Cisco Unified Business/Department/Enterprise Attendant Console - Troubleshooting Guide

August 26th, 2011

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-20150-01

Cisco Unified Business/Department/Enterprise Attendant Console - Troubleshooting Guide

CONTENTS

Preface

Purpose and Audience

This document is intended for the following audience:

Those involved in the planning, implementation and System Administration of a Cisco Unified Attendant Console Solution.

Usage of this document

This document should be used in conjunction with the respective Web administration and operation guides to assist you in the successful planning and implementation of a Cisco Unified Attendant Console system. This document assumes basic knowledge of the Cisco Unified Attendant Console system and an understanding of Cisco Unified Call Manager.

This document will discuss the possible implementation scenarios, taking into account various topologies and environmental issues.

Abbreviation	Description	Comments
CUCM	Cisco Unified Communication Manager	
CUxAC	Cisco Unified Attendant Console	May be used when referring to a common component or to generalize a practice across the product range.
CUBAC	Cisco Unified Business Attendant Console	
CUDAC	Cisco Unified Department Attendant Console	
CUEAC	Cisco Unified Enterprise Attendant Console	
CUP	Cisco Unified Presence	
TSP	Telephony Service Provider	Facilitates communications between CUxAC Server and CUCM

General Information

The CUxAC range of products provide 3 differing levels of Attendant Console functionality, based on both scalability and functionality, however all share the same fundamental backbone and technology.

The solutions all follow a client/server philosophy and use the Cisco TSP to communicate with CUCM and control the relevant calls.

The following limitations apply to the 3 products:-

Table 1 Product Limitations of the Cisco Unified Attendant Console Suite

	Number of Attendants (operators)	Number of Queues	Number of Contacts Supported
CUDAC	10 (2 per department)	5 (1 per department)	750 Contacts
CUBAC	6	3	500 Contacts
CUEAC	25	50	CUCM Capacity

Please refer to the CUxAC Administration Guide for details of the functionality differences between the products.

Cisco Unified Attendant Console Terminology

Within this guide and when using the Cisco Unified Attendant Console system there will be references to various devices with system-recognized names. These devices are referred to throughout this document as the "Controlled CTI Devices". The table below explains the terminology and the types of devices used.

Table 2 Cisco Unified Attendant Console Terminology

Cisco Unified Attendant Console Device Name	CUCM Device Type	Description/Use
CT Gateway Devices	CTI Port	Once a call has reached the Queue DDI, the Cisco Unified Attendant Console Server informs the CUCM to move the call to a CT Gateway device. The CT Gateway is used for queuing calls in the CUxAC system.
Queue DDI	CTI Route Point	Each Cisco Unified Attendant Console queue configured has a DDI. Incoming calls to the Cisco Unified Attendant Console system should be routed to these DDI devices.

Cisco Unified Attendant Console Device Name	CUCM Device Type	Description/Use
Service Devices	CTI Port	The Service Queue devices are used by the Attendant Console application to hold, transfer and camp calls on.
Park Devices	CTI Port	The Park devices are used by the attendant Console to park calls. This Call Park functionality is separate from the generic CUCM Call Park.

CUxAC User Accounts

The CUxAC system uses the Cisco TSP to communicate between the CUxAC Server and the CUCM cluster to which it is registered. In order to function correctly the User profile with which the TSP is registered must have the correct roles assigned to it that all it perform all of the functions required. All CUxAC versions up to 8.0.3 require an End User to be configured. If the CUCM is synchronised with an AD source, then the required End User must also be configured in AD, or it will be deleted when the synch happens.

Note From version 8.0.3 an Application User is required. This has the advantage that these Users are not synched with AD, and therefore there is no risk of the User being deleted this way, and running the risk of the CUxAC server shutting down. It is required that the User is changed from an End User to an Application User when completing an upgrade to version 8.0.3 or higher.

The User requires the following Roles to be assigned:-

- Standard CTI Enabled
- Standard CTI Allow Call Park Monitoring
- Standard CTI Allow Calling Number Modification
- Standard CTI Allow Control of All Devices
- Standard CTI Allow Reception of SRTP Key Material
- Standard AXL API Access
- Standard CTI Allow Control of Phones supporting Rollover Mode*
- Standard CTI Allow Control of Phones supporting Connected Xfer and conf*

Note * are only relevant if using phone models 69xx, 7931, 7965, 89xx and 99xx on CUCM 7.1.2 or greater.

Cisco Unified Attendant Console Device Provisioning

When planning the installation of a Cisco Unified Attendant Console system, thought must be put into calculating the number of "Controlled CTI Devices" to be configured on the CUCM.

The below information will assist in making those decisions

Queue DDI

For each DDI/DID that is to be routed into the Cisco Unified Attendant Console Server, a DDI needs to be configured.

CT Gateway

These devices are used for queuing calls that have not yet been answered. The recommendation is to allow 1 device for each PSTN line, plus a contingency for other incoming system calls if capacity is available within the maximum 255 Controlled Devices.

Tip If there is a 30 line PRI coming into the Cisco Unified Attendant Console system, then create 40 Host PBX Gateway devices.

Service Devices

The Service Devices are used by the Attendant Console to Hold, Transfer and Camp On calls. The recommendation is 4 - 6 Service Devices are configured per Attendant Console user. These devices are only used with the Attendant Console.

Park Devices

The Park Devices are used for the Attendants to park calls. It is recommended that 3 Park devices are configured per Attendant Console user. These devices are only used with the Attendant Console, and does NOT impact on the standard CUCM Call Park functionality.

System Sizing Tool

To assist in planning your system there is a Unified Communications Sizing Tool (UCST) that can be found on the following web site:-

http://tools.cisco.com/cucst

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

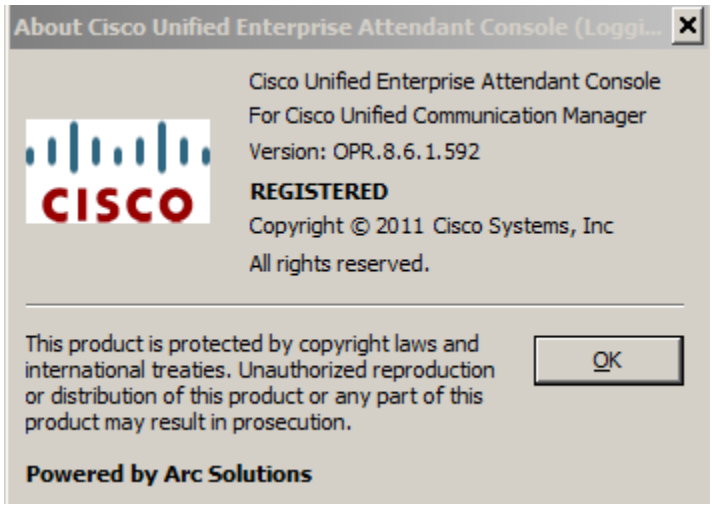
CHAPTER 1

Logging

This chapter describes the Logging functionality that can be used for troubleshooting any issues, and what content is captured.

CUxAC Logs

- CUxAC logs are located in C:\Program Files\Cisco\Logging\OPR\ Log
- To toggle traces on the Attendant Console, navigate to Help->About and press CTRL+ALT+T. The word "Logging" will appear in the title bar if traces are activated



- The following Registry keys on the operator PC determine specific logging items that can be amended:

Location	Options	Use
HKEY_LOCAL_MACHINE\Software\Arc Solutions\Call Connect\Operator\Logging\Database Logging	Yes/No	This setting will enable or disable traces related to Contact Directory and searches
HKEY_LOCAL_MACHINE\Software\Arc Solutions\Call Connect\Operator\Logging\Full Logging	Yes/No	This setting will enable maximum traces if set to On or default traces if set to Off

Location	Options	Use
HKEY_LOCAL_MACHINE\Software\Arc Solutions\Call Connect\Operator\Logging\General Log File	OPRlog.txt	This will give the base name of the logging files
HKEY_LOCAL_MACHINE\Software\Arc Solutions\Call Connect\Operator\Logging\General Log Location	File/directory path	Location of the log files
HKEY_LOCAL_MACHINE\Software\Arc Solutions\Call Connect\Operator\Logging\Host CTI Service Logging	Yes/No	This setting will enable or disable logging related to the Phone Status Icons
HKEY_LOCAL_MACHINE\Software\Arc Solutions\Call Connect\Operator\Logging\Logging On	Yes/No	This setting enables or disables traces being written
HKEY_LOCAL_MACHINE\Software\Arc Solutions\Call Connect\Operator\Logging\Maximum Log Files	Numerical Value	Number of log files to be written
HKEY_LOCAL_MACHINE\Software\Arc Solutions\Call Connect\Operator\Logging\Maximum Log Lines	Numerical Value	Number of lines written in each log file

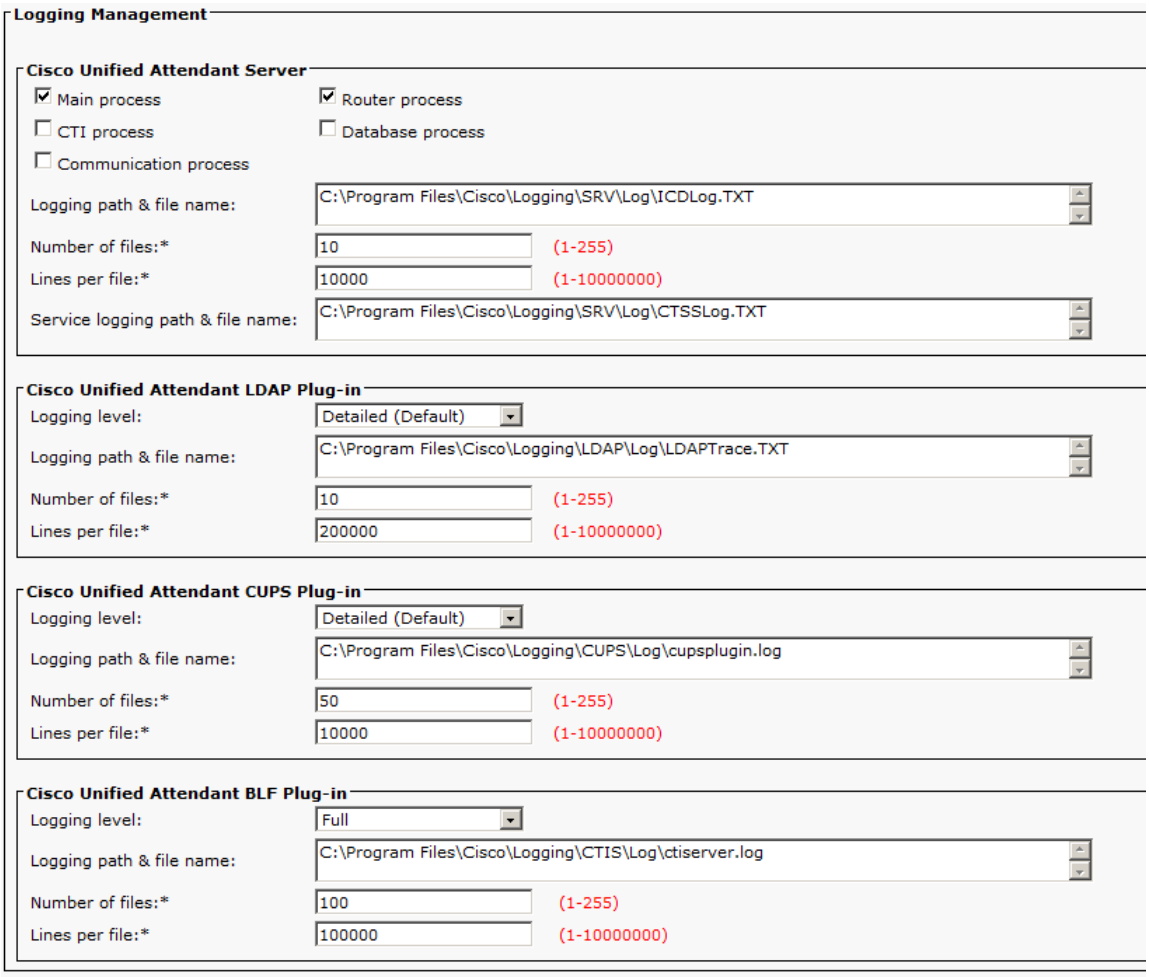
Cisco Unified Attendant Server Logs

Server logs are split between the different components: WebAdmin, Main Server, LDAP, BLF Plug-in, and Presence Plug-in. Each component saves its logs in a different folder in C:\Program Files\Cisco\Logging

Logging is configured from the Engineering > Logging Management section of the Web Administration.

By default, the Main Process and Router Process are the only logs which are enabled. In order to troubleshoot most issues, this logging level will give sufficient information in order to investigate the cause of any problems.

Figure 1-1 Shows the Logging Management page from the Wed Administration software



If however, there are issues which are around specific areas, there maybe a requirement to enable some of the other option, The following is a short description of what is logged with these different options:

- Main Process - This is the Server top layer, this manages the router, database and comms, for example user activity (login, logout).
- Router Process - This logs all the call routing information.
- CTI Process - This covers the TAPI Interface
- Communications Process - This logs the TCP/IP Level Communication between the clients and the server.
- Database Process - This logs all database related activity covering both CUxAC SQL Databases.

Cisco Unified Attendant LDAP Plug-in -

Detailed is the default logging level. However, in the case of discrepancies between the CUxAC and CUCM directory and issues in synching data online to the CUxAC Server or communication issues then logging level should be switched to Full to cover the full activity. In this case it may need to increase the number of lines and files depending the directory size.

Logging lines per file can be set to 100,000 and files up to 100. However, It can be increased in accordance with the nature of issue being experienced and where traces to cover the longer period for as far back as required.

Cisco Unified Attendant CUPS Plug-in

In case of memory leaks, communication issues or sipXTapi (open source third party component) have got any issue, Dot Net stack level exception details or more in-depth information is required then the logging level needs to be set to “Full”.

Make sure, that key (**<add key="sipXtapiLogging" value="true"/>**) to enable the sipXtapi log is set to true in C:\Program Files\Cisco\CUPS\CUPS Presence Server Plug-in.exe.config file.

Logging lines and number of files can be increased in accordance with the nature of issue being experienced and where traces to cover the longer period for as far back as required.

Cisco Unified Attendant BLF Plug-in

By default, the logging level is set to Full.

The default number of files and lines per file can be changed in order to keep log files for a longer period of time. Disk space should be taken into consideration of you are to change these values.

Web Admin

Usually the default logging should be enough to provide traces for troubleshooting of most common issues. However, detailed logging can be enabled for certain issues where default logging is not enough.

Note Note: A backup of “HKEY_LOCAL_MACHINE\SOFTWARE\Arc Solutions\Call Connect\Web Admin\Runtime Logging” registry should be taken before tweaking any registry settings mentioned below. After collecting logs with detailed logging settings, the default logging settings should be restored using the backed up registry. Keeping the logging settings on detailed levels will cause excessive logs to be generated so this should be avoided for normal operations.

Set “HKEY_LOCAL_MACHINE\SOFTWARE\Arc Solutions\Call Connect\Web Admin\Runtime Logging\API Clients Level” registry to 262 decimal (106 hex)

Set “HKEY_LOCAL_MACHINE\SOFTWARE\Arc Solutions\Call Connect\Web Admin\Runtime Logging\Clients Level” registry to 7 decimal/hex.

Set “HKEY_LOCAL_MACHINE\SOFTWARE\Arc Solutions\Call Connect\Web Admin\Runtime Logging\Data Objects Process” registry to YES.

Set “HKEY_LOCAL_MACHINE\SOFTWARE\Arc Solutions\Call Connect\Web Admin\Runtime Logging\Data Objects Level” registry to 7 decimal/hex.

Set “HKEY_LOCAL_MACHINE\SOFTWARE\Arc Solutions\Call Connect\Web Admin\Runtime Logging\API External APIs Level” registry to 519 decimal (207 hex)

Set “HKEY_LOCAL_MACHINE\SOFTWARE\Arc Solutions\Call Connect\Web Admin\Runtime Logging\ Internal Objects Level” registry to 7 decimal/hex.

Set “HKEY_LOCAL_MACHINE\SOFTWARE\Arc Solutions\Call Connect\Web Admin\Runtime Logging\ Internal Objects Process” registry to YES.

Set “HKEY_LOCAL_MACHINE\SOFTWARE\Arc Solutions\Call Connect\Web Admin\Runtime Logging\Management Level” registry to 263 decimal (107 hex)

Set “HKEY_LOCAL_MACHINE\SOFTWARE\Arc Solutions\Call Connect\Web Admin\Runtime Logging\ Request Response Level” registry to 7 decimal/hex.

Set “HKEY_LOCAL_MACHINE\SOFTWARE\Arc Solutions\Call Connect\Web Admin\Runtime Logging\ System Level” registry to 263 decimal (107 hex)

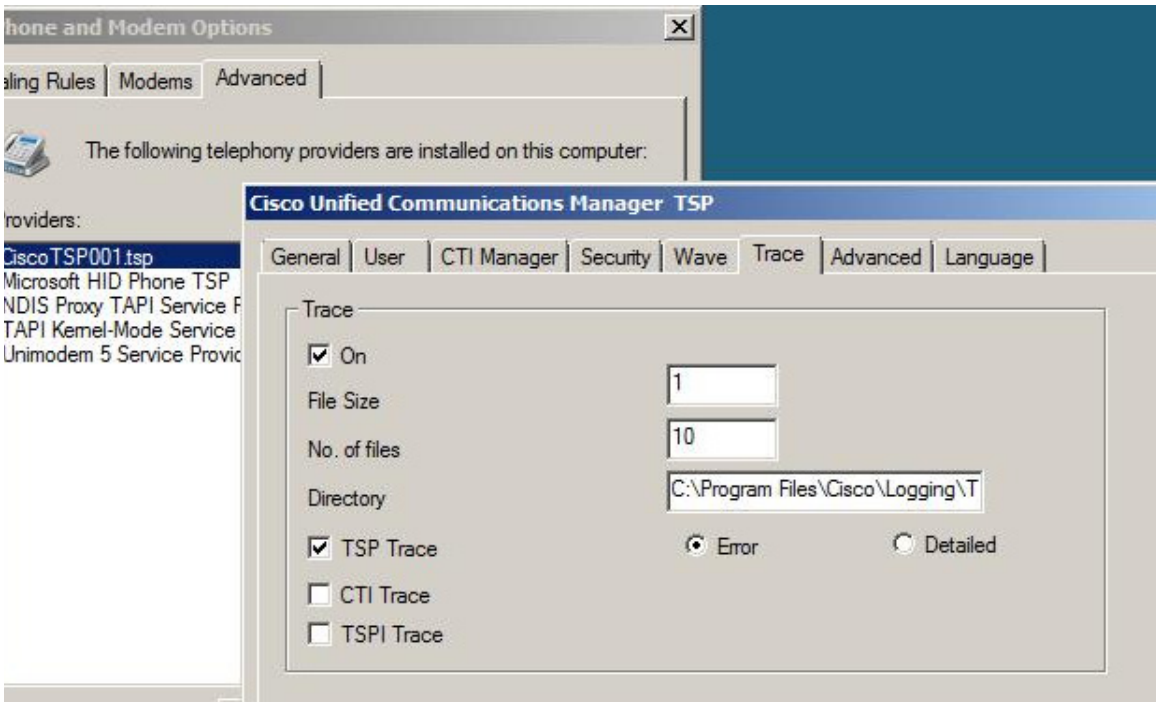
Cisco TSP Logging

To do this, go into the TSP Configuration by opening Windows Control Panel - Phone and Modem Options -

Advanced. Highlight CiscoTSP001.tsp and select Configure.

Click on the Trace Tab and then change the location accordingly:

Note We recommend you change the logging directory path to C:\Program Files\Cisco\Logging\TSP as this makes it easier to gather traces when required. Please note that the TSP folder will need to be created.



There also maybe a requirement to change the trace level to Detailed and to include the CTI Trace and TSPI Trace.

CHAPTER 2

Installation and Connectivity

This chapter looks at troubleshooting issues that can occur during Installation and Connectivity between The CUxAC environment and external resources such as the Unified Communications Manager or LDAP sources.

Unable to connect to CUCM

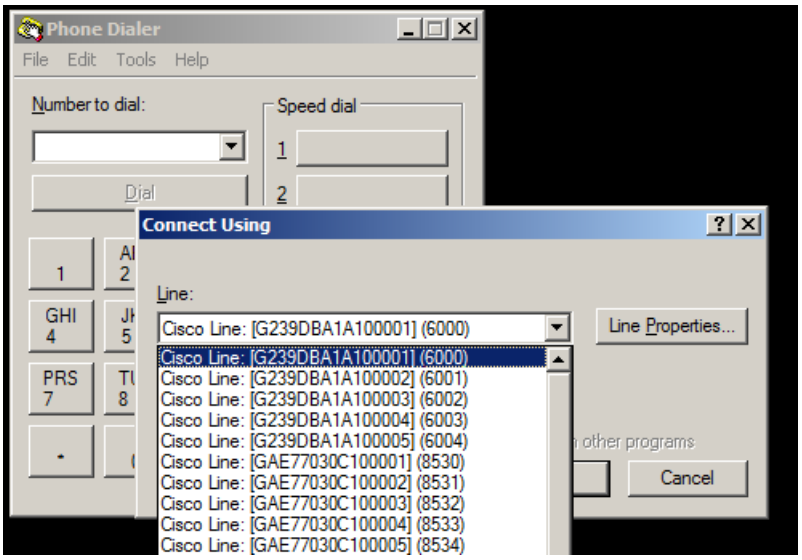
- In the CUxAC WebAdmin navigate to Engineering->CUCM Connection and click the Test Connection button.
- Ensure the Application User username and password are correct by logging into the CUCM with the same credentials.
- Ensure that the user is added to the Standard CUCM Super Users Group.
- Ensure users have the following roles assigned:
  - Standard CTI Allow Call Park Monitoring
  - Standard CTI Allow Calling Number Modification
  - Standard CTI Allow Control of All Devices
  - Standard CTI Allow Reception of SRTP Key Material
  - Standard CTI Enabled
  - Standard AXL API Access
  - Standard CTI Allow Control of Phones supporting Rollover Mode*
  - Standard CTI Allow Control of Phones supporting Connected Xfer and conf*

Note * are only relevant if using phone models 69xx, 7931, 7965, 89xx and 99xx on CUCM 7.1.2 or greater.

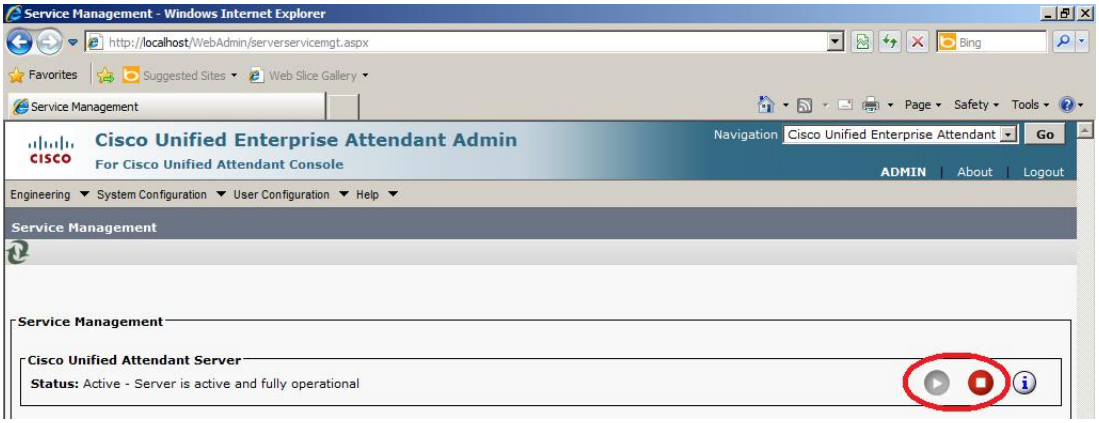
- Ensure that the AXL Service is activated on the CUCM you are trying to connect to.

CTI Devices are not registering on CUCM, their status is Unknown or Unregistered

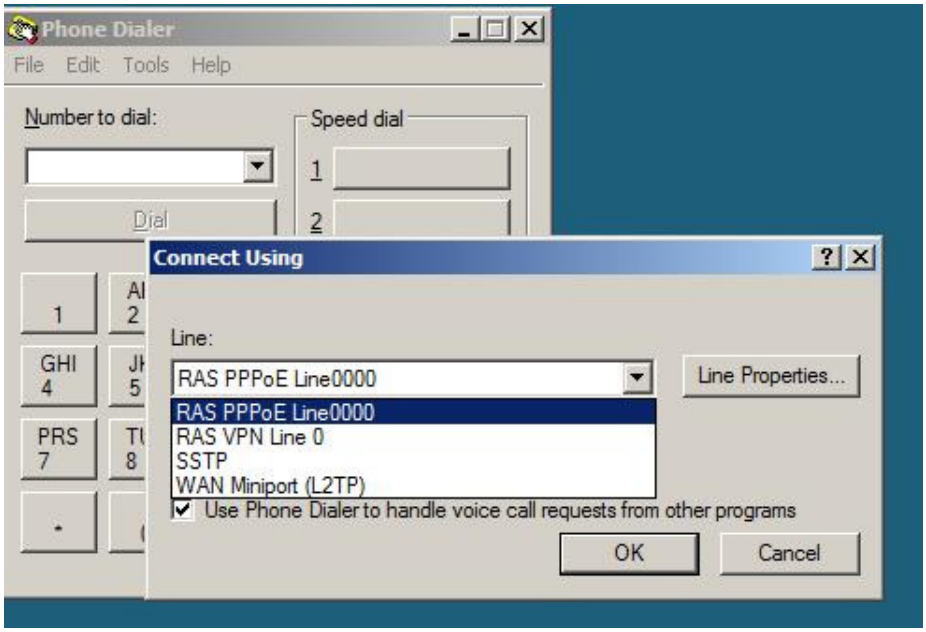
- On the CUxAC server select Start->Run and type "dialer". This will bring up an application to verify that TSP is working: Select Tools > Connect Using and ensure that the Synchronized CTI devices are available in the drop-down list



- If the devices are in the list, ensure the CUxAC server service is started as per the below screenshot



- If the drop down box displays the following, the TSP is not working correctly. Ensure that the TSP Configuration is correct and then reboot the machine to re-establish the TAPI connection.



- If the TSP or Wave Driver has been installed via and RDP connection, this could be the cause of the TSP not functioning correctly. Information on why this is not supported can be found in the Installation and Upgrade Guides under Hardware/Software Requirements at the following link:

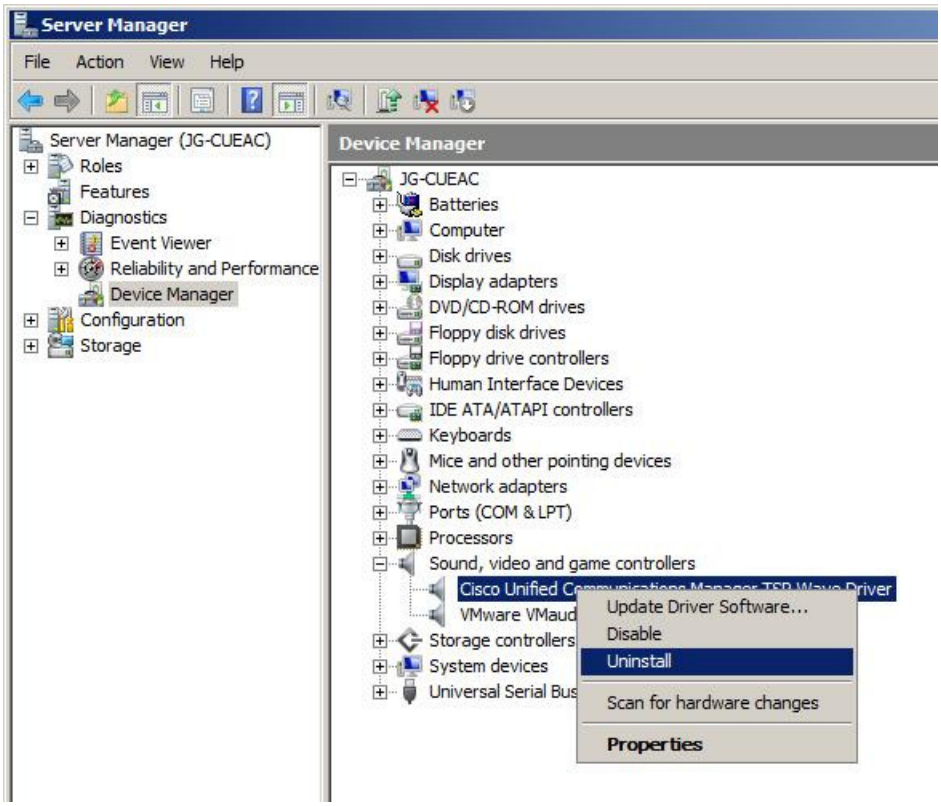
  http://www.cisco.com/en/US/products/ps7282/prod_installation_guides_list.html

- If the TSP and Wave Driver was installed via a session based access method, a reinstall of the TSP and Wave Driver will be required.
- If there is a requirement to uninstall the Cisco TSP then it is should be done using the instructions found in a file called ciscotsp.txt. This file is created when the TSP is installed, and the default location is ***C:\Program Files\Cisco***
- Verify there is only 1 CiscoTSP configuration under "Control Panel-Phone and Modem Options-Advanced"
- Verify the TSP installed is the same version available for download from the CUCM Application Plug-in page
- Verify devices are NOT associated with any other End or Application Users in the cluster

To uninstall the Wave Driver

- Go to Windows Control Panel
- Double Click on Administrative Tools
- Open Computer Management
- Highlight Device Manager
- Expand Sound, video and game controllers
- Right Click and select uninstall on Cisco Unified Communications Manager TSP Wave Driver

– Repeat this process if there are multiple instances or the Wave Driver showing



Once uninstalled reboot the machine and reinstall the TSP and Wave Driver as per the installation guide found here:

http://www.cisco.com/en/US/products/ps7282/prod_installation_guides_list.html

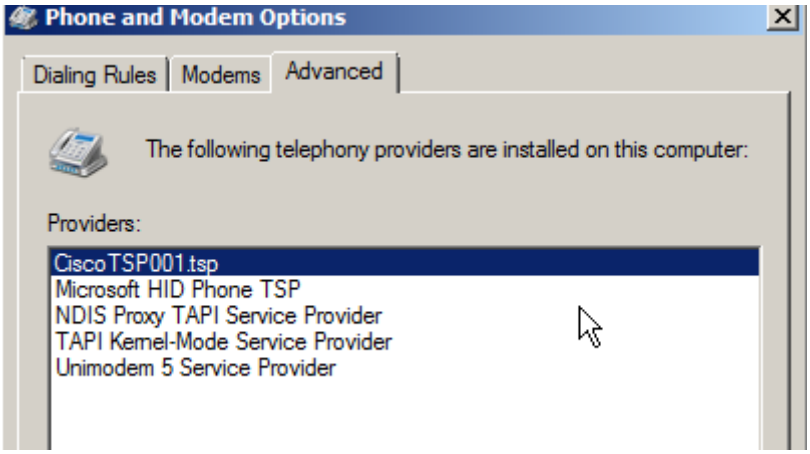
The instructions can be found under Appendix B and Appendix D

It is important that if there is any upgrade to the CUCM, that the CUxAC Server's TSP Installation is also upgraded, if this is not carried out then this could cause unknown call handling issues.

Some CTI Devices are registering, but not all the ones configured in the CUxAC WebAdmin

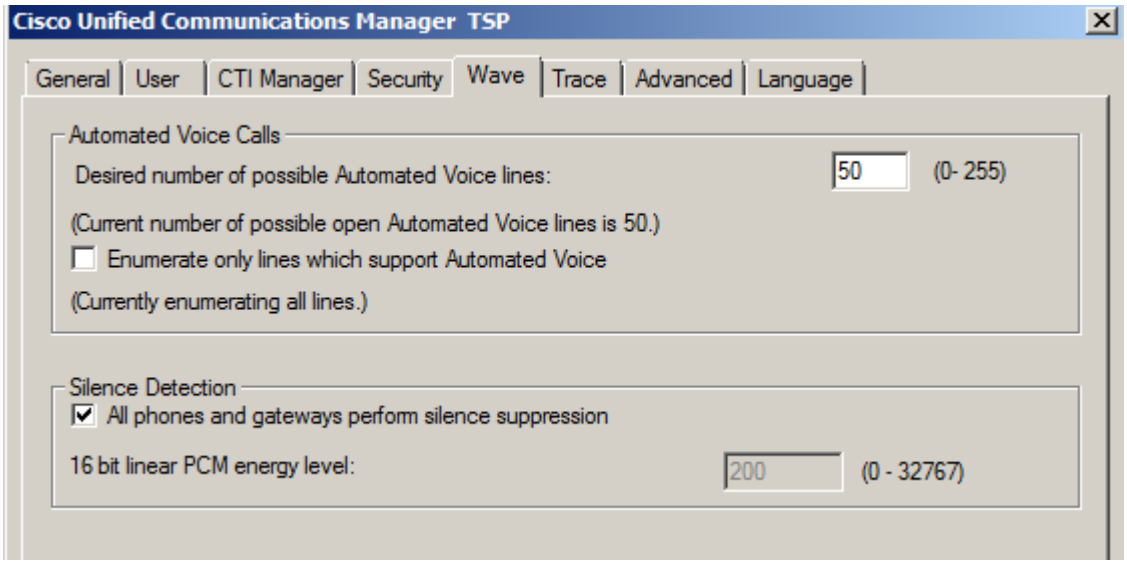
- Navigate to the TSP configuration menu on the CUxAC server:

- Control Panel->Phone and Modem Settings->Advanced->CiscoTSP001.tsp and select configure



- Verify devices are NOT associated with any other End or Application Users in the cluster.
- Select the Wave tab and ensure that the number of automated voice lines is set to 255. If this setting is changed the Wave Driver will have to be uninstalled and reinstalled for the change to take effect. Please see To uninstall the Wave Driver, page 2-3.

Note If using CUCM 8.x, this configuration i.s done automatically by the CUxAC Installation Wizard and the new Cisco Media Driver is used as apposed to the TAPI Wave Driver.



Callers hearing fast busy tone when calling the main reception line

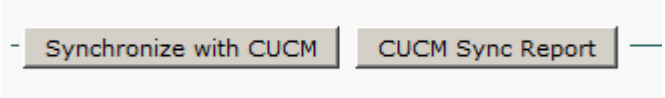
- Ensure that the CTI Route Point associated with this queue is registered in CUCM. If it is registered, the problem is likely between the gateway and the Route Point. Ensure the gateway has the correct Calling Search Space to reach the partitions which is configured against the CTI Route and that the Translation Pattern is correct

- If all CUxAC CTI devices are unregistered refer to "CTI Devices are not registering on CUCM, their status is Unknown or Unregistered" on page 2 - 2
- If some CTI devices are registered and some unregistered refer to "Some CTI Devices are registering, but not all the ones configured in the CUxAC WebAdmin" on page 2 - 4
- In versions prior to 8.6, If only the CTI Route Point for that queue is unregistered refer to SR <CSCtq00285>

CTI Devices not synchronizing to CUCM

Note If you were running a CUxAC Version previous to 8.0.3 and have since upgraded, it is a requirement that you change your End User Account to an Application User Account, not doing this will result in a failure when trying to synchronize the CUxAC Server with the CUCM

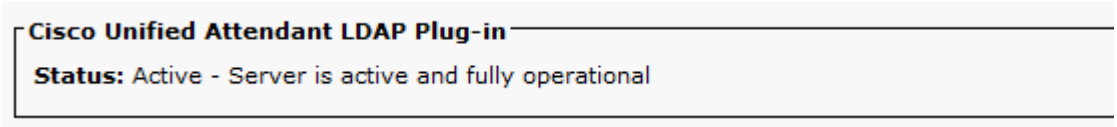
- In the CUxAC WebAdmin navigate to System Configuration > Synchronize with CUCM and select the Synchronize with CUCM button



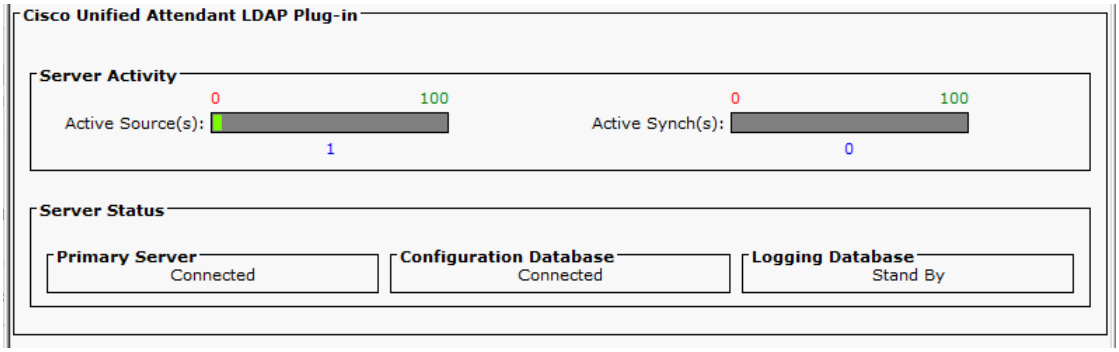
- If the devices fail to synchronize there will be an error code, for example 8500. Reference this code in the CUxAC Configuration and Installation guide as the list is very well detailed and should give an indication of what is going on. This document can be found here http://www.cisco.com/en/US/products/ps7282/prod_installation_guides_list.html

LDAP Server not synchronizing contacts

Step 1 If the procedure outlined in "LDAP not synchronizing contacts" on page 4 - 2 does not resolve the issue, in the CUxAC WebAdmin navigate to Engineering->Service Management and select the information icon for the LDAP Service



Step 2 This will bring up the LDAP Status window displaying the number of active connections and active synchs as well as the connectivity status.



Step 3 If Primary Server connection is displaying as Not Connected:

- Go to Start->Run and type Regedit
- Navigate to HKEY_LOCAL_MACHINE\Software\Arc Solutions\Call Connect\LDAP\Defaults and ensure that the ip address of the LDAP Server is the same as the ip address of the CUxAC Server
- If it is not, Stop the LDAP Service, change the key in the registry to the correct ip address and restart the LDAP Service

Step 4 The LDAP Status window should display all items as Connected at the bottom.

Operators receiving "Invalid Destination" error when attempting to transfer a call

Step 1 Invalid Destination means the TSP is unable to access the number dialed from the Console: either the number was dialed wrong or the phone or CTI Service Queue Port does not have the correct CSS to reach the destination

Step 2 If the number in the directory is correct, in the CUxAC WebAdmin browse to User Settings->General Settings and ensure that the maximum internal extension length is enough to cover all the digits in the number dialed by the operator (including the voicemail prefix if configured). If the number dialed exceeds the configured maximum internal extension length, the prefix will be added to that number.

As an example, if the maximum internal digit length is set to 4 and you have an External Prefix of a 9 configured and the internal number you are trying to dial is 12345, the CUxAC Server will prefix a 9 and try to dial 912345 which will be an invalid destination.

Step 3 If step 2 does not resolve the issue it is most likely a Calling Search Space issue:

- Ensure the Service Queue CTI Ports have the necessary CSS to reach the intended destination:
- With the CUxAC Server shut down, Start->Run, type in "dialer".
- Connect to one of the Service Queue devices
- Dial the number the operator is attempting to transfer calls to
- If the number does not ring, the CSS on the CTI Port needs to be updated to allow sending calls to the destination Partition

Step 4 If the above call is successful then verify if the transfer issue occurs only with external calls by placing a call from an internal extension directly to the CTI Route Point associated with the queue

If Direct Transfers are enabled (see page Direct Transfers - Call Transfer behavior, page 4-7) and the operator is able to transfer the internal call, the issue is with the CSS on the gateway. As CUxAC uses TSP and CTI to move calls, the function of CTI Redirect performed on the call forces it to inherit the CSS of the gateway which does not always allow calls to all phones. Modify the gateway CSS to accommodate this and resolve the problem

Administrator Permissions Issue

Introduction

Cisco Unified Attendant Administrator (Attendant Admin) application uses the local machine default Administrator account for IIS Authentication purposes. Because of security risks many customers remove or disable the default "Administrator" account, and create a different account with local Administrator privileges. But by doing so, customers face licensing & menu display issues on the Attendant Admin application.

This section explains how to configure the Attendant Admin application under a local administrator account other than the default "Administrator" account.

Note - This issue is only present on Windows Server 2003 installations. Windows Server 2008 installations are not dependant on the Administrator account.
- It is assumed that the user has already created a windows user account on local machine and has added this account to the local machine Administrators group.

Steps to configure the Attendant Admin under a local administrator account

This section explains the steps required to configure the Attendant Admin under a local administrator account other than the default Administrator account.

Step 1 Open the "Internet Information Service (IIS) Manager" as shown in Figure 2-1 on page 2-9.

Figure 2-1 Open IIS Manager

Step 2 Now expand the tree menu as shown in the Figure 2-2 on page 2-9 to find the WebAdmin web site. Right click on it and select the Properties option from popup menu.

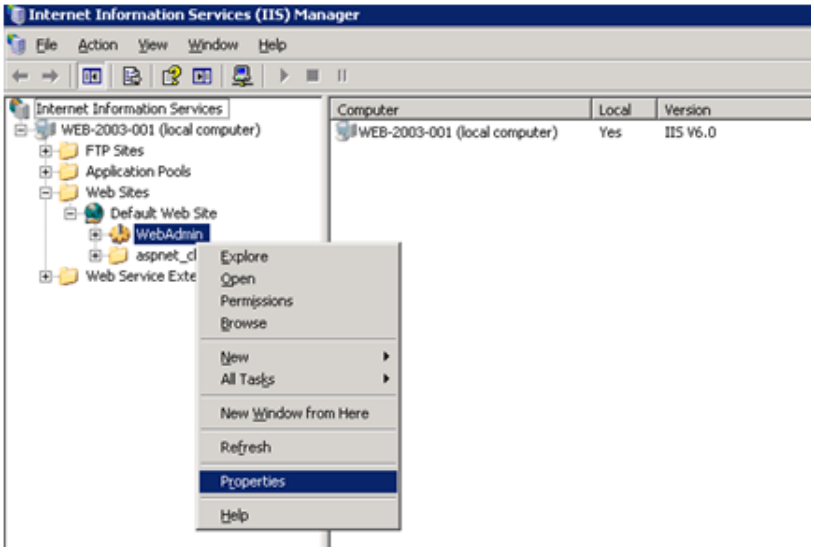


Figure 2-2 Find the WebAdmin web site

Step 3 On "WebAdmin Properties" dialog select the "Directory Security" tab and click Edit button under "Authentication and access control" group box. See Figure 2-3 on page 2-10

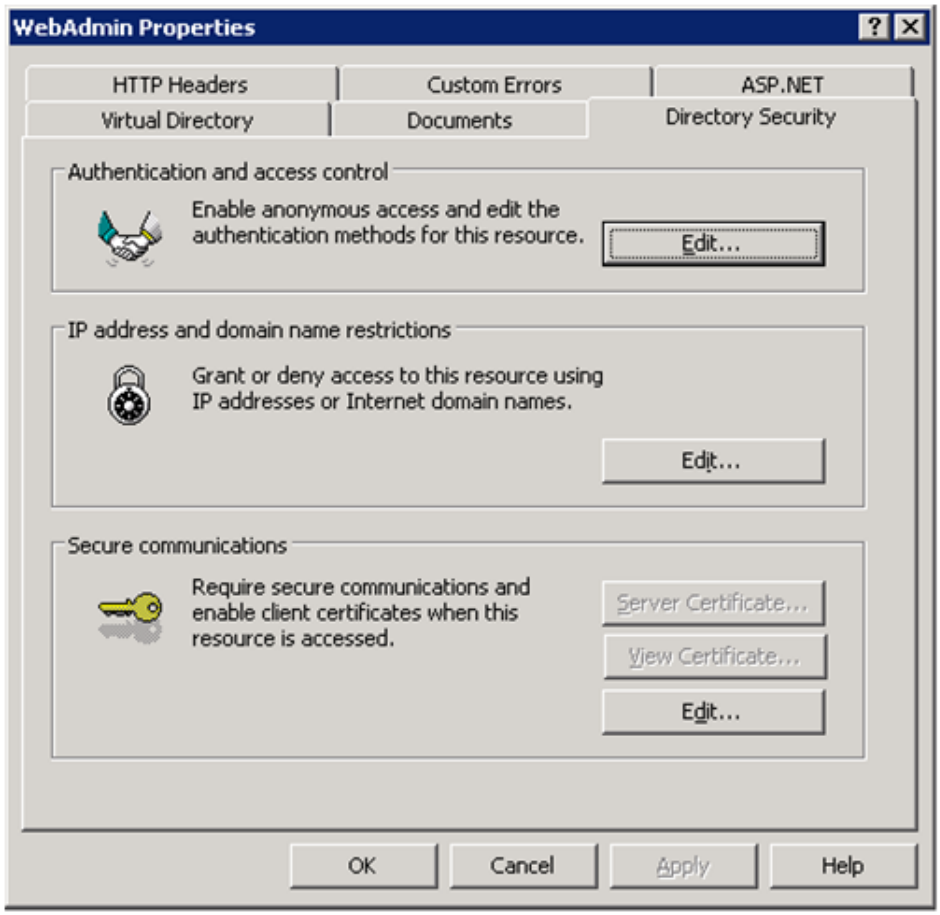


Figure 2-3 WebAdmin Properties Window

Step 4 "Authentication Methods" window shows the user account used for Anonymous access under "Enable anonymous access" group box. In case of default installation, this shows the "Administrator" account. You need to replace it with an alternate local administrator account. SeeFigure 2-4 on page 2-11

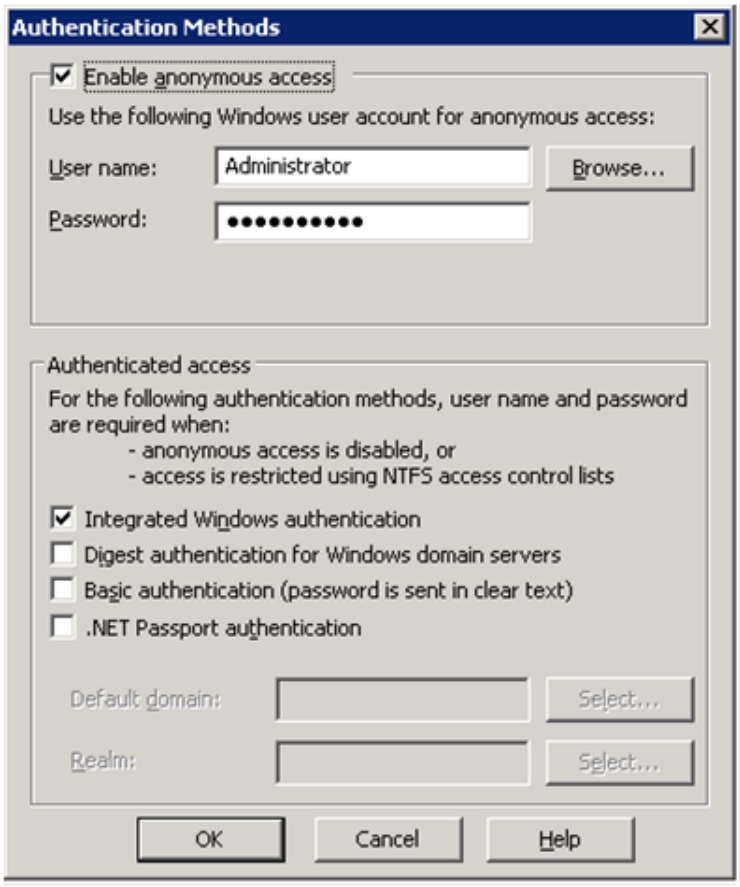


Figure 2-4 WebAdmin Anonymous Access User Name

Step 5 Figure 2-5 on page 2-12 shows that the "Administrator" user is replaced with a local administrator user account called "CUxAC_Admin". Password for this user account also needs to be provided in the Password field. Press the Ok button to apply the change (IIS will ask you to confirm the password).

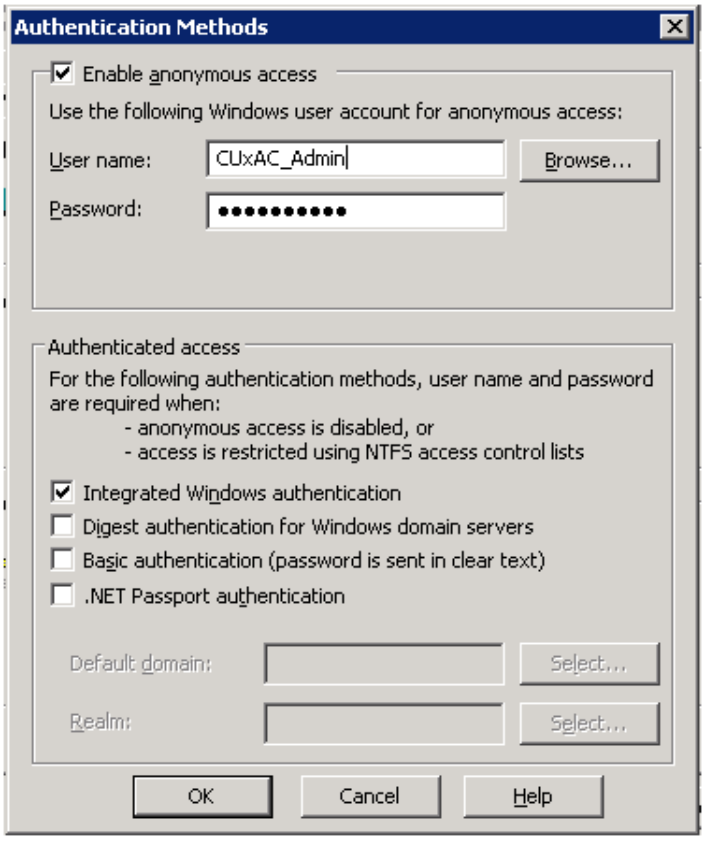


Figure 2-5 Use Local Administrator Account for Anonymous Access

Step 6 Close all open IIS screens by pressing Ok/Apply buttons. Re-start the machine for changes to take effect.

How to change the IP address of a CUxAC Server

The majority of the references of the IP address are contained within the Windows registry of the CUxAC server. It is recommended that you take a backup of your registry before making any of the below changes. Below are the specific registry keys that should be amended. It is recommended that instead changing the old IP address for the new IP address, configuring these settings to use the server machine hostname would remove this from being an issue in the future.

Stop the Cisco Unified Attendant LDAP Plug-in and Cisco Unified Attendant Server Services through Windows Server Manager and then update the following registry keys with the IP address or hostname of the CUxAC server

- HKEY_LOCAL_MACHINE\SOFTWARE\Arc Solutions\Call Connect\Configuration\Defaults
  - Web Server
- HKEY_LOCAL_MACHINE\SOFTWARE\Arc Solutions\Call Connect\Configuration Database
  - Server
- HKey_Local_Machine\SOFTWARE\Arc Solutions\Call Connect\Defaults

  - CTI Server Name
  - Last Connected Server
  - Presence Server Name
  - Server Name
- HKEY_LOCAL_MACHINE\SOFTWARE\Arc Solutions\Call Connect\LDAP Synchronize Server\CT Connection\Primary
  - Server Name
- HKEY_LOCAL_MACHINE\SOFTWARE\Arc Solutions\Call Connect\LDAP Synchronize Server\Defaults
  - Server Name
- HKEY_LOCAL_MACHINE\SOFTWARE\Arc Solutions\Call Connect\Logging Database
  - Server

XML Configuration files

CTI Server

Update the CTI Server configuration file - located in C:\Program Files\Cisco\CTI Server, named 'CTI Server.exe'. This is an XML File and will contain the following key;

<add key="ServerIP" value="xxx"/>

Update this value with the new IP Address/hostname of the CUxAC Server.

Note Please note that the location may vary slightly in different versions of the CUxAC Server

CUPS Server

Update the CTI Server configuration file - located in C:\Program Files\Cisco\CUPS - named ‘Cisco Presence Server Plug-in.exe’. This is an XML File and will contain the following key:

<add key='ServerIP' value='xxx'/>

Update this value with the new IP Address\hostname of the CUxAC Server

Note Please note that the location may vary slightly in different versions of the CUxAC Server

Database Configuration file

Update the Config.DB file located in the **C:\Program Files\Cisco\Utilities** directory.

Open this file using **Windows Notepad** - there will be two lines that display the following information:

ATTCFG,Configuration DB,*xxx.xxx.xxx.xxx*,sa,)hh>(j]n]j)

ATTLOG,Logging DB,*xxx.xxx.xxx.xxx*,sa,)hh>(j]n]j)

Change the IP address above to the new ***IP Address/Hostname***

Clients

Once the server has been changed you will also need to update the Cisco Unified Attendant Console clients with the correct details. Please make sure you log out and close the client before making any changes.

- HKEY_LOCAL_MACHINE\SOFTWARE\Arc Solutions\Call Connect\Defaults
  - Last Connected Server
  - Server Name

CHAPTER 3

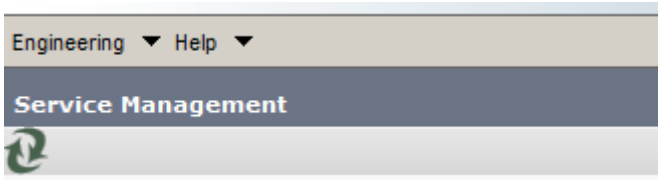
Web Administration

There are several components of a Cisco Unified Attendant Console solution that can fail with the end result of halting or slowing the system. This chapter focuses on the Web Administration and Server issues that can impact on functionality and operability. These are outlined in detail below:

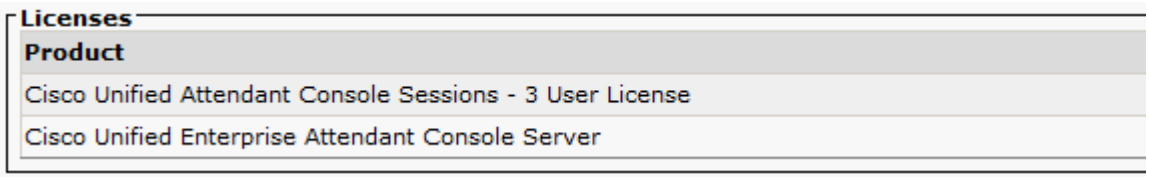
Licensing

Unable to create queues or operators in Web Admin

- If the option is missing from the WebAdmin under User Settings->Queue Configuration or User Settings->Operator Configuration check the license window for correct licenses



- Select Help->License and ensure that the current number of operators is less than the licensed amount



- Add more operator licenses to allow for the creation of more operator usernames and queues.

Unable to activate LAC on the www.cisco.com/go/ac website

- No more activations
  - This message occurs when the LAC has already been activated. Ensure that the correct LAC was entered and that it is the original LAC shipped with the software.
  - If transferring the Server installation to new hardware the license will become invalid and the server will have to be relicensed. The LAC can be refreshed, for this contact Cisco TAC
- Invalid license code

  - If the LAC was typed in properly and this error is received, ensure that the correct product is being activated, as a CUBAC LAC will not activate if CUEAC Software was selected on the Website
- A license file is delivered successfully, however only the Operator Licenses appear in the WebAdmin License screen
  - This indicates that a LAC has already been activated for a particular Server. The Website is able to recognize this based on the registry code entered. If you are unable to register your server, contact Cisco TAC

Accessing Web Admin

Unable to log into WebAdmin Page with error message "DB Error"

- Check Windows Services and ensure that Cisco Unified Attendant Console Server service is started. If it is stopped, start it and ensure it's set to start Automatically
- If the Service is started check the following log file: C:\Program Files\Cisco\Logging\SRV\Log\icdinit.log. This file logs each server start and will contain error messages as to why the CUxAC server cannot start.
- If the error messages are "Unable connect to database ATTCFG" and "Unable to connect to database ATTLOG" Ensure the Microsoft SQL Server service is started and set to Automatically start.
- The problem is generally that SQL is not allowing the CUxAC Service to log onto the databases. Using Microsoft SQL Server Studio Management ensure that BUILTIN\ADMINISTRATORS has SystemAdmin permissions assigned as well as the "sa" username in SQL and that the account is not locked out.

CHAPTER 4

Attendant Console and Client Software

This chapter focuses on the Attendant Console and Client Software issues that can impact on functionality and operability. These are outlined in detail below:

Attendant Console and Client Software.

Directory Issues

Directory will not display and Console shows "Database not connected" message

On the Attendant Console PC:

- Verify that the Windows User has Full Control access to the following registry key and it's child objects: HKEY_LOCAL_MACHINE\Software\Arc Solutions (See, the section "Client preferences do not save / are not retained" section on page 4-4 which shows how the permissions can be found and changed). (If version is older than 8.0.3 verify HKEY_LOCAL_MACHINE\Software\Borland as well)
- Verify that the CUEAC Server can be pinged from the command line by IP Address and Hostname
- If it cannot be reached via hostname, have this added to DNS or to the host file on the machine.

On the CUEAC Server:

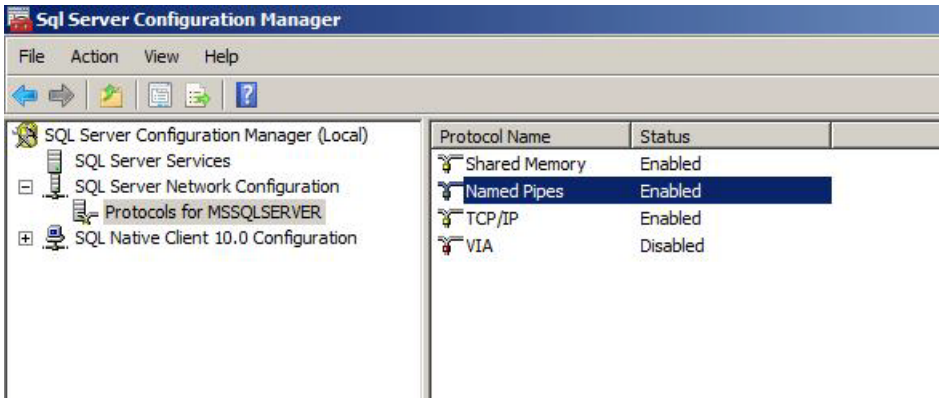
- Ensure that the contact database is populated:
  - Open a synchronization log file in C:\Program Files\Cisco\Logging\LDAP\Log\SSLog_xxxx.txt
  - Check that contacts have been inserted or updated:

```
7/1/2011 6:56:41.317 [Synchronization Start AT:7/1/2011 6:56:41.317] "[MUsage: MU:9516,MPU:9520,VMU:5268,VMPU:5288,PPU:34,NPPU:8]"  EXS000001

7/1/2011 6:56:41.723 CTH100001    INTNL   John    Smith   1234    NoData  Updated  Success  EXS000001

7/1/2011 6:56:42.426 CTH100005    INTNL   Jane    Doe     5555    NoData  Inserted Success  EXS000001
```

- As long as these lines show in the logs, there are contacts in the database
  - Start SQL Configuration Manager utility
  - Navigate to Network Configuration - Enable TCP/IP and Named Pipes connections



  - If you have to enable this then you will need to restart the SQL.

LDAP not synchronizing contacts

LDAP Synchronization is scheduled to run, but no contacts are synchronized

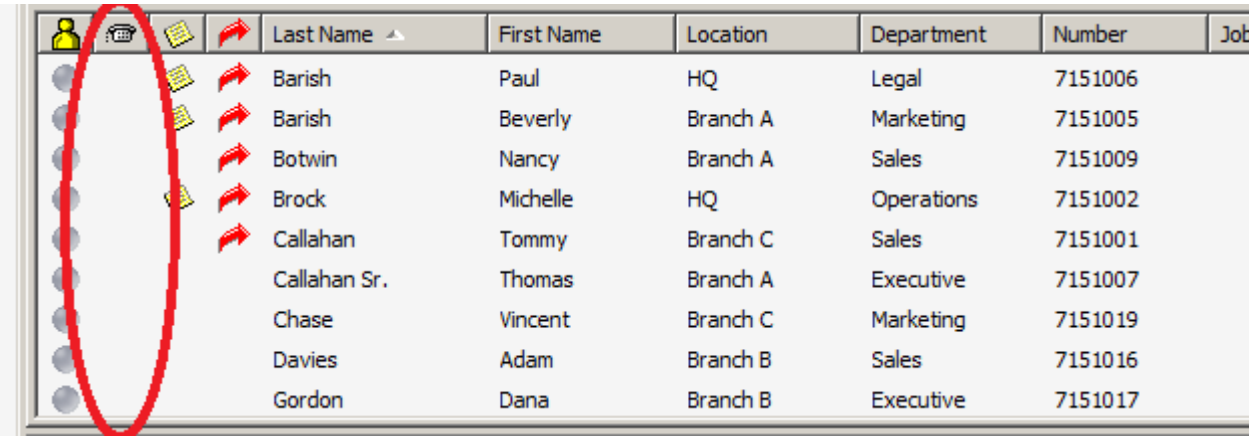
- Identify that synch attempts to run, but does not import anything:
  - Open a synchronization log file in C:\Program Files\Cisco\Logging\LDAP\Log\SSLog_xxxx.txt
  - It should display the following lines:

```
7/1/2011 6:56:41.317    [Synchronization Start AT:7/1/2011 6:56:41.317] "[MUsage:
MU:9516,MPU:9520,VMU:5268,VMPU:5288,PPU:34,NPPU:8]"  EXS000001
7/1/2011 6:56:41.512    [Synchronization End  AT:7/1/2011 6:56:41.512] "[MUsage:
MU:13536,MPU:14904,VMU:8352,VMPU:10228,PPU:36,NPPU:10]"  EXS000001
```

  - In the WebAdmin, navigate to CUCM Synchronization->LDAP Field Mappings
  - Ensure that at least the fields FIRST_NAME, LAST_NAME, and EXTENSION are selected
  - Navigate to CUCM Synchronization->LDAP Rules
  - Ensure that only one rule is configured, select that rule
  - Delete all filters configured for the rule
  - Navigate to Engineering->Services and restart the LDAP Service

Cannot see the phone status of contacts

Directory is displaying the column for phone status, but there is nothing there



Last Name	First Name	Location	Department	Number	Job
Barish	Paul	HQ	Legal	7151006	
Barish	Beverly	Branch A	Marketing	7151005	
Botwin	Nancy	Branch A	Sales	7151009	
Brock	Michelle	HQ	Operations	7151002	
Callahan	Tommy	Branch C	Sales	7151001	
Callahan Sr.	Thomas	Branch A	Executive	7151007	
Chase	Vincent	Branch C	Marketing	7151019	
Davies	Adam	Branch B	Sales	7151016	
Gordon	Dana	Branch B	Executive	7151017	

- BLF Plug-in on the CUxAC Server is not running
  - From the WebAdmin, browse to Engineering->Service Management and start the BLF Plug-in
- CUxAC client is unable to reach the BLF Plug-in service on the CUxAC server
  - Ensure the BLF Plug-in is running
  - Ping the CUxAC Server by hostname and ip address, it should be reachable by ip address, and hostname
  - If is is not reachable by hostname then, add the ip address and hostname in the windows hosts file

Phone status of contact shows out of service

An extension displays out-of-service status regardless of the actual status of the phone

Last Name	First Name	Location	Department	Number	Job T
Barish	Paul	HQ	Legal	7151006	
Barish	Beverly	Branch A	Marketing	7151005	
Botwin	Nancy	Branch A	Sales	7151009	
Brock	Michelle	HQ	Operations	7151002	
Callahan	Tommy	Branch C	Sales	7151001	
Callahan Sr.	Thomas	Branch A	Executive	7151007	
Chase	Vincent	Branch C	Marketing	7151019	
Davies	Adam	Branch B	Sales	7151016	
Gordon	Dana	Branch B	Executive	7151017	

- Verify that the device in question is registered in Call Manager.
- The device might just be taking some time to display status: press F2 to bring up the status window which will send the request right away

- If the F2 window also displays out of service or no phone status at all close this window and press F12 to bring up the contact details
- In the contact details window click on the Numbers tab:
  - ensure that Use Device Name is checked (enabled)
  - ensure the Device Name is that of the device that should be monitored
  - if the device name is incorrect manually add the correct device name or if extension mobility is being used, remove any device name present
  - close the contact details window and refresh the BLF status (by pressing F2 on the contact or clearing the search and searching for that contact again)
  - Ensure that the Device Number is an exact match to the CUCM, any mismatch (including Spaces) will stop BLF from working,
  - If entries are Extension Mobility Users, ensure that allow control of Device from CTI is selected against the End User, the Device Profile and the logged out phone device. If you need to enable this option, the user will need to log out and back into the phone in order to start getting BLF information.

Client preferences do not save / are not retained

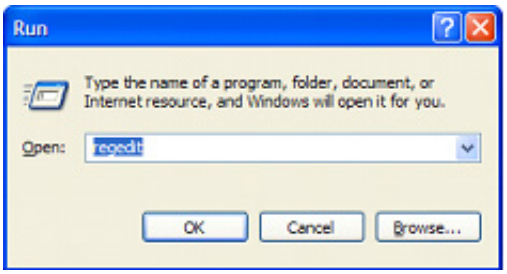
Operator configures preferences on their local machine, however when the PC is rebooted these settings are not retained

To resolve this issue, follow the steps below to grant full access to the Arc Connect registry key(s)

Step 1 On the client machine (i.e. the Attendant Console client PC), log in to the machine as **Local Administrator**

Step 2 Ensure that all Cisco applications are closed.

Step 3 Select **Start>Run**, and type in ***Regedit*** in the **Run** Box

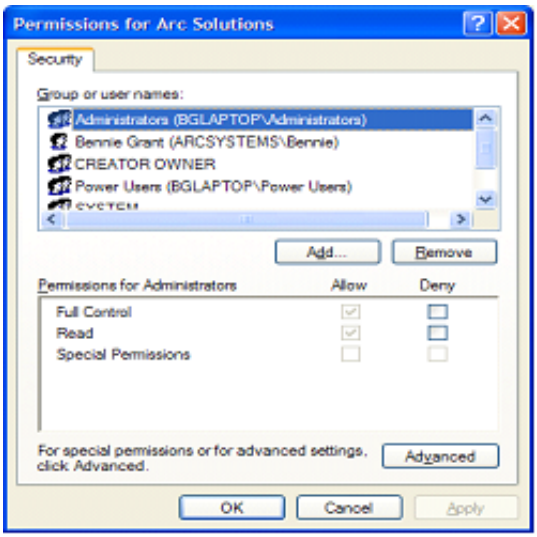


Step 4 The Windows Registry Editor will now open.

Step 5 Browse to **HKLM>Software>Arc Solutions**.

Step 6 Right-click on the **Arc Solutions** registry key, and select **Permissions**

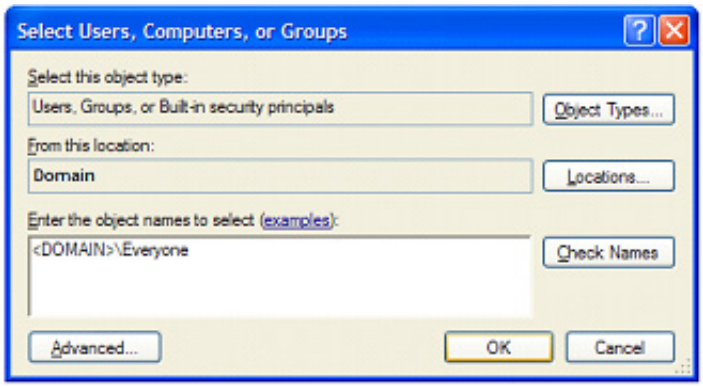
Step 7 The following window will now open:



Step 8 This window allows you to amend the security settings for the Arc Solutions registry key. In order for the Arc Applications to function correctly, all users need to have **Full Control** of this registry key.

Step 9 Press **Add**

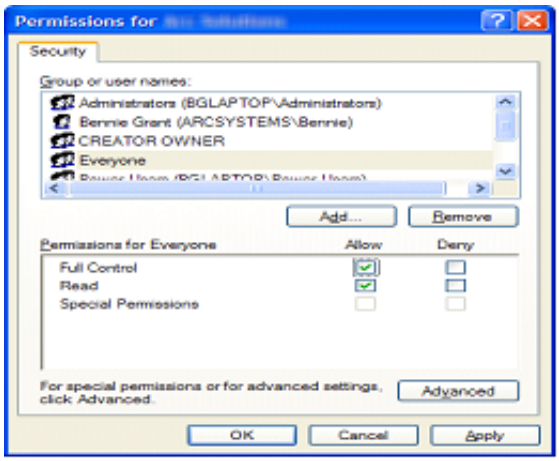
Step 10 Under the **Enter the object name to select box**, type ***<DOMAIN NAME>\Everyone***.



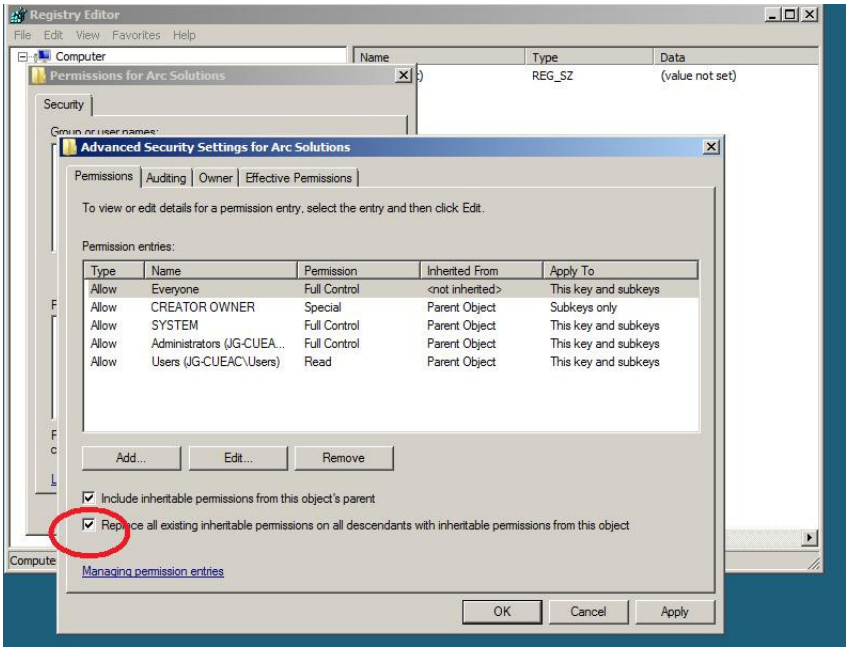
Step 11 The Domain name should be the domain that a standard Desktop user logs in to.

Step 12 Press **OK** to add **Everyone** to the security page. You will now see **Everyone** listed within the window.

Step 13 Select the **Everyone** account, and then select **Allow Full Control** from the permissions section, to grant full access to this registry key



Step 14 Click on **Advanced** and then select **Replace all existing inheritable permissions on all descendants with in heritable permissions from this object**.



Step 15 Now press **Apply**, then **OK**.

Step 16 The access rights have now been granted.

It is now possible to log the PC in as a standard desktop user - the security rights will now allow access to the relevant Registry keys, and the Cisco Unified Attendant Console applications will now save settings

Remove Call Park Window

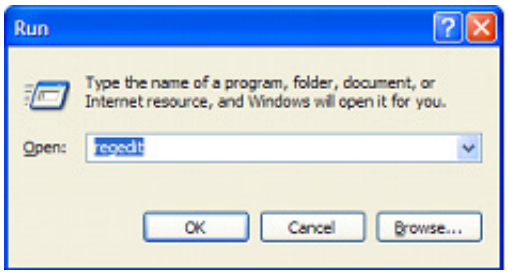
If customer is not using the Call Park functionality with CUxAC, they are able to remove this window from the screen

To achieve this, follow the steps below to hide the Call Park window

Step 1 On the client machine (i.e. the Attendant Console client PC), log in to the machine as **Local Administrator**

Step 2 Ensure that all Cisco applications are closed

Step 3 Select **Start>Run**, and type in ***Regedit*** in the **Run** Box



Step 4 The Windows Registry Editor will now open.

Step 5 Browse to **HKLM>Software>Arc Solutions\Call Connect\Operator\Defaults**

Step 6 Locate the registry key named **Allow Call Parking**

Step 7 Double click on this registry key, and change the value to **No**. Press **OK**

Step 8 Close the registry editor, and reopen the CUxAC application

Step 9 The call park window has now been removed

Direct Transfers - Call Transfer behavior

Direct Transfers can be enabled on the Attendant Console PC, this should be considered if you want to achieve the following:

- When the operator performs a blind transfer, the recipient of the transfer shows the caller ID of a CTI Port (the CUxAC "Service" device), while the call is ringing on the IP Phone, however the desired behavior is that the recipients see's the CLI of the caller

OR

- When a call has been transferred, the caller hears Music-on-Hold while the call is ringing on the other IP Phone, the desired behavior is for the caller to hear "ring tone"

When the operator performs a blind transfer via the CUxAC application, the original caller is moved to a CTI Port (the "Service" device). This CTI Port then answers the call, and makes the transfer to the target extension. It is this call flow that enables the "transfer recall" functionality of CUxAC, however has the effects that are mentioned above

It is possible to disable this functionality - when doing so, Transfer Recall functionality will be lost, however if the IP Phones users have voicemail this is typically acceptable, as calls will forward to the IP Phones users voicemail box, as opposed to recalling back to the operator

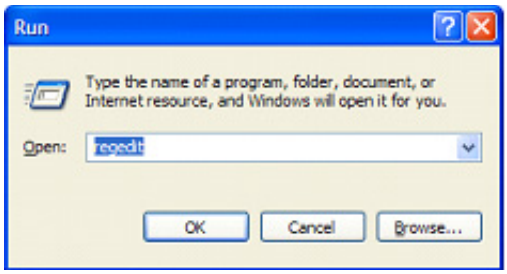
Performing this action is known as enabling "direct transfers"

To enable direct transfers:

Step 1 On the client machine (i.e. the Attendant Console client PC), log in to the machine as **Local Administrator**

Step 2 Ensure that all Cisco applications are closed

Step 3 Select **Start>Run**, and type in ***Regedit*** in the **Run** Box



Step 4 The Windows Registry Editor will now open.

Step 5 Browse to **HKLM>Software>Arc Solutions\Call Connect\Operator\Defaults**

Step 6 Locate the registry key named Direct Transfers

Step 7 Double click on this registry key, and change the value the appropriate option listed below. NOTE: typical option would be to set this to All. Press OK

Step 8 Close the registry editor, and reopen the CUxAC application

Step 9 Direct Transfers is now enabled

The following configurations are available:

- **All** - Enabled for all Transfer types.
- **Off** - Direct Transfers are disabled and Service Queue will be used (Default operation)
- **Internal** - This will only enable Direct Transfers to internal numbers. Transfers to external numbers will still go via the Service Queue.*
- **External** - This will only enable Direct Transfers to external numbers. Transfers to internal numbers will still go via the Service Queue.*

* Internal and External numbers are determined by the configuration in the Web Admin under User Configuration - general Properties.

Technical Considerations for enabling Direct Transfers

When the CUxAC application performs a standard blind transfer, it is using a specific CTI function -

Redirect (SLDST_REDIRECT_RESET_ORIG_CALLED). This redirects the call from the Attendant Console handset to the Service Queue (CTI Port). This in turn will use the first line to hold the call and the second to make the call out - in the same manner as a consult transfer. When the target recipient picks up the two calls are automatically joined together.

When direct transfers is enabled, the blind transfer function still utilizes this same CTI function, however in this scenario the call passes the Service Queue and redirects the call instantly to the physical handset. Therefore, the caller will hear ringing as the call is no longer being placed on hold on a CTI Port. The call will also display the original Caller-ID rather than the Caller ID of the CTI Port.

As the CTI redirect function works slightly differently to a standard blind transfer that would be invoked via a physical handset, the call is never placed on hold. Due to this, the redirect of the call will therefore be using the Calling Search Space of the originating device - in the case of an external call that is inbound to CUxAC, this will be the Calling Search Space of the PSTN gateway.

If the gateway has a restricted Calling Search Space that only allows calls to internal extension, and a call into the attendant console is desired to be transferred to an external number - in this scenario it would fail, and a message of Invalid Destination will be displayed on the CUxAC application. This is because the originating Calling Search Space does not allow the call to be sent to an external location.

Tip **Recommendations**:
If Direct Transfer is enabled, a pre-requisite is that the gateway is configured with the relevant CSS to enable calls to be redirected back out to an external number.

However not all CUCM customers are willing to make changes to their CSS or Gateway configuration.

As such, the following statement applies when using direct transfers:
If you wish to enable Direct Transfers you must accept that the gateway's CSS MUST be configured to allow calls in to be redirected back to an external location