



Administration Guide

18 Apr 2024



Table of Contents

<u>Administration Guide</u>	1/36
<u>Description</u>	1/36
<u>Configuration Task List</u>	2/36
<u>Antivirus recommendations</u>	3/36
<u>Attendant Console client for macOS workstations</u>	4/36
<u>License Activation</u>	5/36
<u>Silent Monitoring and Whisper Coaching</u>	6/36
<u>Troubleshooting</u>	11/36
<u>Product Administration</u>	16/36
<u>Specific Webex client setup</u>	18/36
<u>Microsoft Calendar Integration</u>	19/36
<u>ConvAI integration - Chat feature</u>	28/36
<u>Product Configuration</u>	30/36
<u>Cisco Webex Calling MT Native Call Control - Imagicle Token Authorize</u>	34/36

Administration Guide

Description

Blue's Attendant Server is the server component of the following client-server products:

- Blue's Attendant Professional
- Blue's Attendant Enterprise
- Blue's One CTI Enterprise

Configuration Task List

Warning: you must install and configure the Application Suite before being able to configure the single applications. Please go through the AppSuite Deployment, Main Configuration, and User Management sections before reading on.

The following pages describe the configuration required to run and tune Blue's Attendant / CTI Server, which is the server component for:

- Blue's One CTI Enterprise
- Blue's Attendant Console Professional
- Blues Attendant Console Enterprise

The following directions, if not otherwise stated, apply to all versions of the console, named hereafter console client.

Installation Task list

1. Create the users on the Suite (server side)
2. Assign a valid primary extension to the users
3. Configure TAPI and associate devices
4. Edit Numbering plan parameters
5. Optionally, add external numbers as Speedy contacts

Antivirus recommendations

Installing Attendant Console client on a workstation equipped with AV

It happens sometimes that certain Antivirus applications recognize Imagicle Attendant Console as a foreign, untrusted application, thus avoiding the installation and automatically deleting the relevant executable.

In this case, the solution is to configure the Antivirus to exclude Attendant Console client from the list of monitored folders or to add it in the list of trusted applications.

Typically, Imagicle Attendant Console is installed in this folder: `C:\Program Files (x86)\Imagicle Attendant Console` unless a different path is specified during setup wizard.



Attendant Console client for macOS workstations

Imagicle Attendant Console client for macOS workstations has been effectively discontinued as of October 2023.

Existing customers using this Attendant Console version can keep using it and Imagicle is maintaining and applying fixes on the latest supported version (Summer 2022). There won't be any more updates to support newer macOS versions: last supported is macOS 12.7 "Monterey".

Moreover, Imagicle is not going to add new features in the future, other than those already included in Summer 2022. As an example, Microsoft Calendar OAuth2 integration, SSO support and Conversational AI chat panel features are not included.

Specific mandatory requirements for a macOS-based Attendant Console are evaluated on a project base. Please contact Imagicle for further details.

License Activation

Note: the following acronyms will be used in this WEB page:

BOE = Desktop CTI

BAP = Attendant Console Professional

BAE = Attendant Console Enterprise

Attendant Console and Desktop CTI are licensed on concurrent sessions base, that is the license rules the number of users simultaneously logged on, following a typical **CAL** (Client Access License) licensing model.

Together with each Attendant Console license, you get two Imagicle Advanced Queuing channels, to provide two queue resources to each operator.

While accessing to Imagicle admin web portal: ADMIN > Licenses, you can see how many Attendant Consoles have been licensed, together with relevant Advanced Queuing channels. See below sample:

PRODUCT NAME	QUANTITY	METRIC	LICENSE TYPE	CARE TERM DATE	TERM DATE	LICENSE STATUS
Attendant Console Enterprise (BAE)	40	clients	Perpetual	11/02/2021	-	Licensed
Attendant Console Professional (BAP)	20	clients	Perpetual	11/02/2021	-	Licensed
Desktop CTI (BOE)	40	clients	Perpetual	11/02/2021	-	Licensed
Advanced Queueing	16	channels - shared with Auto Attendant	Perpetual	17/01/2023	-	Licensed
Auto Attendant	16	channels - shared with Advanced Queueing	Perpetual	17/01/2023	-	Licensed

License Activation

- A license code must be provided by Imagicle for each requested product.
- A single license request can be used to obtain the four mentioned license items
- Read [this KB](#) about how to activate the licenses

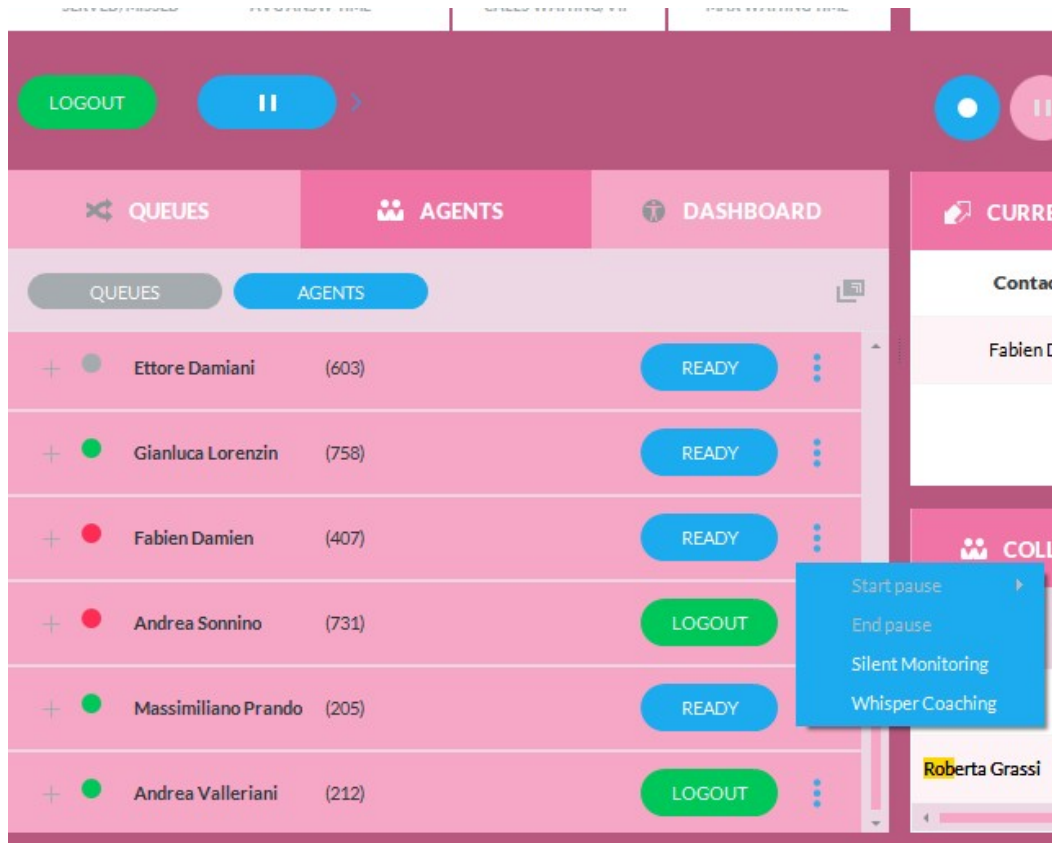
Silent Monitoring and Whisper Coaching

Feature Description

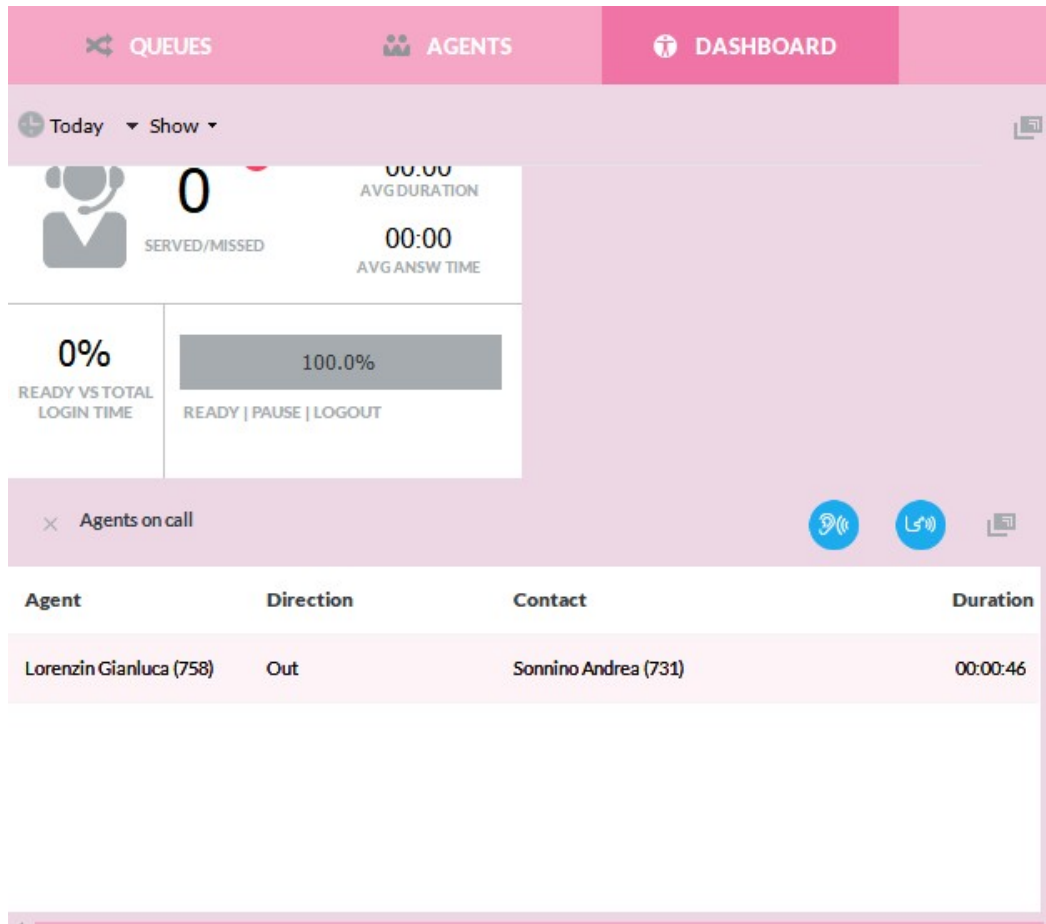
Starting from Summer 2018 Imagicle release, an operator with "Advanced Supervisor" Queue Manager permissions, can perform a Silent Monitoring (SM) or Whisper Coaching (WC) of another agent.

Above two features allows a supervisor to discreetly listen to an agent's conversation and, if required, to suggest a verbal action.

Both SM and WC features are available in Imagicle Attendant Console's "Agents" tab, in a pull-down menu beside a busy agent BLF. See sample below, based on Attendant Console Enterprise layout:



In Supervisor's Dashboard, "Agents on call" panel, you can find two blue buttons to trigger SM & WC. See below sample:



SM & WC Requirements

- Requires CUCM >= 8.5
- Supervisor's phone line should have an adequate "Monitoring CSS", including both Supervisor's and monitored agent's Partitions
- Monitored agent's phone is enabled to Built-In Bridge
- Monitored agent's phone(s) must be TAPI monitored. (Standard CTI Allow Call Monitoring role in Application User is needed) See [here](#)
- Agent's Imagicle user should include own phone's MAC address, if multiple phone devices are associated to same agent.
- Device names of the monitoring and monitored users must be defined on CUCM in upper case.
- Monitored agent's phone is busy (active call) → red BLF
- Monitored agent should be included into an Advanced Queuing queue, where at least an Advanced Supervisor is configured

Limitations

- Silent Monitoring and Whisper Coaching don't work in MRA for Phones/Jabber/Webex Unified CM clients, if Expressway version is prior to rel. X12.6.2
- Recording is not currently supported for the Silent Monitoring and Whisper Coaching features.
- Older versions of Cisco Expressway might have additional limitations. Please check Cisco web site for further details about your relevant Expressway release.
- All TAPI-monitored agent's phone devices can be intercepted by SM/WC. If you need to intercept a specific device only, you can specify it under UC Suite user's "Device name" field ("MAC Address", with Imagicle UC Suite ver. 2020.Summer.1 or older). Pay attention: Device name/MAC Address field is usually populated during [CUCM end users synch](#) (if enabled). So, if you want to monitor ALL agent's phone devices, you need to leave the Device name field empty.
- Whisper Coaching does not work on Cisco IP Communicator softphone, due to a Cisco bug. See [here](#) for more details.

- Imagicle Summer 2018 Attendant Console Enterprise client enables SM & WC buttons upon busy agent condition (red BLF). SM/WC could fail, if call hasn't been answered yet, if the call is on hold or if the call is already subjected to monitoring.
- There's no way to suddenly change from a SM to a WC monitoring session (or vice-versa). To swap monitoring method, supervisor must hang up current session and start a new one.

Interactions with Imagicle Call recording

- Monitored agent can normally record the conversation, even if subjected to SM or WC. Supervisor's speech won't be included in the recording.
- Supervisor can record a SM or a WC session. Relevant recording will include agent's speech and, for WC, supervisor's speech, too.

PBX Configuration

Cisco UCM allows to enable a periodical tone, while a SM or WC monitoring session is triggered. It is possible to decide who is going to hear the tones, by tweaking the following Service Parameters:

Clusterwide Parameters (Feature - Monitoring)		
Play Monitoring Notification Tone To Observed Target *	False	False
Play Monitoring Notification Tone To Observed Connected Parties *	False	False

To enable SM & WC monitoring features on supervisors' phone lines (DN), a specific Calling Search Space (CSS) should be configured in CUCM, including both supervisor's and agent's Partitions. See sample below:

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Directory Number Configuration

Save
 Delete
 Reset
 Apply Config
 Add New

ASCII Display (Caller ID)	<input type="text"/>	the caller.
Line Text Label	<input type="text"/>	
External Phone Number Mask	<input type="text"/>	
Visual Message Waiting Indicator Policy *	Use System Policy ▾	
Audible Message Waiting Indicator Policy *	Default ▾	
Ring Setting (Phone Idle) *	Use System Default ▾	
Ring Setting (Phone Active)	Use System Default ▾	Applies to this line when any line on the phone has a call in progress.
Call Pickup Group Audio Alert Setting(Phone Idle)	Use System Default ▾	
Call Pickup Group Audio Alert Setting(Phone Active)	Use System Default ▾	
Recording Option *	Call Recording Disabled ▾	
Recording Profile	< None > ▾	
Recording Media Source *	Phone Preferred ▾	
Monitoring Calling Search Space	CSS_AllIpPhones ▾	

☒ Log Missed Calls

Troubleshooting

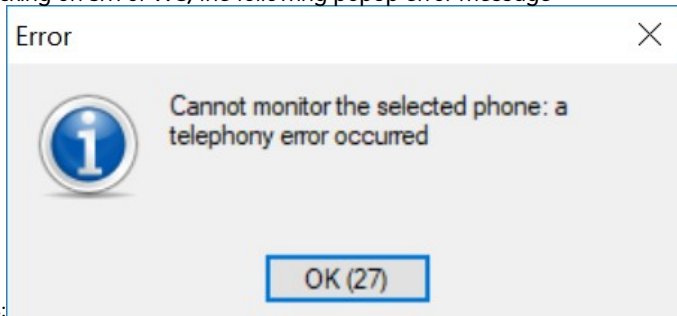
1st case:

While clicking on SM or WC, no error message is generated, Supervisor's phone goes off hook and a voice prompt "unreachable number" is played. Monitoring session is not triggered.

This is caused by wrong or missing "Monitoring Calling Search Space" on Supervisor's phone line.

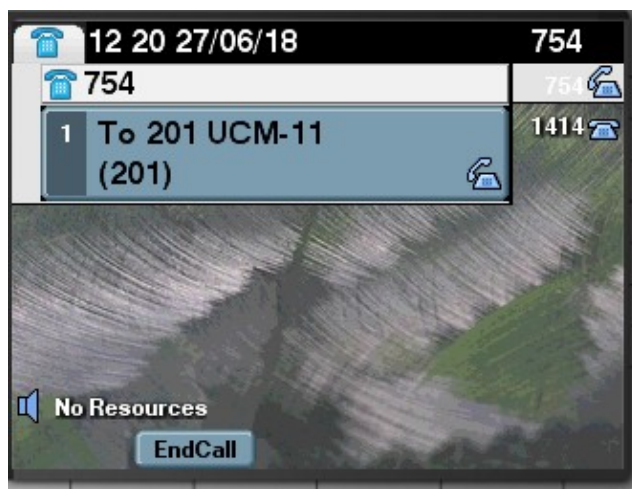
2nd case:

While clicking on SM or WC, the following popup error message



appears:

Supervisor's phone tries to initiate a call to monitored agent's phone, getting a "fast busy" tone and "No Resources" message on Supervisor's phone display (see sample below):

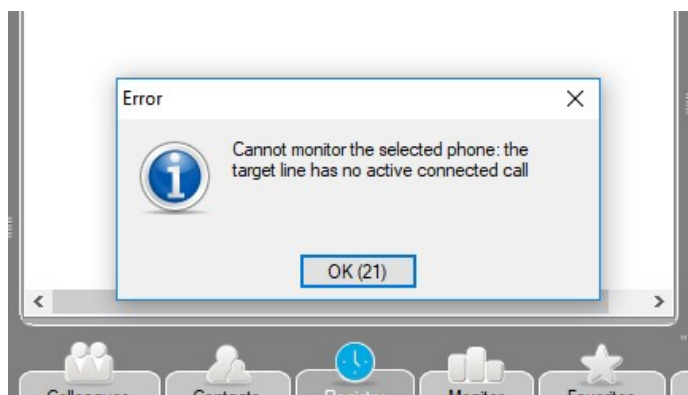


Two possible reasons for above issue:

- Monitored agent's phone does not support Built In Bridge or the feature is disabled.
- Monitored agent's phone is already subjected to a monitoring session

3rd case:

While clicking on SM or WC, an error message "Cannot monitor the selected phone: the target line has no active connected call" pops-up on Attendant Console interface. See sample below:



That means target agent does not have an active call. if the call is in ringing, dialing or on-hold state, monitoring session can't be triggered.

4th case:

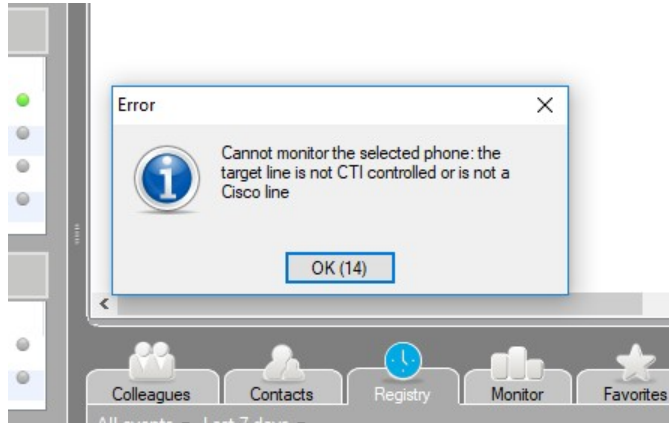
Supervisor's phone device is a Jabber Desktop, connected over MRA. While clicking on SM or WC:

- Session fails for telephony reasons
- Monitored agent receives a standard call from Supervisor

This is due to the fact that a Jabber device over MRA can't trigger any monitoring session.

5th case:

Agent's phone set is not a Cisco device. Supervisor tries to initiate a SM or WC session and it fails, with the following error message:



This is due to the fact that only Cisco TAPI-enabled device are currently supported. Non-Cisco phone sets are not supported.

Troubleshooting

How to use the troubleshooting guide

This page describes basic troubleshooting techniques and most frequent issues you may face during the application setup and usage.

The first part describes the basic tests to be made after you completed the configuration task list. Those test can reveal issues in the configuration and can help you to identify them.

The second part is a list of common issues and their causes. Look for the symptom and follow the tips. To know how to configure the product, please refer to the relevant pages in this guide.

Please understand that the problem may be related to complex PBX and network configurations, and that is not possible to list all them all. This guide must be considered as a tool to guess the origin of the issue.

When launching Attendant Console client, it doesn't connect to Imagicle Server:

- Check network connectivity between Attendant Console PC and Imagicle server:
 - ◆ If unencrypted connection is used, Imagicle server should be reachable on TCP port 51234
 - ◆ If encrypted TLS 1.2 connection is used (2021.Winter.1 release and above), Imagicle server should be reachable on TCP port 51235 and proper Digital Certificate should be in place. Check relevant paragraph below.

When launching Attendant Console, login fails:

- Check Imagicle Server credentials are correct and still valid (i.e. expired domain password).
- Check authentication settings in **Admin** → **System Parameters** → **Users authentication settings**. They should match users' provisioning source, if any (Local or AD/LDAP or CUCM)

When launching Attendant Console, it opens with a wrong console type (i.e. Attendant Console Professional instead of Attendant Console Enterprise or viceversa):

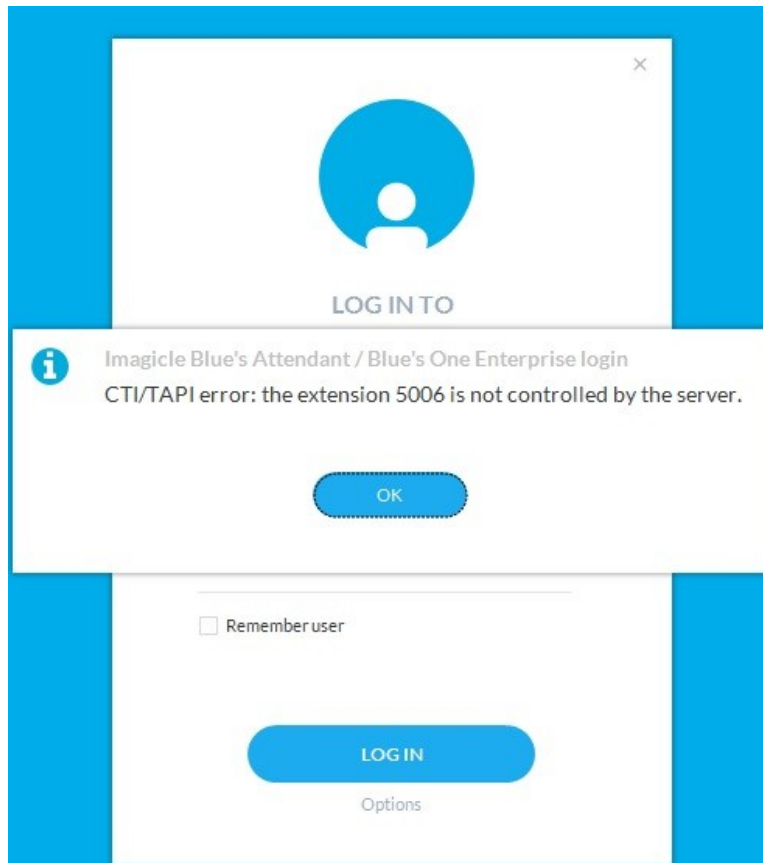
- Check related license type in **Admin** → **User Management**; in "Blue's CTI Server" section, "*Console license type (BOE,BAP,BAE)*" field should be populated with correct license.

"Park Button" in the Attendant Console doesn't work:

- Check on CuCM that CTI park ports range has been defined.

When launching Attendant Console, "*CTI/TAPI error: the related extension is not controlled by the server*" is displayed:

- Check "ImagicleCTI" [Application User](#). It should include operator's phone device into "Controlled Devices" list (Cisco only)
- Check PBX configuration and make sure operator's phone service is associated to an available CTI resource (TAPI, CSTA or TSAPI)
- Check that TAPI Service Provider version is aligned to current PBX release. If versions are misaligned, Imagicle CTI Server can't monitor operators' phones.



When Attendant Console's "Record" button is hit, call recording does not start and an error message is displayed (Cisco only)

- Please check that phone device, and relevant DN, are enabled for "Selective" Call Recording
- Phone device should be included in the list of TAPI-controlled devices

When Supervisor's Silent Monitoring and/or Whisper Coaching buttons are hit, no connection is established with agent on call (Cisco only)

Please check the following:

- Supervisor should be added into the queue with "Advanced Supervisor" permissions
- Supervisor's phone line should have an adequate "Monitoring CSS", including both Supervisor's and monitored agent's Partitions
- Monitored agent's phone must be enabled to Built-In Bridge
- Monitored agent's phone must be TAPI monitored. (Standard CTI Allow Call Monitoring role in Application User is needed) See [here](#)
- Monitored agent's phone should be busy (active call) â red BLF

Additional Troubleshooting hints for encrypted connection (2021.Winter.1 release and above)

Please locate the following log file in your PC workstation:

C:\Users\<windows_user>\Documents\Imagicle Blue's Attendant\Logs\RequestManagerLogFile.txt

Locate the following line includes IP, TCP port and connection type in use:



Opening connection to 192.168.6.5:51234, useSecureConnection=False

If you are experiencing errors related to Digital Certificate validation, you should find a message in same above log file, similar to the following line:

```
OpenConnection          - Exception during certificate validation:
System.Security.Authentication.AuthenticationException: The remote certificate is invalid
according to the validation procedure.
```

Another useful log file available in your PC workstation is the following:

C:\Users\<windows_user>\Documents\Imagicle Blue's Attendant\Logs**ApplicationLogFile.txt**

Here you can find additional error messages related to Certificate validation. See below some typical error messages, for different scenarios:

Digital Certificate non available on UC Suite server

```
Validate server certificate - Ssl Policy Errors [RemoteCertificateNotAvailable]
```

In this case, please instal a Trusted or Self-Signed Certificate on UC Suite node(s), as explained [here](#).

Certificate name is different than UC Suite host name

```
Validate server certificate - Ssl Policy Errors [RemoteCertificateNameMismatch]
```

Attendant Console is trying to connect to a host name which is different than Certificate name. Please make sure that both host and Certificate names are consistent.

Certificate is not Trusted

```
Validate server certificate - Ssl Policy Errors [RemoteCertificateChainErrors]
```

This error means that a non-Trusted Certificate is installed on UC Suite server (i.e. a self-signed Certificate) and you did not instal same certificate on operator's workstation. Please install self-signed Certificate on client side.

How to verify a TLS certificate presented by UC Suite

During troubleshooting of a TLS connection, it might be useful to know if the server is presenting the correct certificate and if a TLS session can be established between local PC and UC Suite server.

Requirements

- openssl installed on operator's PC
- firewall must allow communication between the client and the server on TCP port 51235

Command to perform from operator's PC

```
openssl s_client -crlf -connect <UC_Suite>:51235 -servername <UC_SUITE>
```

where <UC_Suite> is the IP or FQDN of the Imagicle UC on-prem or Cloud Suite.

Expected results with a self-signed certificate

```

CONNECTED(00000005)
depth=0 CN = EC2AMAZ-5F6ALB2, O = Imagicle S.p.a.
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = EC2AMAZ-5F6ALB2, O = Imagicle S.p.a.
verify return:1

---
Certificate chain
 0 s:/CN=EC2AMAZ-5F6ALB2/O=Imagicle S.p.a.
  i:/CN=EC2AMAZ-5F6ALB2/O=Imagicle S.p.a.
---

Server certificate
-----BEGIN CERTIFICATE-----
MIIC4TCCAcmgAwIBAgIBATANBgkqhkiG9w0BAQUFADA0MRgwFgYDVQQDDA9FQzJB
TUFaLTVGnkFMQjIwGDAWBgNVBAoMD0ltYWdpY2x1IFMucC5hLjAeFw0yMTA5MDcx
NDQxMjhaFw0yNjA5MDYxNDQxMjhaMDQxGDAWBgNVBAMMD0VDMkFNQVotNUIyQUxk
MjEYMBYGA1UECgwPSW1hZ21jbGUgUy5wLmEuMIIIBIjANBgkqhkiG9w0BAQEFAAOc
AQ8AMIIBCgKCAQEAA4fE+tlRL3RlgsHbBOWRf8dlVW50025RV6Ak18k50vVrWGkGG
ny/8IFocq9grXgD5oTL+NH2/vmVvwnF2oMSuC2aU6fJwsb3fBDagCD219GENLXP0
GzX5rg0a2UgKU+93wFii+bUHYWUCPPsBO6UmAqPrnhzz1H2OSDXkVxb6HFGw0VIY
u7Aw4focrHnY6madjvDKw3EcnP7sH4Bkl91bLcLAMP/EABjr71ViGiSS0WCXFTgn
lRntYdQ/btNk6UYOnJ8CjQkbnLWYyyp7JPY9cAPMiuwkc/B9BtGUj2AkqOEwiXQ2
XO9IVTj1TRTMh5UJw4DnTNje9+dYC18fmDPlfwIDAQABMA0GCSqGSIb3DQEBBQUA
A4IBAQCyyvwzoL9bNzFlJ88E6rog+cjKilIkTBBJjNnJuxwGAXU3fvNjORRkbbnrrn
PdcSxiF36RV1cVWxEa280jA3j61VRiL/std80aSB6VsGHUdN0XqDg73liAgMdkAX
mscesISLcaUnck197Zgx5/QDx9BvJfHGpRiB0mR8ZYowUQn7mvzuoNsKogbkFSvb
dtuU5VFLcd7aR1rmM+dTRsYyywMVe+7WV1RhC7ULncYu+XlmuXJshmkidkUs1/m
/hGxiVaQRC1872UeZqlRE4ALZ8hjk92kGAhiuanydS1a1NgvCOi6P9s+XS49ZWK1
JNXRE1EOaI8/+R40eoV+jhJbu/kx
-----END CERTIFICATE-----

subject=/CN=EC2AMAZ-5F6ALB2/O=Imagicle S.p.a.
issuer=/CN=EC2AMAZ-5F6ALB2/O=Imagicle S.p.a.

```

- **Line 1** : CONNECTED confirm the server is listening and connection can be established
- **Line 3** : alert if a self-signed certificate is in use
- Rest of the answer provides you details of the certificate presented by remote side

Expected results when implementing a Trusted Certificate from PKI

```

CONNECTED(00000005)
depth=3 O = Digital Signature Trust Co., CN = DST Root CA X3
verify return:1
depth=2 C = US, O = Internet Security Research Group, CN = ISRG Root X1
verify return:1
depth=1 C = US, O = Let's Encrypt, CN = R3
verify return:1
depth=0 CN = canalpopc.imagicle.cloud
verify return:1

---
Certificate chain
 0 s:/CN=uccs.imagicle.cloud
  i:/C=US/O=Let's Encrypt/CN=R3
 1 s:/CN=uccs.imagicle.cloud
  i:/C=US/O=Let's Encrypt/CN=R3
 2 s:/C=US/O=Let's Encrypt/CN=R3
  i:/C=US/O=Internet Security Research Group/CN=ISRG Root X1
 3 s:/C=US/O=Internet Security Research Group/CN=ISRG Root X1
  i:/O=Digital Signature Trust Co./CN=DST Root CA X3
---

Server certificate
-----BEGIN CERTIFICATE-----
MIIFdDCCBFygAwIBAgISA4mhitLj9tpBpjNQBCvmSRdEMA0GCSqGSIb3DQEBCwUA
MDIxZAJBgNVBAYTA1VTMRYwFAYDVQQKEw1MZXQncyBFbmNyeXBOMQswCQYDVQQD
EwJSMzAeFw0yMTA5MDcxMjI2MzJaFw0yMTEyMDYxMjI2MzFaMCMxITAfBgNVBAMT
GGNhbmcFscG9wYy5pbWFnZW50ZS5jbG91ZDCCAS1wDQYJKoZIhvcNAQEBBQAdggEP
ADCCAQoCggEBAAKfJt7vLwPFXlVqzzgKcYrzcXOXuTcBvHRMLsw3mb46ZKC3l3bk

```



```
Tk0nupg3bMroR2ceGBi06pAU2yfx1ZWjuGv17Q5XPUMHqgXucoFQOGZBcSxNzG
v3f1cXi0CcUXzpcFufTFN0T8th2I6v+6azfK2AqZcxKNgsPH45T2M4eUS+v0x96w
U/E4mRuYeLZU+lg/osextxUH7q811C6vGvTz3cMWNaxPM4a4P+/dKy3QG2B1awmE
OWNH29LFkjWpuIU9KTVFw4+tZzHMxU5nXY7tOb2QJObpH5HSXOe2rfMmLTpnJKxb
pGvDuIAvOR71ZGW7USAwHq7KIqnqj5IpchUCAwEAAoCApEwggKNMA4GA1UdDwEB
/wQEAWIFoDAdBgNVHSUEFjAUBgggrBgEFBQcDAQYIKwYBBQUHAWIwDAYDVROTAQH/
BAIwADAdBgNVHQ4EFgQU8OQ+esHwMMNYgiZ3eJILYFDuMcMwHwYDVROjBBgwFoAU
FC6zF7dYVsuuA1A5h+vnYsUwsYwVQYIKwYBBQUHAQEESTBHMCEGCCsGAQUFBzAB
hhVodHRwOi8vcjMubY5sZW5jci5vcmcwIgYIKwYBBQUHMAKGfMh0dHA6Ly9yMy5p
LmxlbmNyLm9yZy8wYQYDVRORBfowWIIbYWMtY2FuYWxwb3BjLm1tYWdpY2x1LmNs
b3Vkggh9jYW5hbHBHbGVzZ3Vkggh9jYW5hbHBHbGVzZ3Vkggh9jYW5hbHBHbGVzZ3V
aW1hZ21jbG9uY2xvdWQwTAYDVROgBEUwQzAIBGZngQwBAGewNwYkYBBAGC3xMB
AQEKDAmBggrBgEFBQcCARYaaHR0cDovL2Nwcy5sZXRzZW5jcn1wdC5vcmcwggEE
BgorBgEEAdZ5AgQCBIIH1BIHyAPAAAdgCUIIWejtWNbIhzH4KLIiwn0dpNXmxPlD1h
204vWE2iwgAAAXvAcFRCAAAEAwBHMEUCIBzfKfBmtUk+jrHo4y4sFSR6a5qK5Yy6
92VNkbBle/boAiEAoe5y8gmcpPg4CND2547/1shV8pSkuPfwyzJhtX5NTX8AdgB9
PvL4j/+IVWgkwsDKnlJJeSvFDngJfy5ql2iZfiLw1wAAAXvAcFRpAAAEAwBHMEUC
IQDxaUSYkuewNbxTYWk9Ubm2zxVFvUrxXAcODSng5f53gIgHvraHOiq2+mUdpIj
cFUR0OpqCAJZ4ANvWMfjR8HOY4wDQYJKoZIhvcNAQELBQADggEBABkbq7ybst0Y
qnp+syq0MBYF0V/FrCcWudw2JW6yWIMxar4ic9XHTI7SNu9KqZmtwNf38HvJKk38
Vbg2we2OYIEx9+87anxsTqwfjfsqwyOXMBvfuY6M0TiAi8A5qSN5mXcpnvvhGINW
ZbW6DLt7ff4gh7L+wYEcp2+MhMPRsg/ovNZAoYAAZhz97GnnXTic42zia+vxtDna
CiyqvM17MXi3sLNNeac6m5LRdcgehJzbaObrjlSaRv4bkjNSWfQeH3Wfc9/D4pnn
wlvPBoE93CTanJLHM8/wtRrtKrEFTFFg+IGk26CCnUYHVHdiAfQ+c2gRNkKf7y6P
gjnyJ8GXHD0=
-----END CERTIFICATE-----
```

```
subject=/CN=uccs.imgacle.cloud
issuer=/C=US/O=Let's Encrypt/CN=R3
```

```
---
No client certificate CA names sent
Server Temp Key: ECDH, X25519, 253 bits
---
```

```
SSL handshake has read 6094 bytes and written 329 bytes
```

```
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES128-GCM-SHA256
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol : TLSv1.2
    Cipher : ECDHE-RSA-AES128-GCM-SHA256
    Session-ID: 54C469AC93D1C7D800B630AE9B7EF62AD7DFF2DE4BA9B7EAB0E33719CC20C374
    Session-ID-ctx:
    Master-Key: A346DA5784ABCE2BF0ED4C73929B6D2D873BAF1CE7782E0E4205196C67877C9000A5D7B9335C9080D8590C988E82A6C9
    TLS session ticket lifetime hint: 86400 (seconds)
    TLS session ticket:
0000 - 31 36 33 31 30 33 33 33-39 38 30 30 30 00 00 00 1631033398000...
0010 - c9 00 49 e1 76 45 94 47-ab fd 76 08 e6 b4 02 3b ..I.vE.G..v...;
0020 - 22 4f 08 e3 a9 2c 2b c1-a2 7c 68 b2 40 af f3 d0 "O...,+..|h.@...
0030 - 61 4e 66 0d 33 b5 d9 c0-92 14 8d 88 28 5d a4 f2 aNf.3.....()..
0040 - 01 ac b7 f1 29 05 7c 97-02 ac 10 0c 71 ef 6b e4 ....).|.....q.k.
0050 - fb f8 86 a0 df 2d b2 ef-f5 ea c6 59 cd ca 27 85 .....-.....Y...'.
0060 - 4f fd 6f 95 8d 5c 78 02- O.O...\x.

Start Time: 1631035955
Timeout : 7200 (sec)
Verify return code: 0 (ok)
```

- **Line 1** : CONNECTED confirm the server is listening and connection can be established
- **Line 3 to 9** : verify the certificate information, if they are trusted or not
- **Line 11 to 19** : Give information about the certificate chain of the presented certificate
- Rest of the answer provides you details of the certificate presented by remote side

Product Administration

Imagicle Attendant Console client compatibility against Imagicle UC Suite version

Latest Imagicle Attendant Console client version is backward compatible with older UC Suite versions. Just keep in mind that client versions equal or newer than Summer 2020 require a UC Suite release greater than 2018.Spring.1.

Imagicle CTI Server Administration

UC Suite administrators can access the Attendant Console / CTI Server configuration page, that shows some parameters affecting the behavior of console clients.

Basic Settings tab

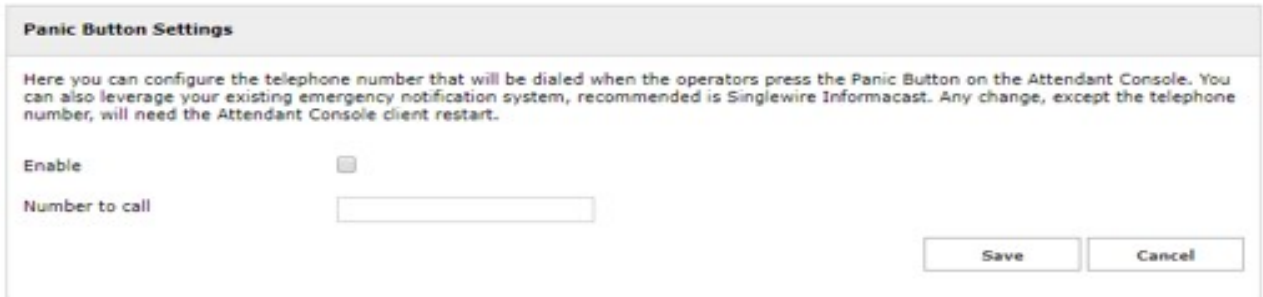
- **Delete data older than (days):** this is the call history data retention, for all Attendant Console/Desktop CTI users
- **SkyStone route prefix:** this is an optional telephony prefix used to route PSTN calls through legacy Imagicle Skystone application (using the SkypeOut service). This allows Attendant Console client to call a number through Skystone.
- **Min Lookup Number Length:** this is the minimum caller number length that triggers a lookup in Contact Manager directories. This avoids **Directory Lookup** when the caller number is an internal extension.
- **Search Max Results:** the maximum number of result items returned by a client search into Contact Manager directories. The maximum admitted value (for performance reasons) is 500
- **Client updates URL:** location from where Attendant Console client update packages will be downloaded. By default this points to Imagicle public web site. If the agents' PCs cannot reach Internet, you can copy the client on a local server and change setting accordingly. E.g. you can place update package in a network share and enter "\\192.168.1.1\Updates" in this field
- **Call forward destination:** This option allows to enable partial digit masking for call forward destination number, displayed on "Colleagues" tab.
- **Operators can see calls parked by other operators:** (Cisco UCM only). By checking this flag, every operator can see call parked by any operator. If unchecked, each operator can see own parked calls only. In a Cisco Webex Calling MT environment, parked calls are always shared among all operators.
- **Display remote party information on dashboard panel:** If checked, advanced supervisors and queue manager can display agents' active calls remote party numbers and other data on Attendant Console Dashboard.

Basic Settings			
Delete data older than (days)	<input type="text" value="10"/>		<input type="checkbox"/> Use default settings
Skystone route prefix	<input type="text"/>		<input type="checkbox"/> Use default settings
Min Lookup Number Length	<input type="text" value="6"/>		<input type="checkbox"/> Use default settings
Search Max Results	<input type="text" value="200"/>		<input type="checkbox"/> Use default settings
Client updates URL	<input type="text" value="http://www.imagicle.com/LiveUpdate/BluesAttendant/"/>		<input type="checkbox"/> Use default settings
Call forward destination	<input type="text" value="Mask last 3 digits"/>		<input type="checkbox"/> Use default settings
Operators can see calls parked by other operators	<input checked="" type="checkbox"/>		<input type="checkbox"/> Use default settings
Display remote party information on dashboard panel	<input checked="" type="checkbox"/>		<input type="checkbox"/> Use default settings

Please note that every parameter can be reverted to its factory value (default settings).

Panic Button Settings (available from 2020.Winter.1 release and above)

- **Enable:** This flag enables a red "Panic" button on Imagicle Attendant Console client interface, placed on top-right corner.
- **Number to call:** When panic button is pressed, an automatic phone call is performed to the number configured in this field. Call can be routed to SingleWire's "InformaCast" application or to any other internal/external emergency number.



The screenshot shows a dialog box titled "Panic Button Settings". Inside, there is a paragraph of text: "Here you can configure the telephone number that will be dialed when the operators press the Panic Button on the Attendant Console. You can also leverage your existing emergency notification system, recommended is Singlewire Informacast. Any change, except the telephone number, will need the Attendant Console client restart." Below this text, there is a label "Enable" followed by a checkbox that is currently unchecked. Below that is a label "Number to call" followed by a text input field. At the bottom right of the dialog box, there are two buttons: "Save" and "Cancel".

Please make sure that every Attendant Console-equipped agent can reach above emergency number.

Microsoft Calendar Settings (available from 2020.Summer.1 release and above)

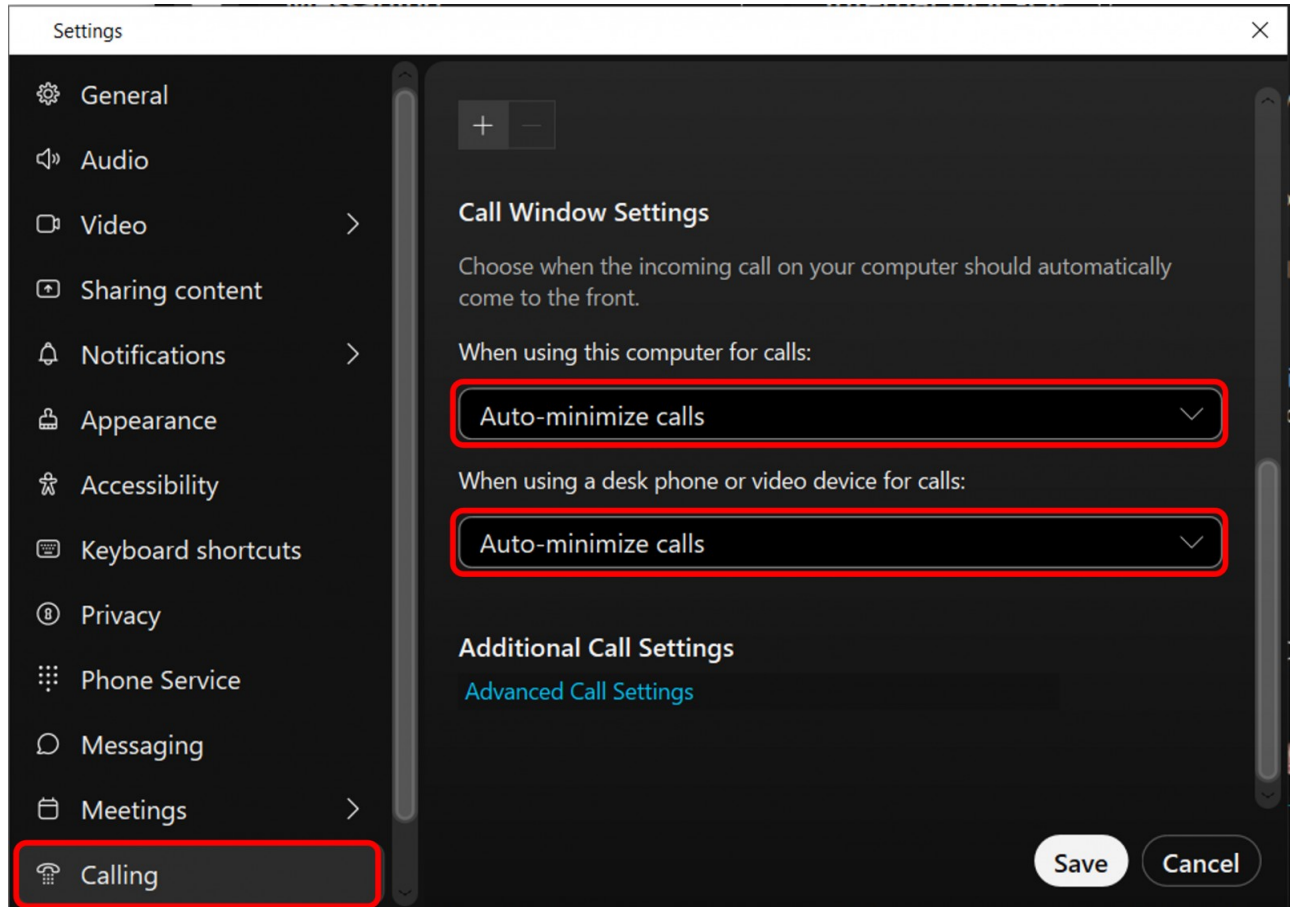
Imagicle Attendant Console can display real-time Microsoft Calendar information into its "Colleagues" tab, including scheduled tasks for the current day. Calendar information can be retrieved from an on-prem Microsoft Exchange server, version 2007 SP1 and above, or from cloud-based Microsoft Office 365 service.

The connections to both on-prem and cloud-based Microsoft email services are fully described in [this KB](#), including Office 365 "OAuth2" modern and secure authentication method, supported starting from 2021.Spring.1 Imagicle release.

Specific Webex client setup

While using Imagicle Attendant Console together with Cisco Webex client, the default client settings are invoking a window pop-up for any inbound call to user. This pop-up is pretty annoying, especially for operators with visual disabilities.

For this reason, we highly suggest to disable incoming call pop-up from Webex client settings. See below screenshot:



This setting is useful for Webex clients registered to Cisco UCM or Webex Calling MT/DI calling platforms.

Microsoft Calendar Integration

Imagicle UCX Suite can retrieve Microsoft Calendar information from both an on-prem MS-Exchange server, typically using Basic Authentication, or from cloud-based Office 365 email service using OAuth2 authentication. Please be aware that Basic Authentication has been dismissed by Microsoft starting from December 2022.

In the following chapters we are describing the configurations to be applied for both authentication options.

OAuth2 Authentication

In order to enable Microsoft Calendar Integration, interfaced to Microsoft Office 365 cloud service using OAuth2 authentication, you must configure an application on [Azure Web Portal](#), taking note of Application ID and Directory ID, needed later on while configuring this authentication method on Imagicle UC Suite. Please read the following procedure to create a new application on Azure portal and add it to UCX Suite web interface.

Azure web portal configurations

Please access to Azure portal and go to "App Registrations"

The screenshot shows the Microsoft Azure portal interface for App Registrations. The top navigation bar includes the Microsoft Azure logo and a search bar. Below the navigation bar, the 'App registrations' section is active, showing a list of owned applications. The table below lists the applications with their display names and application IDs.

Display name	Application (client)
GI GiulianoAppTest	3d62f992-8a29-4fdc
TE TestAuthApp	2a321830-4133-4f6e
CA CallBot	47e27225-b893-417
MY myMessagingBot	83a0bc9b-3c74-457
TE Test1	5025cb0b-e879-46d

Click on "New registration" and choose a name like "AttendantConsoleCalendar". Then select "Accounts in this organizational directory only" and hit "Register"

Microsoft Azure

Search resources, services, and docs (G+)

Home > App registrations >

Register an application

* Name

The user-facing display name for this application (this can be changed later).

AttendantConsoleCalendar

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Imagicle spa only - Single tenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web

e.g. https://myapp.com/auth

By proceeding, you agree to the Microsoft Platform Policies

Register

The following window appears, including Application ID and Directory ID. Please copy both data, for later usage.

Select "Office 365 Exchange online" and then select "Delegated Permissions"

The screenshot shows the Microsoft Azure portal interface. On the left, a sidebar lists navigation options: Overview, Quickstart, Integration assistant, and Authentication. The main content area is titled 'AttendantConsoleCalendar | API permissions'. It includes a search bar, a refresh button, and a 'Got feedback?' link. Below this, there's a section for 'Configured permissions' with a table listing permissions. The table has columns for 'API / Permissions name', 'Type', and 'Description'. One permission is listed: 'Microsoft Graph (1)'. To the right of the table, there are buttons for '+ Add a permission' and 'Grant admin consent for Imagicle spa'. On the far right, a 'Request API permissions' dialog is open, showing 'Office 365 Exchange Online' as the selected API. It asks 'What type of permissions does your application require?' and offers two options: 'Delegated permissions' (selected) and 'Application permissions'. The 'Delegated permissions' option is described as 'Your application needs to access the API as the signed-in user.'

Please flag "EWS.AccessAsUser.All" and then click on "Add permissions"

Administration Guide

Microsoft Azure

Search resources, services, and docs (G+)

Home > AttendantConsoleCalendar

AttendantConsoleCalendar | API permissions

Search (Ctrl+)

Refresh

Got feedback?

Overview

Quickstart

Integration assistant

Expose an API

API permissions

App roles | Preview

Do you want to grant consent for the requested permissions for all accounts in Imagicle spa? This will update the permissions the application needs. [Learn more about permissions and consent](#)

Yes No

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. [Learn more about permissions and consent](#)

+ Add a permission

✓ Grant admin consent for Imagicle spa

API / Permissions name	Type	Description	Admin consent
Microsoft Graph (1)			
User.Read	Delegated	Sign in and read user profile	-
Office 365 Exchange Online (1)			
EWS.AccessAsUser.All	Delegated	Access mailboxes as the signed-in user via Exchange Web Services	-

Now access to "Authentication" section, click on "Add a platform" and then click on "Mobile and desktop application":

Microsoft Azure

Search resources, services, and docs (G+)

Home > AttendantConsoleCalendar

AttendantConsoleCalendar | Authentication

Search (Ctrl+)

Save

Discard

Got feedback?

Overview

Quickstart

Integration assistant

Expose an API

API permissions

App roles | Preview

Authentication

Certificates & secrets

Token configuration

Roles and administrators | Preview

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Imagicle spa only - Single tenant)
 ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

[Help me decide...](#)

Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. [Learn more about these restrictions.](#)

Configure platforms

Web applications

Web

Build, host, and deploy a web server application. .NET, Java, Python

Mobile and desktop applications

iOS / macOS

Objective-C, Swift, Xamarin

Mobile and desktop applications

Windows, UWP, Console, IoT & Limited-entry Devices, Classic iOS + Android

Please flag the first URL option and then click on "Configure":

Microsoft Azure
Search resources, services, and docs (G+/)

> AttendantConsoleCalendar
AttendantConsoleCalendar | Authentication

arch (Ctrl+/)
Save
Discard
Got feedback?

enviwr
ickstart
egration assistant
e
inding
thentication
rtificates & secrets
ren configuration
l permissions
lose an API
p roles | Preview

Platform configurations
Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.
Add a platform
Supported account types
Who can use this application or access this API?
Accounts in this organizational directory only (imgacle spa only - Single tenant)
Accounts in any organizational directory (Any Azure AD directory - Multitenant)
Help me decide...

Configure Desktop + devices
All platforms
Redirect URIs
The URIs we will accept as destinations when returning authentication r after successfully authenticating users. Also referred to as reply URLs. L Redirect URIs and their restrictions
https://login.microsoftonline.com/common/oauth2/nativeclient
https://login.live.com/oauth20_desktop.srf (LiveSDK)
msal34de9ec7-3d2f-480f-ac6b-c3d418b0ab3b://auth (MSAL only)
Custom redirect URIs
https://contoso.com

UCX Suite configurations

Please access to Imagicle web portal as administrator and go to Attendant Console â Application Settings â Calendar Integration Settings.

Please populate the following fields:

- **Provider:** Office 365
- **Grant Basic Authentication:** This flag enables basic EWS authentication, just using username and password. We STRONGLY suggest to keep this flag unchecked.
- **Grant Modern Authentication:** This flag enables OAuth2 authentication, where two new parameters are used to access calendars:
 - ♦ **Directory (tenant) ID:** This is the tenant ID previously retrieved from Azure (see above)
 - ♦ **Application (client) ID:** This is the client ID previously retrieved from Azure (see above)

If you keep both authentications enabled, a warning is displayed once configuration is saved.

Calendar Integration Settings

Here you can configure the options to retrieve the calendar data that can be consulted from the console. Any saved changes will need the Attendant Console client restart.

Enable
Provider
Office 365
Grant Basic Authentication
Grant Modern Authentication
Directory (tenant) ID
Application (client) ID
Selecting both options, Attendant Console users will have two authentication methods available: Basic Authentication (to be discontinued) and Modern Authentication (more secure and flexible).
Data refresh interval
60 seconds
Save
Cancel

EWS Basic Authentication

Please access to Imagicle web portal as administrator and go to Attendant Console → Application Settings → Calendar Integration Settings.

Please populate the following fields:

- **Provider:** Exchange
- **Version:** From Exchange 2007 SP1 up to 2013 SP1 or newer
- **EWS URL:** Customer's EWS access URL (see below sample)
- **Data refresh interval:** Interval in seconds between each calendar refresh. See our troubleshooting notes in the next paragraph.

Calendar Integration Settings

Here you can configure the options to retrieve the calendar data that can be consulted from the console. Any saved changes will need the Attendant Console client restart.

Enable

☒

Provider

Exchange (Active)

Version

Exchange 2013

Exchange Web Service (EWS) URL

https://myexchange.com/ews/exchange.asmx

URL has to follow a valid EWS URL syntax (e.g. http(s)://<exchange hostname>/ews/exchange.asmx)

Data refresh interval

60

seconds

Save

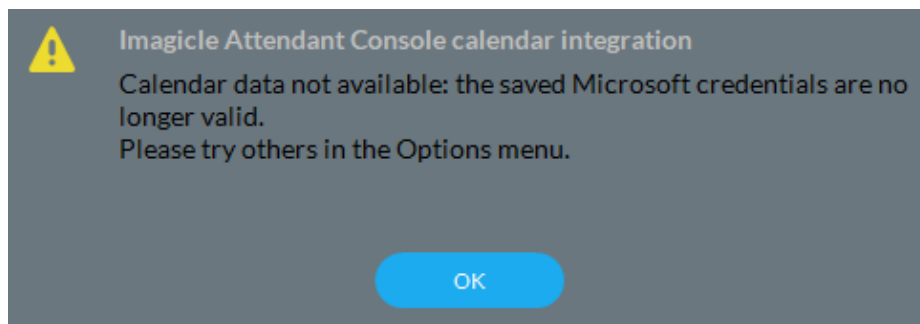
Cancel

Troubleshooting

It might happen that the Microsoft account configured in Imagicle Attendant Console to retrieve presence returns an error, due to the following possible reasons:

1. The Microsoft account has a policy which does not allows too frequent calendar refreshes.
2. Someone has changed the account password, so entered credentials are invalid.
3. Someone changes account credentials while Attendant Console is running.

In all above cases, the Microsoft account is locked within few seconds and you get the following error message on Attendant Console:



More info about this problem are available in Attendant Console logs, stored inside operator's PC workstation. This is the file to consult:

C:\Users\<user name>\Documents\Imagicle Blue's Attendant\Logs\ApplicationLogFile.txt

Calendar data display on Imagicle Attendant Console



To enable this feature on Attendant Console client, please refer to our user's guides, available to download from this [Knowledge Base](#) site.

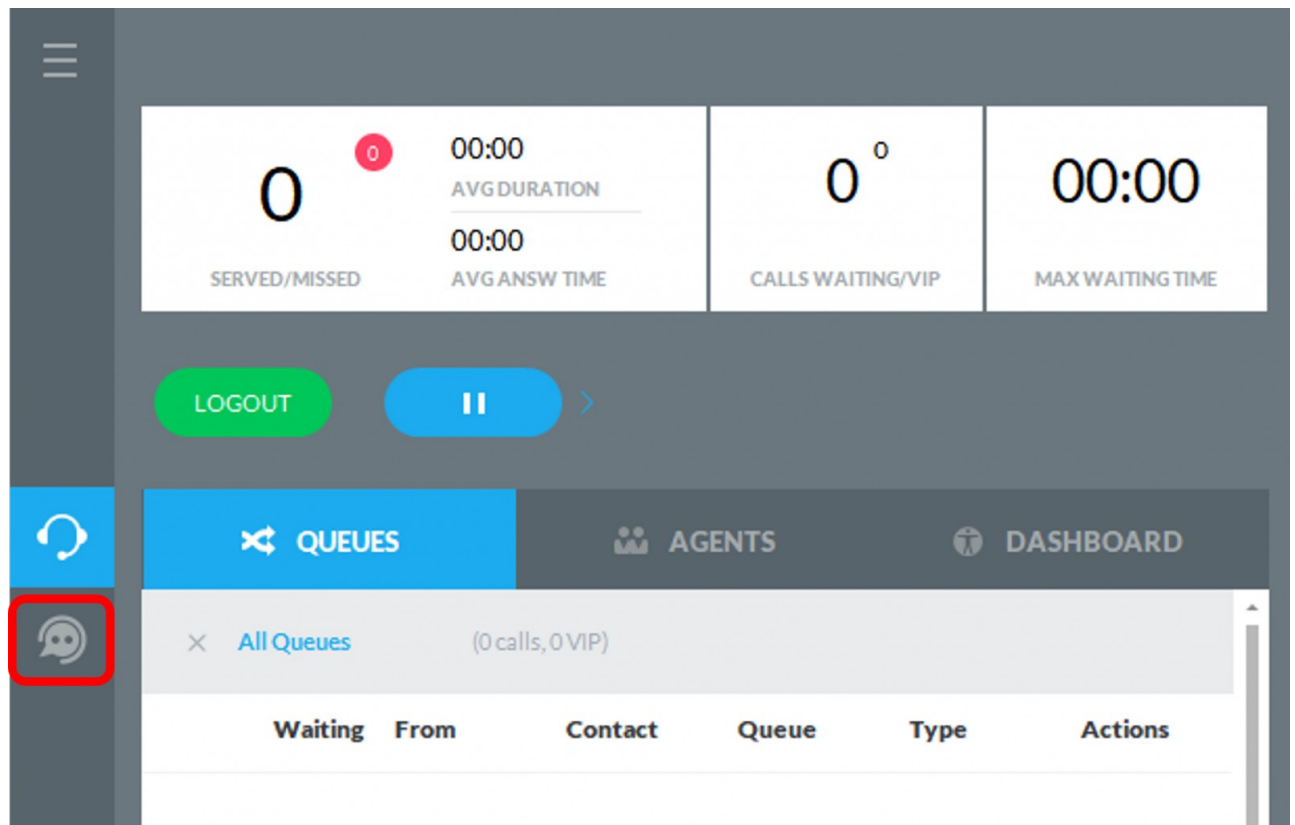
ConvAI integration - Chat feature

Requirements

- Cloud-connected Imagicle on-prem UCX Suite or UCX Cloud Suite ver. 2023.Spring.1 or newer
- Imagicle Attendant Console Enterprise or Professional client ver. 2023.Spring.1 or newer
- Imagicle Operator Essentials ver. 2023.Spring.1 or newer
- Proper Imagicle Conversational AI license

Chat Integration in Attendant Console

Starting from 2023.Spring.1 release, Imagicle Attendant Console clients include a new CHAT panel, selectable from left pane:



If you never enabled this feature, Chat button invokes a web page inviting the customer to start a ConvAI trial, by filling the request form. Once the form is submitted, please stay tuned. Imagicle Sales team will contact you to schedule a call to explain all features related to Imagicle Conversational AI.

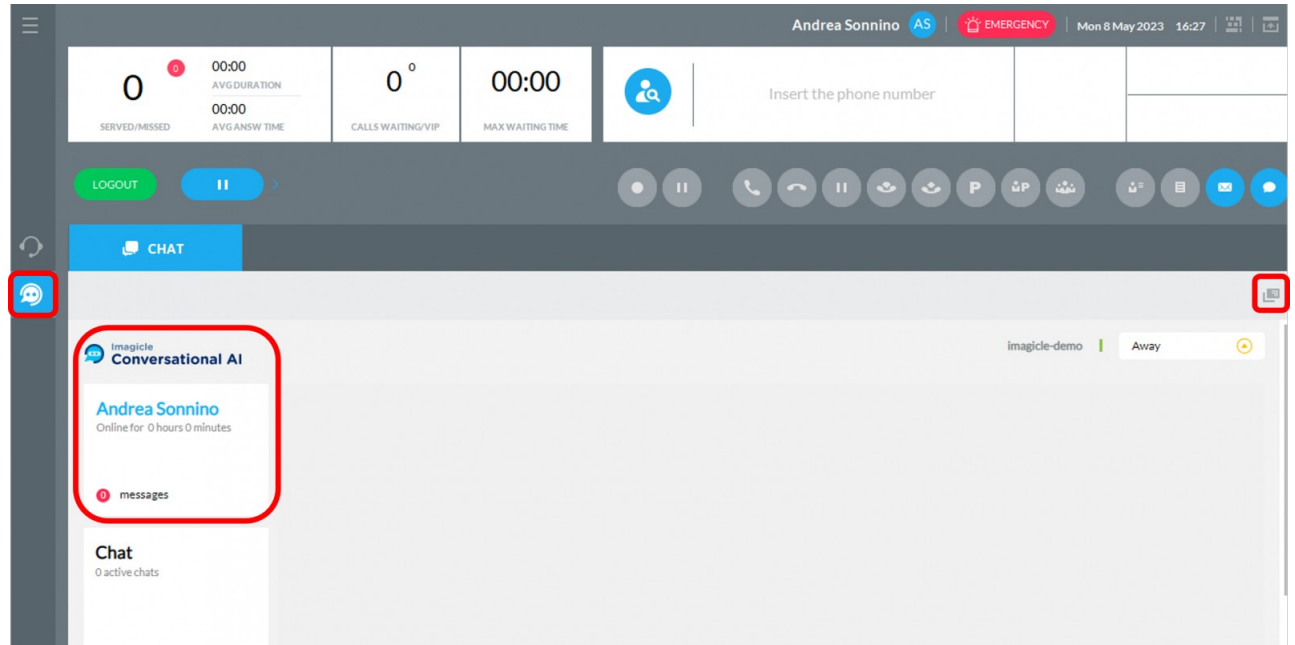
If otherwise you have purchased a ConvAI license, you can enable your operators for chat access by setting the "Conversational AI Username" in User's details:

Screen recording agent username	<input type="text"/>
Conversational AI	
Username	<input type="text"/>

Above field can be automatically populated upon a synch from an external source. Depending on your source, relevant field mapping is available in "Synch rules". See [here](#) for more details.

Chat usage

Once the operator is enabled, it is possible to click on Chat button to trigger the login to ConvAI and be ready to accept incoming queries coming from Whatsapp, FB, Telegram, web, etc. Please contact Imagicle Sales team for further details about available integrations.



As many other Attendant Console embedded panels, CHAT panel can be detached from main GUI and moved to a separate window, by clicking on "Detach" button available on top-right.

Product Configuration

Users list configuration

For each person who wants to run the Attendant Console, you need to create a UC Suite user in the users list with the following information:

- **Username:** required to login the console client if UC Suite local authentication is selected
- **Password:** required to login the console client if UC Suite local authentication is selected
- **First name and Last name:** useful to identify the agent
- **First Extension number:** this is the phone number controlled by the console client.
- **Console License Type:** available options are:
 - ◆ BOE = Desktop CTI client
 - ◆ BAP = Attendant Console Professional
 - ◆ BAE = Attendant Console Enterprise

The following information may be needed under certain conditions:

- **Active Directory username:** required if an Active Directory authentication is used. E.g. john.smith
- **Domain:** the fully qualified domain name, required if Active Directory authentication is used. E.g. imagicle.com
- **Device name: Cisco only** User's device name (SEPxxxxx, CSFxxxx, etc.). This is required if the first extension number of the user is a shared line (i.e. configured on multiple phone devices).

Warning: if the server is not able to control the user's primary extension through TAPI, or if the primary extension is not set, the user won't be able to access the client.

CTI configuration and device association on Cisco UCM

In order to work properly, Imagicle Attendant / CTI Server needs:

- To be able to control the user's phone primary line
- To be able to monitor the status of other telephones (Busy Lamp Field feature)

Such extensions must be monitored by the Attendant Console CTI Server through TAPI association. The procedure is detailed [here](#). Hence, in the PBX you need to associate to the UC Suite application user (*ImagicleCTI*):

- The device controlled by console client
- All devices you want to be monitored for BLF purposes

Note for Cisco users: only IP Phones running SCCP and SIP protocols are supported by the current version of the client. Analog devices are not CTI-enabled and therefore they can't be used.

Numbering Plan Parameters

Calls placed or received by Attendant Console are affected by the numbering plan parameters. Those are configured in the UC Suite server and could transform the calls calling or called number.

The following parameters affect the console client behavior:

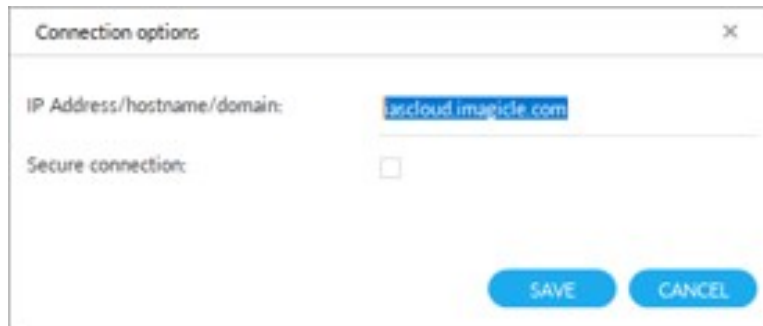
- **Internal Phone Number Patterns**
- **Outgoing Prefix**
- **Incoming Prefix**
- **Local country code**

Their meaning is described [here](#).

Attendant Console First Time Login

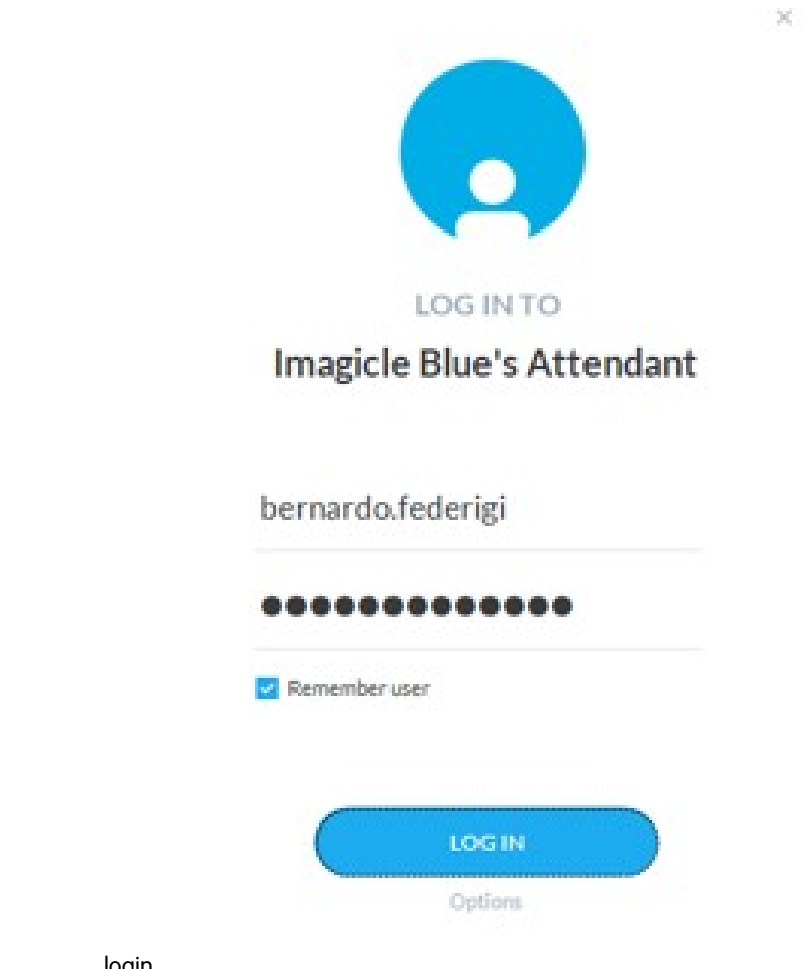
First time you launch Attendant Console client:

- The application prompts you to enter the FQDN or IP address of Imagicle UC Suite server. For HA environments, please enter Primary Imagicle Server's IP/FQDN
- Starting from 2021.Winter.1 release, a "Secure connection" flag is included. If selected, Attendant Console connects to UC Suite through a secure, TLS 1.2 encrypted TCP session on port 51235.



A screenshot of a 'Connection options' dialog box. It has a title bar with a close button. Inside, there is a label 'IP Address/hostname/domain:' followed by a text input field containing 'lancloud.imagicle.com'. Below this is a label 'Secure connection:' followed by an unchecked checkbox. At the bottom right are two blue buttons labeled 'SAVE' and 'CANCEL'.

- Once Connection options are saved, you are prompted to enter your user's credentials.
- If UC Suite is synched with Active Directory, you just have to enter your Windows login credentials
- Click on "Remember User" if you wish the application to store credentials for next



A screenshot of the 'LOG IN TO Imagicle Blue's Attendant' login screen. It features the Imagicle logo (a blue circle with a white stylized 'i') at the top. Below the logo is the text 'LOG IN TO' and 'Imagicle Blue's Attendant'. There is a text input field containing 'bernardo.federigi'. Below that is a password field represented by a row of 12 black dots. Under the password field is a checkbox labeled 'Remember user' which is checked. At the bottom is a large blue button labeled 'LOG IN'. Below the button is a link labeled 'Options'.

login

Digital Certificate requirements for encrypted connections (2021.Winter.1 and above)

Encrypted TLS 1.2 connection between Imagicle Attendant Console and UC Suite server(s) requires to use **trusted** Digital Certificates.

The certificate used to secure the communication channel between the Attendant Console client and the server is the same used by the WEB portal. Therefore, if you need to deploy a trusted certificate, follow the same instructions needed to [deploy a trusted certificate for the suite web portal](#).

Please find below the rules for a proper certificates deployment:

- If you set a FQDN name in Connection options:
 - ◆ Every Imagicle UC Suite node must have own Certificate, where Subject Alternate Name (SAN) should include the FQDN (wildcard is acceptable, to avoid different Certificates for different Imagicle HA nodes). More info [here](#).
 - ◆ If you decide to deploy a Trusted Certificate:
 - ◇ You don't have to install it on operators' workstations. Only on UC Suite node(s)
 - ◇ No additional actions required for both stand-alone or HA environments, leveraging [DNS SRV](#) or not.
 - ◆ If you decide to deploy a self-signed Certificate:
 - ◇ You must install it on both UC Suite node(s) AND operators' workstations.
 - ◇ No additional actions required for both stand-alone or HA environments, leveraging [DNS SRV](#) or not.
- If you configure an IP address in Connection options:
 - ◆ Any Digital Certificate, Trusted or self-signed, can be used.
 - ◆ No need to install it on operators' workstations.

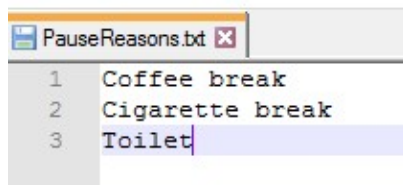
Pause Reasons

Imagicle Attendant Console supports the possibility for an operator to specify a pause reason, that can be selected among the ones configured by the Administrator.

In order to configure a pause reason, it is required to edit file "PauseReasons.txt", located in the <IAS_INSTALLATION_FOLDER>\Apps\QME\ Settings path. (Where <IAS_INSTALLATION_FOLDER> is usually c:\Program files(x86)\StonevoiceAS

NOTE. This file is empty by default and is subject to replication.

Reasons have to be specified in the file, one per line. Empty or space-only reasons will not be considered. In figure below, three pause reasons are configured.



There are three possible configuration scenarios:

- Empty configuration file (default):
 - ◆ No change of interaction on Attendant Console Clients or on the web
- Configuration file with only one reason specified:
 - ◆ No interaction changes on Attendant Console clients or on the web; when the agent sets himself in pause, the reason is displayed (see the following paragraphs for more details).
- Configuration file with more than one reason:
 - ◆ On Attendant Console Clients and on the web page when the agent wants to put himself in pause state, he must select from a menu one of the available reasons. The selected one will then be shown on screen (see the following paragraphs for more details)

Reasons can be added, changed or removed without having to restart the IAS services or Attendant Console Clients. Changes are available in the system within two minutes after the file editing.

Limitations

- Possible reasons are specified by the administrator by editing a configuration file. At the moment there is no GUI to edit this file.
- Reasons are not internationalized
- The motivation for a paused entry is not historicized, nor is there any reporting available.



Cisco Webex Calling MT Native Call Control - Imagicle Token Authorize

Requirements

- Imagicle UCX Cloud Suite, with activated subscription licenses
- Imagicle Attendant Console client ver. 2021.Summer.2 or above
- A Full Admin user belonging to Webex Calling customer organization, with a Webex Professional license.
- **Webex Calling Presence already enabled**, as described [here](#).

Limitations

- Only the primary line of a user can be controlled by Imagicle Attendant Console.

OAuth2 token for UCX Suite integration with Webex Calling Call Control

Customer must authorize Imagicle Webex Calling Integration application called **Attendant Console Call Control Connector** to access own Webex organization data. The following permissions are granted to the Imagicle Webex Calling Integration application:

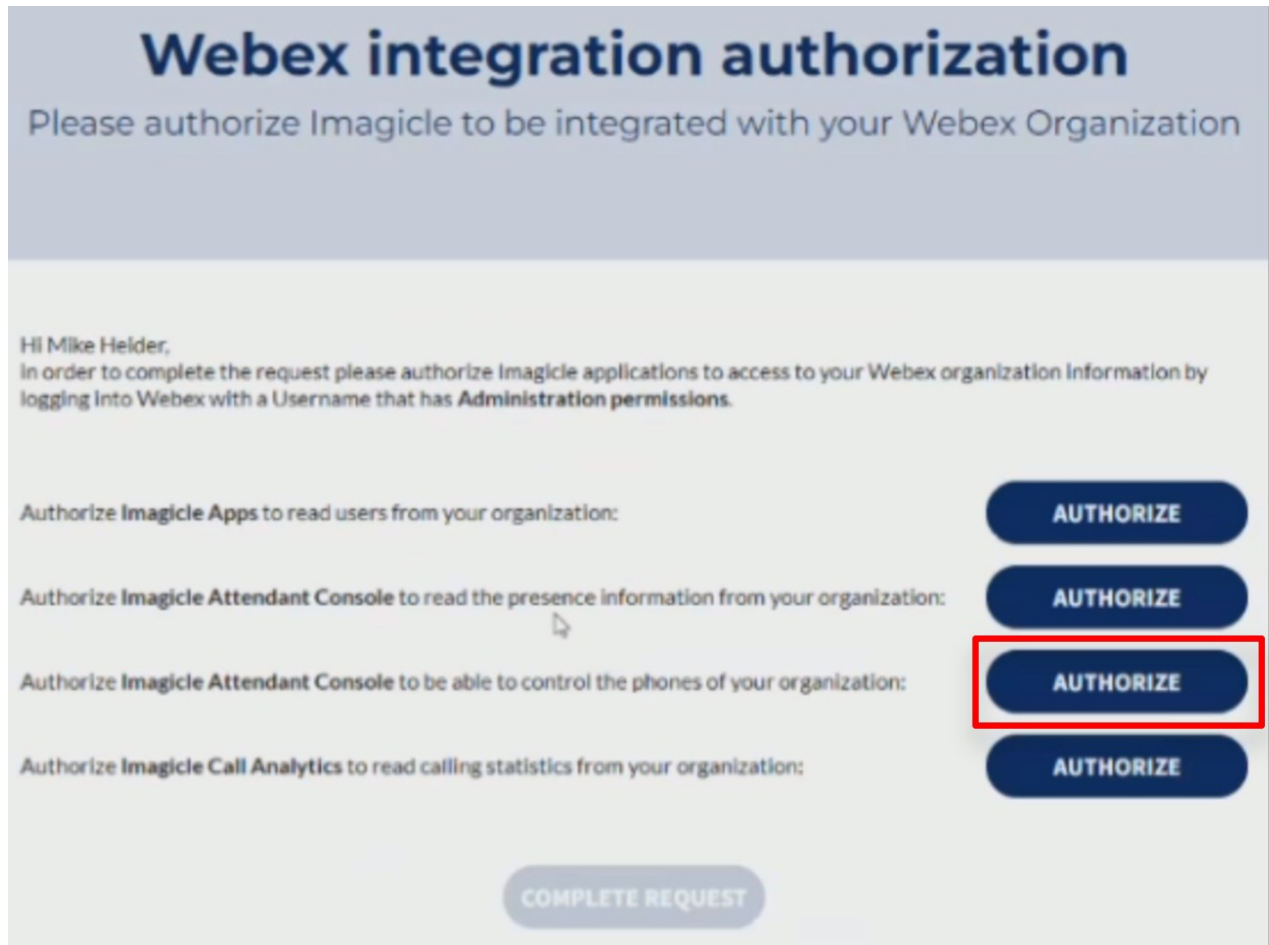
- spark-admin:people_read
- spark-admin:organizations_read
- spark-admin:xsi

These are the minimum permissions required to retrieve basic user information, read organizations information and to invoke the XSI API to perform the call control actions. Without granting such permission, Imagicle can't provide the feature.

Procedure

Please connect to the Imagicle [Onboarding Web Portal](#) for Webex Calling MT and enter customer's data, including above mentioned Full Admin Webex user with Webex Professional license.

Once customer data has been entered, please proceed to next page and authorize the following application highlighted in red:

The image shows a web interface for 'Webex integration authorization'. At the top, the title 'Webex integration authorization' is in a large, bold, dark blue font. Below it, a subtitle in a smaller, lighter blue font says 'Please authorize Imagicle to be integrated with your Webex Organization'. The main content area has a light gray background. It starts with a greeting 'Hi Mike Helder,' followed by instructions: 'In order to complete the request please authorize Imagicle applications to access to your Webex organization information by logging into Webex with a Username that has **Administration permissions**.' Below this, there are four authorization requests, each with a corresponding 'AUTHORIZE' button on the right. The first request is 'Authorize Imagicle Apps to read users from your organization:'. The second is 'Authorize Imagicle Attendant Console to read the presence information from your organization:'. The third is 'Authorize Imagicle Attendant Console to be able to control the phones of your organization:'. The fourth is 'Authorize Imagicle Call Analytics to read calling statistics from your organization:'. The third 'AUTHORIZE' button is highlighted with a red rectangular border. At the bottom center, there is a light blue button labeled 'COMPLETE REQUEST'.

Please note that other tokens might be required for users' synchron from Webex Control Hub and to retrieve presence status from Webex Control Hub. Please consult relevant KB articles.

Once you have authorized all required tokens, please click on "COMPLETE REQUEST" to trigger the Imagicle internal process to enable the tokens.

Remarks

Imagicle apps authorization requires Webex apps integrations to be enabled by default. If not, you might get the following error message:



Access denied

Your administrator denied access to the Integration you selected. We captured your request and will let them know.

Please consult [this troubleshooting article](#) for further details.

Monitored lines

Imagicle Attendant Console can monitor and control user's Primary Line. If same user is also associated to Virtual Lines, those are ignored.