) on a device is active the attendant will see an Active icon. An attendant can then drill down into the device detail via the F2 key. This will open a new form, shown below:



In this example it is 7704 that is the connected line on the device, which is the shared line, however in the next example the device is still shown as Active, against the directory contact at 7704, but this time the actual line that is active is 7705, which is the 3rd line appearance on that particular device:



While these statuses are shown, there is NO activity shown on any other contacts with DN 7704 which have different Device Names configured which means a contact with Phone2 above will not show as active in the F3 Directory, however they would see activity against 7704 in their F2 view. More details of the various states are shown in the table below.

Device state	Device	Directory view	F2 View of shared DN
Off Hook	Actual		
	Other		
Ringing Out	Actual		
	Other		
Connected	Actual		
	Other		
Hold	Actual		
	Other		
Ringing In	Actual		
	Other		
DND	Actual		 (Shows DND against all individual lines on the device)
	Other		
Call Forward All	Actual		
	Other		
Conference	Actual		 Status = Conference or Conference Controller
	Other		 Status = Talking

Multi-cluster support

A single Arc Pro Server will support multiple CUCM clusters by using multiple TSP Instances on the Arc Pro Server.

The Arc Pro CTI Server support limit depends upon the call manager specification and version, this can be anywhere between 1000 and up to 10,000 devices per Cisco TSP Instance/node. Whilst it is possible for these numbers to achieve with the built in load balancing it is best to configure the min and max limits to be close to what you expect the CTI devices to be in terms of monitored BLF and System devices if not the maximum of supported.

Whilst a CUCM cluster can reach up to 40,000 devices (80,000 for a Mega cluster) and there are limits on the number of devices that can be monitored by TSPs, these limits are academic only. This is because our caching engine (mentioned in the doc) has a configurable high water mark of 2000 concurrent monitored devices at any one time. Therefore Arc will never reach the limits of the instance/node – but is able to monitor any one of the devices in the cluster.

In a resilient situation additional TSP profiles would be needed for the Resilient Server.

Dynamic Busy Lamp monitoring using TAPI Super provider		
	Single Server	**Resilient Server**
Max TSP Instances/CTI Manager Nodes	10	20 (10 for each Arc Pro Server)
Max supported system Devices*	10,000 across all TSP Instances	20,000 (10,000 per server)
Max simultaneous BLF monitors*	10,000 in total Dynamically allocated by Arc Pro Server, but set to max 2500 by default per CT Driver/TSP Instance.	200,000 (100,000 per server)

* Statistics are per CT Driver

It must be noted that the cluster limit of monitored devices may include devices being used outside of Arc, and allowance should be made for these. CTI Limits are also influenced by:

- The number of lines per device
- The number of shared occurrences of a line

The number of CTI applications

To calculate the required number of CTI resources according to the following formula:

> Number of CTI Resources = (Total CTI Device Count) * (The greater of {the CTI Line Factor or the CTI Application Factor})

For example:

500 CTI devices deployed with an average of 9 lines per device and an average of 6 applications per device. According to the Cisco SRND 9 lines per device renders a line factor of 1.8 whilst 4 applications per device renders an application factor of 1.0.

> (500 CTI Devices) * (1.8 Line Factor) = 900 total CTI resources required.

All of the above statistics are based on CUCM 10.x. For more details on the maximum supported limits for your CUCM refer to the *Cisco SRND*.

Device selection

The solution uses the CTI Server to monitor all devices as required. The operator sends the requests directly to the CTI Server and will display the busy lamp status based on the response it receives.

The operator sends the following information to the CTI Server:

- DN
- Device Name (if the option is set to use this)
- Partition
- RID (Resource Identifier) – This is the MAC address populated in the Contact Directory if this is set to be used
- CT Driver
- CUCM node based on the DRM of the CT Driver

In turn the CTI Server communicates with the CUCM and sends the following information via AXL :

- DN
- Partition
- RID

The CUCM returns all instances of devices matching the criteria that was sent. The CTI Server then undertakes a process to order those devices to leave it with a single device upon which to request line state for.

When resolving devices for use by Arc (system devices or Line State) the CTI Server will give priority when resolving devices to those using Extension Mobility. EM is supported in the directory but in NOT supported for any System Devices like the CTI Ports and Route Point and also not for the devices used by agents or operators.

The CTI server uses information from the main configuration database to control how it functions. The following examples show the results that would be generated:

- All matching DN's will be ordered initially by EM Count which will ensure that all Extension Mobility profiles are prioritized. Therefore if any of the devices returned have an EM count, the other instances will be deleted from the algorithm.
- Next the existing lines will be ordered by Line Index. A primary line has a Line Index of 0, a second line an Index of 1 and so on. This way priority is given to primary lines. If no primary line exists then the highest order of line will always be selected first.
- If there are multiple instance still in the list they will then be further ordered by Device Description.
- Finally if there are still multiple matches a final parse will be made using Device name, a unique alphanumeric sort of the MAC addresses of the devices.

Once the lines have been ordered according to the sort algorithm described above, the device at the top of the list will be used and its RID (Resource Identifier) returned to the operator. This device will also be queried by the CTI Server via the TAPI TSP to ascertain it Device and individual Line states.

Device line configuration

Profile Type	DN	MAC	Device name	Partition	Line Index	Device Profile	EMCount
Static device	1000	SEP2222 22222222	Martin Primary		0 (Primary Line)	0	
EM Profile	1000	EM_222 222222222	Martin Secondary EM	PartB	1 (Secondary Line)	1	279a22ab-9cb2-42c9-be81-3f26376060cc
EM Profile	1000	EM_111 111111111	Martin Primary EM		0 (Primary Line)	1	
Static Device	1000	SEP3333 33333333	Martin Secondary	PartA	1 (secondary Line)	0	
Softphone	1000	SEP1111 11111111	Martin Softphone		1 (secondary)	1	

The following is a list of expected resolution results depending on the information provided and the configuration settings.

DN	Partition	RID
1000		EM_222222222222
1000	PartA	SEP333333333333
1000	PartB	EM_222222222222

Example 2

DN	MAC	Line Index	Partition
1000	PHONEMAC_A	2	
1000	PHONEMAC_B	1	
1000	PHONEMAC_C	1	PARTITION_X
1000	PHONEMAC_D	2	PARTITION_Y

1. Resolve => (DN:1000, Partition: “empty”) Result: [PHONEMAC_B]
2. Resolve => (DN:1000, Partition: “PARTITION_X”) Result: [PHONEMAC_C]

Example 3

DN	MAC	Line Index	Partition
1000	PHONEMAC_C	2	PARTITION_X
1000	PHONEMAC_D	1	PARTITION_Y

1. Resolve => (DN:1000, Partition: “empty”) Result: [PHONEMAC_D]
2. Resolve => (DN:1000, Partition: “PARTITION_X”) Result: [PHONEMAC_C]

Example 4

DN	MAC	Line Index	Partition
1000	PHONEMAC_A	2	
1000	PHONEMAC_B	1	
1000	PHONEMAC_C	2	PARTITION_X
1000	PHONEMAC_D	1	PARTITION_Y

1. Resolve => (DN:1000, Partition: “PARTITION_Z”) Result: not found
2. Resolve => (DN:1000, Partition: “PARTITION_X”) Result: [PHONEMAC_C]

4: SQL database overview

This chapter contains the following information:

Arc requires Microsoft SQL Server for all database operations including logging, configuration and directory storage. The configuration database keeps a record of the system configuration, while the logging database records all call activities.

Supported versions of SQL Server can be found in the *Arc Pro Compatibility and Performance Guide* and also in the release notes for each software release.

Arc requires two databases to function, and these must be created using the Arc Pro Admin application. These databases can be on the local machine, that is the Arc Pro Server (both Publisher and Subscriber), or can be hosted remotely (non-clustered).

> **Note**
> Arc supports both 64bit and 32bit SQL Server but only supports a 64bit Operating System.

SQL installation prerequisites

There are some required elements to a SQL installation that you should be aware of before continuing.

> **Note**
> If installing SQL locally for a replicated/resilient solution, it is a requirement for the new SQL installation to be built exclusively for an Arc database install to ensure the default collation settings of SQL are set correctly. Providing the prerequisite information below is adhered to, the Arc v6 Resilience Wizard should work first time.

SQL prerequisites

- A valid SQL user with "SysAdmin" privileges must be provided for the ARC installation.
- Ensure the Windows Hostname and SQL hostname are identical (If Windows is renamed then SQL needs to be renamed to match).

SQL prerequisites (for SQL Replication/Resilience only)

- The Publisher server must have a full version of SQL Server installed.
- During SQL server installation, ensure "SQL Server Replication" is selected on the "Feature Selection" screen.
- During SQL server installation, ensure the "Collation" settings are the same on the Publisher and Subscriber machines.
- Name lookup (DNS) over the network must be functioning. SQL replication can only use hostnames and not IP addresses.

Windows prerequisites

- Ensure a Windows user account with administrative privileges is used for the installation.
- If setting up a Standalone Arc SQL Server, ensure the following services are successfully running:
  - SQL Server
  - SQL Server Agent
- If setting up an Arc SQL Publisher for a resilient solution, ensure the following services are successfully running:
  - SQL Server
  - SQL Server Agent
  - Distributed Transaction Coordinator (MSDTC)
- If setting up an Arc SQL Subscriber of a resilient solution, ensure the following services are running:
  - SQL Server
  - Distributed Transaction Coordinator (MSDTC)
- If using SQL replication (only), ensure the MSDTC service has firewall rules and authentication requirements set as per the "Technical Guide" (Allow inbound/outbound and "No Authentication Required")
- If using SQL replication (only), confirm the TSP Instances match across both publisher and subscriber servers. The amount of installed TSP's and the order in which they are listed in Windows must be the same on both servers.

- If using SQL replication (only), ensure the CID of each server (Publisher & Subscriber) is unique. To confirm this open Registry Editor and browse to: *HKEY_CLASSES_ROOT\CID\...*

If any of the CID's listed matches that of your other server hardware then you will need to generate a new CID by reinstalling the MSDTC service. See Resilience installation gotchas for further information.

Firewall prerequisites

Add the following ports, services and executable files as firewall exceptions:

- Windows Management Instrumentation (WMI)
- Distributed Transaction Coordinator – MSDTC (only required if using SQL Replication/Resilience)
- Arc Message Bus (MBUS) – open inbound ports: 61616 (only required if using SQL Replication/Resilience)
- "SQLSERVER.exe"

Example:

"C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Binn\sqlservr.exe"

Utilizing a non-standard SQL port

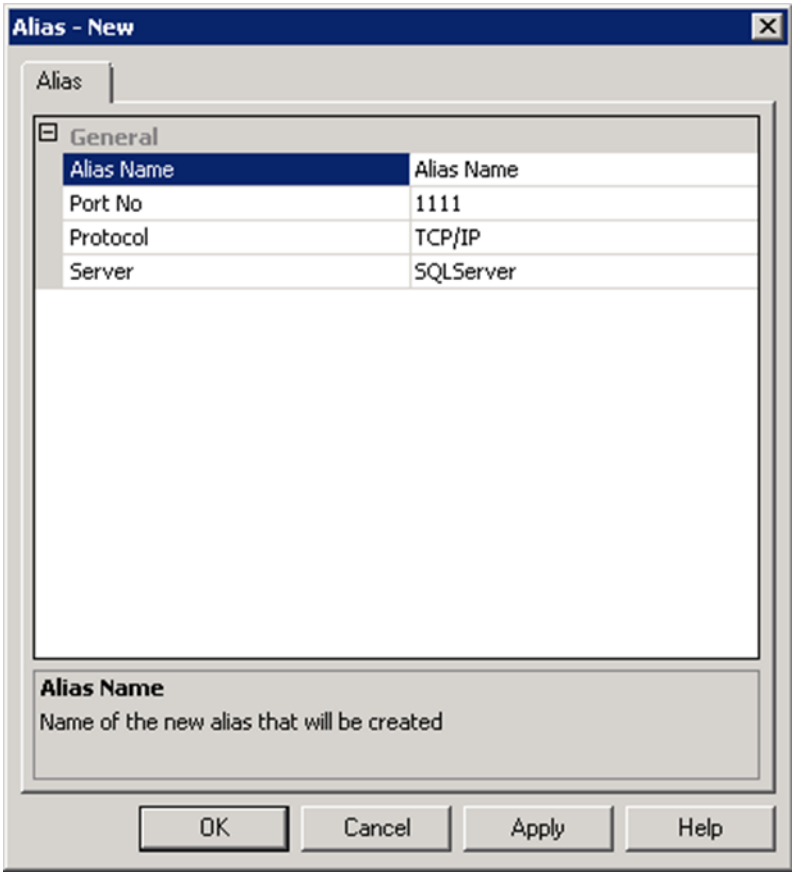
In order for the Arc Pro application to function as expected with non-standard ports, Aliases need to be created on the Arc Pro Server and Client machines. If replication is in place each Server requires an Alias for itself and the supplementary Server.

An Alias is a method of specifying an alternative name and/or parameters that can be used to make a connection to a SQL Server. An Alias can be utilized to:

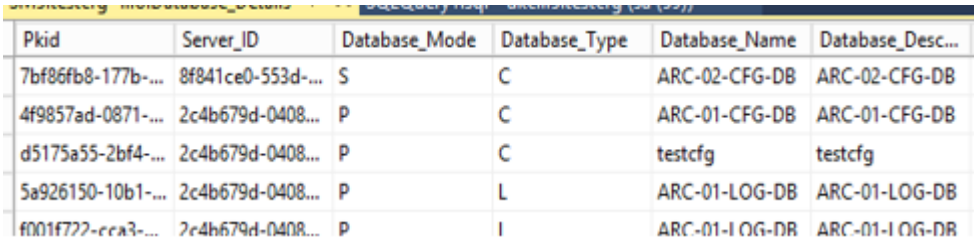
- Specify an easy to remember name of an actual SQL Server Name.
- Redirect a SQL connection with a SQL Server to another SQL Server instance on any machine.
- Establish a connection to a SQL Server using a particular protocol with specific parameters like TCP Port or Named Pipe.

Arc Pro Server Alias configuration

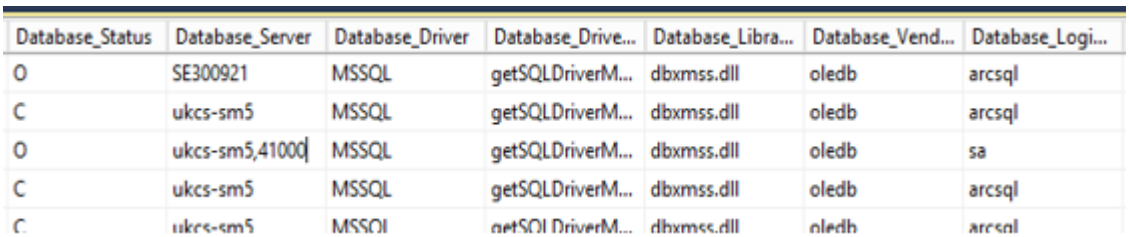
An Alias can be created by opening the SQL Configuration Manager > Expand the SQL Native Client Configuration > Right click Aliases > Select new Alias and enter the appropriate details:



The client Console is not able to connect to the Database until the *Database_Server* column in the *Database_Details* table is amended for both Configuration and Logging databases with *machinename,portnumber*. For example, *ukcs-sm5,41000*.



Pkid	Server_ID	Database_Mode	Database_Type	Database_Name	Database_Desc...
7bf86fb8-177b-...	8f841ce0-553d-...	S	C	ARC-02-CFG-DB	ARC-02-CFG-DB
4f9857ad-0871-...	2c4b679d-0408...	P	C	ARC-01-CFG-DB	ARC-01-CFG-DB
d5175a55-2bf4-...	2c4b679d-0408...	P	C	testcfg	testcfg
5a926150-10b1-...	2c4b679d-0408...	P	L	ARC-01-LOG-DB	ARC-01-LOG-DB



Database_Status	Database_Server	Database_Driver	Database_Drive...	Database_Libra...	Database_Vend...	Database_Logi...
O	SE300921	MSSQL	getSQLDriverM...	dbxmss.dll	oledb	arcsql
C	ukcs-sm5	MSSQL	getSQLDriverM...	dbxmss.dll	oledb	arcsql
O	ukcs-sm5,41000	MSSQL	getSQLDriverM...	dbxmss.dll	oledb	sa
C	ukcs-sm5	MSSQL	getSQLDriverM...	dbxmss.dll	oledb	arcsql

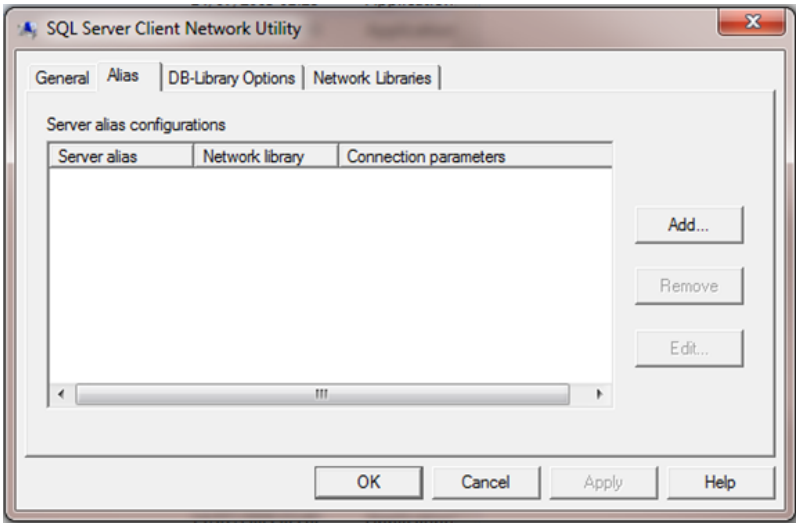
Note

- In a scenario where Arc Replication is intended to be utilized, a SQL Alias needs to be defined on both Servers.
- It is also required that the Alias name match the hostname as well as the instance name if configured. If this is not configured in this way, database replication will fail.

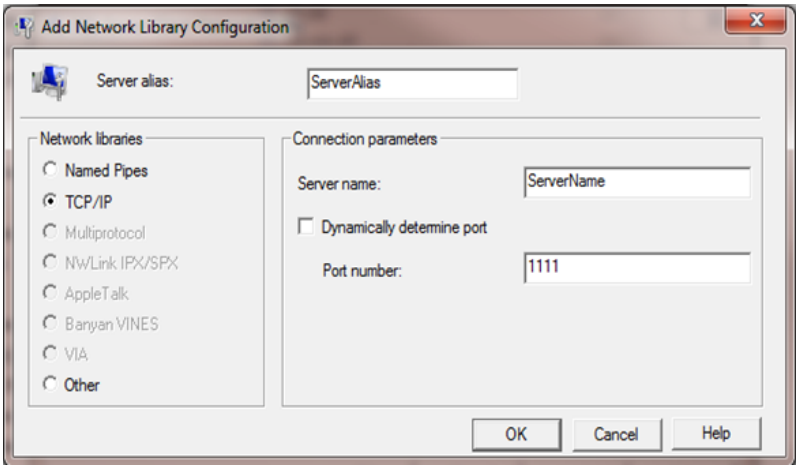
Arc Pro Client Alias configuration

To add an Alias browse to the %windir%\System32 folder > locate and then open the *cliconfig.exe* executable file.

Once the SQL Server Client Network Utility is open > select the **Alias** tab and click **Add...**:



Configure the following options for the Arc Pro Server:



- **Server Alias**: add the Hostname of the Primary or Secondary Arc Pro Server
- **Network Libraries**: select TCP/IP
- **Server Name**: will be populated when typing in the Server Alias field but this should be amended to the correct SQL Server Hostname.
- **Dynamically Determine P**ort: ensure this tick box is unchecked

- **Port Number**: enter the non-standard port number the Arc Pro Clients will use to communicate with the Arc Pro Server.

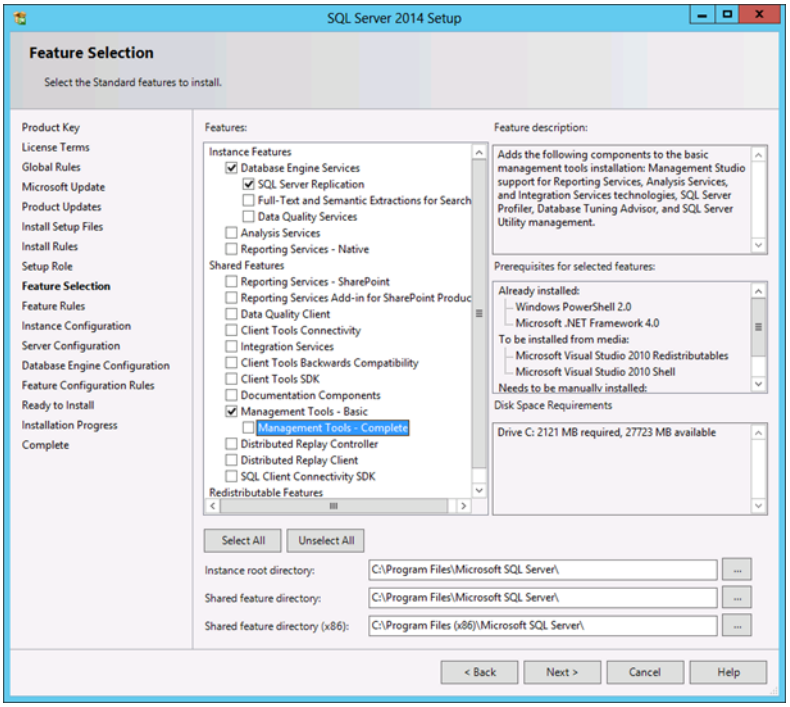
> **Note**
> If a Subscriber is installed, ensure that both the Arc Pro Servers' hostnames are added using this tool.

SQL installation

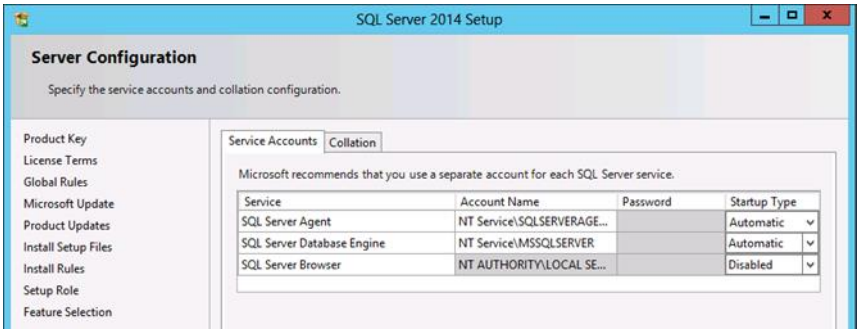
When installing full SQL you should confirm the prerequisites at the start of this document have been adhered too.

Install SQL server using the default options with the exception of the four items listed below:

1. Feature Selection
   - Database Engine Services
   - Management Tools – Basic
   - SQL Server Replication –only required when installing Arc as a resilient pair.

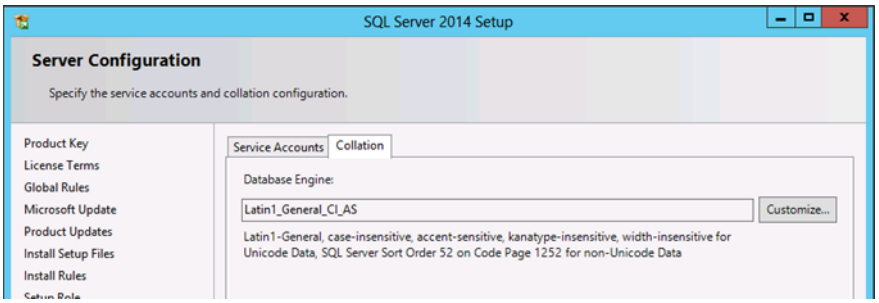


2. Server Configuration – Service Accounts Tab
   - SQL Server Agent > Set start-up type to Automatic
   - SQL Server Database Engine > Set start-up type to Automatic

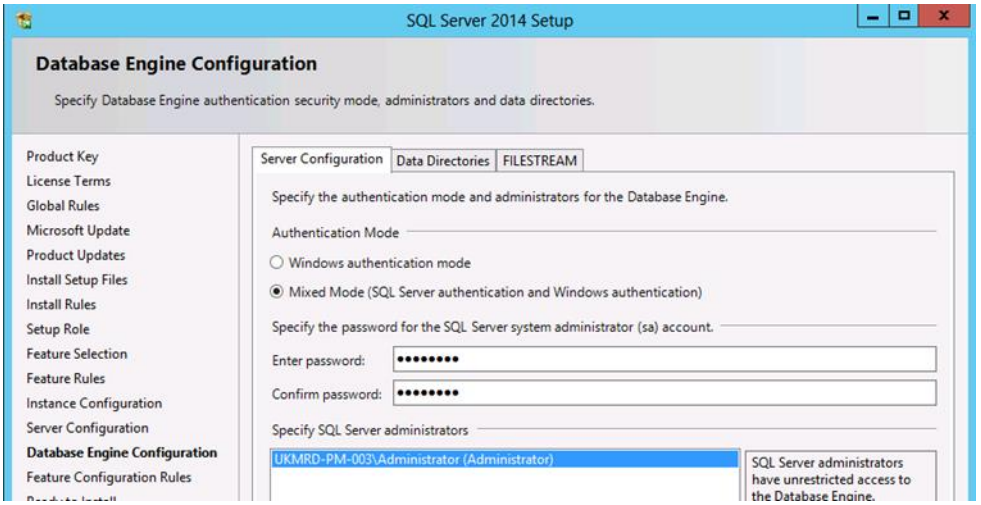


3. Server Configuration – Collation Tab
    - Database engine: Latin1_General_CI_AS

> **Note**
> Make a note of the Collation settings if this is to be different from the above option. This is so you have the option to upgrade to a resilient solution later on as a subscribing SQL server would need to echo the same configuration upon installing SQL.



4. Database Engine Configuration – Account Provisioning Tab
    - Authentication Mode is “Mixed Mode”



5. Continue the rest of the SQL installation choosing the application defaults.

Remote SQL configuration requirements

Both Arc Pro Servers in a resilient setup can be connected to remote (off-box) SQL servers with database replication. However:

- Setting up the off-box SQL server using the Provisioning Wizard is not supported.
- Both Arc Pro Servers cannot be connected to the same SQL server.

For Arc to successfully connect to a remote SQL Server, the following requirements must be satisfied:

- When creating the new databases using the Administrator application, you should specify the name of the remote SQL server, preferably using the hostname rather than the IP address.
- You must perform the following on both SQL servers after the databases have been created:
  1. From the Arc Pro Server, browse to C:\Program Files\Arc\Arc Pro\DLL and into the appropriate 32/64 bit folder.
  2. Before creating the database, do the following:
     i. On the off-box SQL server, create the ArcData folder and also the DLL subfolder within it.
     ii. Copy all files in the *\Arc Pro\DLL* folder to the off-box SQL server's *ArcData\DLL* folder.
     iii. If the remote server is running a 64 bit version of SQL, copy the files from *C:\Program Files\Arc\Arc Pro\DLL\64Bit* to *ArcData\DLL*. If the remote server is running a 32 bit version of SQL, copy the files from *C:\Program Files\Arc\Arc Pro\DLL\32bit* to *ArcData\DLL*.
  3. If it is not already installed there, download and install the Microsoft Visual C++ 2008 redistributable on the off-box SQL server. You can check whether it is already installed using **Control Panel > Programs and Features**. Also, ensure that the correct platform version (64-bit or 32-bit) is installed for your SQL server.

An established Arc Pro Server can have its databases moved to an off-box SQL configuration without having to create new databases. This is done using the Arc Pro Administrator's Database Copy and Move functionality. To use this functionality:

- The SQL server hosting your off-box databases must contain the shared folder ArcData (by default, this is located in *C:\ArcData*)
- The account that the destination SQL Server is running under needs full permissions for the folder that has been shared as ArcData on the destination machine, so that it can access and modify the databases.
- The user running the Administrator application must have Change permission for the shared folder.

The ArcData folder is automatically created by the software when you create the database on-box. When you have an off-box set-up, you have to manually create this folder.

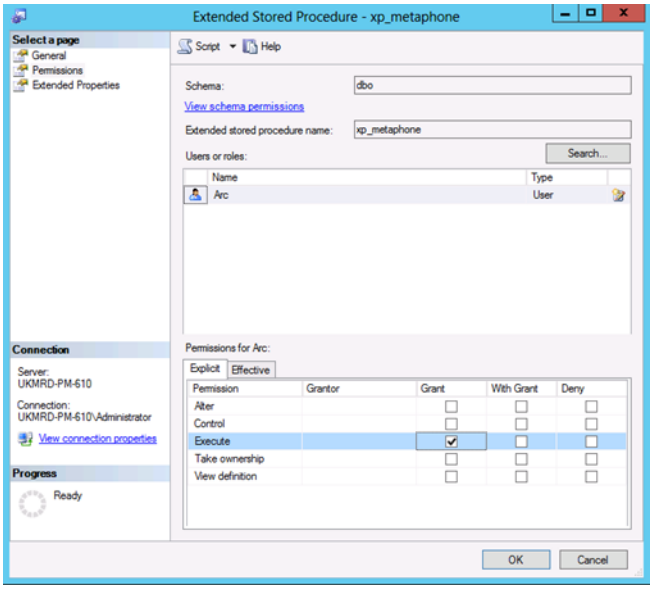
SQL permissions

To create the Arc Databases and install the database resilience they need to be created/installed with an account that has the 'sysadmin' Server role, once created this can be locked down with more granular permissions.

The account will need to be configured with the Public Server role and under the user mappings it will require the following against each of the Arc databases and the master database:

- db_datareader
- db_datawriter
- db_owner - this role is required for Directory exporting.
- public

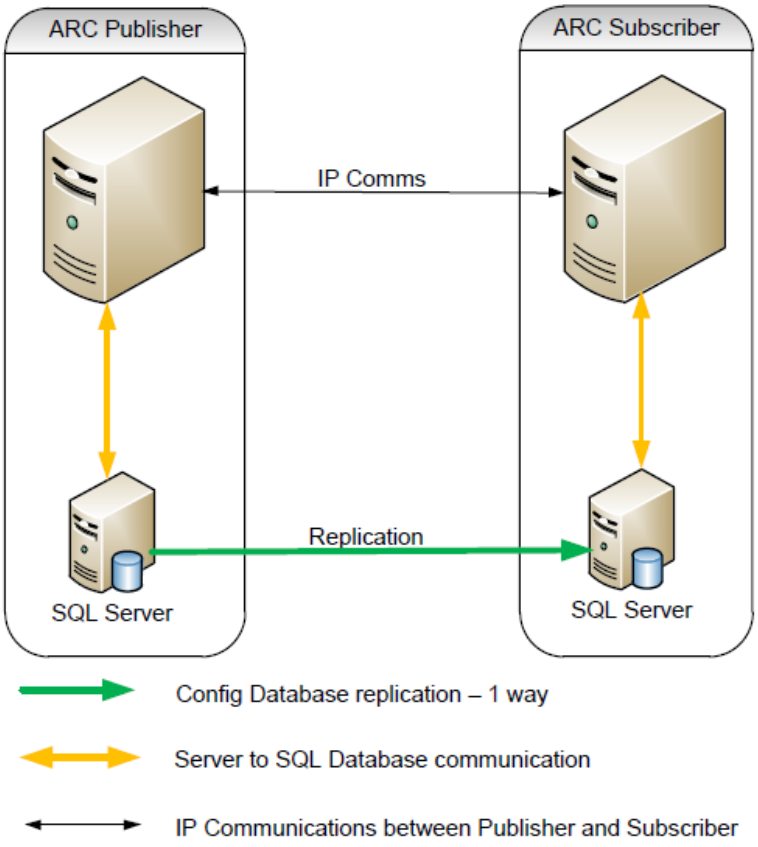
On the publisher and subscriber machine there is also an Extended Stored procedure that you will need to amend permissions on to allow execute control, the stored procedure is called 'XP_Metaphone' and can be found under the following tree menu; **Databases > system Databases > master > Programmability > Extended Stored Procedures**.



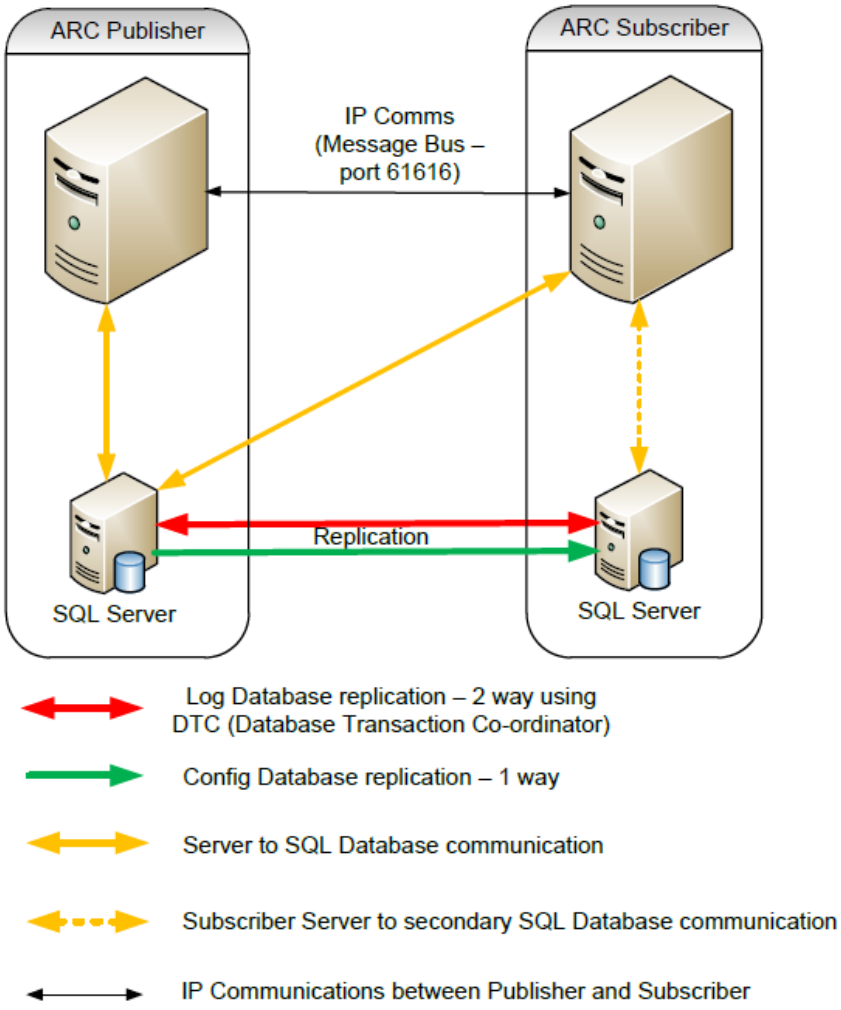
Database changes for Arc v6

There have been some changes to database replication in Arc v6 that you should be aware of. These changes have been detailed as an overview of what you can expect to be a little different when compared to an Arc v5.1.4 (or below) resilient solution. See below for an overview of the changes.

Arc v5.1.4 SQL Replication Diagram



Arc v6 Replication Diagram



- The Config DB is only replicated one way from Publisher to Subscriber.
- The Config DB now contains the settings for both the publishing and subscribing servers.
- Log database replicated both ways for correct statistical information (Reporting)
- New Message Bus (MBUS) increases server intelligence and controls failover/failback
- The Arc Subscriber Server always connects to the primary SQL database unless it is unavailable
- The Subscriber database cannot be edited directly. All changes/configuration must come from the Publisher database. (using Admin application of Publisher)
- This new replication method prevents the need to restart the CT server service on the subscriber for online changes. Offline changes still require both servers services (Pub & Sub) to be restarted.

Overview of SQL database changes for Arc v6.1

There have been a number of changes to the database in order to firstly move the remaining Operator preferences and layout settings into the database as well as creating the predefined layouts/abilities as part of the Operator Roles. Some of the more important new SQL tables are explained further below:

- "Role_Groups" SQL Table

  This new table contains all the information relating to the permissions that a role has within the console. The table is populated with an XML cell that defines what features are Available, un-dockable and whether they can be disabled or not.

  These features are described within the Role_Properties table.

- "Role_Properties" SQL Table

  This table defines the different features of the console to specific sections within the console itself. For example The Directory panel is defined as a feature so that the permissions within the Role_Groups table can define with the pane is firstly available to the user, whether it can be disabled and lastly whether it can be un- docked.

> **Note**
> All the tables listed above are new but should not need any manual configuration. The setup wizards as part of the installation of version 6.3 will configure all the required items.

As well as the above changes, there are now a few changes with regards to the data held within some of the existing tables.

The User_Prefences table will now contain more rows per Operator as it includes the following:

- DP – Directory Preferences
- PDGP – Personal Directory Group Preferences
- PREFS – Users Preference setup
- MWLYT – Multi Window Layout
- SWLYT – Single Window Layout

Creating a database with a specific collation

It may be required for a customer to use a specific collation specified as part of their corporate environment or as part of an upgrade. If different collations have been used it will cause an upgrade to fail.

> **Note**
> The Arc Pro software requires a Case Insensitive Collation so ensure "CI" is included in the changed Collation.

After the Arc Pro Server has been installed but before for the databases have been created, you will need to run the registry editor utility by opening selecting the run command box from the start menu and executing "regedit".

With the registry editor open browse the following tree path:

HKEY_LOCAL_MACHINE\SOFTWARE\Arc Solutions\Call Connect\Configuration\Defaults

> **Note**
> Ensure that all Arc Pro applications are closed before making any changes.

From here you will need to create a new string value named "Database Collation" and edit the data value to contain the collation you wish to create the database with. Once this is completed close down the registry editor and create the Arc Databases.

Resilience installation gotchas

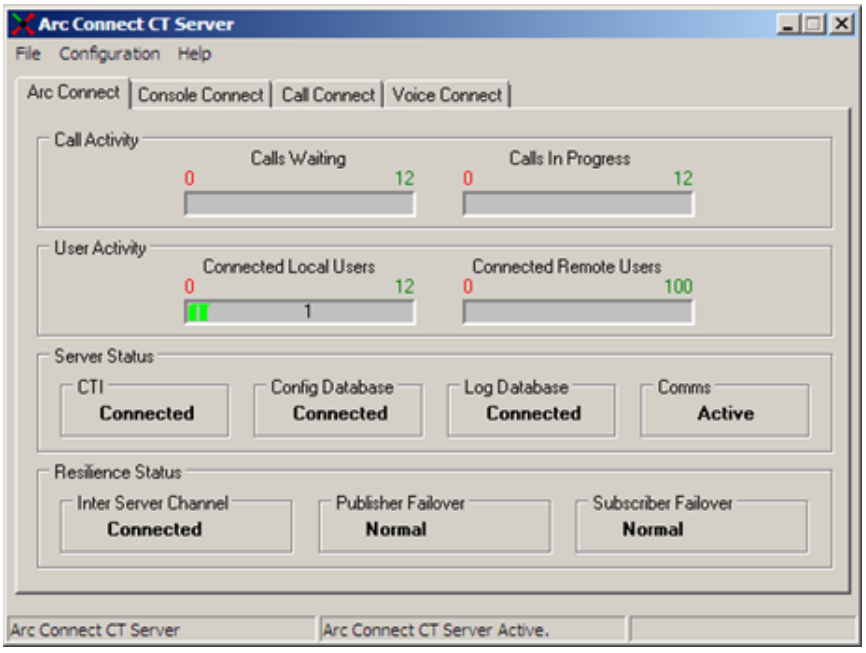
Due to the way the new database resilience is setup, there is a requirement to have a unique server CID for every Publisher/Subscriber scenario. The "CID" is a unique machine identifier and is used within SQL server to identify a specific machine on the network. You should note that if you are setting up a system for replication that each server must have a unique CID. Often lab or production environments make use of machine cloning or copying and this can result in multiple machines (or virtual machines) with the same CID. To view the CID(s) of a given machine open Registry Editor and browse to: *HKEY_CLASSES_ROOT \CID\...*

If the above problem occurs, the MSDTC service can be re-installed to generate a new CID for Windows. If the CID's do match you will need to reinstall the MSDTC service on both Publishing and subscribing servers. In a Command Prompt with admin rights, use the "MSDTC–uninstall" and "MSDTC-install" command(s) to do this. A reboot will be required. Be aware at performing this action on either server may also stop the corresponding MSDTC service on the other server.

> **Note**
> The reinstall may default the MSDTC service back to factory defaults so it will need to be set to "Automatic" start-up in Windows Services.

Resilience in practice

With resilience in place the Arc Pro CT Server has three new fields advising the relevant status information for troubleshooting. This graphic shows a fully working system:



The three new items are shown under the Resilience Status area of the Arc Pro CT Server. These are:

Inter Server Channel	This shows if the server has a connection to the Active MQ service running on the same machine	Connected – The services are connected and running normally Suspended – The Active MQ service is stopped and must be started
Publisher Failover	This reflects the status of the Publisher Server	Normal – Server is up and running as normal Partial – The Server is in a Partial Failover status Full - The relevant server is in a full failover scenario
Subscriber Failover	This reflects the status of the Publisher Server	Normal – Server is up and running as normal Partial – The Server is in a Partial Failover status Full – The relevant server is in a full failover scenario

> **Note**
> If you plan to implement Arc Pro server resilience, you must ensure that the date, time and time zone on your Publisher and Subscriber servers are synchronized. Both servers must be in the same time zone to ensure that any daylight-saving time changes occur simultaneously. If they are not in the same time zone, the operator console will be unable to automatically reconnect to the Publisher when it recovers from failure.

Partial Failover

Partial Failover sits in between the states of a fully running Arc Pro Server and fully failed server. Within a partial failover the client's applications will be moved across from the Publisher to the Subscriber in the same way as they would for a full failover, but the symptoms are less dramatic.

Partial failover is designed to capture scenarios that would otherwise result in calls being missed under previous versions of Arc or requiring a restart of the Arc Pro CT Server to recover. For example if a CTI Route Point was to go out of service on its own, then the Call Forward would send the call to the Subscriber, however with the CT Server still active the clients would remain homed to the Publisher and hence miss the calls. Partial Failover allows this possibility to be managed. Partial Failover also has a built in process to try and rectify the situation without necessarily requiring physical intervention.

There are two Partial Failover scenarios: Global and Community based.

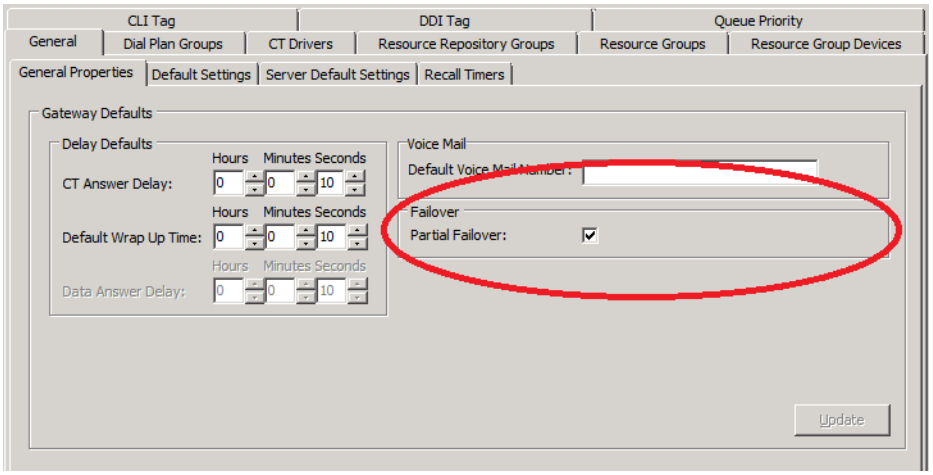
Global Partial Failover

When activated, this failover will come into effect when any of the following failure scenarios occur:

- CT Server loses its TCP/IP connection from the CTI Server.
- CT Link of the default CT Driver becomes inactive.
- Pre CT Gateway devices belonging to default CT Driver becomes OOS.
- Gateway devices belonging to default CT Driver becomes OOS.

For more details see CT drivers.

Global Partial Failover if a preference and is not enabled by default. In order to activate it, it must be selected in the configuration:



In the event of this failover happening all clients across all communities and clusters in the system are failed over to the Subscriber while the Publisher tries to rectify itself.

Depending on the cause of the failover, the following processes are used to normalise the server:

- CT Server loses its TCP/IP connection from the CTI Server.
- CT Server will initiate a mechanism to reconnect with the CTI Server.
- CT Server will clear all the calls objects.
- CTI Server will de-monitor all the system devices for this instance of CT Server.
- Primary CT Server will check the health of Backup CT Server. If Backup server is operational it will mark itself as a global partial failover.
- All the operators will be asked to swap over to backup server
- Once Primary CT Server restores its connection with CTI Server, it will reinitialize all its system devices.
- Primary CT Server will exchange its operational mode with Backup Server.
- Backup Server will ask operators to swop over to primary CT Server will clear all the calls objects.
- CT Link of the default CT Driver becomes inactive.
- CTI Server will initiate a mechanism to reinitialize the CT Driver.
- CT Server will clear all the calls objects.
- Primary CT Server will check the health of Backup CT Server. If Backup server is operational it will mark itself as a global partial failover.
- CTI Server will de-monitor all the system devices for this instance of CT Server. CTI Server will do this based on the primary CT Server going into the partial failover mode.
- All the operators will be asked to swop over to backup server
- Once Primary CT Server restores its CT Link with the default CT Driver, it will reinitialize all its system devices again.
- Primary CT Server will exchange its operational mode with Backup Server.
- Backup Server will ask operators to swop over to primary server once again.
- Pre CT Gateway devices belonging to default CT Driver becomes OOS.
- CT Server will clear all the calls objects.

- Primary CT Server will check the health of Backup CT Server. If Backup server is operational it will mark itself as a global partial failover.
- CTI Server will de-monitor all the system devices for this instance of CT Server. CTI Server will do this based on the primary CT Server going into the global partial failover mode.
- All the operators will be asked to swop over to backup server
- Once Primary CT Server come back to normal mode, it will reinitialize all its system devices once again.
- Primary CT Server will exchange its operational mode with Backup Server.
- Backup Server will ask operators to swop over to primary server once again.
- CT Gateway devices belonging to default CT Driver becomes OOS.
- CT Server will clear all the calls objects.
- Primary CT Server will check the health of Backup CT Server. If Backup server is operational it will mark itself as a global partial failover.
- CTI Server will de-monitor all the system devices for this instance of CT Server. CTI Server will do this based on the primary CT Server going into the global partial failover mode.
- All the operators will be asked to swop over to backup server
- Once Primary CT Server come back to normal mode, it will reinitialize all its system devices once again.
- Primary CT Server will exchange its operational mode with Backup Server.
- Backup Server will ask operators to swap over to primary server once again.

Community Partial Failover

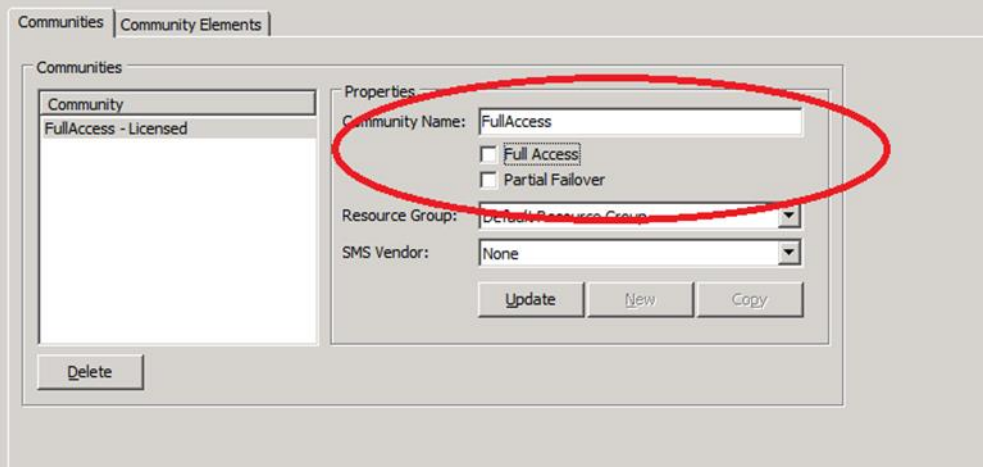
This is a subsection of the Global Partial Failover where only on particular Community within Arc is affected. This has an advantage over previous failover scenarios where all clients are affected in the same way. This is essential to support a multi-tenant solution where the aim is not to affect other tenants in the situation where one tenant has an issue.

Community Partial Failover will activate in the following scenarios:

- CT Link of the community based CT Driver becomes inactive.
- All the Pre CT Gateway (including Queue Locations) devices belonging to one community becomes OOS.
- All the Gateway (Host PBX) devices belonging to one community becomes OOS.

> **Note**
> - The community based partial failover will occur when each community has its own unique driver and system devices.
> - A Full Access community will be based on the global partial failover.

The failover is not activated by default and is a check box in the main Community configuration:



As with Global Partial Failover, the system will try to recover itself without physical intervention. Recovery via a server reboot is the last resort as this would have an effect on all clients in the system across all communities.

Depending on the cause of the failover, the following processes are used to normalize the server:

- CT Link of the community based CT Driver becomes inactive.
- CTI Server will initiate a mechanism to reinitialize the CT Driver.
- CT Server will clear all the calls objects for that CT Driver.
- Primary CT Server will check the health of Backup CT Server for that community. If Backup server is operational it will mark itself as a partial failover for that community.
- Operators belonging to that community will be asked to swop over to the backup server.
- Once the CT Link becomes active, CT Server will initialize all the system devices of that community.
- Primary CT Server will exchange its operational mode with Backup Server.
- Backup Server will ask operators to swop over to primary server once again.
- All the Pre CT Gateway (Including Queue Locations) devices belonging to one community becomes OOS.
- CT Server will clear all the calls objects for that community.
- Primary CT Server will check the health of Backup CT Server for that community. If Backup server is operational it will mark itself as a partial failover for that community.
- Operators belonging to that community will be asked to swop over to the backup server.
- Primary CT Server will exchange its operational mode with Backup Server.
- Backup Server will ask operators to swop over to primary server once again.
- All the Gateway (Host PBX) devices belonging to one community becomes OOS.
- CT Server will clear all the calls objects for that community.
- Primary CT Server will check the health of Backup CT Server for that community. If Backup server is operational it will mark itself as a partial failover for that community.
- CT Server will de-monitor all the Pre Gateway devices for that community.
- Operators belonging to that community will be asked to swop over to the backup server.

- CT Server will monitor the Pre gateway devices once again as soon as gateway devices start becoming in service.
- Primary CT Server will exchange its operational mode with Backup Server.
- Backup Server will ask operators to swop over to primary server once again.

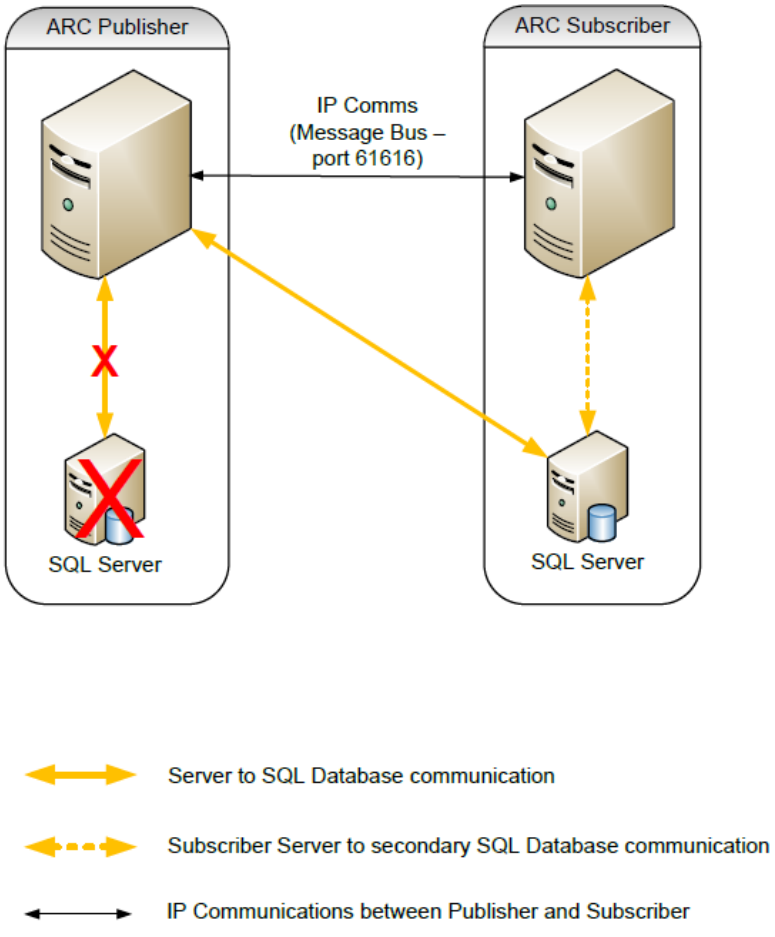
Partial Failover Caveats

- Once a community is in a partial failover (or if the whole system is in global Partial or full failover) mode the system will not allow the Partial Failover setting to be changed online.
- You cannot change the Non-full Access community to the Full Access community if the community is in any kind of Partial Failover.

SQL-only resilience

In resilient Arc Pro systems, if the Publisher DB used by Arc is no longer available but the Arc Publisher server is still active, both the Console and Supervisor clients switch all their connections to the Subscriber DBs, including those used for running reports and directory searches. Clients are notified of the switch-over.

The Publisher Arc Pro Server maintains a connection to its DB, but if it detects a period of inactivity exceeding 15 seconds, it checks the connection status using a SQL query. If the query fails, this triggers the switch to the Subscriber DB, and notifies the clients. The server continues to poll the DBs for a connection, and switches back to the Publisher once a connection is re-established.



SQL Failover limitations

During the SQL failover the Arc Pro Server will not attempt to read or write to either the configuration or logging databases. Also, no configuration changes are allowed during this time, either via the Admin app or the Supervisor. This prevents other server-based activities, such as Contact Matching, being performed on active and ringing calls. This means that the console clients only see the caller's number, which comes from the TSP feed rather than the database.

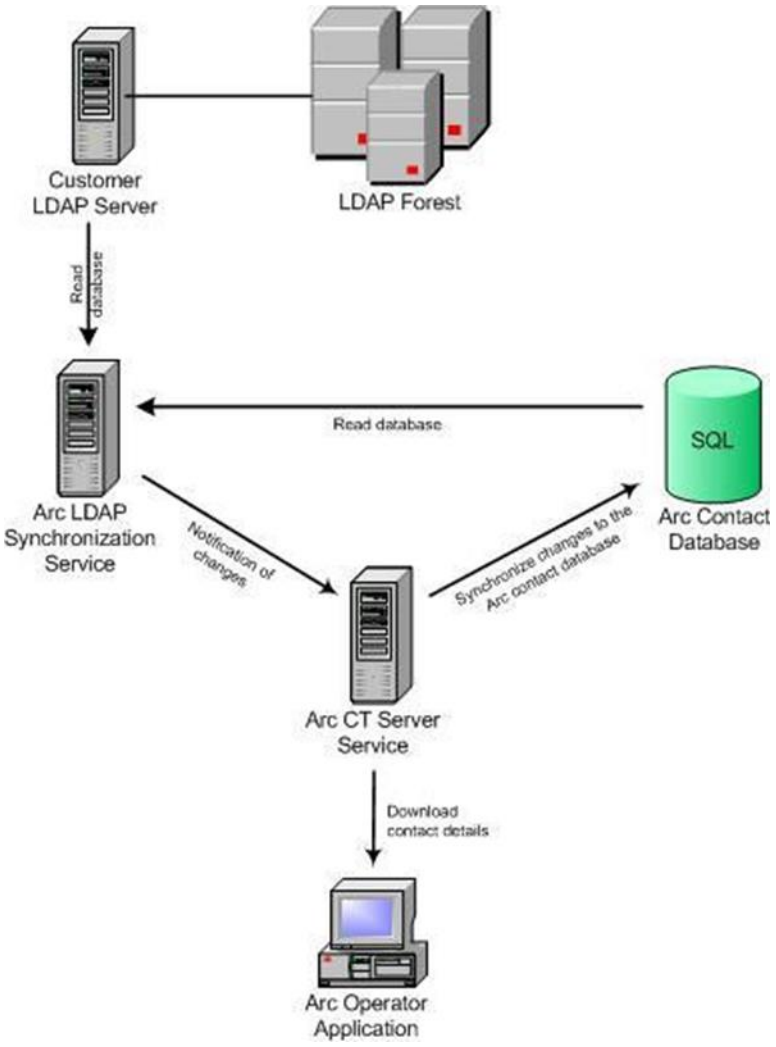
When the system is running in this way no call or client activity events are written to the Log DB; instead they are written to a file of DB updates that gets written to the DB once the Publisher is back online. Once stored on the Publisher, the data is replicated to the Subscriber DB as normal. This means that any reports run during the outage are accurate only up to the start of the outage.

In a non-resilient solution, the Arc Pro CT Server will continue to function but will not attempt to make an further interactions with the DBs. In the connection is still lost and the Server attempts to restart it will fail to activate.

5: Arc Directory

LDAP synchronization

The Internal Directory is a crucial component of the attendant console. The Arc Pro system provides the ability to synchronize with an external LDAP Source.



A separate Arc Pro application, Arc Pro LDAP Server connects to the customers' LDAP contact database. It also reads the Arc contact database and synchronizes contact records between the two databases. The Arc Pro LDAP Server can synchronize with one or many LDAP databases. These synchronized contact details are used by the Arc Console Operator application for directory lookups and call dialing. Arc does not store any data in the external

LDAP database. The LDAP data source is read and data is stored into the Arc contact database for use by the Arc Pro application suite.

Arc Pro supports the synchronization of the following enterprise directories:

- IPlanet (Netscape/Sun Microsystems)
- Active Directory (Microsoft)
- ESTOS
- eDirectory (Novell)
- ADAM
- CUCM
- CSV*

  *This is a one-time sync only and cannot be scheduled to repeat over a period

LDAP synchronization enables external LDAP contacts to be read as Arc contacts. Arc Operators seamlessly integrate with a LDAP source, meaning all contact directory management are online and synchronized. As the LDAP Server records are synched, Arc Console Operator will see the latest details in Directory windows.

Arc Pro LDAP Solution provides a seamless link between the Arc Pro LDAP Server and the LDAP database Server. This solution is useful for customers who have following conditions prevailing in their environments:

- Enterprise Directory is being used for the customers' records or internal contacts or both.
- There is a need to keep the Operators updated about the latest details of the contacts. This can only be achieved by synchronization.
- LDAP Solution is especially beneficial for the customers who have a continuous update going on in their customers' details or internal contacts' details.

Data preparation on LDAP Server

The following items should be considered in order to prepare the data on LDAP database server before the synch takes place:

- Each record on LDAP Server must have a unique property.
- In case of iPlanet, DN is used as the unique property.
- Each internal record must have an internal extension.
- Once the record is added, then unique property must not be changed to avoid the orphan records.
- If the unique property is changed for any record, re-synch the records. It is advised to delete the record, and enter the record with new unique property.
- Ensure that each contact is associated to a Resource Repository Group (RRG) which will then link them to the correct CUCM cluster and ensure that their correct device is used for Line State information. This is configured in the Rules tab of the configuration.

Configuring Arc Pro LDAP synch

Make sure the following before configuring the Arc Components.

- LDAP Server is running.
- User has a Network that fulfils the requirements given below.
- All the contacts' records are updated on LDAP database server.

Tips for Arc configuration for the optimal synch between the LDAP database server and Arc Pro LDAP Server:

Option	Configuration
Rules	More than one rule can be create for each synch. Always make rules that will retrieve different records. Allowing one record to be filtered by more than one rule will affect the synch time
Re-scheduling	This should be used with caution. The time needed for re- scheduling depends upon the volume of the data.
Monitor Change Notification	Enable "Monitor Change Notification" in container tab if immediate change is required to be reflected. If immediate reflection of change is not required then disable "Monitor Change Notification" and schedule re- synch for a complete update. **Note:** The LDAP Server can process a maximum of 4500 Active Directory change notifications in an hour.
Approximate Operator	It is advised not to use the "Approximate operator" while creating rules.
Multiple Filters versus Multiple Rules handing	**Multiple Filters** in one rule are handled with 'AND' operator Whereas Multiple Rules are handled with 'OR' operator.

Searching the Directory

The Contact Directory is used by operators when answering and transferring calls. It is a critical component of the system. To enable searching of the database, a number of the fields are indexed and can be selected as one of the 6 configurable search fields in the client application. The fields are:

- Extension Number
- Department
- First Name
- Last Name
- Job Title
- Location
- User Field 1

Other fields that can be indexed are:

- Business 1
- Business 2
- Company Name
- Company Section
- Cost Center
- Email
- Email 2
- Email 3
- FAX
- Home
- Initials

- Middle Name
- Mobile
- Pager
- PIN
- Room Name
- Title
- User Filed 2
- User Field 3
- User Profile

6: Multi-Tenant including Multiple Cluster Support

This chapter contains the following information:

What is Multi-Tenant Operation?

Multi-tenancy refers to a principle in software architecture where a single instance of the software runs on a server, serving multiple client organizations (tenants).

Multi-tenancy is contrasted with a multi-instance architecture where separate software instances (or hardware systems) are set up for different client organizations. With a multitenant architecture, a software application is designed to virtually partition its data and configuration so that each client organization works with a customized virtual application instance.

In a multi-tenant installation, any change to the configuration for any tenant that requires a server restart affects all tenants; so finding a good time to do this can be difficult. Arc 6.1.1 and later allows you to make online, real-time changes that previously required a restart. Most importantly, it allows a system owner to add a new tenant without having to restart the whole system.

Arc Enterprise can support multi tenancy operation in several different ways, and at different levels of complexity. The key concepts to understand in order to configure multi-tenant operation are:

- Communities
- Permissions
- Resource Groups
- Directory Groups (Console only)
- CT Drivers
- Resource Repository Groups

In multi-tenant environments, there are two ways of operating. Firstly, a single group of Operators or agents answer calls on behalf of various customers. Secondly, each customer has an entirely separate configuration from each other.

In the first scenario it is essential that the caller receives the appropriate treatment for the organization they are calling, and that they do not feel that they are speaking to a "hosted" Operator, such as giving a welcome to the correct tenant for example "Thank you for calling XYZ Limited". Multi-Tenant Operation allows the attendant console Busy Lamp Field (BLF), Internal Directory display and call queue information to change based on the incoming call filter (DID Exact/Pattern match, ANI Exact/Pattern match). With the multi-tenancy functionality with the Arc Pro Console, the Operator has the ability to easily identify the directory contacts pertaining to the "Tenant", and not all tenants within the building.

Arc Pro v6 extends the concept of Multi Tenancy from a single cluster to a multiple cluster solution. This allows a single Arc Pro Server to communicate, and manage devices, on more than one linked CUCM cluster, and allows client devices to be on a different cluster to that on which the call originally arrives.

Configuration considerations

To fully utilize the multi-tenant functionality there are several layers and concepts to understand:

The community stage defines the Arc Pro configuration for each tenant; this will be used to control which parts of the Arc Pro system a tenant will have access to.

The permission stage grants access to specific parts of the different Arc Pro applications. This stage will govern which reports, statistics and online changes are available to a user of the Arc Pro system. The permission stage will be coupled with the community stage and, when combined, will control which parts of the application and the configuration a user has access to.

Configurations between different communities should not be shared. Each community is considered a separate entity and failover rules are applied to its unique set of configurations. If system devices are shared between different communities, they are not considered during community failover decisions.

Resource Groups allow the Arc Pro-controlled CTI Devices to be grouped so that they can be used for specific calls.

Directory Groups allow contacts can be assigned to groups, and in turn these groups can be assigned to different incoming calls.

CT Drivers that are linked to specific instances of the TSP can be created within Arc Pro.

Resource Repository Groups allow the relevant DN to be assigned to a specific partition or groups of partitions. This allows Overlapping Dial Plans to be used which means they will support the same DN's for different customers to be supported via the use of the partition information.

Communities

The host (system owner) will be able to split the Arc configuration into smaller sub-configurations called communities. A community will be managed exclusively by the host and will define the queues, operators, agents, directories to be associated with each tenant.

The host will be able to assign the following access rights to every aspect of a community:

- Creation privilege (create a new operator)
- Deletion privilege (delete an operator profile)

- Amendment privilege (modify an operator profile)
- Read privilege (view an operator profile)

The host will therefore have the ultimate control as to which parts of the configuration are accessible to a tenant.

A community will require a Resource Group, and SMS Vendor (if applicable) assigned when it is initially configured, as they are used for each community irrespective of whether it is a Full Access community or not. All other community elements are chosen on an individual basis. A Full Access community automatically has access to the whole Arc Pro system.

The following items can be associated to a non-full access community:

Parameters	Description
Branches	Used if running a network of branches
Break Hour Reasons	A reason assigned to a break hour time
Break Unavailable Reasons	Reasons for an Agent going unavailable
Completion Groups	Groups of completion codes used in call Connect
Completion Types	Individual completion reasons, which are assigned to Completion Groups
Departments	Departments within the organization, that have been created specifically for the solution
Directory Groups	Groupings of contacts that are associated with specific Call Filters
Dial Plan Groups	Multiple Dial Plan Groups can be configured for assigning to different tenants based on requirements, location.
External Directory Sources	Specific LDAP sources that can be assigned to different tenants
Job Titles	Pre-defined job titles which can be specific to tenants
Permission Groups	Permission Groups associated to users that limited what they can do within their client application
Queues	Queues configured for the system
Regions	Geographical breakdown of operating locations for a tenant
Resource Groups	Groups of Controlled CTI Devices that allow each tenant
Skill Templates	Templates for skills that can be bulk assigned to Agents
Skills	Skills are assigned to agents at differing levels, to associate them to call queues
SMS Vendors	Vendors used to provide SMS messaging services to the Console Operators
Users	Any client login on the Arc Pro system is known as a user.
Voice Messages	Voice Messages are played to callers as in-queue messages or as voice scripts
Voice Phrases	Phrases are used to make up Voice Messages

Parameters	Description
Voice Scripts	Information pertaining to Messages played and then the options applicable to digits pressed on the keypad

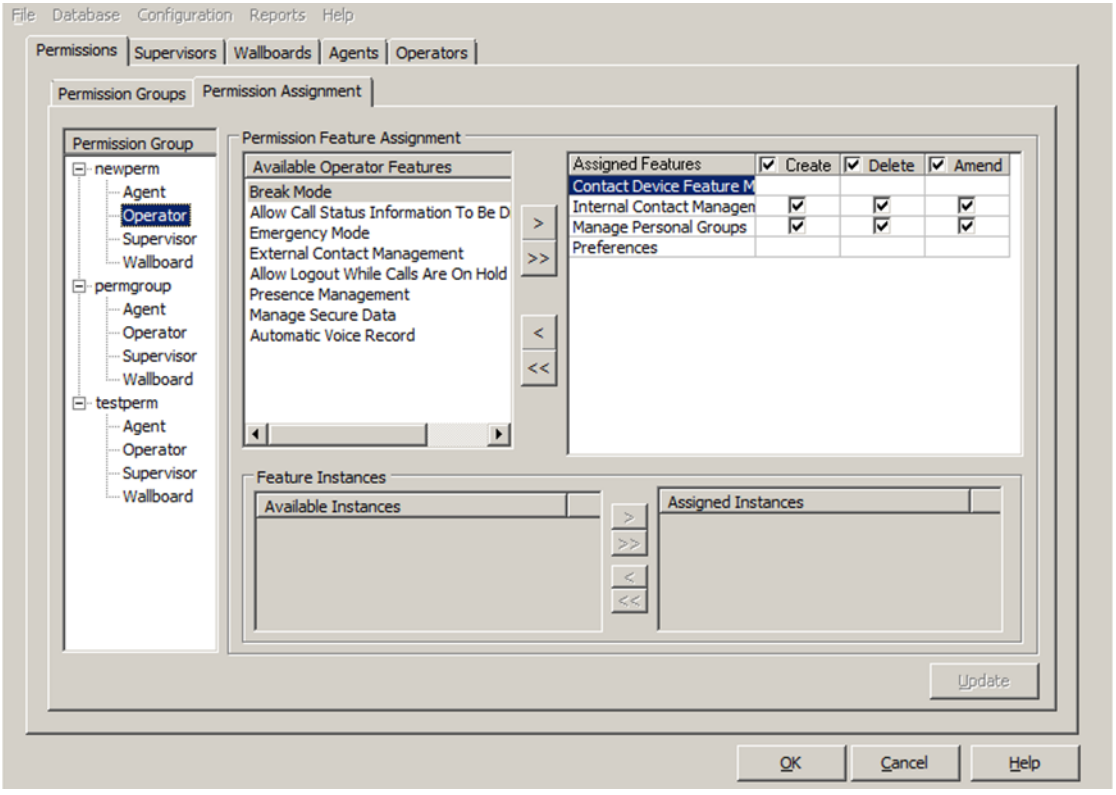
Permissions

Permission groups will define the functionality of the applications that can be accessed by a user. Access rights can be granted at the different levels of functionality:

- Main sections like 'arc reports' or 'console online changes'
- Individual features like report CS01 or 'manage queue details'

A permission group will be associated with a single community, and an Arc User will then be associated with Permission Group. A User can only belong to one Permission Group; however it is possible for a User to be added to other communities outside of the Permission group association. This is mainly for creating Supervisors who can then have access, but not full access to other communities for configuration and reporting purposes. It is not recommended to place Agents or Operators in multiple communities.

If Multi-Tenant operation is not required then a single "Full Access" Community should be created and all Queues will be associated to it.



Multiple Permission Groups can be created and associated to a single community, to allow for different levels of access to users within the same Community. Each Permission Group allows for one level of access for any User, whether it be Agent, Operators, Supervisor or Wallboard, as per the screenshot above.

For example, if two different levels of access are required for Operators, then you will need 2 Permission groups, or you may require different access for different Supervisors, where one may only be able to run queue reports, and a different Supervisor needs access to reports and online updates In this scenario you would still only require two permission Groups, as each group has both operator and Supervisor sections.

The following access rights can be assigned to every element within a privilege group:

Access Right	Description
Creation privilege	Create a new operator
Deletion privilege	Delete an operator profile
Amendment privilege	Modify an operator profile
Read privilege	View an operator profile

Resource Groups

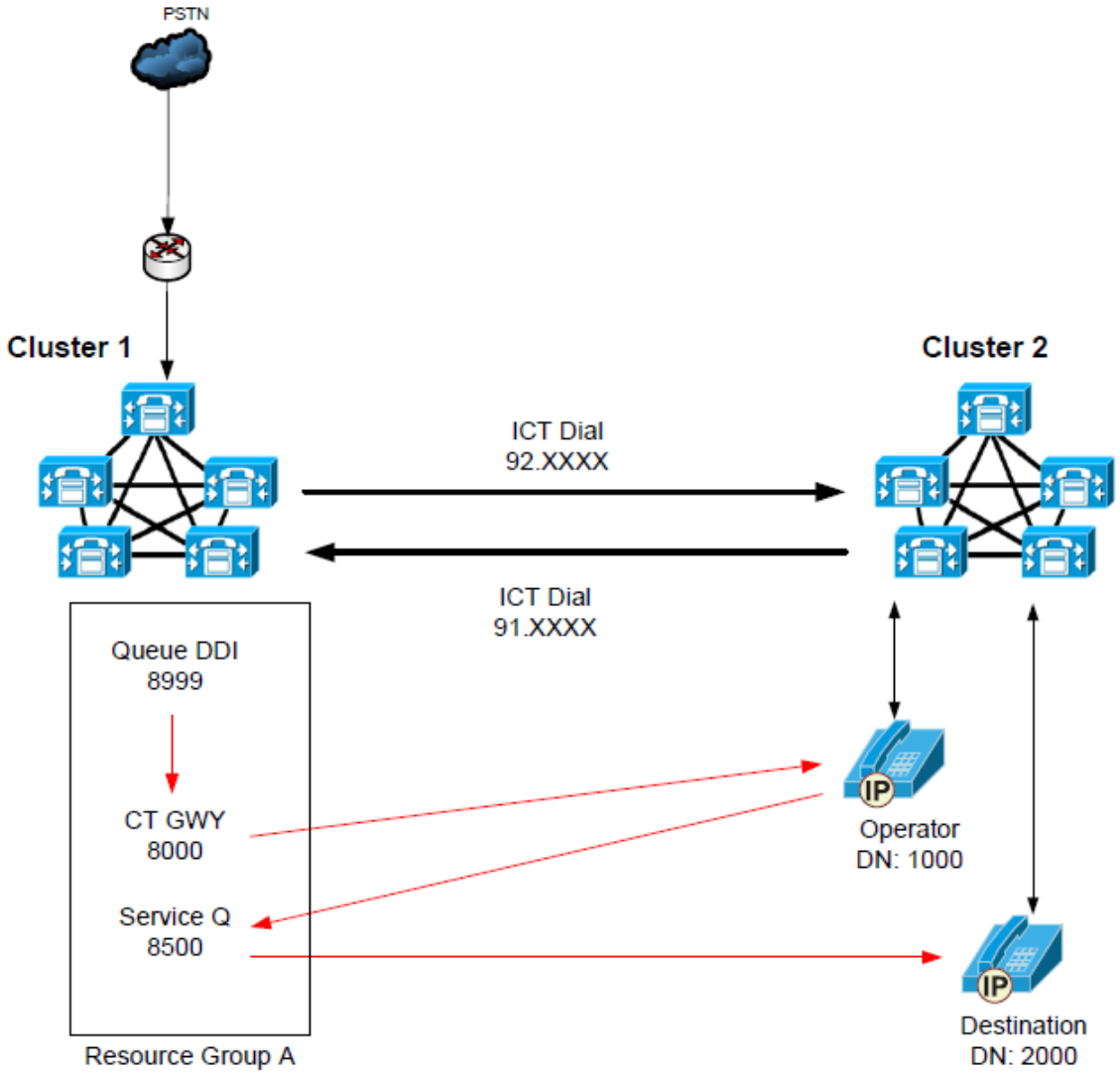
A Resource Group is a subset of Arc Pro system Devices and queues available to the user. The Users can create a number of subsets of available devices and assign different functionality to devices and queues in each queue. The concept of Resource Groups is specifically designed for Multi-tenant operation. Resource Groups allow the Arc Pro Administrator to configure specific groups of devices for specific queues/tenants.

Therefore, the Host PBX Gateway, Pre-CT Gateway, Service Queue and Call Park devices can be split up and associated to each queue/tenant.

Once you have configured Resource Repository Groups, you cannot edit them online. You can only edit them offline using the Admin app, and you then need to restart the Arc Pro CT Server.

When using a multi cluster configuration an entire Resource Group must reside on the same cluster, being managed by the same CT Driver/TSP Instance. However each cluster can have its own Resource Group, and an incoming call must remain within the same Resource Group as it moves through the system. It can however be handled by an operator/agent on a device on a different CUCM. An example of call flow is shown below.

The following graphic shows an example of a multi-cluster:



- Call hits 8999 on Cluster 1
- Gets routed to CT GWY 8000 on Cluster 1
- Operator requests call on DN 1000 on Cluster 2
- Call must get delivered to the operator across Inter Cluster Trunk 92.1000
- The system detects a different RRG between the Host PBX Gateway device and the operator device, so applies the Access Dial Plan needed to reach the RRG of the operator which in this case applies the 92 prefix.
- Operator answers the call and searches directory for contact
- Contact is found on DN 2000 also on Cluster 2. There are also contacts on same DN on clusters 1 and 2
- Operator dials 2000, but the call is going to be blind transferred via the Service Queue. The call needs to go back over the ICT to a CTI Port on Cluster 1, therefore the system uses the Access Dial Plan for reaching back to Cluster 1 and append the 91 prefix.

- Call goes to Svc Q 8500. The call is answered, put on hold and dials an enquiry call to 2000. Again the RRGs are different so the Access Dial Plan to reach cluster 2 is used, appending 92 and 8500 makes enquiry call to 92.2000

Once this is configured, the devices on the Call Manager can be configured with specific Music on Hold (MoH) sources for each tenant – further enhancing the service offered to the Tenant Companies within the organization.

A further benefits of using Resource Groups is that in a geographically dispersed system with multiple Gateways and CUCM nodes is that devices can be kept local to the operators reducing (in some instances considerably) traffic over the WAN.

Examples

Multi-Site – single cluster

A company has offices in London and Berlin, and has gateways and CUCM nodes in both locations, although they are on the same cluster. A Resource Group can be created for each location, and the CUCM devices for each location can be associated to a Device Pool homing them to relevant local CUCM. The Operators would still be able to transfer calls across the WAN if required, but would expect to make most transfers within their relevant office location.

The company may also wish to set Music on Hold (MOH) specifically for different call types such as English speaking, German speaking. In this instance the user would create a resource group for the English speaking MOH, and another for the German speaking MOH.

Multi Cluster

A company has two separate CUCM clusters in Europe and the US linked by Inter Cluster Trunks (ICT). Each operation has its own operators, but they are required to field calls for the other cluster out of hours. Each cluster will have its own Resource Group of System Devices allowing regional MOH to be played, however when the Europe offices close down for the day, the US operators take over. The calls will still arrive at the European cluster and use the local System Devices, however they are then transferred over the ICT to an operator in US. They can answer the call, and can also then see the relevant contact in their directory with full Line State information, in the same was as they could for local US contacts.

All of this is managed on a single Arc Pro Server, which may be located in either territory. This is subject to the CTI over the WAN rules supported by Cisco. See the relevant *Cisco SRND* for more details.

Directory Groups

Directory Groups allow specific groupings of contacts within the directory to be associated with tenants. The Groups are linked to incoming Call Filters, and in cases where a match is made, the operator will only see the contacts within the Group displayed. They can switch between the group view and their full directory view.

In the multi-tenant environment there will still be one large directory containing all the contacts for all the tenants behind the scenes. These should then be grouped initially for each tenant, and each DG should be associated to the tenant at the Community level. This need to be done carefully to ensure that tenants cannot see each other's contacts. This group should then be assigned to each operator belonging to the tenant under the Operator Groups tab of the Admin application, and this then constitutes the Operator's default directory view. Any DG assigned via a call filter will change the directory shown as configured.

Resource Repository Groups

Arc v6 and later extends the multi-tenant functions of the system, by allowing support for overlapping, or non-unique, dial plans, and multiple CUCM clusters. This means that DN's on the same cluster or other clusters do not need to be unique in order for full support to be provided to them by Arc. Full Support in this case means the ability to use a DN as an operator handset, to get the correct Busy Lamp status, and the ability to transfer the call to the correct DN instance. Essentially the Arc Pro Server will now support identical DN's on the same or multiple clusters, as long as they can be differentiated at their Partition level. A DN that is used more than once within the same partition is a shared line, and all caveats regarding the support of shared lines remain in place – that is to say that shared lines are not supported as operator handsets. For shared lines Arc uses an algorithm to manage which devices are to be monitored. For more details see 3: CTI integration.

Essentially the RRG pulls together the concepts of linking an element to a CT Driver, which in turn links to a CUCM Node. These can be nodes within the same cluster to provide resilience or can be nodes on different clusters. The example below illustrates the process that is followed to when an operator wants to call a contact.

The system first looks up which RRG the contact is assigned to. Based on this it looks to see if there is a match between the RRG that the operator is in and that the destination is in. If these are the same then the Dial Plan Group is used to manipulate the dial string and place the call. If the 2 devices are in different RRGs then the system uses the Access Dial Plan Group is used to manipulate the dial string.

All System elements need be assigned to an RRG either directly of via membership of another element within the Arc configuration such as being a member of a Resource Group. Being part of an RRG is the only way that allows the system to dial the correct DN to reach that destination, as explained above.

There are some rules that need to be understood:

1. Multiple customer configured in Arc as tenants are mutually exclusive:
    - Attendant Console users at Customer A cannot see or answer calls from Customer B's inbound call routes
    - Attendant Console users at Customer A cannot see or dial directory contacts from Customer B's directory
    - Partitions for a specific CUCM customer must not be shared with other CUCM customers. This is a Cisco configuration requirement.
    - This is because the concept of CUCM 'partition ' is not an entity that is associated with an Arc tenant or community, however, grouping functions will be provided to manage the calls.

2. Partition information must be available via a configured and selected LDAP source. The partition name stored must be an exact textual match to the partition name on the CUCM server.
3. Individual customers may have more than one partition and this is supported.
4. Support will be provided for multiple DNs across multiple partitions with the following caveats:
   - Operators must be able to receive calls on Primary DNs. Operators using DNs which are shared lines in the same partition will NOT be supported. This applies to System Devices (which includes Operator Devices)
   - More than one instance of the same DN/Partition in the same customer (tenant) is NOT supported as an operator phone. An example of this would be the deployment of shared lines (or boss / secretary) where the boss and the secretary both have an appearance of the same DN on their phone. This is Cisco CUCM CTI limitation and NOT an Arc limitation.
5. Operator phones cannot support two identical DNs on different partitions on the same device. Example, DN1000 from Partition A and DN1000 from Partition B on the same operator phone would NOT be supported. This applies to System Devices (which includes Operator Devices). This scenario can be supported for Line State providing Device State monitoring is used (as opposed to line state or DN state monitoring).
6. The CTI System devices used by each individual tenant must be unique. This means that within a single Resource Group no CTI System Device DN's are allowed to be identical. A CTI System Device for a different tenant can use the same DN but this must be in a different partition.

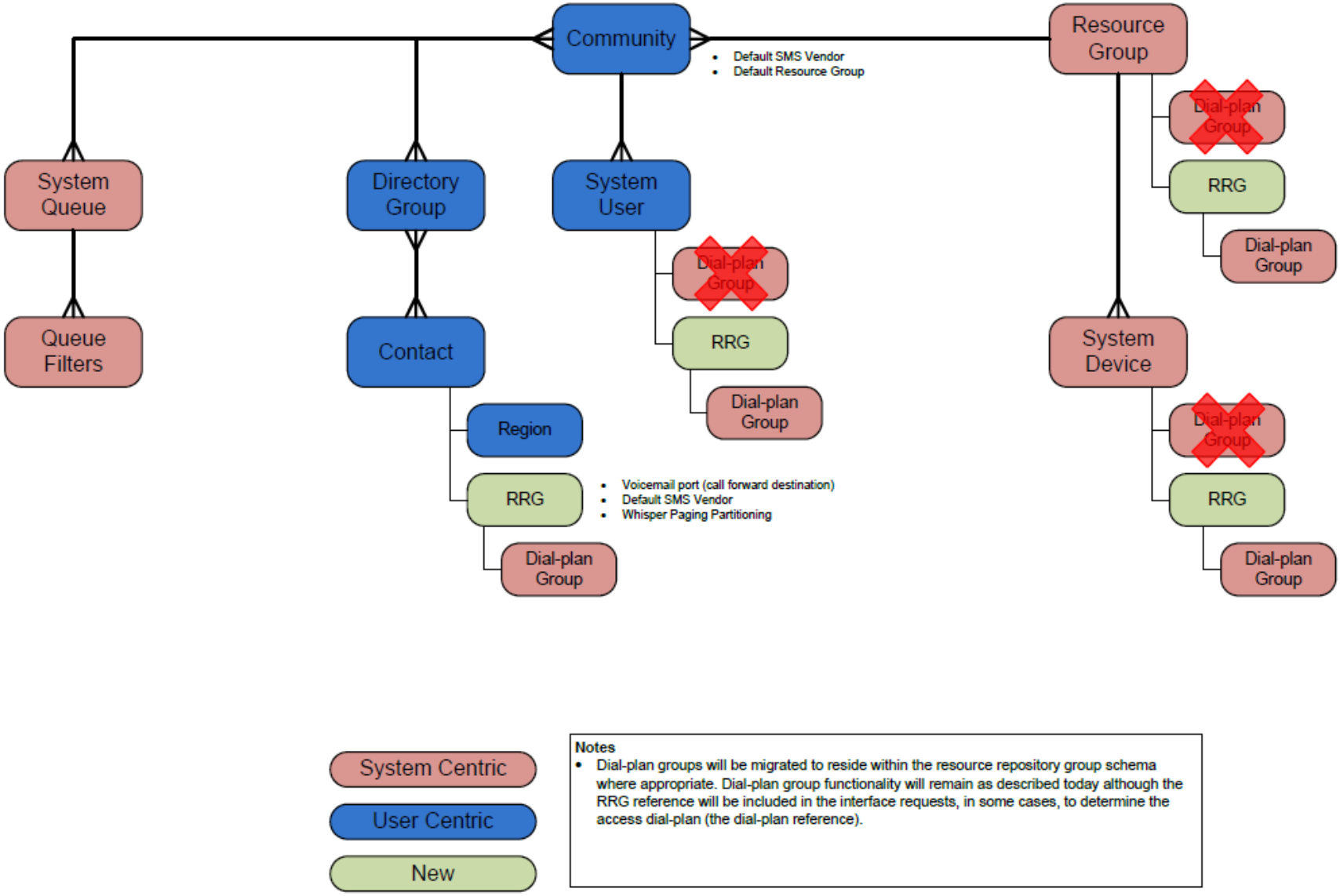
Configuring Resource Repository Groups

This additional configurable item effectively allows devices, dial plans, users and contacts to be linked up to partitions to allow the necessary segregation. Importantly for multi cluster configurations it is also where all of these items are connected to a specific CUCM cluster by means of the CT Drivers/Cisco TSP instances which point to different clusters. The following items can be configured for an RRG:

Tab	Property	Description
General	Resource Repository Group Name	User defined text description of the Resource Repository Group.
	Realm	User defined text property used to describe the user grouping of the resource repositories. Will list previously entered realms against other RRGs, as well as allow the user to manually type a new realm.
	Dial Plan Group	User can select any of the dial plan groups from the fixed combo box list. **Note:** Association of a dial plan group with the Resource Repository Group is optional if the select RRG is not the Systems Default RRG. If no dial plan group is selected then this field will be kept blank in the database.
	Access Group	User defined text property used to describe the grouping of accessible resource repositories. Will list previously entered access groups against other RRGs, as well as allow the user to manually type a new access group. Once an Access Group has been entered, it will appear in the drop down list for this and any other RRG's.

Tab	Property	Description
	Access Dial Plan Group	User can select any of the dial plan group from the fixed combo box list. **Note:** Association of a dial plan group with the Resource Repository Group is optional. If no dial plan group is selected then this field will be kept blank in the database.
CTI	System Driver	This is the CT Driver configured within Arc that will be used to monitor and manage the System Devices in this RRG. The CT Driver will have already been configured to use a specific Cisco TSP Instance running on the Arc Pro Server, and it's this TSP Instance that is configured to connect to a CUCM node/cluster.
	BLF (Extension) Driver	This is the CT Driver that will be used when devices are to be monitored for their sine state. This can be the same driver as used for the System Devices, or can be a separate Driver. The advantages of using a different driver are that: ▪ You spread the CTI load across different nodes within the cluster ▪ CTI resilience is extended
	Partition Management	Displays a list of currently selected partition names for the RRG. Partition Names will be imported from the CUCM via the AXL protocol. This requires an Application User profile to be used which has the AXL API roles assigned. Multiple Partitions can be added to each RRG, and then ordered in terms priority. No RRG can include any partition that is already assigned to a different RRG. To select, add, remove or re-prioritize partitions use the Edit option.

Even with the addition of RRG's the concept of a Community is still the main differentiator of a tenant. The RRG sits below a community in the system hierarchy, as shown in the diagram below.


Community
Default SMS Vendor
Default Resource Group
System Queue
Queue Filters
Directory Group
Contact
Region
RRG
Dial-plan Group
Voicemail port (call forward destination)
Default SMS Vendor
Whisper Paging Partitioning
System User
Dial-plan Group
RRG
Dial-plan Group
Resource Group
Dial-plan Group
RRG
Dial-plan Group
System Device
Dial-plan Group
RRG
Dial-plan Group
System Centric
User Centric
New
Notes
Dial-plan groups will be migrated to reside within the resource repository group schema where appropriate. Dial-plan group functionality will remain as described today although the RRG reference will be included in the interface requests, in some cases, to determine the access dial-plan (the dial-plan reference).

The main concepts of an Arc configuration all feed into a Community. A Resource Group contains the System Devices used within the community for handling calls. Each Resource Group contains a single RRG, which in turn contains a single Dial Plan for that community, which is used by those System Devices. A Community also contains Users, who in turn can be assigned an RRG. Contacts are also assigned on a Community basis, via membership of a Directory Group, to ensure that they are not visible to Users in other Communities. However, they can be assigned an RRG individually (normally assigned by a rule when importing via LDAP). If they don't have an RRG then the User (Operator's) RRG will be used for getting Line State information.

Once a driver has been assigned to an RRG, you cannot change it on-line. You must amend it offline using the Admin app, and then restart the Arc Pro CT Server.

RRG assignments

Operator/Agent

Operator/Agent – relevant to the devices they can use to take calls. This will be determined in a priority order:

Users can be directly assigned to an RRG.

Users can be assigned via their membership of a Community where that community had a default RRG assigned.

If neither of the above are used then the user will be assigned the RRG associated to the system wide default resource group.

As an agent/operator logs in they will be shown all the devices that match their DN, and will be able to select which device they actually want to use.

The following use case illustrates the process:

Login Use Cases

Consider the following IP phones are available:

MAC.A		
1000	Partition.1	1
2000	Partition.1	2

MAC.B		
2000	Partition.1	1
1000	Partition.1	2
2000	Partition.2	3

MAC.C		
1000	Partition.2	1

Scenario A - Operator sends a login request with DN 1000. No MAC is stored in registry and No partition information is defined in the RRG.

CT Server will resolve 1000 with CTI Server and get the following devices (DDIDs) back from the CTI Server:

[MAC.A:1000:1]

[MAC.B:1000:2]

[MAC.C:1000:1]

CT Server will send all the Mac Addresses along with the line instance numbers back to the Operator.

However, the Operator will show only the primary devices on the screen and will have to select one MAC to proceed with the login process:

MAC.A MAC.C

Operator selects MAC.C

Operator will resend the login request with DN "1000" and MAC "MAC.C" and Line Instance Number "1".

CT Server will resolve 1000 along with the RID/MAC "MAC.C" and get the following devices back.

[MAC.C:1000:1]

As this is the only primary device therefore CT Server will not go back to the operator, but will continue with the login process and allow operator to log in on MAC.C:1000:1.

The Agent/Operator also needs to be able to successfully make outbound calls and transfers. These abilities are controlled by the Dial Plan Group and by the relevant Calling Search Spaces on their device and that of any System Devices (see below). Dial Plans are now associated to an RRG and follow the same priority selection as Dial Plans did previously:

- User profile RRG
- Device RRG
- Device resource Group RRG
- Community Default RRG
- System RRG

System devices

The introduction of RRG's allows support for identical DN's in different partitions and on different clusters. Devices can be individually given an RRG as they are configured or can take on the RRG assigned to their Resource Group. A Device RRG is a higher priority than a Resource Group assigned RRG. This in turn allows a partition to be assigned to the device. If the device resolution undertaken as the Arc Pro Server initializes returns more than one device for a given DN, then none of the matching devices will be used. Care should be taken to ensure that this scenario is not encountered. Arc would recommend that, wherever possible, the system devices should be given unique DN's to reduce this possibility. This is not always going to be possible, therefore the examples below illustrate how the device resolution is used.

The following priority order will be applied to determine the RRG for a system device:

- Device's RRG (High) - RRG associated with a system device. (Ignore if RRG is not specified for a device).
- Device Resource Group's RRG (Low) – RRG associated to the resource group of system device. System device must have a resource group and a resource group must have an RRG. Both relations are mandatory therefore it is regarded as catch all.

System devices use cases

Consider following system devices are available in the CUCM Configuration:

GWY.A		
1000	Partition.1	1

GWY.B		
1000	Partition.1	1

GWY.C		
1000	Partition.2	1

GWY.D		
1000	Partition.1	1

Arc Configuration:

- RRG:

Name	CT source	Partition
RRG.1	Default	Partition.1
RRG.2	Default	Partition.2

- Resource Group:

RG	RRG
RG.1	RRG.1
RG.2	RRG.2
RG.3	RRG.2
RG.4	RRG.1

- System Devices:

Device	DN	RID/MAC	Resource Group	RRG
Device.1	1000		RG.1	NULL
Device.2	1000		RG.2	NULL
Device.3	1000		RG.3	RRG.2
Device.4	1000	GWY.D	RG.4	NULL

CTI Server will resolve all of the above mentioned system devices with the CTI Server.

To resolve Device.1:

CTI Server will use the RRG of device's resource group which in this case will be RRG.1.

CTI Server will use the partition information (Partition.1) of the RRG.1 while resolving it. (DN = 1000, RID = NULL, Partition = Partititon.1, Driver = Default)

CTI Server will return the following devices.

[GWY.A:1000:1]

[GWY.B:1000:1]

[GWY.D:1000:1]

As there is more than one device obtained from CTI server therefore, CT Server will

not load this system device. This is regarded as the configuration issue. To resolve Device.2:

CTI Server will use the RRG of device's resource group which in this case will be RRG.2.

CTI Server will use the partition information (Partition.2) of the RRG.2 while resolving it. (DN = 1000, RID = NULL, Partition = Partititon.2, Driver = Default)

CTI Server will return the following device.

[GWY.C:1000:1]

As this is the only device obtained from CTI Server, therefore CT Server will load this as a valid system device.

To resolve Device.3:

CTI Server will use the RRG of the device which in this case will be RRG.2.

CTI Server will use the partition information (Partition.2) of the RRG.2 while resolving it with CTI Server. (DN = 1000, RID = NULL, Partition = Partititon.2, Driver = Default)

CTI Server will return the following device.

[GWY.C:1000:1]

As CT Server has already loaded a system device (Device.2) with the same device therefore this device will be ignored and CT Server will not load this system device. This is regarded as configuration issue.

To resolve Device.4:

CT Server will use the RRG of the device's resource group which in this case will be RRG.1.

CT Server will use the partition information (Partition.1) of the RRG.1 while resolving it with CTI Server. (DN = 1000, RID = GWY.D, Partition = Partititon.1, Driver = Default)

CTI Server will return the following device.

[GWY.D:1000:1]

As this is the only device obtained from CTI Server, therefore CT Server will load this as a valid system device.

Contacts (BLF)

Ensuring contact confidentiality is essential to this multi-tenant process, and this is managed via the Community process. However getting the correct device monitored is a main driver of the use of RRG's. Each contact can be assigned to an RRG, and to be used by an operator, the RRG MUST be assigned to the same Community as the operator. If the contact is not assigned an RRG, it will assume the properties of the operator or the operator's RRG when the line state is required.

The RRG is assigned to an individual contacts for line state in the following priority order:

- **Contact's RRG (High)** - RRG associated with a contact. (Ignore if RRG is not specified for a contact).
- **User's RRG** – RRG associated to the system user (Operator/Agent). (Ignore if RRG is not specified for a user).
- **Community Default Resource Group's RRG** – RRG associated to the default resource group of system user's community. (Ignore if community does not have any default resource group).
- **System Resource Group's RRG (Low)** – RRG associated to the system wide default resource group. This is regarded as a catch all.

Other Multi-Tenant options

Tenant-specific greetings:

The Operator can greet the caller appropriately as the Arc Console will provide the operator with the tenant specific greeting message on the screen – a unique greeting can be provided for each tenant and for multiple queues within a tenant.

Tenant-specific directory filter:

When the call comes into the Operator, the Console can be configured to show the Operator only the directory listings for the tenant that the call is being answered on behalf of. With the multi-tenancy functionality with the Arc Console, the Operator has the ability to easily identify the directory contacts pertaining to the "Tenant", and not all tenants within the building.

Tenant-specific voice messages (Voice Connect)

The Arc Pro Voice Connect module can be used to play specific messages for each queue. It is also possible to use Voice Connect as an Auto Attendant/IVR to play a greeting message for each queue Both the In Queue Messaging and AA/IVR functionality is configured on a "Per Queue" basis. Therefore, the caller can hear a message saying "Thank you for calling Company A your call will be answered shortly", then this message can be repeated at a configurable interval. A separate message saying "Thank you for calling Company B, your call will be answered shortly" can be configured and associated to a different Console queue. For both queues, the same physical Operator will answer the call, with the relevant salutation.

Time/Day Routing per Queue

The Time/Day Routing gives complete control of day and night service. Time/Day routing is configured on a per-Queue basis, therefore allowing each Tenant to specify their opening & closing times, as well where calls should be routed when the queue(s) is closed This in turn allows each tenant to have complete flexibility with where their calls should be routed – either a Voicemail Box, phone within the tenant premises, or any other internal or external number

Operator email

In many multi-tenant Operator environments, the Operator will take a message on behalf of people within the tenant companies. The Operator Email functionality allows the Operator to simply select the relevant Directory Contact, and press CTRL- M to open the Microsoft Email client

Alternate number support

If the workers are not in the office, or work from multiple offices, the Operator will be given a list of alternative phone numbers to use for each individual.

Personal Directory Groups

This function allow individual operators to create their own Directory Groups that are visible on screen to them. The Directory display has changed from the previous F3 Internal Directory and F4 External Directory. By Default each operator will see a "Full Directory" in a single tab. Contacts seen in this view are those contained in the Directory Groups as assigned to the operator as Operator Groups in the admin application.

Each Operator can create up to 9 other groups that are personal to them, and they are a subset of contacts that they have in their Full Directory.

Adding contacts

Operators can add new contacts to their Personal Directory Groups, as they wish. These may not match the filter that was used to select the contacts, but they will always be shown regardless. It should be noted that each contact added will consume 1 contact license as configured on the Arc Pro Server, so if the system has a larger number of operators and they all create many contacts of their own, then care should be taken to ensure enough contact licenses are purchased.

Permissions and Community Elements

Operators can only create/amend groups or add/delete contacts if they have to right permissions or Community Elements. The table below shows which combinations need to be assigned to allow each action to be undertaken:

PDG = Personal Directory Group **SDG = System Directory Group**	**COMMUNITY**			**PERMISSIONS**				
	Community Directory Group - Create	Community Directory Group - Delete	Community Directory Group - Amend	Internal/ External Contact Management - Create	Internal/ External Contact Management - Delete	Internal/ External Contact Management - Amend	Manage Personal Directory Group- Create	Manage Personal Directory Group - Delete
Create a PDG	x						x	
Edit details of a PDG (filters/description)			x					
Delete a PDG		x						x
Create a contact in the Full Directory			x (add to a SDG)			x		
Edit a contact in the Full Directory						x		
Edit the BLF Flag of a Contact in the Full Directory			x			x		
Delete a Contact in the Full Directory			x (remove from SDG)		x			
Link a Contact in the Full Directory to a PDG								
Create a new Contact in a PDG				x		x		
Edit a linked Contact in a PDG						x		
Edit a non-linked Contact in a PDG						x		
Edit the BLF Flag of a linked Contact in a PDG						x		
Edit the BLF Flag of a non-linked Contact in a PDG			x			x		
Delete a linked Contact from a PDG			x		x			
Delete a non-linked Contact from a PDG			x (remove from PDG)		x			

Tenant online configuration improvements

You can now change an individual tenant's TSP devices device configuration without having to restart the Arc Pro CT Server, and without affecting any other tenants. Changes to System Devices previously required using the Admin application and a system restart. The only time now that a system outage is required is when a new TSP instance is added to the Cisco TSP running on the Arc Pro Server, and the Telephony Service on the server must be restarted. While this does not require a machine reboot, it does cause the system devices running the Arc Pro system to briefly go Out Of Service, thus temporarily putting the system into failover.

Once the TSP is configured correctly, the rest of the tenant's configuration can be completed online using the Supervisor. This configuration includes, adding queues, including adding or amending the Queue Location, and adding/removing Host PBX, Service Queue, VM, User or Park Devices.

Adding a new Tenant

When you add a new tenant you must manually create a new instance on the Cisco TSP on the Arc Pro Server, and then restart the Telephony Service. First, however, you must create a new Application User on the CUCM. The next steps depend on whether you are allowed to stop the system for the new system devices to be synchronized with the CUCM.

If the system can be stopped, use the Arc Pro Supervisor to complete the configuration, including creating the new CUCM devices via the CUCM synch function under **Arc Pro > Online Updates > CT Gateway > Manage Resource Group Devices**.

If the system cannot be restarted, do the work on the CUCM first: manually create all System Devices required for the tenant, and a new Application User to which you manually associate all the devices.

Amending an existing Tenant

You can change an existing tenant's System Devices using the Arc Pro Supervisor application under **Arc Pro > Online Updates > CT Gateway > Manage Resource Group Devices**.

If you need to add some new devices to the tenant, add them to the CUCM and associate them with the Application User manually. Then, in the Supervisor, simply add those devices into the appropriate list. Any attempt to create these automatically via a CUCM synch will reset ALL the system devices across all tenants.

Devices that are removed from a configuration for a tenant remain on the CUCM but will not be used. They can be removed manually if required, but can be left and will be removed when the next CUCM synch is run.

> **Note**
> - If the user runs a CUCM synch, this cannot be restricted to the single tenant, but puts all system devices out of service for a while. This means that all tenants are temporarily in failover mode. Any calls residing on System Devices at that point become disconnected. Once the synch is complete the system fails back to the Arc Publisher.
> - When adding a new tenant the work on the CUCM is done first. This would mean a manual creation of all System Devices required for the tenant, creating a new Application User and associating all the devices manually. On the Arc Pro Server add a new instance to the TSP, configure it with the new app user and restart the telephony service at an appropriate time.

7: Arc features

This chapter contains the following information:

Personal Call Park (PCP)

Personal Call Park (PCP) is a feature that is an extension of standard Call Park. With standard Call Park, a "tannoy" style system is used to inform the target contact that "A call is parked on Bay 2000".

PCP extends this feature. When this is being used, the tannoy system is simply used to inform the target contact that "A call is parked". The caller then dials into the PCP system, and the system automatically connects the caller based on the calling extension

PCP has 2 modes of operation:

- "Recognized" number
- "Unrecognized" number

"Recognized" number

When the Operator answers the call and makes the decision to park the call, the Operator selects the contact that call is to be parked for. For example "Mark Smith". "Mark Smith" has an extension number of 1000.

When "Mark Smith" calls into the PCP system, it looks at the number that is calling into the system. If "Mark Smith" is calling into PCP from his own extension (1000) the PCP system recognizes this and automatically connects the call.

"Unrecognized" number

As per the example above, the call is parked for "Mark Smith". However, in this occasion, "Mark Smith" is not at his desk, and dials into the PCP system from another extension (for example Extension 1235).

In this scenario, there is no call parked for extension 1235 (the call is parked for extension 1000). Because the PCP system cannot match a call for extension 1235, a tone is played through the handset.

When this occurs, "Mark Smith" enters his own extension number (1000), the PCP checks that this extension DOES have a call parked for it, and therefore connects the call.

Considerations

The PCP system can be used in many specific environments. The system has the advantage of only having one number for the users to remember (as opposed to the Operator tannoying out the Park DN number). In particular, the PCP feature is a very powerful tool in shop floor and hospital environments.

The numbers that are dialed to enter the PCP system are configured as CTI Ports on the Cisco Unified CUCM.

The PCP system heavily relies on the accuracy of the Arc Contacts Directory, as it is this Directory that is used when the Operator parks a call for a specific contact.

Therefore, it is imperative that the Directory is maintained accurately.

Serial Calling

Serial Calling is a traditional telephony feature that allows an incoming call to be transferred to multiple destinations in consecutive order, without recourse to the transferring party.

This feature has been enabled through the use of the Conference facility on the CUCM. Once the operator has started the Serial Call, the call is maintained on a CTI Port within the Service Queue, with each destination being first called as an enquiry call from the CTI Port, and then once the call is connected a conference is created between the caller, the CTI Port and the destination. When the destination hangs up the caller is placed on hold at the CTI Port, and the next enquiry call is made.

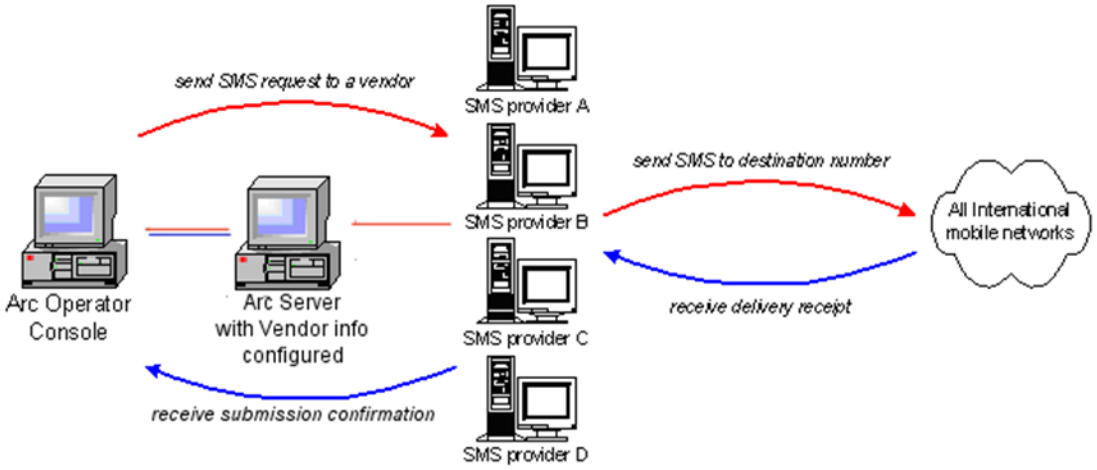
If FAC or CMC codes are in use for any of the destinations required by the serial call, only the default codes configured in the Arc Pro Admin application will be used.

SMS Messaging

Overview

The Arc Pro Attendant Console Operator console can send an SMS to any number, either in its contact list or any other valid number, using a simple interface. The configuration is simple, uncomplicated and easy-to-do.

This is achieved by using third party SMS providers. The Arc Pro solution will have accounts of one, or more, of these vendors. The Arc Operator will send SMS to these vendors, and in return, will receive a delivery receipt. The third party SMS providers will do the job of actually sending the SMS to the destination number. The account details are entered onto the Arc Pro Server and details downloaded to each of the attendant console clients as they login. The operator then communicates with the vendor directly via the local internet connection.



Using the Arc Pro Operator application, an operator will be able to send an SMS to a colleague or a customer, or in general, to any valid number. The operator can send a single message (limit 160 characters), and multiple messages as well.

The operator will define the following:

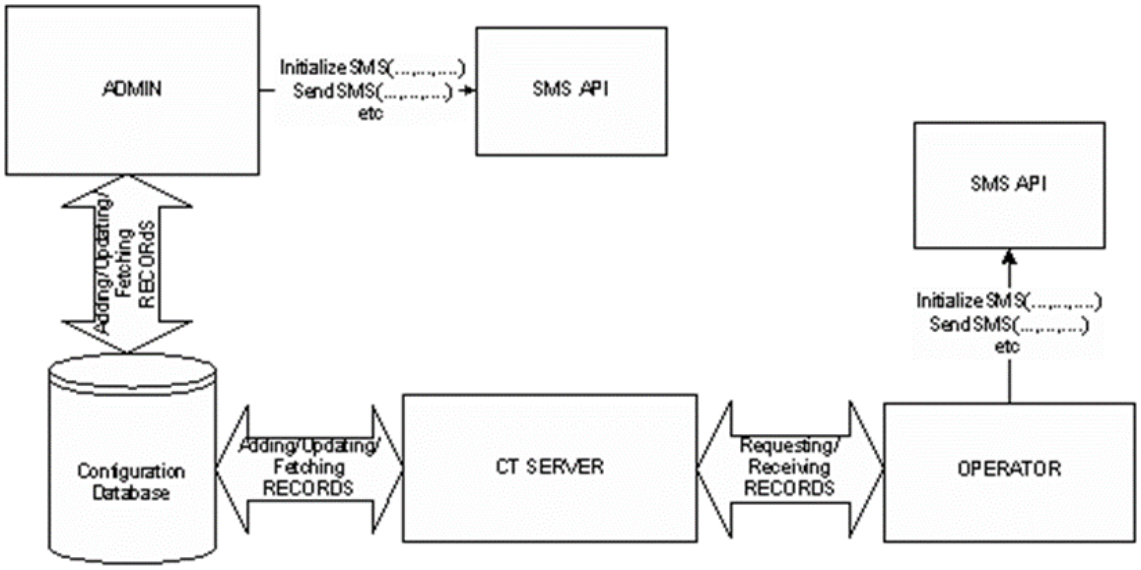
SMS number:	This number can be selected from the internal contact database, speed dial or can be entered as a new number.
SMS message:	It's the text to be sent as a SMS message. Agent can choose from a list of predefined messages, or can write a new message, or can combine both.

Provide Arc Operator with the option to send SMS' longer than the typical SMS length.

Architecture

The architecture has been kept straightforward. The Operator will enter the SMS content, Send, and then receive a confirmation of success or failure of delivery.

The SMS is sent using 3rd party SMS-Services providers. The customer will require an account of one or more of these vendors. Vendors will be added and configured in the Arc Pro Admin. The SMS is sent via HTTP to the selected vendor. Once the vendor receives the SMS successfully, it will send back an acknowledgement, and after that, it will be the duty of the vendor to send the SMS to the destination number.



The architecture remains the same. CT Server and Admin application will interact will Configuration Database as before. Operator, as a client application, will get data from CT Server. At the time of sending the SMS, Operator application will call SMS API's function and pass the data to it.

Protocols

This solution currently makes use of HTTP/HTTPS protocol for working. So, it is compatible with all those vendors in the market that provide HTTP/HTTPS solutions.

Tenancy

This SMS feature will work in a multi-tenant environment. Arc's solution works in a way that all the contacts are divided into different Regions. These different Regions are dealt differently. Each Region can be assigned an SMS vendor. In the case that no vendor is assigned to a Region, the system will use the default vendor to send the SMS.

For multi-tenant systems, a default vendor can be able to be set for a community.

Voice Connect

Voice Connect provides in-queue messaging to callers waiting in queues to be answered, and also scripts allowing callers to enter digits to route their calls based on instructions played to them. The only additional system requirement is the configuration of a single CTI Port for use as a Static Voice Port. This is used for the recording and management of phrases and messages within the system. The voice port must be configured on the CUCM and added to the Arc Configuration in the CT Gateway>Resource Group Devices>Voice Devices section. A device should be created for each Resource Group that will be using Voice Connect.

Calls entering the Arc Pro system are handled in the normal way via a Pre CT Gateway device and then on a CTI Port in the Host PBX Gateway. If the call is destined for a Voice Queue (known as a Voice Session) where it will be played a script then the call is routed onto a standard Host PBX Gateway port, and the message is streamed without moving the call anywhere else. The caller will hear the script and make their choices via DTMF tones from their handset. The call is then either routed logically to an Arc Call Queue, without moving from the Host PBX Gateway port, or can be transferred out of the Arc Pro system.

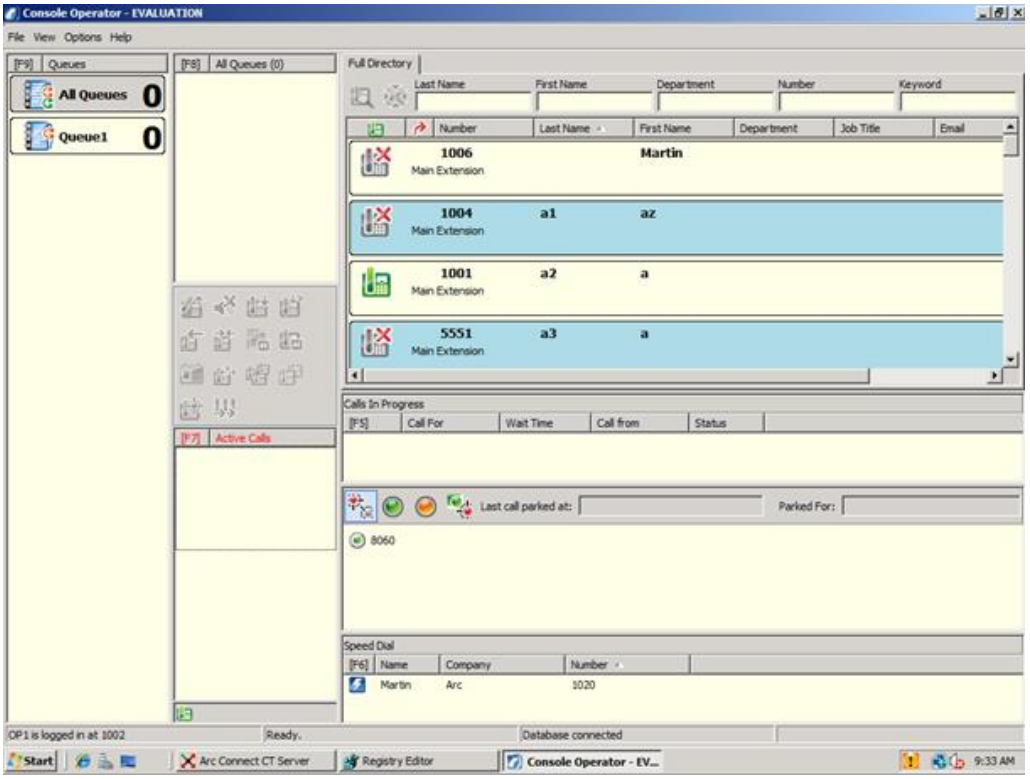
In- queue messaging can only be played to callers waiting to be answered in Arc Call Queues. The voice message is streamed to the caller while the call is waiting on the Host PBX Gateway port.

On the first instance that Voice Connect is used the call will be connected, and will be placed on hold between subsequent messages, and until the call is answered by an agent/operator.

Voice Connect requires the Windows Firewall to be opened up to allow the voice stream to be recorded. If this is blocked a phrase will be saved but it will be silent. All correctly recorded phrases can be played back through the firewall without additional configuration.

Enhanced Directory View

The operator has been enhanced, specifically in the Directory area so that it is easier to distinguish between each line/contact.



The Color selection is based on registry settings in:

HKEY_LOCAL_MACHINE\SOFTWARE\Arc Solutions\Call Connect\Operator\Preferences\Alternate Row Colour Enabled (set to Yes)

HKEY_LOCAL_MACHINE\SOFTWARE\Arc Solutions\Call Connect\Operator\Preferences\Alternate Row Colour (colors should be added in Hexadecimal form some examples are :

Light Grey is Hex CCCCCC Medium Grey is 999999

Light Blue is E6D8AD (example above) Medium Blue is CD0000

For more information on colors refer to http://en.wikipedia.org/wiki/Web_colors.

For each color, take the Hex and reverse the 3 RGB figures, for example Light Blue shows ADD8E6, and becomes E6D8AD as shown above.

> **Note**
> When making any changes to the operator registry these should be done with the application closed.

8: Dial plans and expression handling

This chapter contains the following information:

Overview

The Arc Pro product suite has been adapted to support advanced dial plan processing for both inbound and outbound call handling.

The Dial Plan feature incorporates a rule based system using regular expression processing to identify a number based on a pattern algorithm. Numbers can be identified as internal or external to the telephone system and can be modified for presentation to applications. In addition, for outbound dialing the number can be converted using ITU E.164 telephone numbering standards and associated with specific prefix information.

Multiple dial plan rules can be created and associated with a resource group that can be used to manage the calls processed by the Arc Communication server.

Technical overview

When a number is received from the telephone system (inbound) or sent to the telephone system (outbound), the number can be processed against defined groupings of expressions and the Arc Pro system will therefore be able to identify the numbers origin as internal or external to the telephone system.

Additional features supported for inbound dial plans:

- Support multiple rules (using regular expressions to identify a number pattern)
- Perform modifications on the number for display (using regular expressions)

Additional features supported for outbound dial plans:

- Support multiple rules (using regular expressions to identify a number pattern)
- Perform modifications on the number (using regular expressions)
- ITU E.164 telephone numbering conversion to a dial string
- Support prefix and postfix operations for local, domestic and international numbers.
- Support Authorization codes and Account codes (FAC\CMC respectively used for Cisco Unified Call manager)

Dial Plan overview

A new concept of dial plan groups will be created to manage multiple dial plan configurations. Users will be able to create and manage one or many dial plan configurations.

The dial plan implementation is a device and resource group centric model. Each resource group will be assigned to a dial plan configuration; however, each device within a resource group can have a unique and different dial plan.

A dial plan configuration will consist of the following elements:

- Default internal and external access configuration and account management (this configuration will serve as a direct replacement for the parable configuration that exists today).
- Inbound dial plan processing (ability to identify and modify call information supplied by the telephone system).
- Outbound dial plan processing (ability to identify and modify a number for dialing, including the ability to localize the internal\external access and account management configuration).

Associations with a dial plan are:

Parameter	Description
User	A dial plan configuration can be associated with a user of the system. The dial plan will follow the user and can therefore provide a user centric solution.
Resource Group	A resource group will be associated with a dial plan configuration; this is a mandatory requirement for all resource groups.
Device	A device that is associated to a resource group will be coupled with the dial plan configuration or alternatively the device can have its own unique dial plan association. A device not related to a resource group will be logically related to the system wide default resource group.
Community	The default resource group for a community will be used to identify the default dial plan configuration for each community.

Process flow model

The process flow model will describe how a dial plan is selected by the server to manage inbound and outbound dial plan processing.

Inbound dial plan model

The inbound dial plan model uses the following hierarchy, when processing call information, to determine the correct dial plan group:

Device (High)	Default dial plan assigned to a device (ignored if a dial plan group is not specified for the device)
Device Resource Group	Default dial plan assigned to a resource group related to the device (ignored if a resource group is not specified for the device)
Community Default Resource Group	This applies only if the device is a recognized client device (agent, operator) and is therefore associated with a community profile. In this scenario use the default dial plan assigned to the communities default resource group.

System Default Resource Group (Low)	Default dial plan assigned to the system wide default resource group. This is regarded a catch all.

Once a selected dial plan group is assigned to a call, the dial plan group will always follow the call throughout its life, including if the call is routed to another device that has a different dial plan group assigned.

For incoming calls, after the inbound dial plan matching process has completed, the original CLI (callers number) will be stored with the call and the new (possibly modified) CLI will be stored as the CLI. If the CLI changes due to a transfer or other events then the inbound dial plan matching process will be re-run. However, this process will only be re-run if there is a change.

For outgoing calls, after the inbound dial plan matching process has completed, the original DDI (called number) will be stored with the call and the new (possibly modified) DDI will be stored as the DDI. If the DDI changes due to a transfer or other events then the inbound dial plan matching process will be re-run. However, this process will only be re-run if there is a change.

The call origin will be identified for incoming and outgoing calls. The call origin identification will be assigned to the call to identify the call to be internal or external to the telephone system. For system calls, all calls will be applied with inbound dial plan rules based on the queued device or the devices associated resource group (see note below).

> **Note**
> Resource groups associated by call filters cannot be used for inbound rule processing for system queued calls. This is because inbound rules will need to be processed before the filtering process starts.

Outbound dial plan model

The following scenarios are catered for when managing outbound dial plans:

Scenario	Description
Queue Routing	Calls routed via the system queues like Overflow, Night service.
Client Rerouting	Calls re-routed from the client application (operator, agent) like transfer, camp-on ▪ **Local** – Re-routing performed at the client device ▪ **Server** – Re-routing performed at the server (service queue) ▪ **Client Instigated Calls** – Client dialing

The following solutions will need to be catered for when managing outbound dial plans:

Solution type	Description
Normal	Normal small enterprise set-up with one dial plan configuration servicing all calls.
Serviced	More than one company is serviced in a single server solution with one operator (or a group of operators) servicing many companies. Typically an operator can take calls simultaneously for each company and there may be specific dial plan configurations for each company. For example: Call C1 is received by the operator for customer A and outgoing calls need to be prefixed with 5* Call C2 is received by the operator for customer B and outgoing calls need to be prefixed with 6*

Solution type	Description
Tenant	More than one company is serviced in a single server solution. Operators, queues and other configuration elements are local to a company and the system is partitioned so the each company is blocked from accessing each other's resources. Basically each company will not be aware that other companies are using the same system.
Large Enterprise (Roaming)	A large enterprise may be distributed by location. In this scenario the clients will log into their profile but may be in different locations as part of their role. Each location requiring specific dial plan requirements. For example: Operator logs into location A (x1000), calls need to be prefixed to be with 8* to route calls from location A to location B. Same operator logs into location B (x2000) next day, calls need to be prefixed to be with 7* to route calls from location B to location A.
Large Enterprise (Fixed)	A large enterprise may be distributed by location. In this scenario the clients will log into a fixed location or device, however, many clients may service the same queue but reside in different locations. For example: Operator X logs into location A (x1000), calls need to be prefixed to be with 8* to route calls from location A Operator Y logs into location B (x2000), calls need to be prefixed to be with 7* to route calls from location B
Large Enterprise (User Centric)	A large enterprise may want to allocate different dial plans to each user profile. In this scenario the clients will log into their profile but may be in different locations as part of their role. Each user will always retain their specific dial plan configuration. This solution may also be used as a way of restricting access for some users.

The outbound dial plan model will use the following hierarchy, when dialing a number, to determine the correct dial plan group:

Hierarchy level	Description
User Profile (High)	Default dial plan assigned to a user profile (ignored if a dial plan group is not specified for the user)
Device	Default dial plan assigned to a device (ignored if a dial plan group is not specified for the device)
Device Resource Group	Default dial plan assigned to a resource group related to the device (ignored if a resource group is not specified for the device)
Community Default Resource Group	This applies only if the device is a recognized client device (agent, operator and others) and is therefore associated with a community profile. In this scenario use the default dial plan assigned to the communities default resource group.
System Default Resource Group (Low)	Default dial plan assigned to the system wide default resource group. This is regarded a catch all.

If the dial plan algorithm modifies the outbound number to have a blank value (no characters\all characters have been stripped) then the solution will assume that the number has been blocked or is invalid.

Dial Plan pass-through

Clients of the system will have a special case when processing calls via the service queue. During normal operation, when a call is routed to the service queue for processing by the server, the server will use the dial plan configuration that is local to the Service Queue device (this may include the system devices associated resource group). Hence, this will not include any consideration for a dial plan configuration that has been associated with the user profile or community profile.

In some cases this is considered to be fine as the server may be in another location and hence the dial plan configuration may need to be different. However, this does mean that the client application (operator) could have a different dial plan when routing calls locally (consultation transfer) or via the server (transfer, camp-on, serial calling). In some cases could be an issue when providing a customer solution.

A dial plan pass-through indicator will be associated with a client profile. When enabled, the server will automatically process the dial plan requirements based on the client profile that issued the request. Therefore the same dial plan configuration will be used as if the client issued the request local to their device.

9: Arc Pro Server environment

This chapter contains the following information:

Server naming convention

The actual machine name of the Arc Pro Server must conform to the requisite Microsoft conventions on machine naming. These can be found on the following link:

http://support.microsoft.com/kb/909264/en-us

Arc hardware compatibility matrix

The Arc Pro system relies on the server platform being a known and tested version.

To confirm that your proposed server platform and operating system is supported check the Arc solutions compatibility matrix in the document *Arc Pro Compatibility and Performance Guide* available from http://enghouseinteractive.co.uk/console-cisco-enterprise-edition-technical-documentation.

The compatibility matrix shows supported operating system, database and virtual environments supported.

VMWare virtual server support

Arc supports a virtualized environment for the Server elements using VMWare. Support is based on the market-leading VMware ESXi 5.x and 6.x.

The resource allocation of the virtual machine running the server must adhere to the minimum specifications listed above, and these resources must be permanently reserved to the Arc Pro Server VM machine. For allocation recommendations see the following guide:

http://enghouseinteractive.co.uk/console-cisco-enterprise-edition-technical-documentation

The Arc licensing will still use the same 8 characters Registration Code to license against, so there are no outward changes visible. There are changes at the back end which mean that move the VM Machine, copying or making a snapshot will disable the licenses already running, with the result that a new license must be requested.

Antivirus support on an Arc Pro Server

Arc Pro server supports many antivirus products. You can find guidelines on antivirus software below:

Exclusions

The files in certain folders are constantly being accessed by the Arc Pro software. Consequently, your antivirus software will constantly try to scan them for viruses, which will slow down the server. Therefore, your chosen antivirus product must support exclusions, which you use to specify the following files and folders that are not to be scanned by the antivirus software:

Default folder	Contains
ArcData	System Databases
Program Files (x86)\Arc\	Software and application trace files
Apache	Active MQ folder
Temp\CiscoTSP0xxLog\	Cisco TSP Trace files

> **Note**
> Your System Administrator may have set up your Arc Pro server to use different folders for these files.

Recommendations

> **Note**
> Your System Administrator may have set up your Arc Pro server to use different folders for these files.

With any anti-virus product, configuration is a balance of scanning versus the performance of the server. The more you choose to scan, the greater the potential performance overhead. The role of the system administrator is to determine what the optimal configuration requirements will be for installing an anti-virus application within a particular environment. Refer to your particular anti-virus product documentation for more detailed configuration information.

The following list highlights some general best practices:

- Update AV software scanning engines and definition files on a regular basis, following your organization's current policies.
- Upgrade to the latest supported version of the third-party anti-virus application. Newer versions improve scanning speed over previous versions, resulting in lower overhead on servers.
- Avoid scanning of any files accessed from remote drives (such as network mappings or UNC connections). Where possible, ensure that each of these remote machines has its own anti-virus software installed, thus keeping all scanning local. With a multi-tiered antivirus strategy, scanning across the network and adding to the network load should not be required.

- Schedule full scans of systems by AV software only during scheduled maintenance windows, and when the AV scan will not interrupt other Unified Console Server activities.
- Do not set AV software to run in an automatic or background mode for which all incoming data or modified files are scanned in real time.
- Due to the higher scanning overhead of heuristics scanning over traditional anti-virus scanning, use this advanced scanning option only at key points of data entry from untrusted networks (such as email and Internet gateways).
- Real-time or on-access scanning can be enabled, but only on incoming files (when writing to disk). This is the default setting for most anti-virus applications. Implementing on-access scanning on file reads will yield a higher impact on system resources than necessary in a high-performance application environment.
- While on-demand and real-time scanning of all files gives optimum protection, this configuration does have the overhead of scanning those files that cannot support malicious code (for example, ASCII text files). Cisco recommends excluding files or
- directories of files, in all scanning modes, that are known to present no risk to the system.
- Schedule regular disk scans only during low-usage times and at times when application activity is lowest.
- Disable the email scanner if the server does not use email.
- Additionally, set the AV software to block port 25 to block any outgoing email.
- Block IRC ports. IRC uses TCP protocol to communicate on default port 6667. It can also to connect to other TCP ports if TCP port 6667 is blocked.
- If your AV software has spyware detection and removal, then enable this feature. Clean infected files, or delete them (if these files cannot be cleaned).
- Enable logging in your AV application. Limit the log size to 2 MB.
- Set your AV software to scan compressed files.
- Set your AV software to not use more than 20% CPU utilization at any time.
- When a virus is found, the first action is to clean the file, the second to delete or quarantine the file.
- If it is available in your AV software, enable buffer overflow protection.
- Set your AV software to start on system start-up.

Supported remote access applications

As part of the support provided by the Arc Partner or Arc Solutions directly, remote access to the Arc Pro Server is often required.

There are various remote access products available in the marketplace, most of which are supported with the Arc Pro Server. These include

- Real VNC
- Symantec PCAnywhere

All of the above applications should be installed as per the manufacturers' recommendation.

> **Note**
> Session-based remote access applications such as Remote Desktop Protocol (RDP), Remote Desktop Services (RDS) and Terminal Services (TS) are not supported. This is because the TAPI Service used by the Cisco TSP is not multi-user aware. For more information visit http://support.microsoft.com/kb/308405.

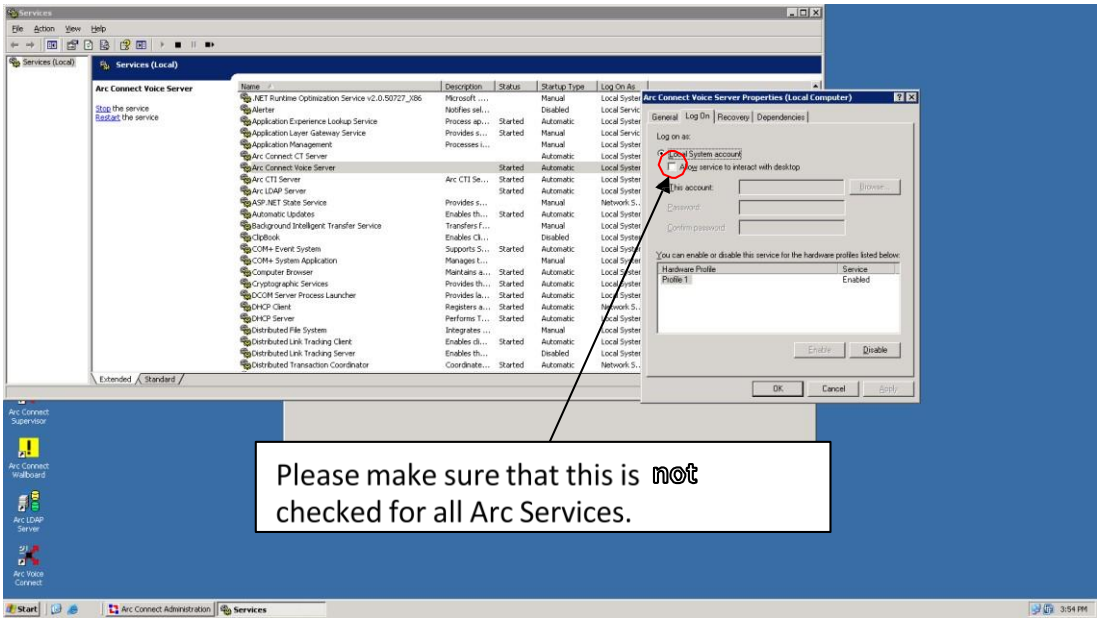
Windows updates

Windows updates are supported on the Arc Pro Server, and encouraged to ensure the smooth running of the system. There are no known issues around the downloading and installation of these updates, however care should be taken to control when these updates are applied, in order to ensure that any required reboots are undertaken at a suitable time for the business, and do not result in unscheduled server reboots and service interruptions.

NIC Teaming

NIC Teaming is not supported and therefore should be disabled, this feature has been found through testing to have detrimental effects to the stability of the system and should be disabled at all times.

Interact with desktop



Allowing the Arc Pro services to interact with the Desktop may lead to issues with the system. Ensure that these items are not checked as per the graphic above.

Client/Server communications

Arc recommends that all installations are configured with Fully Qualified Domain Name (FQDN) based communication rather than IP addresses. An FQDN can only be interpreted in a single way and includes all domain levels to remove any ambiguity. An example of an FQDN is myhost.example.com . When the system is being configured care should be taken to ensure that DNS names are resolved to allow all client/server communications.

Licensing

The Arc Pro suite of products is licensed concurrently, meaning the Arc Pro Client software can be loaded on as many client machines as desired, though only as many users can log into the system as are the number of user licenses.

Example: "I have 3 attendant console Licenses".

The Arc Pro Attendant Console Operator console can be installed on as many machines as necessary, however only 3 Operators can be logged in at any one time.

TCP Ports reserved for Arc use

The Arc Pro Suite uses a series of TCP/IP Ports to communicate between applications. The following ports are used:

TCP/IP Port	Use
1859	This is the Port used to communicate between the Arc Pro Server and the client applications
6600	This is the port used by the Cisco IP Phones for the Arc Pro Server to push RTP Audio data for playback –recording or playing back voice phrases
1659	This is the Port used to communicate between the Arc Pro Voice Server and the Arc Pro Server
1862	This is the port used by the Arc Pro LDAP Server
389	This is the Microsoft Active Directory port – used by the Arc Pro LDAP Server to communicate for Active Directory Integration
45109	This is the Sun iPlanet Directory port – used by the Arc Pro LDAP Server to communicate for Sun iPlanet Integration
2748*	This is the Port used by the Cisco TSP. The Arc Pro Server uses this port to communicate with the Cisco Unified CUCM
1863	TCP communication between the Operator clients and the Arc Cups Server uses this port
5222	Used for communication between the Arc and the Cisco Presence servers
1433 and 1434	Default SQL Ports between servers and between server and clients (Operator and Supervisor)
1864	Communication between the Console Clients and the Arc Pro CTI Server
443*	AXL communication between Arc Pro Server applications and CUCM database
61616	Used by Active MQ Message Bus
49152 to 65535	Dynamic remote ports used to communicate between the Arc Pro Server, Cisco Unified Communications Manager, and the Operator PCs (running Windows Server 2008 and later, or Windows Vista and later). For further information on Dynamic remote ports: http://support.microsoft.com/kb/832017.

TCP/IP Port	Use
1025 to 5000	Dynamic remote ports used to communicate between the Arc Pro Server, Cisco Unified Communications Manager, and the Operator PCs (running Windows XP and Server 2003). For further information on Dynamic remote ports http://support.microsoft.com/kb/832017.

* This port is allocated by Cisco Systems and is not the responsibility of Arc Solutions.

In large networks (often involving a WAN) there could be a need to prioritize these ports across the network switches. In this scenario, the following ports should be prioritized:

Source Port Number	Destination Port Number	Source Address	Destination Address	Application	TCP/UD P	Direction
Any	1659	All Arc Pro Clients and Servers	Arc Pro Servers	Arc Pro Voice Server	TCP	In
Any	1859	All Arc Pro Clients and Servers	Arc Pro Servers	Arc Pro CT Server	TCP	In
Any	1433	All Arc Pro Clients and Servers	Arc Pro Servers	SQL	TCP	In
Any	1434	All Arc Pro Clients and Servers	Arc Pro Servers	SQL	TCP	In
Any	1759	All Arc Pro Clients and Servers	Arc Pro Servers	Presence	TCP	In
Any	2748	Arc Pro Servers	Cisco Call Managers	Cisco TSP	TCP	In
Any	443	Arc Pro Servers	Cisco Call Managers	AXL Connection	TCP	In
Any	389	Arc Pro Servers	Active Directory Server	Active Directory	TCP	In
Any	Any	Primary Arc Pro Server	Secondary Arc Pro Server		IP	Both

10: Third party integration

This chapter contains the following information:

Unity voicemail integration

Cisco Unified CUCM has the ability to configure a "Voicemail Prefix". This means that from anywhere within the CUCM system a prefix can be dialed to enter a specific mailbox. For example, if the prefix is "*", then dialing *1002 will take the caller directly to the mailbox of extension 1002.

More details on this functionality are available at: http://www.cisco.com/en/US/partner/products/sw/voicesw/ps556/products_tech_note09186a00800dea82.shtml.

Integrating with the Arc Console Operator

The Arc Console can use the "Voicemail Prefix" functionality within the Cisco Unified CUCM to transfer calls directly to a Contacts mailbox.

To configure Voicemail Access with the Arc Pro Attendant Console Operator console, follow the steps below:

1. Configure the **Voicemail Prefix** using the Cisco whitepaper (URL above).
2. From the Arc Pro Attendant Console Operator console, select **Options > Preferences > Dialing**.
3. Change the **Voicemail Prefix** setting to whichever the prefix is configured as on the CUCM (typically, it is set to *).
4. Press **Apply**, then press **OK**.

Now, when the Operator is connected to a call, the right-click menu will display an additional option – "Transfer to Voicemail".

How it works

When the Operator selects the **Transfer to Voicemail** option, the Arc Pro Server takes the extension number of the selected contact, and prefixes the number with the Voicemail Prefix number that has been configured. The call is then blind transferred to this extension. The Arc Pro Server has the dependency that the Voicemail Prefix functionality is configured on the Cisco Unified CUCM.

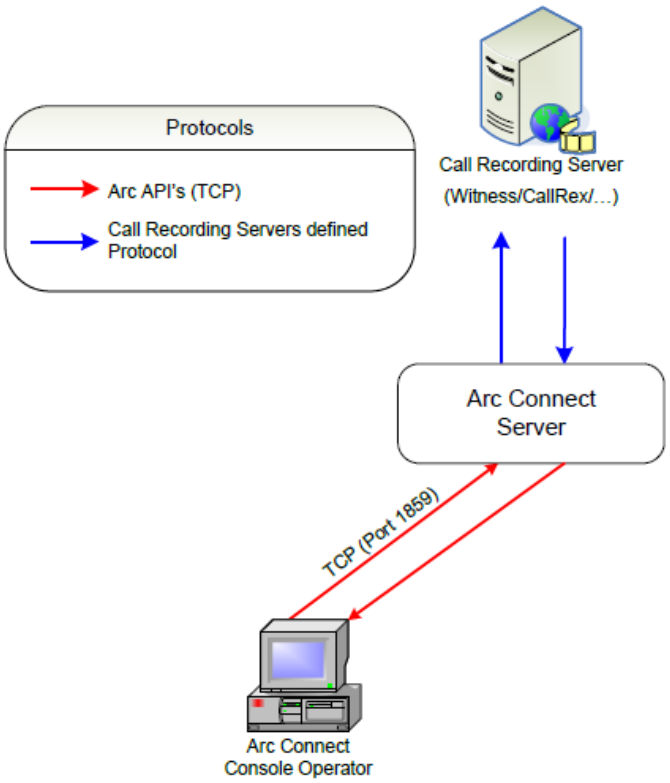
Call recording integration

The Arc Pro software allows a user to initiate call recording of the user's current call via the suites agent and operator clients. Upon the request of the user, the application sends a command to the CT Server. The CT Server then looks at the user's current call and retrieves information of that call. This call information, along with user details, is then packaged up and sent to the specified call recording server.

Arc Pro supports integration with Verint Impact 360 and CallRex from TelRex call recording packages.

Generic integration

The diagram below shows the integration flow in a simple form.



Arc Pro call recording overview

The following data is sent to the call recording server:

- Users Extension DN
- Arc Call ID
- Arrival Queue (Name)
- Arrival Queue (Type)
- Agent Full Name
- Delivery Queue Name
- Delivery Queue Type
- Filter Tag Text

The data that is sent to the call recording server is then stored against that call so that the user at a later date can easily retrieve recorded calls (by searching with that data) and see which queue the call arrived on and who answered it.

Once the record request has been sent, the CT Server then continues with normal operation, but allows for a response back from the call recording server to be processed. Any response from the call recording server is then passed back to the client so it can update its GUI so that the user can see if the call is being recorded or not.

The Arc Pro system allows for all calls to be automatically recorded. This works by the client following the above process if it has been configured to record all calls and once it has a connected call.

QMS

In addition to the information being sent from the Arc Pro Server to the QMS server, there are 2 caveats required to be followed.

Arc needs to connect to the QMS server using an Administrator account set up on the QMS server.

Secondly all extension numbers that are being used for agents or operators that MAY need to be recorded need to be set up on the QMS server to allow recording.

Verint

The following versions of Verint Impact 360 are supported:

- Recorder Versions
  - 7.8.1 – Untested
  - 7.8.3 – Compatible
  - 7.8.3 HFR04 - Compatible
  - 7.8.3 HFR06 – Incompatible
  - 7.8.3 HFR08 – Compatible (Additional Configuration Required)
- Enterprise Manager Versions
  - 7.8.3 - untested
  - 10.0.3 – Compatible

The following steps are required to join Arc to the Recorder:

1. Install and Configure Enterprise Manager
2. Install and Configure VCR as per Standard Recording

   Recorder Control Type must be set to Recorder Controlled.

   Extensions must be configured application controlled; this is the case for On Demand and Bulk recording. Further recorder configuration is not covered in this document, see standard guides.
3. Join Recorder with Enterprise Manager

   Not covered in this document, see standard guides.

   > **Note**
   > The methodology used for ARC Console Recording is the same as ContactExec.

4. Create Data Source in Enterprise Manager, Adaptor in Recorder Manager

   There must be at least one Data Source in Enterprise Manager, labels are unimportant with respects to functionality.

In Recorder Manager a Unify TCP Adaptor must be enabled, by default this will be using TCP port 6666.

If a custom TCP port is required then this must be changed here and on the Arc Pro Server.

5. Add Custom Fields to Viewer Attributes (Optional)

   Firstly the fields are added as custom attributes in Enterprise Manager as follows:

   - Access - System > Attributes >Attributes
   - Create 8 custom attributes each as String variables using these names:
     - ARCCLI
     - EXTENSION1
     - ARCDATA1
     - ARCAGENT
     - ARCCALLID
     - ARCDDI
     - ARCQUEUE
     - ARCDATA2
   - Access – System > Attributes > UDF
   - Create a User Selected Mapping for each Custom Attribute:
     - UDF8 > ARCCLI
     - UDF9 > EXTENSION1
     - UDF10 > ARCDATA1
     - UDF11 > ARCAGENT
     - UDF12 > ARCCALLID
     - UDF13 > ARCDDI
     - UDF14 > ARCQUEUE
     - UDF15 > ARCDATA2

   Next the fields are mapped to events in the Recorder Managers Integration Services as follows:

   - Access – System > Integration Services > Attributes
   - Map each custom attribute to the event:
     - event.ARCCLI
     - event.EXTENSION1
     - event.ARCDATA1
     - event.ARCAGENT
     - event.ARCCALLID
     - event.ARCDDI
     - event.ARCQUEUE
     - event.ARCDATA2

6. Map fields to Live Monitor for Observer (Optional)
   - Access – System > Live Monitor > Observer Column Mapping
   - Create and Map each Observer Colum to the Attribute Source Tag –
     - ARC CLI > udf8
     - ARC Extension > udf09
     - ARC Data1 > udf10
     - ARC Agent > udf11

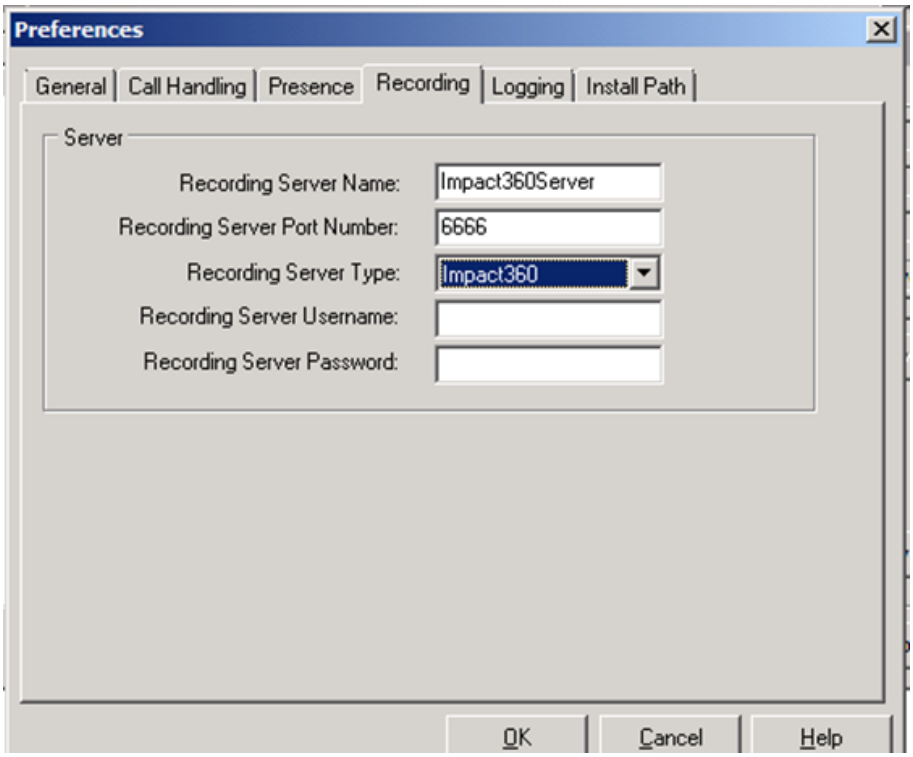
- ARC Call ID > udf12
- ARC DDI > udf13
- ARC Queue > udf14
- ARC Data2 > udf15

7. License ARC Console for Recording

   Access Arc Pro Administration > Login > Help > Registration Confirm or add Recording licenses.

8. Configure Arc Pro CT Server for Recording

   Access Preferences and set the Recorder IP and Port (not applicable – the username and password will not be editable).



9. Configure Arc Pro Administration for Recording Mode

   Access Configuration > Users > Permissions > Permission Assignment

   By default automatic recording is disabled, to enable add 'Automatic Voice Record' to the assigned features list for the relevant user group(s) under AGENT or OPERATOR.

10. Configure ARC Agent / Console Clients (Bulk Only)

    Access Options > Preferences > Call Recording

    Select the relevant radio button to record either; All Calls, Internal only or External only.

Note

- For internal call recording functionality the SPAN must be extension side not trunk side.
- For version 7.8.3 HFR8 the following additional configuration must be completed:
  - Rename *integrationservice-conf.sample.xml* to *integrationservice-conf.xml*.
  - Restart Integration Service.

11: AXL/Database Field Mappings

This section lists the following AXL to Cisco Unified Communications Manager DB Field Mappings used for the device synchronization:

- Phone Mappings
- CTI Route Point Mappings
- Directory Number (Line) Mappings
- Devicenumplanmap Mappings

Phone Mappings

AXL tag	DB Field/default value	CUCM property
<name>	Name	Device Name
<description>	Description	Description
<product>	Tkproduct CTI Port	N/A
<model>	Tkmodel CTI Port	N/A
<class>	Tkclass CTI Port	N/A
<protocol>	Tkdeviceprotocol SCCP	N/A
<protocolSide>	Tkprotocolside User	N/A
<callingSearchSpaceName>	Fkcallingsearchspace	Calling Search Space
<devicePoolName	Fkdevicepool As per Cisco recommendations, this is the most used device pool.	Device Pool
<networkLocation>	Tknetworklocation	N/A
<locationName>	Fklocation	Location
<commonDeviceConfigName>	Fkcommonphoneconfig	Common Device Configuration
<mediaResourceListName>	Fkmediaresourcelist	Media Resource Group List
<networkHoldMOHAudioSourceId>	Networkholdmohaudiosourceid	Network Hold MOH Audio Source
<userHoldMOHAudioSourceID>	Userholdmohaudiosourceid	User Hold MOH Audio Source
<automatedAlternateRoutingCSSName>	Fkcallingsearchspace_aar	AAR Calling Search Space

AXL tag	DB Field/default value	CUCM property
<aarNeighborhoodName>	Fkaarneighborhood	AAR Group
<mlppDomainID>	Fkmlppdomain	MLPP Domain
<cgpnTransformationCSSName>	Fkcallingsearchspace_cgpntransform	Calling Party Transformation CSS
<geoLocationName>	Fkgeolocation	Geo Location
<joinAcrossLines>	Tkstatus_joinacrosslines	Join Across Lines
<useTrustedRelayPoint>	Tkstatus_usetrustedrelaypoint	Use Trusted Relay Point
<alwaysUsePrimeLine>	Tkstatus_alwaysuseprimeline	Always Use Prime Line
<alwaysUsePrimeLineforVoiceMessage>	Tkstatus_alwaysuseprimelineforvm	Always Use Prime Line for Voice Message
<userLocale>	Tkuserlocal	User Locale
<builtInBridgeStatus>	Tkstatus_builtinbridge	N/A
<callInfoPrivacyStatus>	Tksipprivacy	Privacy
<hlogStatus>	Not known	N/A
<ownerUserID>	Fkenduser	Owner User ID
<ignorePresentationIndicators>	Ignorepi	Ignore Presentation Indicators (internal calls only)
<subscribeCallingSearchSpaceName>	Fkcallingsearchspace_restrict	SUBSCRIBE Calling Search Space
<unattendedPort>	Unattended_port	Unattended Port
<phoneSuite>	Not known	N/A
<deviceMobilityMode>	Tkstatus_devicemobilitymode	Device Mobility Mode
<remoteDevice>	Remotedevice	N/A
<dndOption>	Tkdndoption	DND Option
<dndRingSetting>	Tkdndoption	DND Incoming Call Alert
<dndStatus>	Dndtimeout	Do Not Disturb
<label>	Label	Line Text Label

CTI Route Point Mappings

This table lists the mappings related to CTI Route Points in the DB device table.

AXL tag	DB Field/default value	CUCM property
<name>	Name	Device Name
<description>	Description	Description

AXL tag	DB Field/default value	CUCM property
<product>	Tkproduct CTI Route Point	N/A
<model>	Tkmodel CTI Route Point	N/A
<class>	Tkclass	N/A
<protocol>	Tkdeviceprotocol SCCP	N/A
<protocolSide>	Tkprotocolside User	N/A
<callingSearchSpaceName>	Kcallingsearchspace	Calling Search Space
<devicePoolName>	Fkdevicepool As per Cisco recommendations, this is the most used device pool.	Device Pool
<networkLocation>	Tknetworklocation	N/A
<locationName>	Fklocation	Location
<commonDeviceConfigName>	Fkcommonphoneconfig	Common Device Configuration
<mediaResourceListName>	Fkmediasourcelist	Media Resource Group List
<networkHoldMOHAudioSourceId>	Networkholdmohaudiosourceid	Network Hold MOH Audio Source
<userHoldMOHAudioSourceId>	Userholdmohaudiosourceid	User Hold MOH Audio Source
<automatedAlternateRoutingCSSName>	Fkcallingsearchspace_aar	AAR Calling Search Space
<aarNeighborhoodName>	Fkaarneighborhood	AAR Group
cgpntransformationCSSName>	Fkcallingsearchspace_cgpntransform	Calling Party Transformation CSS
<geoLocationName>	Fkgeolocation	Geo Location

Directory Number (Line) Mappings

This table lists the mappings related to Line or Directory Number in the dnorpattern DB Table.

AXL tag	DB Field/default value	CUCM property
<pattern>	Dnorpattern Directory Number Provided	Directory Number
<description>	Description ASD-<Mac>-<DN>	Description
<usage>	Tkpatternusage Conference	N/A
<routePartition>	Fkroutepartition None	N/A

AXL tag	DB Field/default value	CUCM property
<aarNeighborhoodName>	Fkaarneighborhood	AAR Group
<aarKeepCallHistory>	Aarkeepcallhistory	Retain this destination in the call forwarding history
<aarVoiceMailEnabled>	Aarvoicemailenable	Voice Mail
<PresenceGroup>	Fkmatrix_presence	Presence Group
<callForwardAll>		Forward All
<forwardToVoiceMail>	Cfaptvoicemailenabled	Voice Mail
<callingSearchSpace>	Fkcallingsearchspace_cfapt	Calling Search Space
<destination>	Cfaptdestination	Destination
<callForardBusy>		Forward Busy External
<forwardToVoiceMail	Cfbintvoicemailenabled	Voice Mail
<callingSearchSpace>	Fkcallingsearchspace_cfbint	Calling Search Space
<Destination>	Cfaptdestination	Destination
<callForwardBusy>		Forward Busy External
<forwardToVoiceMail>	Cfaptdestination	Destination
<callForwardBusyInt>		Forward Busy Internal
<forwardToVoiceMail>	Cfbintvoicemailenabled	Voice Mail
<callingSearchSpace>	Cfbintdestination	Destination
<callForwardNoAnswer>		Forward No Answer External
<forwardToVoiceMail>	Cfnavoicemailenabled	Voice Mail
<callingSearchSpace>	Fkcallingsearchspace_cfnat	Calling Search Space
<destination>	Cfnadestination	Destination
<callForwardNoAnswerInt>		Forward No Answer Internal
<fowardToVoiceMail>	Cfnaintvoicemailenabled	Voice Mail
<callingSearchSpace>	Fkcallingsearchspace_cfnaint	Calling Search Space
<destination>	Cfnaintdestination	Destination
<callForwardNoCoverage>		Forward No Coverage External
<forwardToVoiceMail>	Pffvoicemailenabled	
<callingSearchSpace>	Fkcallingsearchspace_pff	
<destination>	Pffdestination	
<callForwardNoCoverageInt>		Forward No Coverage Internal
<forwardToVoiceMail>	Pffintvoicemailenabled	

AXL tag	DB Field/default value	CUCM property
<callingSearchSpace>	Fkcallingsearchspace_pffint	
<destination>	Pffintdestination	
<callForwardOnFailure>		Forward on CTI Failure
<forwardToVoiceMail>	Cfdfvoicemailenabled	
<callingSearchSpace>	Fkcallingsearchspace_devicefailure	
<destination>	Devicefailuredn	
<callForwardNotRegistered>		Forward Unregistered External
<forwardToVoiceMail>	Cfurvoicemailenabled	
<callingSearchSpace>	Fkcallingsearchspace_cfur	
<destination>	Cfurdestination	
<callForwardNotRegisteredInt>		Forward Unregistered Internal
<forwardtoVoiceMail>	Cfurintvoicemailenabled	
<callingSearchSpace>	Fkcallingsearchspace_cfurint	
<destination>	Cfurintdestination	
<callForwardAlternateParty>		MLPP Alternate Party Settings
<callingSearchSpace>	Fkcallingsearchspace_cfapt	MLPP Calling Search Space
<destination>	Cfaptdestination	Target (Destination)
<duration>	Cfaptduration	MLPP No Answer Ring Duration (Seconds)
<callPickupGoup>	Not known	Call Pickup Group
<networkHoldMOHAudioSourceId>	Networkholdmohaudiosourceid	Network Hold MOH Audio Source
<userHoldMOHAudioSourceId>	Userholdmohaudiosourceid	User Hold MOH Audio Source
<alertingName>	Alertingname	Alerting Name
<asciiAlertingName>	alertingNameascii	ASCII Alerting Name
<sharedLineAppearanceCSS>	Fkcallingsearchspace_sharedlineappear	N/A
<voiceMailProfile>	Fkvoicemessagingprofile	Voice Mail Profile
<hrInterval>	hrInterval	Hold Reversion Notification Interval (Seconds)
<hrDuration>	hrDuration	Hold Reversion Ring Duration (Seconds)

AXL tag	DB Field/default value	CUCM property
<parkMonForwardNoRetrieveDN>	Parkmonforwardnoretrievedn	Park Monitoring Forward No Retrieve Destination External
<ParkMonForwardNoRetrieveIntDN>	Parkmonforwardnoretrieveintdn	Park Monitoring Forward No Retrieve Destination Internal
<ParkMonForwardNoRetrieveVMEnabled>	Parkmonforwardnoretrievevmenabled	Voice Mail
<ParkMonForwardNoRetrieveIntVMEnabled>	Parkmonforwardnoretrieveintvmenabled	Voice Mail
<ParkMonForwardNoRetrieveCSSName>	fkcallingsearchspace_pkmonfwdnoret	Calling Search Space
<ParkMonForwardNoRetrieveIntCSSName>	fkcallingsearchspace_pkmonfwdnoretint	Calling Search Space
<ParkMonReversionTimer>	Parkmonreversiontimer	Park Monitoring Reversion Timer
<partyEntranceTone>	Tkstatus_partyentrancetone	Party Entrance Tone

Devicenumplanmap Mappings

This table lists the mappings related to the Device and Line join table (the properties appear on the Directory number GUI).

AXL tag	DB Field/default value	CUCM property
<label>	Label	Line Text Label
<display>	Display	Display (Internal Caller ID)
<displayASCII>	Displayascii	ASCII Display (Internal Caller ID)
<ringSetting>	Tkringsetting_activepickupalert	N/A
<e164Mask>	E164mask	External Phone Number Mask
<dialPlanWizardId>	Dialplanwizardgenid	N/A
<maxNumCalls>	Maxnumcalls 2 for CTI Route Point, 4 for CTI Port)	Maximum Number of Calls
<busyTrigger>	Busytrigger 1 for CTI Route Point, 2 for CTI Port	Busy Trigger
<monitoringCSSName>	Fkcallingsearchspace_monitoring	Monitoring Calling Search Space
<callInfoDisplay>	Callinfodisplaymask 9	Forwarded Call Information Display on Device