Presence Service Configuration

06 May 2024

imagicle

Table of Contents

Presence Service Configuration **1/14**
Imagicle Presence Service Configuration 1/14
Configuration for Microsoft Skype for Business Presence 6/14
Configuration for Microsoft Teams Presence 11/14

imagicle

Presence Service Configuration

Imagicle Presence Service Configuration

The **Presence** feature allows you to view the presence status of other users belonging to your organization. If a presence server is available, this service offers **rich presence status** and telephony presence status of your pbx phones. The Presence feature is available for all pbx and presence servers that support SIP/Simple presence (SIP SUBSCRIBE/NOTIFY - RFC 3265, 4662, PIDF/XML - RFC 3863).

Thanks to the Presence service you will be able to monitor the **presence status** of your colleagues in your Blue's Attendant Console, without the need of monitor all the phones via a CTI link. You'll also be able to monitor the **rich presence status** of your external contacts, when a suitable presence server is available.

Directly from your Attendant Console you can monitor:

- **Telephony status of internal contacts**, knowing if they are busy in a call
- **Rich presence status**, knowing if they are available, not to be disturbed or just out for a while. I.e. Available, Away and Custom status messages, that the users can set in their client

Imagicle applications can leverage the presence feature provided that appropriate configuration is made. See below.

Imagicle Notes

Imagicle Application Suite includes the **Notes** feature, that is an enhanced presence feature allowing to associate custom messages to an Application Suite user, directly from Imagicle Attendant client. This feature is useful to write a note on important information about a user, (e.g. if he is out of office for a long time or only for a day), saving time in trying to contact him. Notes are shared and aligned between all the Attendant users in real-time.

The Imagicle Notes feature is does not need any additional configuration.

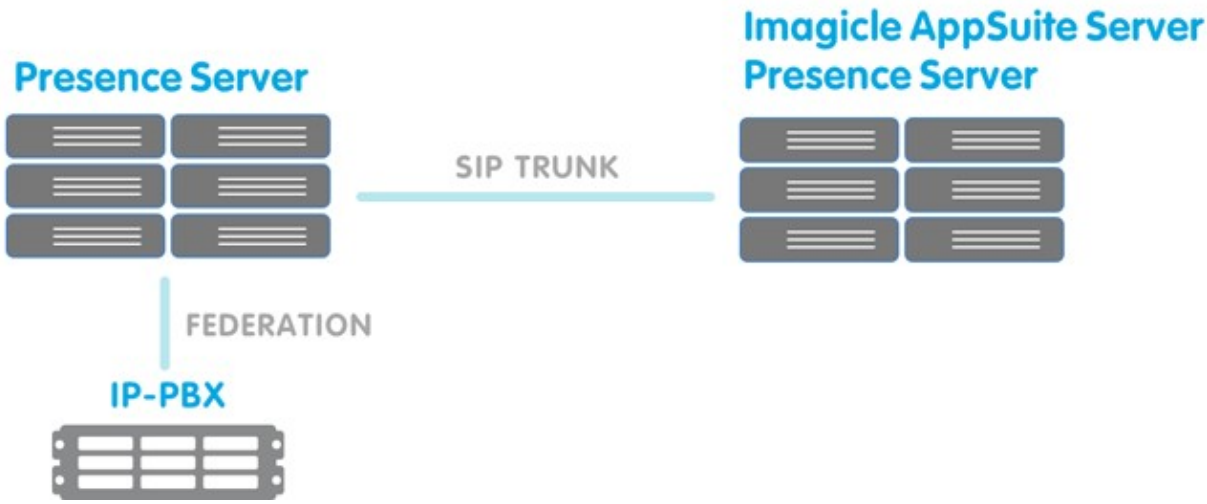
Note: Imagicle Notes on HA deployment has limited functionality. The content of the note is displayed to operators registered to a different node only after the next search.

Architecture

Imagicle Presence can work in two reference architectures:

- With an IP-PBX, that supports SIP/Simple Presence interactions and **No Presence Server**

- **With a Presence Server** that supports SIP/Simple Presence interactions. Presence Server can be federated with an IP-PBX, this means that it will work as gateway for presence subscription requests coming from Presence Server and directed to IP-PBX, e.g. phone status requests



Configuration

As usual, the configuration steps involve user settings and service settings.

User settings

Telephony presence works thanks to the First extension number. Rich presence requires a Presence server and need a SIP URI.

- **Without a presence server**: you need to fill the First Extension number of the users, and you only get telephony presence status
- **With a presence server**: you need to fill both the First Extension number and the SIP URI fields of the users, and you get telephony presence plus rich presence status

If you synchronize the users' list with an external source, such as the PBX or a LDAP server, you need to have the the SIP URI fields filled only if your architecture includes a presence server. If you get the presence status from the PBX, you can safely ignore the field.

Service settings - Sip Simple configuration

In order to configure Presence Service click on Admin -> Presence, Configuration tab.

Here you have to enable the presence services (flagging the checkbox causes Imagicle SIP Connector presence service to start) and enter the server address and protocol.

- **Without a presence server**: enter the IP address or FQDN of the PBX
- **With a presence server**: enter the IP address or FQDN of the Presence server (federated with the PBX)

Port and Protocol

By default, a connection will be attempted from the Imagicle Presence Service to the PBX or Presence serve towards port 5060. If the PBX or the Presence Server listen for connections on a different port, just fill the Server Address field in the format ip:port. E.g. 192.168.100.1:5070.

As protocol to use, choose between UDP or TCP, depending on which protocol is supported by your presence server or IP-PBX.

Credentials

While is mandatory to fill all the Credentials fields (because Imagicle Presence Service needs a user for sending SIP requests), depending on your presence server or ip-pbx this user or extension can be dummy. Usually, if the SIP connection requires authentication these fields need to be filled accurately, in other cases (e.g. if there is the possibility to configure a trusted SIP trunk

between Presence Server or IP-PBX and Imagicle Application Suite) it's possible to fill the field with dummy values such as presence@domain.com. Imagicle Presence Service diagnostic will warn you about not existing credentials but you can safely ignore the warning.

- **URI**: this is the SIP address of the entity used for presence monitoring.
  With presence server: it could be an ad hoc created user or extension in the format user@domain. E.g. imagicle.presence@imagicle.com.
  Without presence server: you can set it as EXTENSION@PBX-IP e.g. 1000@192.168.1.100.
- **Auth ID**: mandatory if your presence server requests authentication, in other case only set the first part of the URI field, e.g. imagicle.presence
- **Password**: mandatory if your presence server requests authentication, in other case leave empty
- **Domain**:
  With presence server: the domain of the presence server. E.g. IMAGICLE.COM
  Without presence server: the IP address or FQDN of the IP-PBX

How to configure more than one presence server

If you want to use more than one presence server at a time, and they are not federated, you must activate the connectors flagging the "enable" checkbox and configuring the parameters as described in the related sections.

Then you must choose the priority server in the "Preferred Presence Server" dropdown list at the top of the page. When conflicting presence information for a user is reaching the Application Suite, the presence status supplied by the priority server will be displayed.

Diagnostics

This page is intended for service monitoring, and it could be useful after first configuration, to check Sip Connector Status and try to subscribe a user, making an exhaustive test on configuration.
Note that page is not auto refreshing, so after user subscription it could be necessary to wait some seconds to obtain all the information. Use the **reload** button on the top of the table if the presence status has not changed after a while.

Connector Status

In the Diagnostics Tab you can check the status of the SIP Presence Connectors.

Possible values are:

Negative

- **Server Not configured**: Service enabled but not yet configured, go to Configuration tab to complete the configuration
- **Disabled**: Service is disabled, go to Configuration tab to enable it
- **Forbidden**: Access denied, check the credentials entered and if your presence server is accessible by Imagicle Application Suite server
- **ConnectionError**: Presence Server is unreachable, this could be due to a network error or a wrong address configuration

Positive

- **UpAndRunning** (Successfully connected): Service is active, you can monitor presence
- **Credentials entered not found**: Service is active, credentials you entered has not been found, but this could not be a problem, you should be able to monitor presence

Users list with presence status

The following table contains the list of configured Imagicle Application Suite users and shows the following columns:

- **User**: username of Imagicle Application Suite user and user's Imagicle Note, if existing.

- **Rich Presence**: rich presence status of the user and associated custom message. If the page shows a warning such as "User not configured or not enabled for this type of presence" this means that the user field *sip uri* has not been populated.
- **Telephony Presence**: telephony presence status of the user.
  In this field you can monitor the telephony status of a user. The information can come from the TAPI link or from the SIP Presence Connector, or both. In the case that both information are available, system gives priority to TAPI information.
  If the page shows a warning such as "User not configured or not enabled for this type of presence" this means that the user field "First extension number" has not been populated.
- **Action**: possible actions for the user. You can subscribe to a user presence if nobody has requested to subscribe it before. After one minute the subscription is automatically removed.

Filters

The diagnostic page lets you filter the user list by **User**, **Rich Presence and Telephony Presence**.

This is the meaning of the Presence modes, as displayed for diagnosting, also available for filtering.

Standard:

- **Available**
- **Busy**
- **Do not disturb**
- **Offline**
- **Forwarded to voice mail**: when the user's phone is diverted to a user's voicemail number or to the voicemail pilot
- **Forwarded to phone number**: when the user's phone is diverted to any other number

Error:

- **Access denied**: there is no SIP access to presence server
- **Error**: there have been an error, it could be a temporary network down
- **Not Found**: presence server replied with a Not Found, so field in sip uri could be incorrect or not configured on presence server

Service status:

- **Not requested by anyone**: there are no request for this user
- **Requesting**: request has been sent, but answer hasn't't arrived yet
- **Server not configured**: somebody requested the user presence, but Imagicle Presence Server has not been configured yet

Notes:

- The *DND* status overrides the *Forwarded* status
- The *Forwarded* presence status overrides the *Available* and *Occupied* status. That is, when an IP phone is diverted, the status is always *Forwarded* regardless it is free or in busy. The TAPI details are always displayed
- The voicemail pilot is recognized by the IP telephony settings. If you are using a third party voicemail (e.g. Cisco Unity) you must enter it's pilot number in the Admin -> System Parameters -> IP Telephony Parameters web page. The users' voicemail number must be configured in the users list
- If you make changes to the users' voicemail numbers or to the voicemail pilot number, you have to restart the Presence Server to make IAS correctly evaluate the presence status

Manage Services

This page allows administrators to monitor the status of the Presence Services. There are two services involved in the Imagicle Presence feature:

- **Imagicle Presence Server**: the main service that collects and aggregates all the presence information and provides them to the services that need them. If this service is stopped, no Presence information as available. This service automatically starts the TAPI connector service

- **Imagicle Presence SIP/SIMPLE Connector**: this service connects and gets presence information from the Presence server (or ip-pbx that supports SIP/Simple protocol). If this service is stopped, rich presence information won't be available.

Configurations changes are immediately loaded by the services and, usually, there is no need to restart them. Specific issues can be fixed stopping and starting the services. E.g. if the SipSimple status in diagnostic page it's "Error" for all users, try restarting the Imagicle Presence SIP/SIMPLE Connector.

Presence server configuration (SIP generic version)

Create a trunk between Imagicle Application Suite and the Presence Server or IP-PBX. If this trunk requires SIP authentication, create an ad-hoc user and configure the Presence Service as described above.

imagicle

Configuration for Microsoft Skype for Business Presence

Architecture

Imagicle Presence Service connects directly to Microsoft Lync / SfB Frontend Service through Microsoft UCMA API.

Requirements

- Imagicle presence service is compatibile with Microsoft Lync 2010 server and above (Skype for Business server).
- Connection to Microsoft Lync / SfB requires Windows Server 2008 R2 64 bit or better (32 bit not supported).

Configuration Task List

The main configuration steps are:

1. Choose the EndPoint type
2. Configure Microsoft Lync/Skype for Business Server
3. Configure Imagicle AppSuite Server
4. Configure Imagicle Presence Service

Choose EndPoint Type

An UCMA application can connect to Microsoft Lync / SfB in three different modes, that have different requirements. Here they are, ordered from the quicker to setup to the slower:

- User End Point without Secure TLS Connection
- User End Point with Secure TLS Connection
- Trusted Application End Point (manually provisioned)

User End Point without Secure TLS Connection

In this mode, Imagicle Presence Service impersonates a standard Microsoft Lync / SfB user to queries for other users' presence. Hence, a Microsoft Lync / SfB user is required to be created specifically.
This mode doesn't require the Imagicle Application Suite to be been joined to the Microsoft Lync / SfB Server domain.
This mode uses a non-secure SIP connection.

User End Point with Secure TLS Connection

It's like *User End Point without Secure TLS Connection*, except that a secure TLS SIP connection to Microsoft Lync / SfB Server is used. So you need to install a Web Server certificate from the network Certification Authority (see below).

Trusted Application End Point (manually provisioned)

In this mode, Imagicle Presence Service does not represent an individual user, hence it is not required to create a dedicated Microsoft Lync / SfB user. A secure TLS SIP connection to Microsoft Lync / SfB Server is used. You need to to install a Web Server certificate from the network Certification Authority (see below). On the other hand, it's mandatory to join the Imagicle Application Suite to the Microsoft Lync / SfB Server domain.

Microsoft Lync / SfB Configuration

User End Point without Secure TLS Connection

The configuration task list is:

1. Create an ad-hoc user on Active Directory
2. Enable user on Microsoft Lync / SfB Server
3. Enable non secure standard SIP port on Microsoft Lync / SfB Server:
   On a Microsoft Lync / SfB Server node, open "Lync / SfB Server Management Shell" and execute the command:

```
Set-CsRegistrar "registrar:fqdn-registrar.domain" -SipServerTcpPort 5060
```

4. Ensure that port 5060 of Microsoft Lync / SfB Front End Server is reachable via TCP from the Imagicle Application Suite server

User End Point with Secure TLS Connection

The configuration task list is:

1. Create a dedicated user on Active Directory
2. Enable the user on Microsoft Lync / SfB Server

Application End Point (manually provisioned)

A trusted application requires an entry in the Microsoft Lync / SfB Server topology document that specifies the computers on which the application runs. The main steps to configure Microsoft Lync / SfB Server are:

1. Create a Trusted Application Pool for Imagicle Server
2. Create a Trusted Application for Imagicle Presence Service
3. Enable modification to the topology

On a Microsoft Lync / SfB Server node open the "Lync / SfB Server Management Shell" and execute all commands explained in this section.

Create a Trusted Application Pool for Imagicle Server

First of all, the Imagicle Server must be configured as a Trusted Application Pool server within Microsoft Lync / SfB topology. You can skip this step if you have already configured a Trusted Application Pool to activate Queue Manager Enteprise integration.
To check whether a Trusted Application Pool already exists for Imagicle server, execute command:

```
Get-CsTrustedApplicationPool -Identity fqdn-ImagicleApplicationServer
```

If you get an error, the Trusted Application Pool does not exist. You can create it executing the following command (pay attention to adjust the FQDN of Front End node):

```
New-CsTrustedApplicationPool -Identity fqdn-ImagicleApplicationServer -Site site-ImagicleApplicationServer -registra
```

Create a Trusted Application for Imagicle Presence Service

To configure Imaigcle Presence Service as a Trusted Application within Microsoft Lync / SfB, execute the following command:

```
New-CSTrustedApplication -ApplicationId ImagicleLyncConnector -TrustedApplicationPoolFqdn fqdn-ImagicleApplicationSe
```

This will return a result similar to:

```
Identity: fqdn-ImagicleApplicationServer/urn:application:imagiclelyncconnector
ComputerGruus: {fqdn-ImagicleApplicationServer sip:fqdn-ImagicleApplicationServer@youtdomain..uu;opaque=srvr:imagicle
ServiceGruu: sip:fqdn-ImagicleApplicationServer@yourdomain..uu;opaque=srvr:imagiclelyncconnector:atifA-VpOFO2x9rrBUE
Protocol: Mtls
ApplicationId: urn:application:imagiclelyncconnector
TrustedApplicationPoolFqdn: fqdn-ImagicleApplicationServer
Port: 14001
LegacyApplicationName: imagiclelyncconnector
```

Copy the **ServiceGruu** paste into a temporary text file - this will be required later, in step "Presence Service Configuration".

Enable modification to the topology

To apply all above modifications, execute command:

```
Enable-CsTopology
```

Imagicle Server Configuration

Imagicle server needs to be configured once, through these steps:

1. Instal UCMA Runtime 3.0
2. Join Active Directory Domain (only when using Trusted Application End Point)
3. Install Web server Certificate (only when using a secure SIP connection)

Install UCMA Runtime 3.0

Imagicle Presence Service with Microsoft Lync / SfB integration needs Microsoft UCMA **version 3.0** runtime to run. You must download it from www.imagicle.com/go/UCMA and install it on Imagicle Application Server.

Note: Microsoft UCMA version 3.0 is compatible with Microsoft Lync 2010, 2013 and SfB 2015.

Note: while Presence integration requires UCMA 3.0, QME integration with Microsoft Lync / SfB requires UCMA 4.0, that does not replace UCMA 3.0. So, if you plan to use both QME and Presence, you have to install first UCMA 4.0 Runtime, then UCMA 3.0 Runtime.

Join Active Directory Domain

If you have planned to configure Presence integration as Trusted Application End Point, Imagicle Server must be joined to the Microsoft Lync / SfB Server domain.

Install a Web server Certificate

If you have planned to configure Presence integration to use secure connection to Microsoft Lync / SfB Front End Server (i.e. if you have choosed either *User End Point with Secure TLS* or *Trusted Application*), you have to get a Web Server certificate from the network Certification Authority and install it as a computer certificate on the Application Suite server.

Certificate enrollment

1. Log in to the Imagicle Application Server as an administrator with permission to *Enroll for a Web Server Certificate* (e.g. a Domain Administrator)..
2. Click the **Start** button, then **Run**, type **cmd.exe**, right click over **Command Prompt** and click on **Run as administrator**
3. In the Command prompt shell, type **mmc.exe**.
4. Open the **File** menu and select **Add/Remove snap-in**.
5. In the Add or Remove Snap-ins window, select **Certificates**, and click **Add**.
6. Choose **Computer Account**, and click Next.
7. Choose **Local Computer**, and then Finish.
8. Click OK on the Add or Remove Snap-ins window.
9. Expand **Certificates**.
10. Expand **Trusted Root Certification Authorities** and click **Certificates**. Make sure the root certificate is present for the Enterprise Certificate Authority in the domain.
11. Right-click Personal and select All Tasks, then **Request New Certificate**.
12. Click Next.
13. If prompted to select a Certificate Enrollment Policy, select one under the category of Configured by your administrator. Click Next.
14. Select **Web Server** (If Web server is unavailable see the WebServer certificate section), and click the link for *More information is required to enroll for this certificate*. Click here to configure settings.
15. Click the **Subject** tab.
16. For Microsoft Lync Server 2010/2013/SfB:
    1. Under the Subject Name section, change the **Type** to Common Name, and change the **Value** of the Fully Qualified Domain Name of the Microsoft Lync / SfB Server Pool (e.g. sfb.mydomain.com), and then click **Add**.
    2. Under the **Alternative Name** Section, change the Type to **DNS**, and change the **Value** to the Fully Qualified Domain Name of the Microsoft Lync / SfB Server Pool (e.g. sfb.mydomain.com), and then click **Add**.
    3. Again, under the Alternative Name Section, leave the Type specified as DNS, and change the **Value** to the Fully Qualified Domain Name of the server hosting the Imagicle Application Suite (e.g. ias.mydomain.com).
    4. Click Add.
17. Click the General tab.
18. Type **OCSConnector** for the Friendly Name, then click Apply, and OK.
19. On the Certificate Enrollment window, click Enroll.
20. Verify that the **STATUS** is Succeeded, and click Finish.

WebServer certificate

If there is no available WebServer certificate, you have to create it.

1. On the CA computer, click **Start**, type **certtmpl.msc**, and then press ENTER.
2. In the contents pane, right-click the **Web Server** template, and then click **Properties**.
3. Click the **Security** tab, and then click **Add**.
4. Click **Object Types**
5. Flag **Computers** checkbox
6. In **Enter the object names to select**, type the name of Imagicle Application Suite Server, and then click **OK**.
7. In **Permissions**, click **Enroll** under **Allow**, and then click **OK**.

Imagicle Presence Service Configuration

Please configure the users properties as described in the Imagicle Presence Service configuration section of this guide.

Login into Imagicle Application Suite web portal with global administrative privilege. Go to *Administration*, *Presence* web page, select *Configuration* tab and then:

- **Enable rich presence services (Microsoft Lync / SfB based)** by flagging the checkbox
- Select the End Point of your choiche

User End Point Configuration

Fill all the following fields:

- **Microsoft Lync / SfB Server Address:** FQDN of Microsoft Lync / SfB Front End server
- **Use TLS:** flag if connection with Microsoft Lync / SfB Server is Secure SIP (needs a valid certificate released by the network Authority - see above)

Credentials

Fill the following fields with credentials of the ad-hoc created user (see paragraph "*Microsoft Lync /SfB Configuration - User End Point*"):

- **Username:** enter the username of the ad hoc created monitoring user
- **URI:** enter the sip address of the ad hoc created user, in the format user@mydomain.com. E.g. imagicle.presence@imagicle.com
- **Password:** enter the password of the ad hoc created monitoring user
- **Domain:** enter the domain of the presence server e.g. IMAGICLE.COM

Application End Point Configuration

- **Microsoft Lync / SfB Server Address:** enter FQDN of Microsoft Lync / SfB Front End server
- **Application Contact URI:** enter an existing Lync / SfB SIP URI (e.g. Lync / SfB_administrator@yourdomain.com)
- **Application Gruu:** enter the **ServiceGruu** value returned by New-CSTrustedApplication command
- **Certificate Name**: enter the Friendly Name of the certificate installed on Imagicle server
- **Application Host**: check that matches value used for **Identity** parameter in **New-CsTrustedApplicationPool** command
- **Application Port**: check that matches the **Port** value returned by **New-CSTrustedApplication** command

imagicle

Configuration for Microsoft Teams Presence

Requirements

- Imagicle UCX Suite rel. 2021.Spring.1 and above
- Imagicle UCX Cloud Suite is in place, or an online-activated Imagicle UCX Suite reaching Imagicle Cloud through TCP port 443
- A user belonging to the customer organization, enabled to login Microsoft 365/Microsoft Teams without MFA. Preferably, use a dedicated service account whose password does not expire (see remarks below).

Feature Description

Imagicle UCX Suite includes a cloud-based integration to interact with Microsoft Teams cloud.

To accomplish this integration, Imagicle developed in own Cloud a multi-tenant Azure Enterprise Application called **Teams connector for Imagicle UCX Suite**, with the purpose of collecting presence and CTI information on behalf of the customers' tenants. To authorize Imagicle to retrieve such data, customers must grant Imagicle Enterprise Application a specific set of permissions and generate a valid OAuth 2 token. The set of needed permissions are the following:

- Presence.Read.All
- User.ReadBasic.All
- offline_access

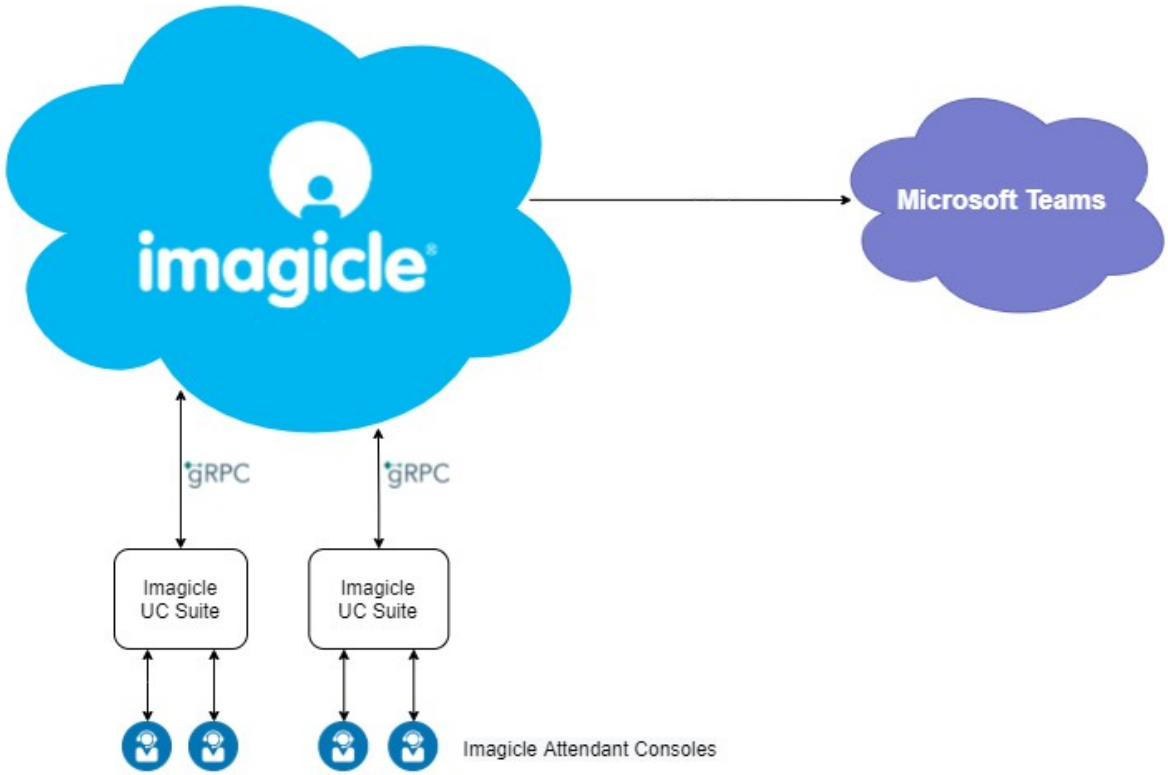
Architecture

Imagicle Attendant Console operators registered to Imagicle UCX Suite subscribe to the Rich Presence status events of their colleagues, supplied by their own Imagicle UCX Suite instance. This request is in turn converted to a gRPC session (https) to this Internet URL: **https://grpc.imagicle.com**, corresponding to an Imagicle Cloud presence service.

If required, a Proxy can be configured to allow reaching above URL. See here for more details.

Once gRPC session is initiated by Imagicle UCS, presence subscription requests are collected by the Teams Presence Service in Imagicle Cloud and subsequently they are sent to Microsoft Teams Cloud, leveraging MS-Graph APIs.

Below schematic depicts whole communications routing:



On-prem UCX Suite Settings

To enable MS-Teams presence integration, some parameters must be configured within the following setting file:

C:\Program Files (x86)\StonevoiceAS\Apps\Presence\Settings**Presence.ini**

- **MSTeamsPresence.Enable=1**
  This parameters allows to enable/disable MS-Teams presence retrieval. Please set it to 1. Default value is 0.
- **RichPresence.WinningTechnology=MSTeams**
  This parameter defines the Rich Presence technology priority while assigning and showing presence status on Attendant Console. For MS-Teams priority, please set this parameter to MSTeams. Default value is SipSimple.

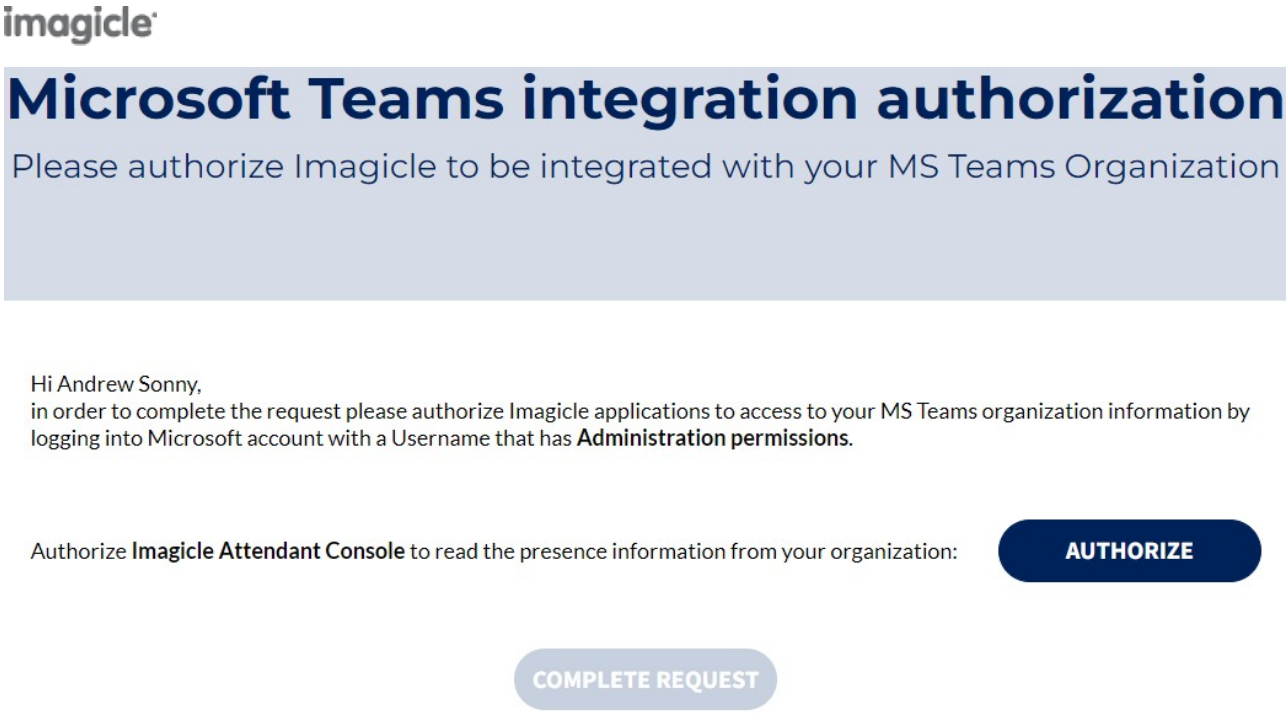
Users' Settings

MS Teams users are identified by their UPN, whose URI string should be included into **Rich Presence Microsoft URI** user's field, manually populated or automatically set upon a synch against Azure AD or any other external source.

Microsoft Tenant Authentication

To allow Imagicle Cloud to retrieve the Microsoft Teams presence status of company users, customer needs to connect to the Imagicle Onboarding web page, compile the form with own MS-Teams tenant data, including the email account of a FULL ADMIN MS-Teams user. Once the form is submitted, customer is invited to AUTHORIZE the presence acquisition and subsequently log in to own Microsoft tenant.

The Microsoft user authorizing the application must grant above mentioned permissions for its tenant, even if she/he is not a Microsoft tenant administrator. Please make sure that above user's authentication does not leverage Multi-Factor Authentication (MFA). If that's the case, you need to add an exclusion in "Conditional Access policies", as explained in this Microsoft article.



If the presence authorization is successfully accomplished, the blue button turns to green and you can COMPLETE REQUEST.

Presence Update Notes

When user turns off MS-Teams client (or turns off own PC), the client does not update Microsoft Cloud about its status change to **Offline**. This is reflected to Attendant Console rich presence display, which keeps on showing the client in its latest known status for some minutes (variable), eventually changing to:

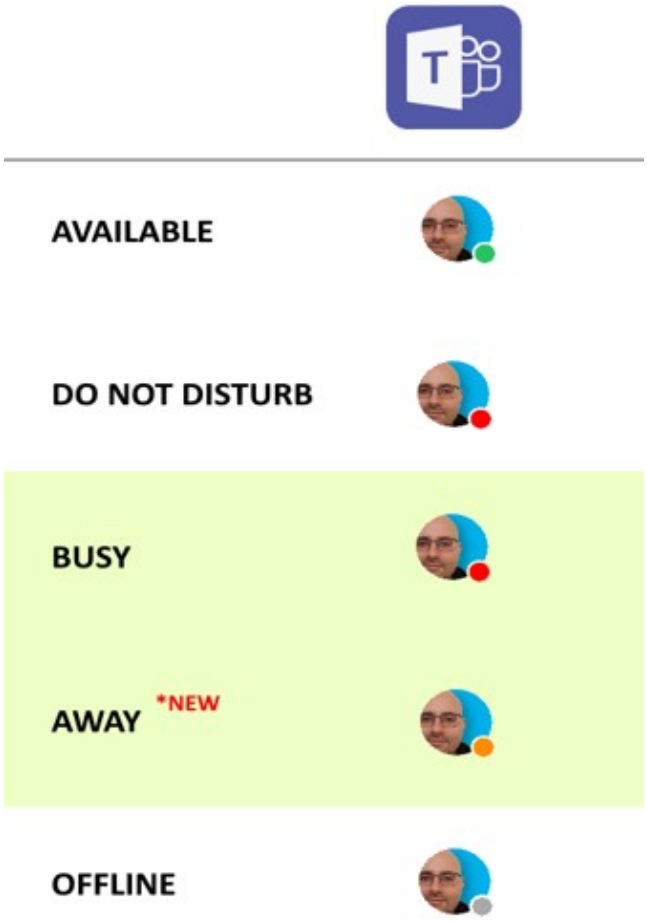
- Available â AvailableIdle
- Busy â BusyIdle

After a further variable time interval, rich presence status turns eventually to Offline.

Both above temporary status are also displayed on other MS-Teams clients.

Presence Icons on Attendant Console

Imagicle Attendant Console client for Microsoft UC includes specific presence status for MS-Teams, identified by different colors. See below screenshot sample:



Â«AwayÂ» status is shown in Orange and Â«busyÂ» status in Red. Please note that these two presence status are shown in different way, while using other calling platforms.