imagicle

# 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 â System Parameters â 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):

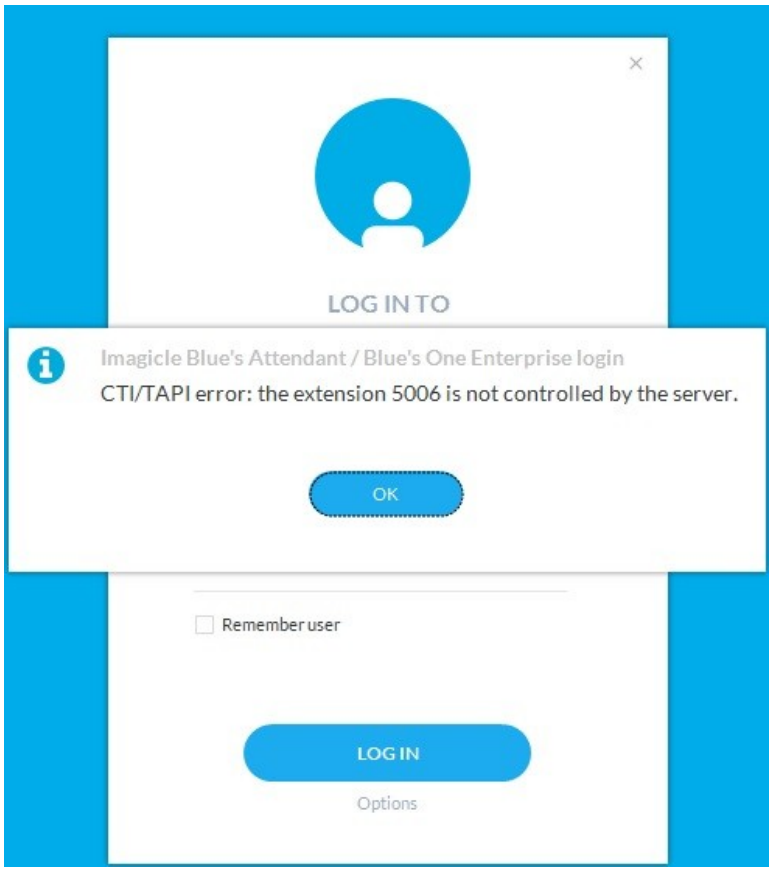
- Check related license type in **Admin â User Management**; in "Blue's CTI Server" section, "*Console license type (BOE,BAP,BAE)*" field should be populated with correct license.

## "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
TUFaLTVGNkFMQjIxGDAWBgNVBAoMD0ltYWdpY2xlIFMucC5hLjAeFw0yMTA5MDcx
NDQxMjhaFw0yNjA5MDYxNDQxMjhaMDQxGDAWBgNVBAMMD0VDMkFNQVotNUY2QUxC
MjEYMBYGA1UECgwPSW1hZ2ljbGUgUy5wLmEuMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEA4fE+tlRL3R1gsHbBOwRf8dlVW50025RV6Akl8k50vVrWGkGG
ny/8IFocq9grXgD5oTL+NH2/vmVvwNF2oMSuC2aU6fJwsb3fBDagCD219GENLXP0
GzX5rg0a2UgKU+93wFii+bUhYWUCPPsBO6UmAqPrnhzz1H2OSDXkVxb6HFGw0VIY
u7Aw4focrHnY6mAdjvDKw3EcnP7sH4Bkl91bLClAMP/EABjr71ViGiSS0WCXFTgn
lRntYdQ/btNk6UYOnJ8CjQkbnLWyYyp7JPY9cAPMiuwkc/B9BtGUj2AkqOEWiXQ2
XO9IVTj1TRTMh5UJw4DnTNjE9+dYC18fmDP1fwIDAQABMA0GCSqGSIb3DQEBBQUA
A4IBAQCyvwzoL9bNzFlJ88E6rog+cjKIlIkTBBJjNnJuxwGAXU3fvNj0RRkbbnrn
PdcSxiF36RV1cVXWEa280jA3j61VRiL/std80aSb6VsGHUdN0XqDg73liAgMdkAX
mscesISLcaUnCKl97Zgx5/QDx9BvJfHGpRIb0mR8ZYoWUQn7mvzuoNsKoqbkFSvb
dtaU5VFLcD7aR1rmM+dTRsIyyweMVe+7WV1RhC7ULncYu+XlmUXJshmkiDkUs1/m
/hGxiVaqRCl872UeZq1RE4ALZ8hjk92kGAhiuanydS1a1NGvCOi6P9s+XS49ZWK1
JNXRElEOaI8/+R4OeoV+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
MDIxCzAJBgNVBAYTAlVTMRYwFAYDVQQKEw1MZXQncyBFbmNyeXB0MQswCQYDVQQD
EwJSMzAeFw0yMTA5MDcxMjI2MzJaFw0yMTEyMDYxMjI2MzFaMCMxITAfBgNVBAMT
GGNhbmFscG9wYy5pbWFnaWNsZS5jbG91ZDCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAKfJt7vLwPFxlVqzzgKcYrzcfXOXuTcBvHRMLsw3mb46ZKCu3lbk
```

```
Tk0nupg3bMroR2ceGBi06pAU2yfx1ZWjuGvl7Q5XPUFMHqgXucoFQOGZBcSqxNzG
v3f1cXiOCcUXzpcFufTFNOT8th2I6v+6azfK2AqZcxKNgsPH45T2M4eUS+v0x96w
U/E4mRuYeLZU+lg/osextxUH7q8llC6vGvTz3cMWNaXPM4a4P+/dKy3QG2B1awmE
OWNH29LFkjWpuIU9KTVFw4+tZzHMxU5nXY7tOb2QJObpH5HSXOe2rfMmLTpnJKxb
pGvDuIAvOR71ZGW7USAwHq7KIqnqj5IpchUCAwEAAaOCApEwggKNMA4GA1UdDwEB
/wQEAwIFoDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwDAYDVR0TAQH/
BAIwADAdBgNVHQ4EFgQU8OQ+esHwMMNYgiZ3eJILYFDuMcMwHwYDVR0jBBgwFoAU
FC6zF7dYVsuuUAlA5h+vnYsUwsYwVQYIKwYBBQUHAQEESTBHMCEGCCsGAQUFBzAB
hhVodHRwOi8vcjMuby5sZW5jci5vcmcwIgYIKwYBBQUHMAKGFmh0dHA6Ly9yMy5p
LmxlbmNyLm9yZy8wYQYDVR0RBFowWIIbYWMtY2FuYWxwb3BjLmltYWdpY2xlLmNs
b3Vkgh9jYW5hbHBvcGMtcHVibGljLmltYWdpY2xlLmNsb3VkghhjYW5hbHBvcGMu
aW1hZ2ljbGUuY2xvdWQwTAYDVR0gBEUwQzAIBgZngQwBAgEwNwYLKwYBBAGC3xMB
AQEwKDAmBggrBgEFBQcCARYaaHR0cDovL2Nwcy5sZXRzZW5jcnlwdC5vcmcwggEE
BgorBgEEAdZ5AgQCBIH1BIHyAPAAdgCUILwejtWNbIhzH4KLIiwN0dpNXmxPlD1h
204vWE2iwgAAAXvAcFRCAAAEAwBHMEUCIBzfKFbMtUk+jrHo4y4sFSR6a5qK5Yy6
92VNkbBle/boAiEAoe5y8gmcpPg4CND2547/1shV8pSkuPfwyzJhtX5NTX8AdgB9
PvL4j/+IVWgkwsDKnlKJeSvFDngJfy5ql2iZfiLw1wAAAXvAcFRpAAAEAwBHMEUC
IQDxaUSYkuewNbxxTYwK9Ubm2zxVFvwUrXAcoDSng5f53gIgHvraHOiq2+mUdpIj
cFuUR0OpgCAJZ4aNVWMfjR8HOY4wDQYJKoZIhvcNAQELBQADggEBABkbq7ybst0Y
qnp+syq0MBYF0V/FrCcWudw2JW6yWIMxar4ic9XHTI7SNu9KqZmtwNf38HvJKk38
Vbg2we2OYIEx9+87anxsTqwfjfsgwyOXMBvfuY6M0TiAi8A5qSN5mXcpnvvhGINW
ZbW6DLt7ff4gh7L+wYEcp2+MhMPRsg/ovNZAoYAAZhz97GnnXTic42zia+vxtDna
CiyqvM17MXi3sLNnEaC6m5LRdcgehJzbaObrjlSaRv4bkjNSWfQeH3Wfc9/D4pnn
wlvpBoE93CTaNjLHM8/wtRrtKrEFTFfG+IGk26CCnUYHVHdiAfQ+c2gRNkKf7y6P
gjnyJ8GXHD0=
-----END CERTIFICATE-----

subject=/CN=uccs.imagicle.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