Cisco Unified 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 Attendant Console - Troubleshooting Guide

CONTENTS

Preface

This document is intended for anyone involved in the planning, implementation and system administration of Cisco Unified Attendant Console. It assumes basic knowledge of the Cisco Unified Attendant Console system and an understanding of Cisco Unified Call Manager, and it should be used in conjunction with the *Cisco Unified Attendant Console Installation and Administration Guide*.

Cisco Unified Attendant Console is available in the following editions:

Edition	Number of Attendants (operators)	Number of Queues	Number of Contacts
Department Edition	2 per instance (5 instances per server)	1 per instance (5 instances per server)	150 per instance (5 instances per server)
Business Edition	12	3	500
Enterprise Edition	40	50	100K
Premium Edition	50	100	100K

All Editions have a client/server architecture.

Cisco Unified Attendant Console User Accounts

Cisco Unified Attendant Console uses the Cisco TSP to communicate between the Cisco Unified Attendant Console Server and the Cisco Unified Communication Manager 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 Cisco Unified Attendant Console versions up to 8.0.3 require an End User to be configured. If the Cisco Unified Communication Manager 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 synchronized with AD, and therefore there is no risk of the User being deleted this way, and running the risk of the Cisco Unified Attendant Console 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 AXL API Access

- Standard CTI Allow Calling Number Modification
- 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 Allow Reception of SRTP Key Material
- Standard CTI Enabled

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

Cisco Unified Communications Manager System Devices

Cisco Unified Communications Manager uses the following system devices:

- Queue DDI (Direct Dial In)—the number dialed to route calls into a queue. Each DDI is configured on Cisco Unified Communications Manager as a CTI Route Point, and any call intended for this queue must be directed to this port, either directly or through a translation pattern.
- CT Gateway Devices—CTI Ports that are created by the Admin application when synchronized with Cisco Unified Communications Manager; they queue calls awaiting distribution to Cisco Unified Attendant Console.
- Service Queues—CTI Ports that are used to manage calls after they leave the operator's handset, for example when transferring or holding calls.
- Park devices—CTI Ports that are used when an attendant parks a call. The attendant can either select the preferred Park port or allow the system to select the port for them. A parked call can then be picked up by anyone on the system by dialling the Park port number.

  The Cisco Unified Attendant Console Call Park functionality is additional to the standard Cisco Unified Communications Manager call park and directed call park functions. Operators can see what Park devices are available and choose whether to use a specific device or allow the system to select a park device for them. As these Park Devices are exclusive to the console attendants they are situated on the Cisco Unified Attendant Console server and require an additional range of DNs.

System Sizing Tool

To help you plan your system you can use the Unified Communications Sizing Tool (UCST) at http://tools.cisco.com/cucst.

Obtaining Documentation and Submitting a Service Request

For information on:

- Obtaining documentation
- Obtaining support
- Submitting service requests

- Providing documentation feedback
- Security guidelines
- Recommended aliases
- Gathering additional information
- A list of all new and revised Cisco technical documentation

see the monthly *What's New in Cisco Product Documentation* at:
http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to *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 you can use to troubleshooting the system.

To configure logging, run Cisco Unified Attendant Console Web Admin and choose **Engineering > Logging Management**.

Cisco Unified Attendant Console Logs

Cisco Unified Attendant Console logs are located in C:\Program Files\Cisco\Logging\OPR\ Log.

To toggle logging on and off, in the Attendant Console choose **Help > About,** and then press **Ctrl-Alt-T**. The word *Logging* is displayed in the title bar when logging is activated.

You can use the following registry keys on the Attendant's PC to control logging:

Location	Use
HKEY_LOCAL_MACHINE\Software\Arc Solutions\Call Connect\Operator\Logging\Database Logging	**Yes** enables Contact Directory and search logging, **No** disables it.
HKEY_LOCAL_MACHINE\Software\Arc Solutions\Call Connect\Operator\Logging\Full Logging	**Yes** enables full logging. **No** enables default logging.
HKEY_LOCAL_MACHINE\Software\Arc Solutions\Call Connect\Operator\Logging\General Log File	The logging files base name. Default is **OPRlog.txt**.
HKEY_LOCAL_MACHINE\Software\Arc Solutions\Call Connect\Operator\Logging\General Log Location	The path to the log files folder. By default, this is C:\Program Files\Cisco\Logging.
HKEY_LOCAL_MACHINE\Software\Arc Solutions\Call Connect\Operator\Logging\Host CTI Service Logging	**Yes** enables phone status icons logging. **No** disables it.
HKEY_LOCAL_MACHINE\Software\Arc Solutions\Call Connect\Operator\Logging\Logging On	**Yes** turns logging on. **No** turns logging off.
HKEY_LOCAL_MACHINE\Software\Arc Solutions\Call Connect\Operator\Logging\Maximum Log Files	The maximum number of log files to save before overwriting the oldest.
HKEY_LOCAL_MACHINE\Software\Arc Solutions\Call Connect\Operator\Logging\Maximum Log Lines	Number of lines written in each log file

Cisco Unified Attendant Server Logs

Cisco Unified Attendant Console server logs every event that it generates. The following processes are logged:

• Main Process - manages the router, database and comms, for example user activity (login, logout).

• Router Process - logs all the call routing information.

• CTI Process - logs the TAPI Interface

• Database Process - logs all activity on both databases.

• Communication Process - logs the TCP/IP communication between the clients and the server.

By default, the Main and Router processes are selected for logging; these will provide sufficient information to solve most problems. To keep the log file to a manageable size, log the fewest processes possible. You should only need to amend these settings if requested as part os a support case investigation.

Each component saves its logs in a different sub-folder of C:\Program Files\Cisco\Attendant Server\Log.

Cisco Unified Attendant LDAP Plug-in

The default logging level is *Detailed*. If any of the following occur, you may have to change the level to *Full*:

- Discrepancies between the Cisco Unified Attendant Console directory and the Cisco Unified Communication Manager directory,
- Problems when synchronizing data online to the Cisco Unified Attendant Console Server
- Communication problems

You may also need to increase the number of lines and files depending the directory size and the length of time over which you want to record data. You can have up to 100 files, each containing up to 100000 lines.

Cisco Unified Attendant CUPS Plug-in

If any of the following occur, you should set the logging level to Full:

- Memory leaks,
- Communication problems
- sipXTapi (open source third party component) problems

This will provide .Net stack level exception details.

Make sure that in *C:\Program Files\Cisco\CUPS\CUPS Presence Server Plug-in.exe.config*, the key to enable the sipXtapi logging is set to true. For example:

(<add key="sipXtapiLogging" value="true"/ >)

You may also need to increase the number of lines and files depending the directory size and the length of time over which you want to record data. You can have up to 100 files, each containing up to 100000 lines.

Cisco Unified Attendant BLF Plug-in

By default, the logging level is set to Full.

You may also need to increase the number of lines and files depending the directory size and the length of time over which you want to record data. You can have up to 100 files, each containing up to 100000 lines.

Web Admin

The default logging level is usually sufficient to troubleshoot most common problems. You can set logging to detailed by changing the registry keys listed below.

Note You should make a backup of *HKEY_LOCAL_MACHINE\SOFTWARE\Arc Solutions\Call Connect\Web Admin\Runtime Logging* registry key before changing any registry settings mentioned below. After collecting logs with detailed logging settings, you should restore the default logging settings from the backed up registry; this will prevent huge logs from being generated.

Key	Setting
HKEY_LOCAL_MACHINE\SOFTWARE\Arc Solutions\Call Connect\Web Admin\Runtime Logging\API Clients Level	262 decimal (106 hex)
HKEY_LOCAL_MACHINE\SOFTWARE\Arc Solutions\Call Connect\Web Admin\Runtime Logging\Clients Level	7 decimal/hex
HKEY_LOCAL_MACHINE\SOFTWARE\Arc Solutions\Call Connect\Web Admin\Runtime Logging\Data Objects Process	YES
HKEY_LOCAL_MACHINE\SOFTWARE\Arc Solutions\Call Connect\Web Admin\Runtime Logging\Data Objects Level	7 decimal/hex
HKEY_LOCAL_MACHINE\SOFTWARE\Arc Solutions\Call Connect\Web Admin\Runtime Logging\API External APIs Level	519 decimal (207 hex)
HKEY_LOCAL_MACHINE\SOFTWARE\Arc Solutions\Call Connect\Web Admin\Runtime Logging\ Internal Objects Level	7 decimal/hex
HKEY_LOCAL_MACHINE\SOFTWARE\Arc Solutions\Call Connect\Web Admin\Runtime Logging\ Internal Objects Process	YES
HKEY_LOCAL_MACHINE\SOFTWARE\Arc Solutions\Call Connect\Web Admin\Runtime Logging\Management Level	263 decimal (107 hex)
HKEY_LOCAL_MACHINE\SOFTWARE\Arc Solutions\Call Connect\Web Admin\Runtime Logging\ Request Response Level	7 decimal/hex
HKEY_LOCAL_MACHINE\SOFTWARE\Arc Solutions\Call Connect\Web Admin\Runtime Logging\ System Level	263 decimal (107 hex)

Cisco TSP Logging

To perform Cisco TSP logging, do the following:

Step 1 If you have not already done so, create the folder, C:\Program Files\Cisco\Logging\TSP.

Step 2 In Control Panel, select **Phone and Modem**.

Step 3 Click the **Advanced** tab, select **CiscoTSP001.tsp**, and then click **Configure**.

Step 4 In the Cisco Unified Communication Manager TSP dialog box, click the **Trace** tab and then change the Directory to C:\Program Files\Cisco\Logging\TSP.

Step 5 Optionally, select **CTI Trace** and **TSPI Trace**, and select **Detailed**.

Step 6 Click OK.

CHAPTER 2

Installation and Connectivity

This chapter describes problems that can arise during installation. It also covers problems cause by the connection between the Cisco Unified Attendant Console and external resources, such as the Unified Communications Manager or LDAP sources.

Unable to Connect to Cisco Unified Communication Manager

If you are unable to connect to the Cisco Unified Communication Manager, firstly run Cisco Unified Attendant Console Web Admin, choose **Engineering > CUCM Connection**, and then click **Test Connection**.

If this does not reveal the cause of the problem, do the following:

Step 1 Ensure the Application User username and password are correct by logging into the Cisco Unified Communication Manager with the same credentials.

Step 2 Ensure that the user is added to the Standard Cisco Unified Communication Manager Super Users Group.

Step 3 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 * These are relevant only if you are using phone models 69xx, 7931, 7965, 89xx and 99xx on Cisco Unified Communication Manager 7.1.2 or greater.

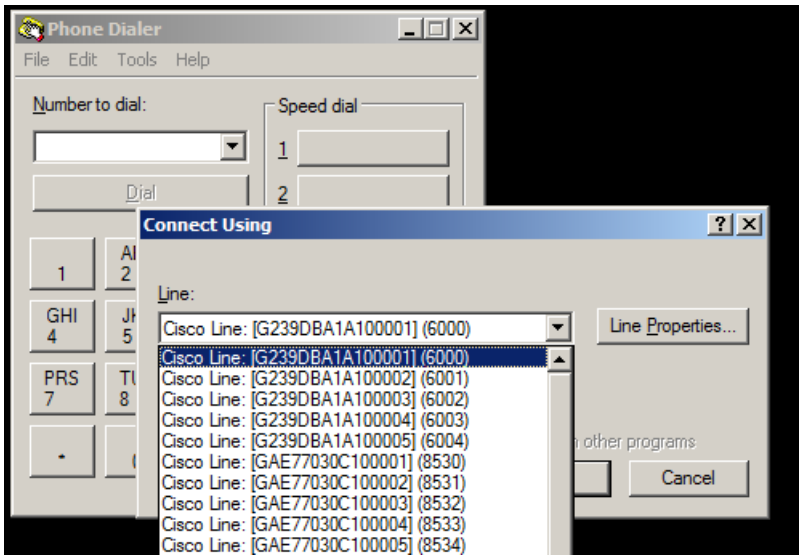
Step 4 Ensure that the AXL Service is activated on the Cisco Unified Communication Manager.

CTI Device Problems

If CTI devices are not registering on Cisco Unified Communication Manager, or their status is Unknown or Unregistered, do the following:

Step 1 On the Cisco Unified Attendant Console server, click the **Start** button, and then, on the **Start** menu, click **Run**, and then type **dialer**.

Step 2 In the Phone Dialer, choose **Tools > Connect Using** and check that the Synchronized CTI devices are listed



- If the devices are in the list, start the Cisco Unified Attendant Console Web Admin, choose **Engineering > Service Management**, and ensure that the Cisco Unified Attendant Server service is running.
- If the devices aren't in the list, the TSP is not working correctly. Ensure that the TSP Configuration is correct and then reboot the machine to re-establish the TAPI connection.

Installing the TSP or Wave Driver via an RDP connection can cause the TSP to malfunction. For more information on this, see the Install and Upgrade Guides at http://www.cisco.com/en/US/products/ps7282/prod_installation_guides_list.html.

If the TSP and Wave Driver were installed via a session-based access method, you will have to reinstall them. If you need to uninstall the Cisco TSP follow the instructions in the *C:\Program Files\Ciscociscotsp.txt* file, which is created when the TSP is installed.

Other check you can perform:

Step 1 In Control Panel, select **Phone and Modem**.

Step 2 Click the **Advanced** tab, and verify there is only one CiscoTSP configuration.

- Verify that the TSP installed is the latest version available for download from the Cisco Unified Communication Manager Application Plug-in page.
- Verify that CTI devices are *not* associated with any other End or Application Users in the cluster.

Uninstalling the Wave Driver

To uninstall the wave driver, do the following:

Step 1 Click the **Start** button. In the search box, type **Device Manager**, and then, in the list of results, click **Device Manager**.

Step 2 Expand **Sound, video and game controllers**.

Step 3 Right-click **Cisco Unified Communications Manager TSP Wave Driver**, and then click **Uninstall**.

Step 4 Repeat this process for each instance of the Wave Driver installed.

Step 5 Reboot the machine and reinstall the TSP and Wave Driver as described in the installation guide at http://www.cisco.com/en/US/products/ps7282/prod_installation_guides_list.html.

Caution If the Cisco Unified Communication Manager is upgraded, you must also upgrade the Cisco Unified Attendant Console Server's TSP Installation.

Some CTI Devices Not Registering

If some of the CTI devices configured in the Cisco Unified Attendant Console Web Admin do not register, do the following:

Step 1 In Control Panel, select **Phone and Modem**.

Step 2 Click the **Advanced** tab, select **CiscoTSP001.tsp**, and then click **Configure**.

- Verify devices are *not* associated with any other End User or Application User in the cluster.
- Select the **Wave** tab and ensure that the **Desired number of possible Automated Voice lines** is set to 255. If you change this setting, you must also uninstall and then re-install the Wave Driver (as described in Uninstalling the Wave Driver, page 2-3) for the change to take effect.

Note If you are using Cisco Unified Communication Manager 8.x, this is done automatically by the Cisco Unified Attendant Console Installation Wizard, and the new Cisco Media Driver is used instead of the TAPI Wave Driver.

Callers To Main Reception Hear Fast Busy Tone

If callers to the main reception are hearing the fast busy tone, do the following:

- Ensure that the CTI Route Point associated with this queue is registered in Cisco Unified Communication Manager. If it is registered, the problem is probably between the gateway and the Route Point. Ensure the gateway has the correct Calling Search Space to reach the partition that is configured against the CTI Route, and that the Translation Pattern is correct.
- If all Cisco Unified Attendant Console CTI devices are unregistered refer to "CTI Device Problems" on page 2 - 2.
- If some CTI devices are registered and some unregistered refer to "Some CTI Devices Not Registering" on page 2 - 3.
- 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

Note If you have upgraded from a Cisco Unified Attendant Console Version earlier than 8.0.3, you must change your End User Account to an Application User Account. If you do not do this, attempts to synchronize the Cisco Unified Attendant Console Server with the Cisco Unified Communication Manager will fail.

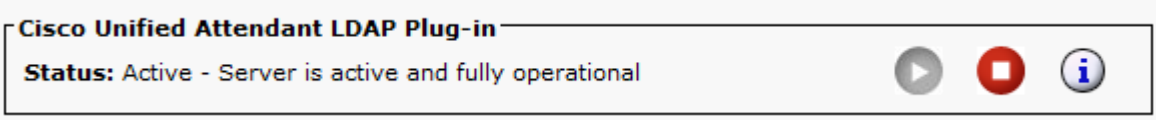
If CTI Devices are not synchronizing to Cisco Unified Communication Manager, do the following:

Step 1 In Cisco Unified Attendant Console Web Admin, choose **System Configuration > Synchronize with CUCM** and select the Synchronize with CUCM.

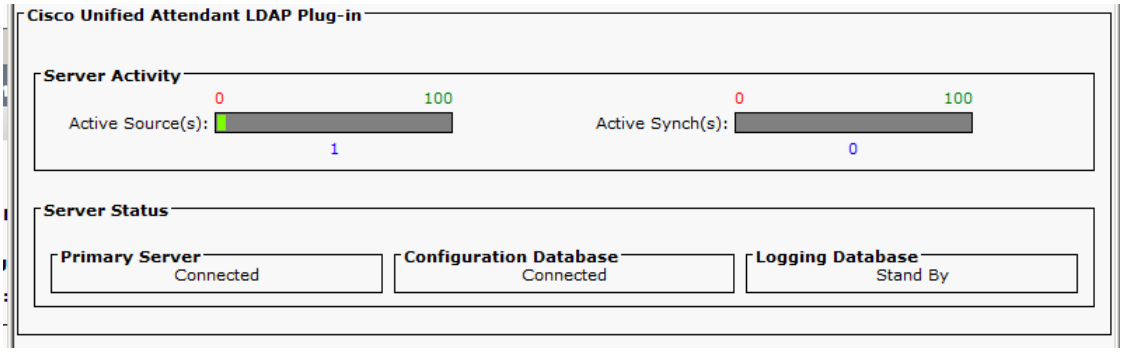
Step 2 If the devices fail to synchronize there will be an error code, for example 8500. Reference this code in the Cisco Unified Attendant Console Configuration and Installation guide as the list is very well detailed and should give an indication of what is going on. This document can be found here http://www.cisco.com/en/US/products/ps7282/prod_installation_guides_list.html

Ldap Server Not Synchronizing Contacts

Step 1 In Cisco Unified Attendant Console Web Admin choose **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. For example:



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

a. Click the **Start** button, and then, on the **Start** menu, click **Run** and then type **Regedit**.

b. Locate 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 Cisco Unified Attendant Console Server. If it is not the same, stop the LDAP Service, change the key in the registry to the correct IP address, and then restart the LDAP Service.

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

Operators Receive *Invalid Destination* Error When Transferring Calls

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

Step 1 If the number in the directory is correct, in Cisco Unified Attendant Console Web Admin choose **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.

Step 2 If step 1 does not resolve the issue, the problem is most likely to be with the Calling Search Space. To check this, ensure that the Service Queue CTI Ports have the necessary CSS to reach the intended destination:

a. With Cisco Unified Attendant Console Server shut down, click the **Start** button, and then, in the **Start** menu, click **Run**, and then type **dialer**.

b. Connect to one of the Service Queue devices.

c. Dial the number the operator is attempting to transfer calls to.

d. If the number does not ring, the CSS on the CTI Port needs to be updated to allow sending calls to the destination Partition.

e. If the call is successful, determine whether the transfer problem 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 Enabling Direct Transfers, page 4-5) and the operator can transfer the internal call, the issue is with the CSS on the gateway. As Cisco Unified Attendant Console 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

Cisco Unified Attendant Console Web 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 Cisco Unified Attendant Console Web Admin application.

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

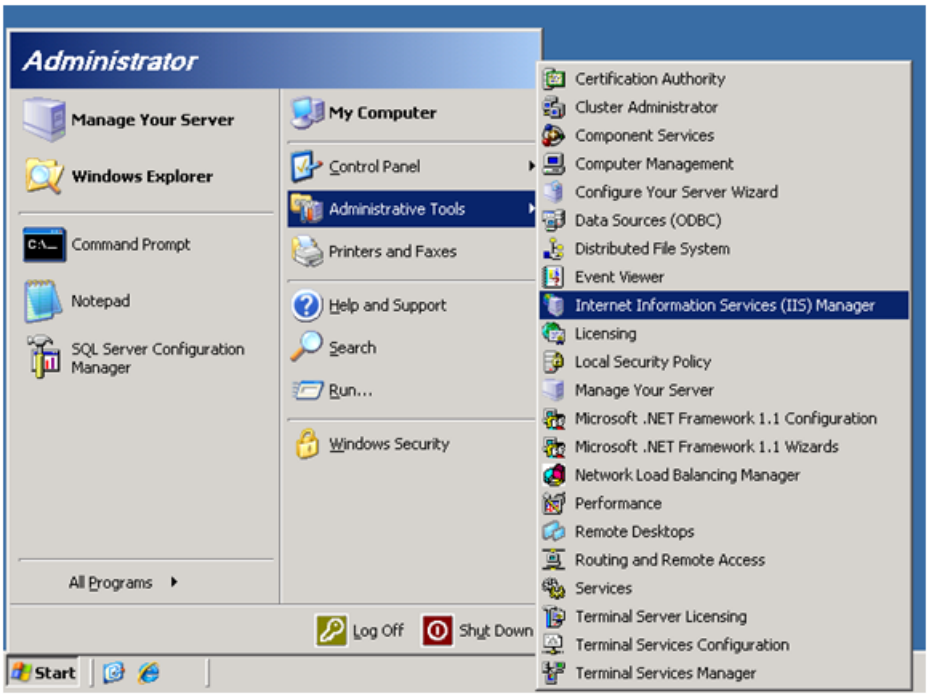
Note - This issue is only present on Windows Server 2003 installations. Windows Server 2008 installations are not dependant on the Administrator account.
- It is assumed that the user has already created a windows user account on local machine and has added this account to the local machine Administrators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

Configuring Cisco Unified Attendant Console Web Admin under a local administrator account

This section explains the steps required to configure the Cisco Unified Attendant Console Web 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.

Figure 2-1 Open IIS Manager



Step 2 Now expand the tree menu as shown in the Figure 2-2 on page 2-7 to find the Web Admin web site. Right click it and select the Properties option from popup menu.

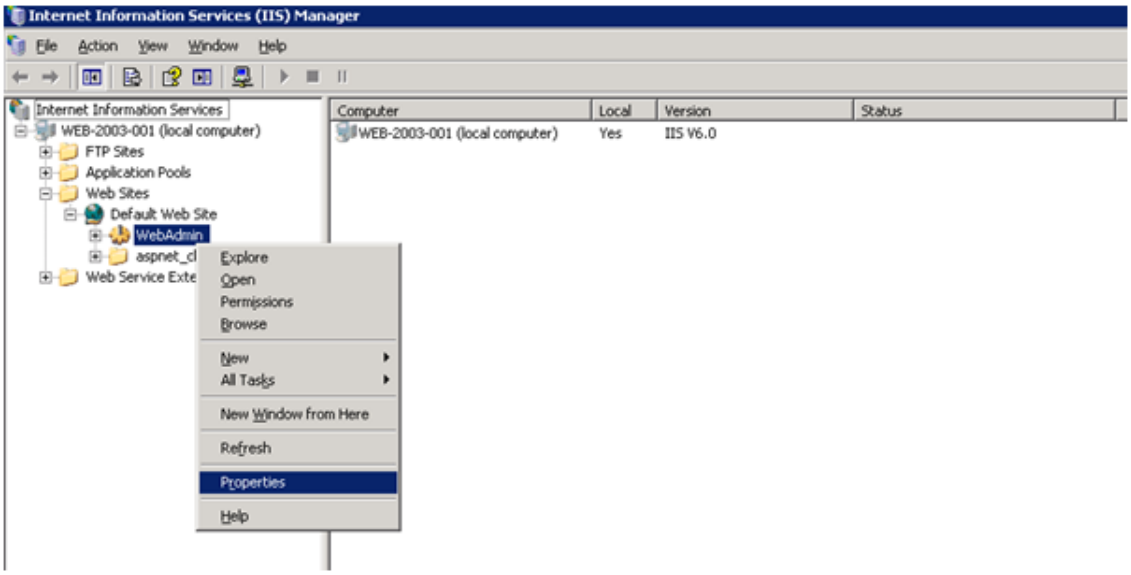


Figure 2-2 Find the Web Admin web site

Step 3 On "Web Admin Properties" dialog select the "Directory Security" tab and click Edit button under "Authentication and access control" group box. See Figure 2-3 on page 2-8

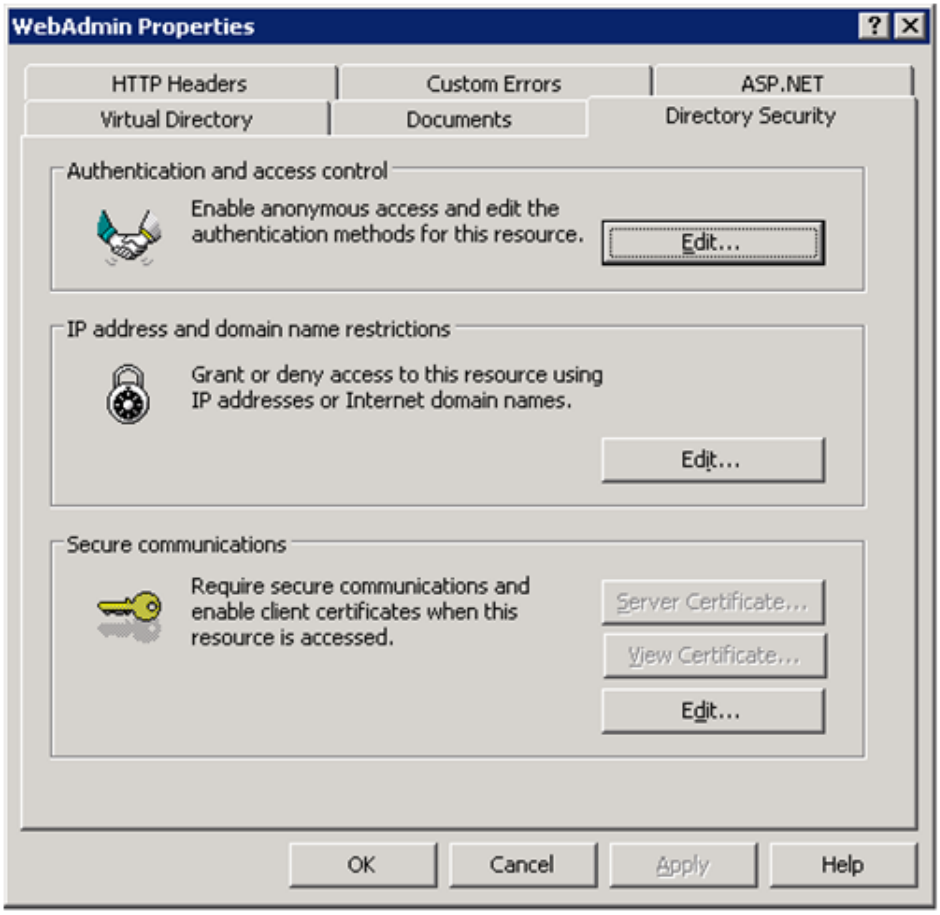


Figure 2-3 Web Admin Properties Window

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 2-9

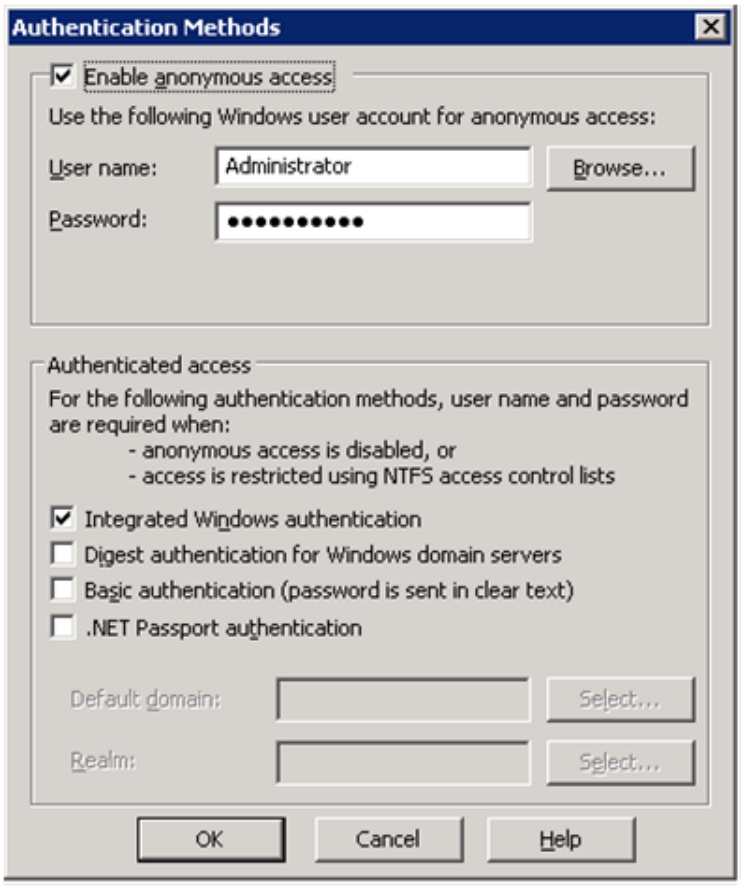


Figure 2-4 Web Admin Anonymous Access User Name

Step 5 Figure 2-5 on page 2-10 shows that the "Administrator" user is replaced with a local administrator user account called "Cisco Unified Attendant Console_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).

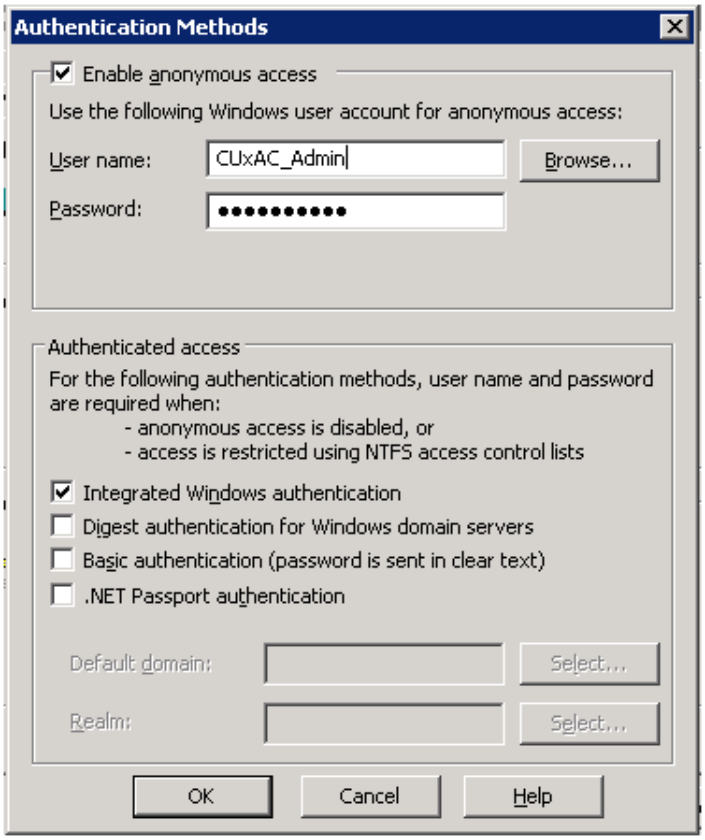


Figure 2-5 Use Local Administrator Account for Anonymous Access

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

Changing Cisco Unified Attendant Console Server IP Address

The majority of the references of the IP address are contained within the Windows registry of the Cisco Unified Attendant Console 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 Cisco Unified Attendant Console 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

xxxxxxx

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 Cisco Unified Attendant Console Server.

Note Please note that the location may vary slightly in different versions of the Cisco Unified Attendant Console 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 Cisco Unified Attendant Console Server

Note Please note that the location may vary slightly in different versions of the Cisco Unified Attendant Console 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

Unable To Make Online Changes Because Channel Link Is Down

The error *Unable to make online changes because Channel Link is down* is displayed when the ActiveMQ service is not active. To start the service, do the following on the host server:

Step 1 In Control Panel, select **Administrative Tools**.

Step 2 In the browser, double-click **Services**.

Step 3 In the Service window, locate the ActiveMQ service.

Step 4 If the status of the service is blank (meaning that it is stopped), select the service and then click **Start**.

Note If the ActiveMQ service fails to start this is probably because the latest version of Java is not installed. To install the latest version of Java, visit java.com and follow the instructions.

CHAPTER 3

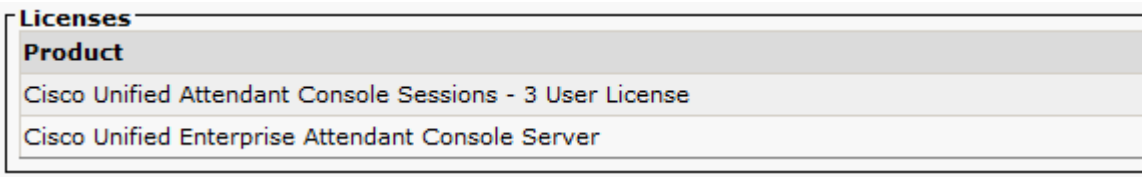
Web Administration

This chapter describes some of the Cisco Unified Attendant Console Web Admin problems that can occur.

Unable to Create Queues or Operators

If you cannot create queues or operator profiles under **User Configuration > Queue Management** or **User Configuration > Operator Management**, check the license window for correct licenses.

Choose **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 Cisco Website

If you cannot activate LAC on thewww.cisco.com/go/ac website you may see these error messages:

- No more activations

  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 Cisco Unified Attendant Console Edition is being activated.

- A license file is delivered successfully, however only the Operator Licenses appear in the Web Admin 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

Logging in to Web Admin Causes "DB Error" Message

Step 1 Check Windows Services and ensure that the Cisco Unified Attendant Console Server service is started.

If the service is stopped, start it and ensure that it is set to start automatically.

Step 2 If the service is started, check the log file: C:\Program Files\Cisco\Logging\SRV\Log\icdinit.log. This file logs each server start and will contain error messages describing why the Cisco Unified Attendant Console server cannot start.

Step 3 If the error messages are *Unable connect to database ATTCFG* and *Unable to connect to database ATTLOG* ensure that the Microsoft SQL Server service is started and set to automatically start.

Step 4 Sometimes SQL does not allow the Cisco Unified Attendant Console service to log onto the databases.

Step 5 Using Microsoft SQL Server Studio Management ensure that

- BUILTIN\ADMINISTRATORS and the sa username haves System Admin permissions assigned
- The account is not locked out.

CHAPTER 4

Attendant Console and Client Software Issues

This chapter describes the following Attendant Console and Client software issues that can impact on functionality and operability:

- Directory Issues
- Contact Phone Status Shows Out Of Service
- Client Preferences Are Not Saved
- Remove Call Park Window
- Enabling Direct Transfers

Directory Issues

This section describes the following directory issues:

- Directory Does Not Display and Console Shows Database not connected
- Contact Phone Status Not Displayed
- Contact Phone Status Shows Out Of Service

Directory Does Not Display and Console Shows *Database not connected*

On the Attendant Console PC, do the following:

Step 1 Verify that the Windows User has Full Control access to the HKEY_LOCAL_MACHINE\Software\Arc Solutions registry key. For instructions on how to grant this access level, see Client Preferences Are Not Saved, page 4-3.

Note If the Cisco Unified Attendant Console version is earlier than 8.0.3 verify that HKEY_LOCAL_MACHINE\Software\Borland has this access as well.

Step 2 Verify that the Cisco Unified Attendant Console 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 Cisco Unified Attendant Console Server, do the following:

Step 1 Ensure that the contact database is populated:

a. Open a synchronization log file in C:\Program Files\Cisco\Logging\LDAP\Log\SSLog_xxxx.txt

b. Check that the following lines show in the logs:

```
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,P
PU: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
```

If the lines are there, there are contacts in the database.

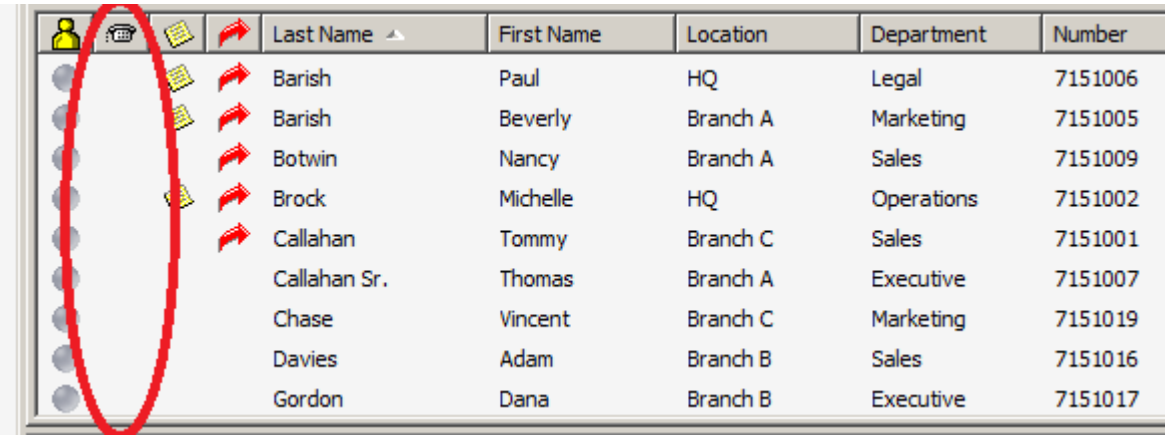
c. Start the SQL Configuration Manager utility.

d. In the utility, choose **Network Configuration** and make sure that **TCP/IP** and **Named Pipes** connections are enabled.

e. If you have to enable either of them, restart SQL for the changes to take effect.

Contact Phone Status Not Displayed

The phone status column in the directory is empty. For example:



Last Name	First Name	Location	Department	Number
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

Reasons for this include:

- The BLF Plug-in on the Cisco Unified Attendant Console Server is not running. To fix this, log in to Cisco Unified Attendant Console Web Admin, choose **Engineering > Service Management**, and then start the BLF Plug-in.
- Cisco Unified Attendant Console client is unable to reach the BLF Plug-in service on the Cisco Unified Attendant Console server. If so:

a. Ensure the BLF Plug-in is running, as described above.

- Ping the Cisco Unified Attendant Console Server by hostname and IP address, it should be reachable by IP address and hostname. If it is not reachable by hostname, add the IP address and hostname in the windows hosts file

Contact Phone Status Shows Out Of Service

If the phone status of an extension displays out-of-service status regardless of the actual status of the phone, do the following:

- 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 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 Cisco Unified Communication Manager, 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 Are Not Saved

The operator configures preferences on their PC, but these settings are lost when they restart their PC.

You need to amend the security settings for the Arc Solutions registry key so that all users have **Full Control** of this registry key.

Step 1 On the Attendant Console client PC, log in as **Local Administrator**.

Step 2 Ensure that all Cisco applications are closed.

Step 3 Click the **Start** button, and then, from the **Start** menu, select **Run**.

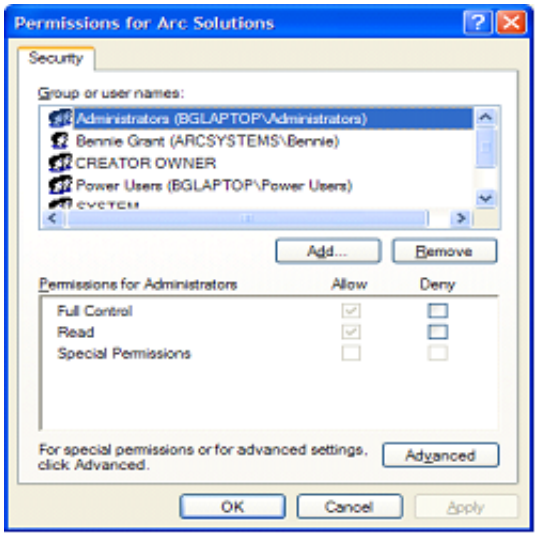
Step 4 In the **Run** dialog box, type **Regedit**.

The Windows Registry Editor opens.

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

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

Step 7 The **Permissions for Arc Solutions** dialog box appears. For example:

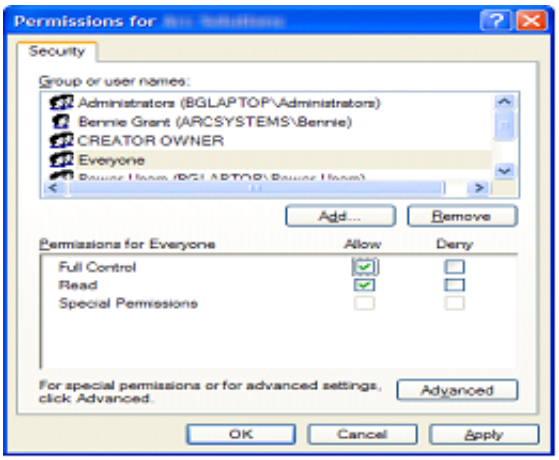


Step 8 Click **Add**.

Step 9 In **Enter the object name to select**, type **<domain_name> \Everyone**, where <domain_name> is the domain that a standard desktop user logs in to.

Step 10 Click **OK** to add the user Everyone.

Step 11 From Group or user names, select **Everyone**, and then, in the Permissions for Everyone list, select the **Allow Full Control** check box, to grant full access to this registry key.



Step 12 Click **Advanced** and then select the **Replace all existing inheritable permissions on all descendants with in heritable permissions from this object** check box.

Step 13 Click **Apply**, and then click **OK**.

The access rights have now been granted and Cisco Unified Attendant Console will now save settings.

Remove Call Park Window

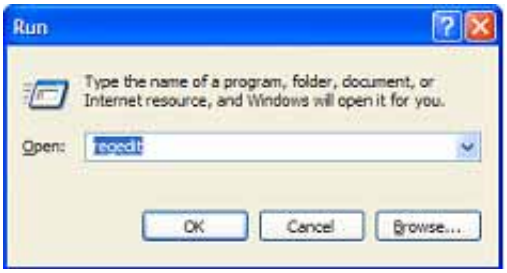
If customer is not using the Call Park functionality with Cisco Unified Attendant Console, they are able to remove this window from the screen.

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 ***Regedit*** in the **Run** Box



Step 4 The Windows Registry Editor opens.

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 this registry key, and change the value to **No**. Press **OK**

Step 8 Close the registry editor, and reopen the Cisco Unified Attendant Console application

Step 9 The call park window has now been removed

Enabling Direct Transfers

Direct Transfers can be enabled on the Attendant Console PC. You should consider doing this if you want to achieve either of the following:

- When the operator performs a blind transfer, the recipient of the transfer shows the caller ID of a CTI Port (the Cisco Unified Attendant Console *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
- 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 Cisco Unified Attendant Console 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 Cisco Unified Attendant Console, 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

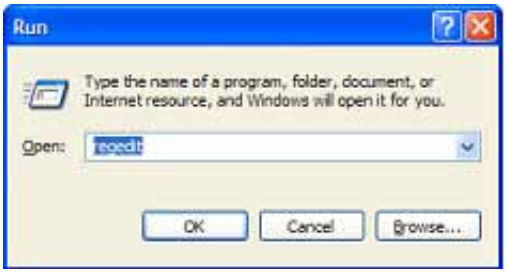
Performing this action is known as enabling "direct transfers"

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 ***Regedit*** in the **Run** Box



Step 4 The Windows Registry Editor opens.

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 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 Cisco Unified Attendant Console 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 Cisco Unified Attendant Console 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 Cisco Unified Attendant Console, 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 Cisco Unified Attendant Console 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 Cisco Unified Communication Manager 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