

# Main Configuration

05 May 2024



## Table of Contents

<b>Main Configuration</b> .....	<b>1/35</b>
<u>Configuring the Framework</u> .....	1/35
<u>Licensing</u> .....	2/35
<u>Accessing the Web Interface</u> .....	8/35
<b>System Parameters</b> .....	<b>10/35</b>
<u>Outgoing Email Shared Parameters</u> .....	10/35
<u>Microsoft OAuth2 Authentication for email sending</u> .....	14/35
<u>Numbering Plan</u> .....	25/35
<u>Users Authentication Settings</u> .....	26/35
<u>Proxy settings</u> .....	27/35
<u>Imagicle Cloud services authentication data</u> .....	29/35
<u>Web Server setting</u> .....	31/35
<b>Monitoring</b> .....	<b>33/35</b>
<u>Monitoring service configuration</u> .....	33/35

## Main Configuration

### Configuring the Framework

All the application of the suite are installed and updated through one single package.

The applications of the Suite are built upon a common framework. They share the User Management and some common setting. After installation of the package, you have to configure some general parameters which are shared between the applications, such as the PBX IP address or the email parameters. Then create the user's list and configure the applications you want to evaluate or activate.

The Application Suite can be configured through a web based interface. It has to be properly configured by these simple tasks:

- Configure the parameters common to all applications: PBX settings, Email settings, Numbering Plan parameters
- Configure the list of users, which can be edited manually, imported from a file or synchronized via LDAP
- Setup specific parameters for each application, as described in each application section
- Configure the PBX
- Configure CTI on the PBX (CTI controller). This may not be needed by all the applications
- Start the services through the web interface
- Activate the licenses. No license is needed during the evaluation period

## Licensing

**Admin** **Licenses** web portal menu shows the list of the available applications and if they are licensed, in evaluation mode, permanent mode or if the licenses are expired.

### Evaluation period

After the first installation/deployment, each application runs for 30 days in evaluation mode.

Evaluation may be extended upon request to Imagicle Sales department.

### License Activation

Starting from Imagicle 2019.Summer.1 release, we have added a brand new cloud-based activation method, using an "Activation Token" generated by Imagicle Cloud portal. The existing "offline" activation method", based on "Request String" + "Response Strings" is still available for backward compatibility.

In the following paragraphs, we are describing both methods, starting from most recent one.

### Cloud Licensing (available from Imagicle 2019.Summer.1 release)

Cloud-based activation method requires IAS server to reach a specific Internet URL: <https://api.imagicle.com>

If Internet access is controlled by a Proxy Server, then please make sure that it allows a transparent connection to above web URL (i.e. tunnel), **not** using "Decrypt and Scan" mode. Proxy configuration instructions are available [here](#).

Test Cloud Connection:

Open a browser in Application Suite Server and go to <https://api.imagicle.com/test> this message confirms the correct connection to our Cloud.

```
{
  "message": "successfully connected!"
}
```

From Imagicle web portal Admin **Licenses**, it's possible to view current licenses status. See below sample:

#### Imagicle ApplicationSuite activation

Activation mode *Offline*

PRODUCT NAME	QUANTITY	METRIC	LICENSE TYPE	CARE TERM DATE	TERM DATE	LICENSE STATUS
Blue's Attendant Professional	12	clients	Trial	-	19/07/2019	Expiring
Blue's One Enterprise	2	clients	Trial	-	19/07/2019	Expiring
Call Recording	22	channels	Subscription	-	26/07/2019	Expiring
Billy Blue's 4	100	extensions	Perpetual	-	-	Licensed
SSAM Professional		channels	Subscription	-	02/05/2019	Expired
Hotel Link		rooms	Unknown	-	-	Invalid

For every license, the following information are included:

<u>Column Name</u>	<u>Content Description</u>
PRODUCT NAME	Application name
QUANTITY	License volume
<u>METRIC</u>	License based on " <u>channels</u> " or " <u>Clients</u> "
LICENSE TYPE	License type <sup>1</sup>
CARE TERM DATE	<u>Imagicle CARE expiring date</u>
TERM DATE	License <u>expiring date</u>
LICENSE STATUS	License <u>activation status</u> <sup>2</sup>
LICENSE CODE	License ID code. <u>Included for older, offline activations</u>

## Ã¹ License Type

Supported IAS license types are:

- Perpetual: never expires
- Subscription: it expires, depending on annual subscription
- Evaluation: trial license for evaluation purposes, expiring in 30 days from deployment
- Unknown: Wrong or not recognized license

## Ã² License Status

Each license is associated to own status:

- Licensed: active license
- Expiring: trial or subscription license, expiring within 30 days
- Expired: trial or subscription license, already expired
- Invalid: invalid license code

Perpetual licenses never expires.

Licenses web page shows offline/online activation mode. If that's a brand new IAS, this information is not shown. Moreover, for each node, the following data is shown:

- Node ID
- Customer name
- Customer ID

If you are updating a IAS with a release older than 2019.Summer.1, some of above information are not available and subsequently not displayed. See below:

### Application Suite activation

Activation mode **Offline**

### Node: Massarosa

Customer Name: **Imagicle S.p.a**  
 Customer ID: **002902927**

## First time activation

From "Licenses" web page, please click on **Activate Now** button to initiate the license activation procedure. You are immediately prompted to select desired activation mode:

- **Online Activation:** Self-service activation through Imagicle cloud service
- **Offline Activation:** Offline activation, through Imagicle Delivery team

### Online Activation

It requires an "Activation Token", generated from [Imagicle Cloud licensing portal](#). Please make sure you have received a "Smart Account" from Imagicle, otherwise you can request it from above Imagicle Cloud portal.

Once you have the token, pls. enter it in the relevant field "Activation Token". Hit **Save** to enable licenses or **Cancel** to go back to initial license screen.

**Imagicle  
Cloud Licensing**

A new way to make the assignment and management of Imagicle licenses faster, smarter and easier.

FIND OUT MORE



Online Activation

**Activation token**

0d88e0d51a76a04929b8d7cb78b467e38ffea05d6eea6cb0b848c5a773054936

If activation is successful, you are redirected to initial license page, which now shows:

- ActivationMode: **Online**
- A **Change** button which allows to change activation mode or add/remove licenses by updating the Activation Token.

### Application Suite activation

Activation mode **Online**

#### Node: Massarosa

Customer Name: **Imagicle S.p.a**  
 Customer ID: **002902927**

PRODUCT NAME	QUANTITY	METRIC	LICENSE TYPE	CARE TERM DATE	TERM DATE	LICENSE STATUS
Blue's Attendant Enterprise	5	clients	Trial	-	09/08/2019	
Blue's Attendant Professional	5	clients	Trial	-	09/08/2019	
Blue's One Enterprise	25	clients	Trial	-	09/08/2019	
Queue Manager Enterprise	4	channels - shared with IVR Module	Trial	-	09/08/2019	
IVR module for Queue Manager Enterprise	4	channels - shared with QME	Trial	-	09/08/2019	
IVR Manager Professional	20	channels	Trial	-	09/08/2019	
Call Recording	1	channels	Trial	-	09/08/2019	
Speedy Enterprise	100	users	Perpetual	-	-	Licensed
StoneFax	2	channels	Trial	-	09/08/2019	
Billy Blue's 4	250	extensions	Trial	-	09/08/2019	
Budget Control			Trial	-	09/08/2019	
StoneLock	100	users	Trial	-	09/08/2019	
SSAM Professional	1	channels	Trial	-	09/08/2019	
Hotel Link	50	rooms	Subscription	30/11/2019	31/12/2019	Licensed
UIC Licenses	100	users	Perpetual	-	-	Licensed

## Offline Activation

First you need to retrieve the Request String from Imagecle Licenses web page.

Then you can generate the "Response String" from [Imagecle licensing portal](#), by entering License Code (provided by Imagecle) and above Request String.

Once you have the string, pls. enter it in the relevant field "Response String". Hit **Save** to enable licenses or **Cancel** to go back to initial license screen.

### Imagecle ApplicationSuite activation

**Imagecle  
Cloud Licensing**

A new way to make the assignment and management of Imagecle licenses faster, smarter and easier.

FIND OUT MORE

Offline Activation

**Request string**

```
REQ=1|app=sas|ops=6.2_(build_9200)|pkg=2019.6.1|vm=1|reqdate=2019-10-14|SupKey=3.32A243K6.A51K|MachineKey2=4.9URA517T.A51K|84bc91925f7110c4ec63175d8a14512c
```

**Response string**

```
RESP=1;app=bib;extensions=250;virtual=1;lic=Normal;lictype=EU;cust=;supkey=3.32A243K6.A51K;97fabf56d56a12c5cbaca0bac0711e11|RESP=1;app=bdg;liccode=PRODUCTION;virtual=1;lic=Normal;lictype=EU;supkey=3.32A243K6.A51K;b907bf6952e04a7aae0c1128a8684121|RESP=1;app=slo;users=250;liccode=PRODUCTION;virtual=1;lic=Normal;lictype=EU;supkey=3.32A243K6.A51K;34186afb14d5cecaaf744d0a918f226f|RESP=1;app=s
```

If activation is successful, you are redirected to initial license page, which now shows:

- ActivationMode: **Offline**
- A **"Switch to online or update your license"** button which allows to change activation mode or add/remove licenses by updating the Response String.

### Imagecle ApplicationSuite activation

Activation mode
*Offline*

Switch to online or update your license

PRODUCT NAME	QUANTITY	METRIC	LICENSE CODE	LICENSE TYPE	CARE TERM DATE	TERM DATE	LICENSE STAT
Blue's Attendant Enterprise	40	clients	PRODUCTIO	Perpetual	-	-	Licensed
Blue's Attendant Professional	40	clients	PRODUCTIO	Perpetual	-	-	Licensed
Blue's One Enterprise	40	clients	PRODUCTIO	Perpetual	-	-	Licensed
Queue Manager Enterprise	8	channels - sl	PRODUCTIO	Perpetual	-	-	Licensed
IVR module for Queue Manager Enterprise	8	channels - sl	PRODUCTIO	Perpetual	-	-	Licensed
IVR Manager Professional		gateways		Subscription	-	08/05/2019	Expired
Call Recording	30	channels	PRODUCTIO	Perpetual	-	-	Licensed
Speedy Enterprise	250	users	PRODUCTIO	Perpetual	-	-	Licensed
StoneFax	4	channels	PRODUCTIO	Perpetual	-	-	Licensed
Billy Blue's 4	250	extensions		Perpetual	-	-	Licensed
Budget Control			PRODUCTIO	Perpetual	-	-	Licensed
StoneLock	250	users	PRODUCTIO	Perpetual	-	-	Licensed
SSAM Professional	8	channels	PRODUCTIO	Perpetual	-	-	Licensed

## Limitation

- CARE TERM DATE field is empty, when offline activation is selected. It might include outdated information

# imagicle

- While updating to latest IAS, from an existing, production 2019.Spring.1 or older release, resulting activation mode is Offline. No need for further activation activities.
- New IAS installations are configured by default with Online activation.
- "Licenses" web page is accessible to Admin users only, with level 10 permissions (Complete Management)
- Replacing an existing activation token with a new one is allowed
- If an empty Activation Token/Response String is configured, all active licenses are removed. If you are within evaluation period, it doesn't make any difference. To re-activate the node, please enter previously removed valid Activation Token/Response String.

## License renewal upon crash or migration

If your server crashes or your configuration is corrupted, you can resume full operativity by restoring all data and configurations, previously saved with a backup. See [here](#) the procedure for data backup/restore.

If you do not have a backup, or if you want to **migrate** IAS to a new OS or a new hardware, please reinstall Imagicle Application Suite as described in the Installation section. A new Activation Token/Response String will be generated, so you'll need to run through the activate procedure to enable licenses in new server.

## Offline-only Licensing (available up to Imagicle 2019.Spring.1 release)

Prior to Imagicle 2019.Summer.1 release, **Admin** **License** web portal menu includes almost same information available through latest "Offline Activation" method:

- Request String
- Customer name
- The list of all applications, with relevant license code, status and size

General Information	
Detected Operating System	Windows 2012 Server 6.2 (Build 9200)
SAS Version and Platform	Imagicle Application Suite for Cisco UC 2018.1.1
Request String	<pre>REQ=1 app=sas ops=6.2_(build_9200) pkg=2018.1.1 vm=1 reqdate=2018-01-11 SupKey=3.6FMU9LME.K7TE MachineKey2=4.37K5T27M.K7TE fa6823857ae56072f50db95cb980a71c</pre>
Customer Name	<input type="text" value="Imagicle"/>
Reseller Name	<input type="text" value="Imagicle"/>

### Installed Applications

Name	License code	License Status	Size
UCL Users			0 users
Billy Blue's 4		Licensed	250 extensions
Budget Control		Expired	
StoneLock		Licensed	
StoneFax		Licensed	4 channels
Speedy Enterprise		Licensed	
IVR Manager Enterprise		Expired	
IVR module for Queue Manager Enterprise		Licensed	8 channels - shared with QME
Queue Manager Enterprise		Licensed	8 channels - shared with IVR Module
Blue's CTI Server		Licensed	40 Blue's One Enterprise Clients 40 Blue's Attendant Professional Clients 40 Blue's Attendant Enterprise Clients
Call Recording	Production02	Licensed	30 channels
SSAM Enterprise		Licensed	8 channels
Hotel Link		Expired	

"Response String" field is available, too. Instead of having a single, long Response String, here you have to enter a Response String for each license/application you need to activate, like below screenshot sample:

### Attiva licenze - i

Nome	Response String
UCL Users	RESP=1;app=mai;ucls=145;liccode=TQ4X9XC3;virtual=1;tel=ccm;lic=Normal;lictype=EU;cust=UnCliente;res=Tele
Billy Blue's 4	RESP=1;app=bib;extensions=1000;liccode=TQ4X9XC3;virtual=1;tel=ccm;lic=Normal;lictype=EU;cust=UnCliente;r
Budget Control	
StoneFax	RESP=1;app=sfx;ports=8;virtual=1;lic=Normal;lictype=EU;supkey=3.ARM61R1T.15F9;44bee7440756b4aac18fe4d
Speedy Enterprise	RESP=1;app=spd;users=1000;liccode=TQ4X9XC3;virtual=1;tel=ccm;lic=Normal;lictype=EU;cust=UnCliente;res=T
IVR Manager Enterprise	
Queue Manager Enterprise	RESP=1;app=qme;Channels=30;liccode=TQ4X9XC3;virtual=1;tel=ccm;lic=Normal;lictype=EU;cust=UnCliente;res:
Blue's CTI Server	RESP=1;app=att;bae_clients=10;liccode=TQ4X9XC3;virtual=1;tel=ccm;lic=Normal;lictype=EU;cust=UnCliente;res
StoneLock	RESP=1;app=slo;devices=1000;liccode=TQ4X9XC3;virtual=1;tel=ccm;lic=Normal;lictype=EU;cust=UnCliente;res=
SSAM Enterprise	RESP=1;app=sam;ports=8;virtual=1;lic=Normal;lictype=EU;cust=LABS;supkey=3.ARM61R1T.15F9;86e8148f2e51i

Hit **Save** to enable licenses.

## Accessing the Web Interface

The UC Suite provides a web interface for both administrator and users purposes.

You can reach the web interface typing this URL in the web browser:

**http://Server\_UCS/** or **https://Server\_UCS**

where Server\_UCS is the IP address or DNS name of the server the UCS is installed on.

The URL is the same for administration and common usage. The setup program also creates a Desktop shortcut on the server and a link in the Start menu.

To log in as the main administrator, enter the username and password **you** provided during installation.

Default values: **admin/admin**.

There is no way to recover this password once lost. If you loose the password, you can use the [guide to reset it](#).

Once you are logged in, your session will expire after 4 hours of inactivity.

## Supported browsers

The web interface can be best used with the following browsers:

### Desktop browsers

- Mozilla Firefox (latest version)
- Chrome (latest version) **recommended**
- Microsoft Edge (latest version)
- Safari (latest version)

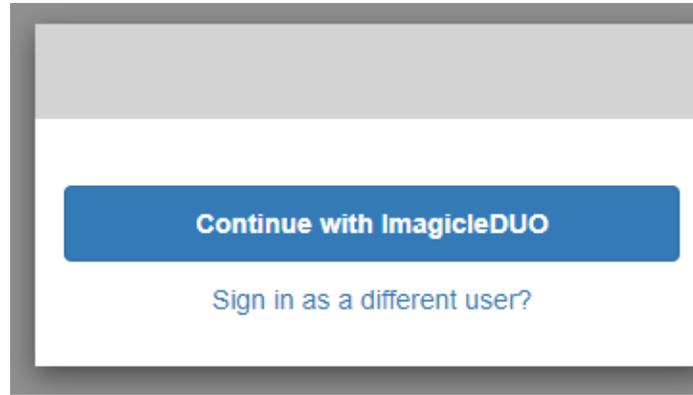
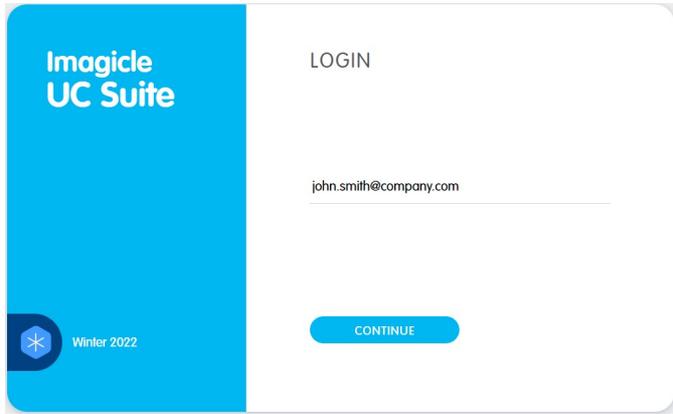
Internet Explorer 6, 7, 8, 9, 10 and 11 are no longer supported.

### Mobile browsers

- Safari (latest version)
- Chrome (latest version) **recommended**

## SSO - Single Sign On

Starting from Imagicle UC Suite 2022.Winter.1, Single Sign-On is supported, based on SAML or OpenID Connect protocols. If this feature is enabled, user should enter own SSO user ID and eventually the authentication request is redirected to the federated SSO Identity Provider (IDP), where a password and/or a multifactor token should be entered. See below sample:



To learn how to enable SSO in your UC Suite or UC Cloud Suite, please consult [this KB](#).

## System Parameters

### Outgoing Email Shared Parameters

Common email parameters enable Imagicle UCX On-prem/Cloud Suite to send email notifications through your company email server. Imagicle UCX Suite leverages this feature to forward voicemail messages, incoming faxes, scheduled reports, alarms, and to notify to the administrators about applications events.

This section describes those settings and their meaning. You can change them by clicking the **System parameters** link in the **Admin** menu, then pressing the **Outgoing Email Parameters** button.

#### SMTP Configuration

Typically, on-prem email servers like MS-Exchange or Lotus Domino leverage this protocol. In this case, you can select "SMTP" from **Protocol Type** pull-down menu. Please fill the resulting form based on your own email system:

The screenshot shows the 'Imagicle UCX Suite' administration interface. The top navigation bar includes 'Administration', 'User Management', 'System Parameters', 'Licenses', 'Support', 'Monitoring', and 'Presence'. The 'System Parameters' section is active. Below the navigation is a 'Back' link. The main content area is titled 'Outgoing Email Parameters' and contains the following configuration fields:

- Enable Outgoing Mail:**
- Protocol Type:** SMTP (selected in a dropdown menu)
- Email From Address:** fax-ha@imagiclevg.lab
- Server Name:** 192.168.4.6
- Server Port:** 25
- Use Authentication:**
- Username:** fax-admin@imagiclevg.lab
- Password:** [masked with dots]
- Proxy:** NoProxy (selected in a dropdown menu)

Below the Proxy field is a link: [Change proxy settings](#). At the bottom right of the form are two buttons: **Test connection** and **Save**.

- Enable Outgoing Mail: must be checked to enable Imagicle UCX Suite to send emails. **This is mandatory for fax-to-email feature**, if you are leveraging Imagicle Digital Fax application.
- Protocol Type: SMTP

## imagicle

- **Email Form Address:** This is the address which appears in the "From" field of the mail sent by UCX Suite. Depending on SMTP relay server, this might be a dummy address or an actual email account.
- **Server Name:** enter the FQDN or the IP address of the email server.
- **Server Port:** enter the port number on which the mail server is listening (example 25 for SMTP and 465/587 for Secure SMTP).
- **Use authentication, Username, and Password:** fill these fields if authentication is required.
- **Proxy:** If a Proxy is in place, please select it. More info [here](#).

**Secure SMTP is also supported.** The protocol to be used is auto-detected from the remote server choosing the safest first: TLS (we do support 1.2 - 1.0) or SSL (3.0 - 1.0) or plain.

Press the "Test" button to test the connection. Remember to press the "Update" button to save the changes before leaving.

**Warning:** even if the connection test succeeds, some email server might reject the "email from" address at the moment the email message is sent. Please check your email server configuration.

### OAuth2 Configuration

If you are leveraging a Cloud-based email service, like Office365 or Google Mail, then likely you wish to enable email sending by leveraging OAuth2 modern authentication. In this case, you first need to create an App Registration (if not available yet), by following this [KB article](#).

Then you need to create a DEDICATED email account in your Office365 Tenant, used by UCX Suite to populate the "From" field of the emails to be sent to users.

Please select "Office 365" from **Protocol Type** pull-down menu. Please fill the resulting form based on your own email system:



### Outgoing Email Parameters

Enable Outgoing Mail	<input checked="" type="checkbox"/>
Protocol Type	<input type="text" value="Office 365"/>
Application (client) ID	<input type="text" value="34325325"/>
Directory (tenant) ID	<input type="text" value="432432432"/>
Client secret	<input type="text" value="••••"/>
Email Address	<input type="text" value="jhonny@imagicle.com"/>
Proxy	<input type="text" value="NoProxy"/>

[Change proxy settings](#)

Configuration summary

The mail server connection is ready for verification. You are encouraged to proceed with testing the connection and save the parameters.

- Enable Outgoing Mail: must be checked to enable Imagicle UCX Suite to send emails. **This is mandatory for fax-to-email feature**, if you are leveraging Imagicle Digital Fax application.
- Protocol Type: Office 365
- Application (client) ID: This field must be populated based on [App Registration](#)
- Directory (tenant) ID: This field must be populated based on [App Registration](#)
- Client secret: This field must be populated based on [App Registration](#)
- Email Address: This is the dedicated email account created on purpose for email sending.
- Proxy: If a Proxy is in place, please select it. More info [here](#).

### Companies leveraging a custom Office 365 URL

Some companies are leveraging a custom Office 365 URL to access their email service (like Office 365 Business service).

To change from default Office 365 URL to a custom URL, you must change two internal Windows system variables, by access Imagicle instance through a RDP session:

## imagicle

- IMAGICLE\_OUTGOING\_O365\_AUTHENTICATION\_URL
  - ◆ (default: <https://login.microsoftonline.com>)
- IMAGICLE\_OUTGOING\_O365\_SERVER\_URL
  - ◆ (default: <https://outlook.office365.com>)

If you are leveraging an Imagicle UCX Cloud Suite, please contact Imagicle team to let them apply the change for you.

### **Email queuing for high reliability**

Imagicle UCX Suite integrates an email messaging queue which prevents losing notifications when the connection with the email server fails.

If Outgoing Email Parameters has never been configured (especially the server IP address), connection is not attempted, outgoing emails are not generated, voicemail messages and incoming faxes may never reach their recipients.

If Outgoing Email Parameters are wrong, or if the email server cannot be reached at the moment, email messages are generated and stored in a local folder ("StonevoiceAS\Var\Spool\Pickup"). As soon as the connection is available, all the messages stored in queue are sent.

The queue service tries to reconnect to the email server every 30 seconds. The email messages are sent one by one in sequence.

## Microsoft OAuth2 Authentication for email sending

This authentication method is supported by Imagicle UC Suite, starting from 2021.Winter.2 release, and it relays on advanced OAuth2 authentication available for cloud-based Office 365 email service. Previous Imagicle releases are supporting OAuth2 basic authentication, which is dismissed by Microsoft starting from July 2021.

### Requirements

In order to enable Imagicle UCX Suite to send email notifications and to handle email-to-fax service, leveraging Microsoft Office 365 cloud service and OAuth2 authentication, you must configure an application on [Azure Web Portal](#), taking note of Application ID, Directory ID and Client Secret data, needed later on while configuring this authentication method on Imagicle UCX Suite. Please read the following procedure to create a new application on Azure portal.

### Azure web portal configurations

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

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 "MyOAuth2App". Then select "Accounts in this organizational directory only" and hit "Register"



Home > App registrations >

## Register an application

### Name

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

MyOAuth2App ✓

### 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.

Public client/native (mobile ... e.g. myapp://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.

The screenshot shows the Microsoft Azure portal interface. At the top, there is a navigation bar with the Microsoft Azure logo and a search bar. Below the navigation bar, the breadcrumb path is 'Home > App registrations > MyOAuth2App'. The main content area is divided into two columns. The left column contains a navigation menu with the following items: Overview (selected), Quickstart, Integration assistant, Manage, Branding, Authentication, Certificates & secrets, Token configuration, and API permissions. The right column displays the 'Essentials' section for the application 'MyOAuth2App'. It lists the following details: Display name: MyOAuth2App, Application (client) ID: 1cb8b5d2-8724-4f32-8152-a16a230b682b, Directory (tenant) ID: 969d5b92-bc05-403f-b576-97201b665e65, and Object ID: 2c6bb16d-26b0-4910-8f6a-cff87b64bb2e. Below the Essentials section, there are two informational messages: one about the new and improved App registrations and another about the deprecation of the Azure Active Directory Authentication Library (ADA) in favor of the Microsoft Authentication Library (MSAL).

Now please click on "Certificates & secrets" option, included in left pane, and add a new "client secret" with the name of your choice and a long expiration period.

# MyOAuth2App | Certificates & secrets

Search (Ctrl+/)

Got feedback?

- Overview
- Quickstart
- Integration assistant

Manage

- Branding
- Authentication
- Certificates & secrets**
- Token configuration
- API permissions
- Expose an API
- App roles | Preview
- Owners
- Roles and administrators | Preview
- Manifest

Support + Troubleshooting

## Add a client secret

Description

DigitalFaxMailServiceSecret

Expires

- In 1 year
- In 2 years

Add

Cancel

## Client secrets

A secret string that the application uses to prove its identity when requesting a tok

+ New client secret

Description	Expires	Value
-------------	---------	-------

No client secrets have been created for this application.

Once added, you'll get some data associated to it. Please copy "Value" field for later usage. Copy the field immediately after having created the client secret, because it will be automatically hidden after few minutes, for security reasons.

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

Home > App registrations > MyOAuth2App

## MyOAuth2App | Certificates & secrets

Search (Ctrl+/) Got feedback?

Copy the new client secret value. You won't be able to retrieve it after you perform another operation or leave this blade.

**Certificates**  
 Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as

Upload certificate

Thumbprint	Start date	Expires
No certificates have been added for this application.		

**Client secrets**  
 A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as applicati

New client secret

Description	Expires	Value
DigitalFaxMailServiceSecret	12/31/2299	wJO9k3_x03-d-7cF~TptM9YDAEV84QJNv6

Now click on "Add permissions" and select "API's my organization users". Then search for "Office 365 Exchange online".

permissions

Refresh Got feedback?

onfigured permissions  
 Applications are authorized to call APIs when they are granted permissions by us  
 l the permissions the application needs. [Learn more about permissions and cor](#)

+ Add a permission ✓ Grant admin consent for Imagicle spa

API / Permissions name	Type	Description
Microsoft Graph (1)		
User.Read	Delegated	Sign in and read user pr

view and manage permissions and user consent, try [Enterprise applications](#).

### Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Apps in your directory that expose APIs are shown below

Office 365

Name	Application (client)
Office 365 Enterprise Insights	f9d02341-e7aa-456c
Office 365 Exchange Online	00000002-0000-0ff1
Office 365 Information Protection	2f3f02c9-5679-4a5c
Office 365 Management APIs	c5393580-f805-4401
Office 365 Search Service	66a88757-258c-4c7:
Office 365 SharePoint Online	00000003-0000-0ff1

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

## Request API permissions

< All APIs

 Office 365 Exchange Online  
<https://outlook-tdf-2.office.com/>

What type of permissions does your application require?

### Delegated permissions

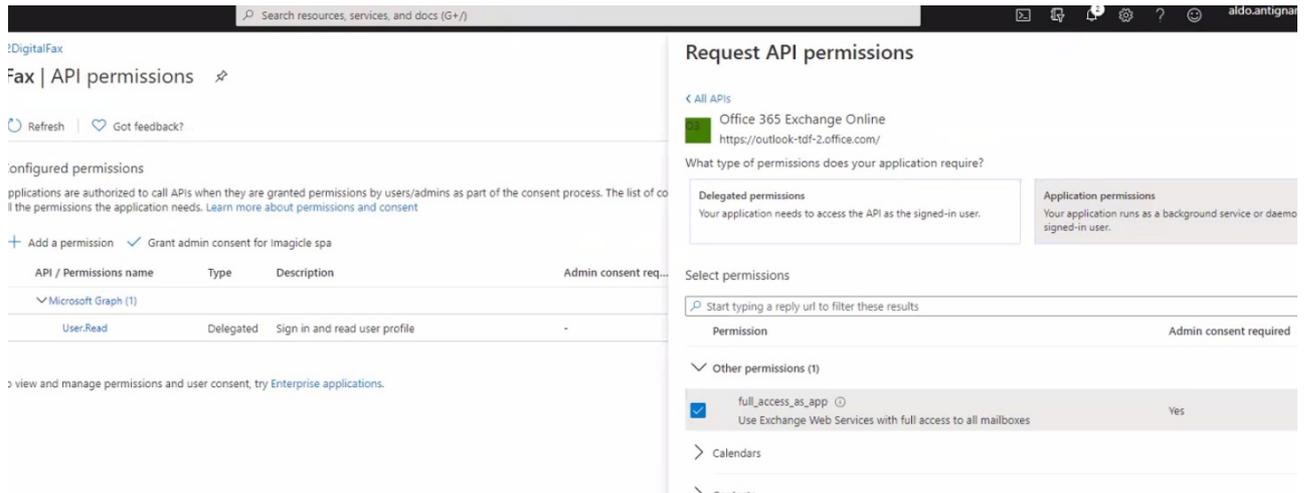
Your application needs to access the API as the signed-in user.

### Application permissions

Your application runs as a background service or daemon without a signed-in user.

Your application runs as a background service or daemon without a signed-in user.

From the list of available permission levels, please select "full\_access\_as\_app" from "Other permissions" category.



!DigitalFax

Search resources, services, and docs (G+)

Fax | API permissions

Refresh | Got feedback?

Configured permissions

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

+ Add a permission | Grant admin consent for imagicle spa

API / Permissions name	Type	Description	Admin consent req...
Microsoft Graph (1)			
User.Read	Delegated	Sign in and read user profile	-

> view and manage permissions and user consent, try [Enterprise applications](#).

### Request API permissions

< All APIs

 Office 365 Exchange Online  
<https://outlook-tdf-2.office.com/>

What type of permissions does your application require?

Delegated permissions  
Your application needs to access the API as the signed-in user.

Application permissions  
Your application runs as a background service or daemon without a signed-in user.

Select permissions

Start typing a reply url to filter these results

Permission	Admin consent required
Other permissions (1)	
<input checked="" type="checkbox"/> full_access_as_app Use Exchange Web Services with full access to all mailboxes	Yes
Calendars	
Contacts	

Once permission has been assigned, you must authorize it for your organization, by clicking on "Grant admin consent for <company\_name>".

Mail2DigitalFax

MailFax | API permissions

Refresh | Got feedback?

**⚠** You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission  Grant admin consent for Imagicle spa

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	-	...
Office 365 Exchange Online (1)				
full_access_as_app	Application	Use Exchange Web Services with full access to all mailb...	Yes	<b>⚠</b> Not granted for Imagicl... ...

To view and manage permissions and user consent, try [Enterprise applications](#).

This is the resulting page.

Permissions

Refresh | Got feedback?

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission  Grant admin consent for Imagicle spa

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	-	<input checked="" type="checkbox"/> Granted for Imagicle spa ...
Office 365 Exchange Online (1)				
full_access_as_app	Application	Use Exchange Web Services with full access to all mailb...	Yes	<input checked="" type="checkbox"/> Granted for Imagicle spa ...

To view and manage permissions and user consent, try [Enterprise applications](#).

**Optional configurations to restrict EWS Application to a mailbox set (Imagicle Digital Fax only)**

Above described API Permission level privileges allows the application to access all EWS API on all organization mailboxes.

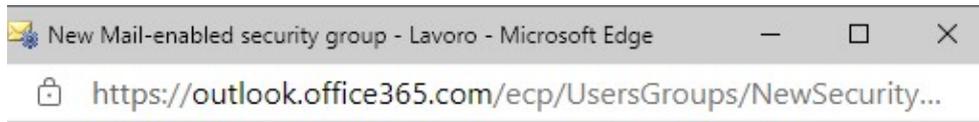
However, it's possible to optionally apply an advanced configuration on Microsoft Office 365 to restrict the application to access only a specific mailbox.

This is accomplished by accessing Exchange Online Administration Portal and create a new mail-enabled security group: Go to **Recipients** > **Groups** > **New mail-enabled security group**

The screenshot shows the Exchange Admin Center interface. On the left is a navigation sidebar with the following items: dashboard, recipients (highlighted), permissions, compliance management, organization, protection, advanced threats, mail flow, mobile, public folders, unified messaging, and hybrid. Below the sidebar is a blue button labeled 'New Exchange admin center'. The main content area has a top navigation bar with 'mailboxes', 'groups' (selected), 'resources', 'contacts', 'shared', and 'migration'. Below this is a blue banner: 'Manage your Distribution Lists, Groups and more in New Exchange Admin Center.' A card titled 'GROUPS IN OUTLOOK' contains the text 'More than a DL—even new members get all prior conversations and attachments.' and a 'Create a group' button. Below the card is a '+ New Microsoft 365 group' button with a dropdown menu open, showing options: 'Distribution list', 'Mail-enabled security group' (highlighted), and 'Dynamic distribution list'. Below the menu is a table of groups:

DISPLAY NAME	STATUS
All Company	Active
imagicleucdev	Active

Fill the form with a name and an alias. Those will be used later as a target of an Application Policy.



## new mail-enabled security group

Mail-enabled security groups can be used to distribute messages and to assign access permissions to Active Directory resources. [Learn more](#)

\*Display name:

\*Alias:

\*Email address:

 @ 

Notes:

\*Owners:

+ -

Save form and edit the newly created group, go to **membership**, add a member, search for the mailbox to be granted to Digital Fax and add it:

Imagicle Digital Fax

- general
- ownership
- membership
- membership approval
- delivery management
- message approval
- email options
- MailTip
- group delegation

Members:

DISPLAY NAME	EMAIL ADDRESS
Adele Vance	AdeleV@imagicleucdev.onmicrosoft.com
Alex Wilber	AlexW@imagicleucdev.onmicrosoft.com
Diego Siciliani	DiegoS@imagicleucdev.onmicrosoft.com
Digital Fax	fax@imagicleucdev.onmicrosoft.com
Grady Archie	GradyA@imagicleucdev.onmicrosoft.com
Henrietta Mueller	HenriettaM@imagicleucdev.onmicrosoft.com
Imagicle Digital Fax	imagicle.digital.fax@imagicleucdev.onmicrosoft.com
Isaiah Langer	IsaiahL@imagicleucdev.onmicrosoft.com
Johanna Lorenz	JohannaL@imagicleucdev.onmicrosoft.com
Joni Sherman	JoniS@imagicleucdev.onmicrosoft.com
Lee Gu	LeeG@imagicleucdev.onmicrosoft.com
Lidia Holloway	LidiaH@imagicleucdev.onmicrosoft.com

1 selected of 20 total

add -> Digital Fax[remove];

OK Cancel

Connect to [Exchange Online PowerShell](#) and create an [Application Access Policy](#) to allow Digital Fax application to only access the newly created mail security group, by executing the following command, where:

- **AppId** value corresponds to the application "Client ID" value created within Azure app registration portal
- **PolicySecurityGroupId** corresponds to "Display Name" of the previously create security group

```
New-ApplicationAccessPolicy -AccessRight RestrictAccess -AppId <AppId> -PolicyScopeGroupId "Imagicle Digital Fax" -D
```



Output should be:

```
RunspaceId      : 2d08b315-81dd-4140-8a28-4a49431fb44d
ScopeName       : Imagicle Digital Fax
ScopeIdentity   : Imagicle Digital Fax
Identity        :
8f8ccdec-23bd-4452-bdb3-becc0c415a99\da34af4b-b01f-47e4-bfac-2f9fc3f1383e:S-1-5-21-2724517575-989
AppId           : da34aq4b-b01f-47e4-bfac-2f9fc3f1383e
ScopeIdentityRaw :
S-1-5-21-2724537575-989916663-4003715733-16076635;697c48d2-f812-4072-a10f-4455db66025e
Description     : Restrict Imagicle Digital Fax accessible mailboxes
AccessRight     : RestrictAccess
ShardType       : All
IsValid         : True
ObjectState     : Unchanged
```

Verify the rule, to check if the application can properly access the needed mailbox by executing the following command:

```
Test-ApplicationAccessPolicy -Identity <mail2fax address> -AppId <clientId>
```

Output should be:

```
RunspaceId : 2e08b315-81dd-4143-8a28-4a49431fa44d AppId :
da34ee4b-b01f-44e4-bfac-2f9fc3f1383e Mailbox : fax MailboxId :
c82eee91-a3e0-43f0-9a43-03e7ec7b1e96 MailboxSid :
S-1-5-21-2722357575-989916663-4003711733-159675946 AccessCheckResult : Granted
```

Then please verify the application can't access any other mailbox, by executing the following command:

```
Test-ApplicationAccessPolicy -Identity <any other mail address> -AppId <clientId>
```

In this case, output should be similar to below sample:

```
RunspaceId : 2d08b235-81dd-4140-8a28-4a49431fa44d AppId :
da34af4e-b01f-47e4-beec-2f9fc3f1383e Mailbox : fax MailboxId :
c82eee91-a3e0-43f0-9a43-03c7ec7b1e96 MailboxSid :
S-1-5-21-272451125-989916663-4003715733-15450946 AccessCheckResult : Denied
```

## Numbering Plan

You can edit these parameters through the **Admin** -> **System parameters** link in the App Suite menu, pressing the **Numbering Plan Parameters** button. These settings apply to the applications that make and receive calls such as Attendant Console and Speedy. To be able to modify a parameter, you have to deselect "Use default settings".

### General

General settings affect both incoming and outgoing calls.

- **Internal Phone Number Patterns:** These patterns identify the internal PBX extensions and, in general, all numbers that do not require the PSTN access code to be dialled. The usual range is 1 - 5. The list of patterns is checked top-down. To know how to build the pattern, please refer to the online help in the web page.
- **PBX supports E.164 dialling:** flag this checkbox if you use the + to dial external numbers (e.g. +123456789)
- **Local Country Code:** This prefix will be stripped from the caller number before looking for it in Speedy directories (e.g. +44). Incoming prefix will be stripped first, then the Local country code. You can specify only one prefix.
- **International Dialling Prefix:** This is the prefix needed to reach international numbers when the + sign is not used. E.g. 00 in European countries, +1 in US.

### Incoming calls

- **Prefix** for incoming calls: This prefix will be stripped from the caller number before looking for it in Speedy directories. Example: if your outgoing prefix is 0, it is likely that the PBX adds 0 to the caller number to allow redialling. In this case enter 0 as incoming prefix.

### Outgoing calls

- **Prefix** for outgoing calls: This prefix will be automatically added to outgoing calls, e.g. to calls placed by Speedy towards external numbers. This prefix won't be added to internal calls nor to calls towards the users' primary extension configured in the users list
- **Suffix** for outgoing calls: On some telephony systems, a suffix can be used to quicken the destination selection (for instance #)
- **TAPI events include the prefix:** set this flag to on if the called number which the pbx signals through TAPI calls includes the prefix for outgoing calls, so that it will be stripped. This should happen only if the outgoing prefix is removed by a voice gateway instead of the PBX. This setting affects the lookup in Speedy directories for the **called** numbers of outgoing calls.

## Users Authentication Settings

This important setting dictates the authority in charge of authenticate users upon accessing Imagicle web portal, gadgets and Attendant Console. Within same page, you can also setup the https session expiration timeout for Imagicle web portal and gadgets.

This setting is available from Imagicle UCX Suite web portal: Admin > System Parameters > Users authentication settings.

### Users authentication preferences

As you can see in above screenshot sample, it includes several different authentication authorities. Please configure the one corresponding to your synchronization source:

- **SSO > AD/LDAP > Local:** Choose this option when you import users from Active Directory, from Azure AD, from a generic LDAP server or from Imagicle LDAP Module.
- **SSO > Cisco UCM > Local:** Choose this option while importing users from Cisco UCM (via AXL) or from Cisco Webex Control Hub.
- **SSO > Local:** This is the local authentication, leveraging a local username and password assigned to each Imagicle user and stored into Imagicle SQL Server instance.
- **SSO > AD/LDAP > Cisco UCM > Local:** Choose this option to authenticate users against Active Directory or generic LDAP. If AD/LDAP username is missing and PBX Username is configured, users are authenticated against Cisco UCM.
- **SSO > Cisco UCM > AD/LDAP > Local:** Choose this option to authenticate users against Cisco UCM. If PBX Username is missing and AD/LDAP username is configured, users are authenticated against Active Directory or generic LDAP.

Please note that all above options include SSO authentication against a configured Identity Provider. If SSO is not used, and relevant User's field is left empty, then authentication is skip to next listed option.

All above choices include "Local" as last authentication option, meaning UCX Suite authentication leveraging a local username and password assigned to each Imagicle user and stored into Imagicle SQL Server instance.

### User session management

This setting allows to enable a persistent active web session for users leveraging Imagicle web portal and/or Imagicle gadgets.

If this feature is enabled, by configuring "Remember logged in user" to Yes, users can shut down own workstations or close the web browser without losing entered login credentials. Next time they access to Imagicle web portal or gadget within configured inactivity period, they are redirected to web portal's home page or gadgets' main pages.

The feature is enabled by default, with an inactivity timeout of 8 days. You can increase this parameter up to 30 days.

## Proxy settings

This article is applicable to Imagicle UC Suite 2019.Summer.1 or later and it allows to apply a Proxy configuration to reach Internet addresses, specifically for the following features:

- Imagicle Online License Activation, where you need to reach Imagicle Cloud services at [https://\\*.imagicle.com](https://*.imagicle.com)
- Imagicle Cloud Services Authentication
- Cloud-based email services, like Office365 or Google mail
- Imagicle Webex connector for users' synchronization
- Microsoft Teams phone control and presence Cloud services (2021.Summer.1 and above)

You can edit these parameters through the Admin  System parameters link in the App Suite menu, hitting "Proxy settings" button.

System parameters	
IP Telephony system parameters	<input type="button" value="Set »"/>
SMTP parameters	<input type="button" value="Set »"/>
Numbering plan parameters	<input type="button" value="Set »"/>
Users authentication settings	<input type="button" value="Set »"/>
Proxy settings	<input type="button" value="Set »"/>
Secure communications certificate	<input type="button" value="Set »"/>
Imagicle Cloud services authentication data	<input type="button" value="Set »"/>

## Proxy

You can either enable a HTTP/HTTPS-based proxy server and/or a SOCKS v4/v5 proxy server. In both cases, these are the field to be compiled:

- **Address:** this is the proxy URL or IP address. This parameter is **mandatory**
- **Port:** This is the TCP port used by proxy. If above address is entered, port is **mandatory**
- **Username:** the username for proxy authentication (if needed). Currently, username can't include "@" character.
- **Password:** the password for proxy authentication. If above username is entered, password is **mandatory**. Currently, password can't include "@" character.

**Proxy**

If this machine needs proxies to reach external resources, you can set them here. Please make sure the proxy configurations complies with the requirements described at the following link: <https://www.imagicle.com/go/IASProxy>

**HTTP/HTTPS**

Address  Port

Username

Password

**SOCKS**

Address  Port

SOCKS v4  SOCKS v5

Username

Password

Configuring a proxy directly on the UC Suite server network settings is discouraged. If needed for specific requirements (e.g. allow SO Updates), below options are available:

- enable it temporarily and then disable it when it is not longer necessary
- enable it and allow all direct communications between UC Suite and all other Imagicle cluster nodes (in case of HA installation), the PBX and all other 3rd party elements (e.g. AD/LDAP sources)

In case of HA installation, proxy configuration is not replicated among Imagicle cluster nodes.

**Warning:** The UC Suite should obtain api.imagicle.com SSL certificate and not the proxy certificate, otherwise security check fails. The proxy works in transparent way, so it should not perform https "decrypt & scan".

**Warning:** Every time you apply a new proxy configuration, please **reboot Imagicle UC Suite server** to enable it.

## Imagicle Cloud services authentication data

### Applies to

Imagicle UC Suite 2022.Winter.1 and above.

### Description

Several Imagicle Cloud-based services require to enable communication and data exchange between UC Suite and Imagicle Cloud. This is accomplished by entering authentication parameters, as below explained.

### Requirements

Please make sure you have the following data upfront:

- Customer name
- License activation token of Cloud-connected Imagicle UC Suite or Imagicle UC Cloud Suite

Please send above data to Imagicle Support Team.

Once the authentication is enabled on Imagicle side, Support Team returns you via email a "Client ID" and a "Client Secret" strings, to be applied by following below procedure.

### Solution

Please access Imagicle UC Suite web portal as administrator and go to ADMIN â System Parameters â Imagicle Cloud services authentication data

Fill both Client ID and Client secret fields with OAuth2 authentication data provided by Imagicle Cloud Services and hit Save. See below screenshot sample:

The screenshot shows the Imagicle UC Suite web portal interface. At the top, there is a blue navigation bar with the 'Imagicle UC Suite' logo and several icons representing different system functions. Below the navigation bar, a breadcrumb trail shows the path: Administration > User Management > System Parameters > Licenses > Support > Monitoring > Presence > Jabber > High Availability > Audit Trail. The 'System Parameters' link is highlighted. Below the breadcrumb trail, there is a '< Back' link. The main content area is titled 'Imagicle Cloud services authentication data'. It contains a paragraph of instructions: 'Here you can enter the data required to authenticate this UC Suite to Imagicle Cloud services. This data is provided by the Imagicle Cloud platform. To set up communication and data exchange between UC Suite and Imagicle Cloud, fill in all fields with valid data; in case no connection is expected, remove the data in memory and keep all fields empty.' Below this text, there are two input fields: 'Client ID' with the value 'clientId' and 'Client secret' with a masked value of '.....'. A 'Save' button is located at the bottom right of the form.

Credentials are encrypted and locally stored. The following window appears:



[← Back](#)

### Imagicle Cloud services authentication data

Here you can enter the data required to authenticate this UC Suite to Imagicle Cloud services. This data is provided by the Imagicle Cloud platform.

To set up communication and data exchange between UC Suite and Imagicle Cloud, fill in all fields with valid data; in case no connection is expected, remove the data in memory and keep all fields empty.

Credentials saved using Client ID:**clientId**

**Forget**

If, in the future, a credentials change is required, you can hit "Forget" button to remove existing credentials and enter new ones.

If your company is leveraging a Proxy server to provide Internet access, you should enter relevant parameters, as described in [this](#) article.

## UC Suite cluster

In High Availability environments or UC Cloud Suite implementation, above configurations must be performed in each node of the cluster, since the data are not duplicated and are not managed by the Backup/Restore procedure.

Each node just uploads its own recordings.

## Troubleshooting

If an error occurs upon loading the OAuth2 credentials, you can retry credentials saving. More error details can be found in the following log file:

```
C:\Program Files (x86)\StonevoiceAS\Var\Log\w3wp\ApplicationSuite.log
```

## Web Server setting

This article is applicable to Imagicle UCX Suite 2023.Spring.1 or later and it allows to change the embedded web server's URL to reach Imagicle web portal and leverage Imagicle APIs.

### How to change web server's URL

Please click on "Set >>" beside "Web server settings" menu option. See below:

The screenshot shows a 'System parameters' menu with several options. The 'Web server settings' option is highlighted with a red rectangular box. Each option has a 'Set >>' button to its right.

System parameters	
IP Telephony system parameters	Set >>
SMTP parameters	Set >>
Numbering plan parameters	Set >>
Users authentication settings	Set >>
Proxy settings	Set >>
Secure communications certificate	Set >>
Imagicle Cloud services authentication data	Set >>
<b>Web server settings</b>	<b>Set &gt;&gt;</b>

The following window pops-up:

The 'Web server settings' window contains the following text and fields:

**Web server settings**

Enter your custom UCX Suite base URL here to make this UCX Suite node reachable. If no base URL has been specified, the default `https://<servercomputername>` URL will be used.

Please note that this configuration is valid on this node. If your environment consists of multiple nodes, be sure to configure the URL on each of them according to the needs of your network.

UCX Suite base URL

To save your base URL, please enter it in this order: < `https://example.com/...` >

Save

Here you can enter the URL of your choice, keeping in mind that https usage means involving a Digital Certificate which should be associated to the new URL within IIS. New URL overrides the existing `https://<ServerComputerName>` standard FQDN.

Once new URL is entered and saved, this is the result:

## Web server settings

Enter your custom UCX Suite base URL here to make this UCX Suite node reachable. If no base URL has been specified, the default `https://<servercomputername>` URL will be used.

Please note that this configuration is valid on this node. If your environment consists of multiple nodes, be sure to configure the URL on each of them according to the needs of your network.

UCX Suite base URL: **https://test.imagicle.com**

Forget

"Forget" button allows to revert to standard FQDN. New web server URL is saved in: `C:\Program Files (x86)\Apps\ApplicationSuite\Settings\ApplicationSuite.Local.ini`

# Monitoring

## Monitoring service configuration

Imagicle UCX Suite includes a monitoring services which can send alerts to the system administrator when some important events occur. Examples of monitored events are:

- Insufficient disk space
- An Imagicle service failing
- Low database space
- Bad service performance
- License issues
- License overcome (e.g. calls dropped in Advanced Queuing because the licensed channels are too few)
- Authorization issues related to Webex Calling MT tokens

The monitoring service includes auditing features. The list of events can be displayed through a web page and can also be exported in CSV or XLS formats.

## Architecture

The monitoring service (MAM) is installed on the machine by the setup program together with Imagicle applications. It is runs automatically when the machine starts. The service performs two main operations:

- **ALARM:** It monitors the local machine. If some of the monitored parameters are out of range (low disk space, low memory, high CPU, low DB space...), it records an error or a warning in the application event log named "IAS"
- **NOTIFY:** When an error is logged in the event log, it notifies the System administrator through email. It can also generate a SNMP trap messages.

Other Imagicle services can log errors or warnings to the custom UCX Suite event log; the monitor service will take care of the notifications.

Specific event notification can be enabled or disabled through the web interface.

UCX Suite event log can also be browsed through the standard Windows Event Viewer.

The monitoring service is also in charge of deleting old log files (retention period is 30 days by default).

The MAM web interface can be accessed through the main Application Suite menu, selecting "Main" and then "Monitoring". It is available to the UCX Suite administrators only.

## Alarms status

On the **Alarms** tab you can quickly check the health of the system. You can selectively disable the alarms if you think they are not needed. Warnings and errors are displayed here. To read the details of the current status, move your mouse pointer over the little dot with the "i".

## Mail Configuration

Click on **Mail Configuration** to set the list of the recipients of the email notifications. Recipients addresses must be valid email addresses separated by comma (,).

Please make sure that Outgoing Email Parameters have been correctly set for the email notifications to run. See [here](#) for more details.

## Event History

# imagicle

The list of events raised by the monitoring service and other Imagicle service can be examined through the web interface in the **Events History** page. The controls on the top of the list will allow you to filter the displayed events by date, by type, by application and by category. Each event has a unique id.

The type of the event represents its severity: information, warning or error.

To enable or disable further notifications, use the checkbox in the event row.

**Warning:** the filter lists are dynamic. If an application, event type or category is not available in the list, this means that no event with that property has been raised yet. As a consequence, you can only disable events that have been notified once.

The list of events can be downloaded in CSV or XLS formats by clicking on the small icons in the upper right corner of the list.

## Monitored events details

The MAM monitors a lot of parameters and can raise a lot of events. Here are some relevant caveats and additional details.

**High Availability:** Replication link status and time alignment

**Service failing:** The error stating that an Imagicle service is failing is raised if the process disappears for more than 15 seconds from the process list.

**Low disk space:** when the disk space is low, the Monitor will warn the user and will also try to gain space by deleting old log files

**Database full:** if no space is left in the database, Imagicle Billing Miner service will be stopped. The call data will be stored in local files until the database is purged. This way no call will be lost.

**Call Recording:** Expired Digital Certificate or not reachable external storage

**Webex integrations authorizations:** Users' synch, Rich Presence, Call Control and Call Analytics authorization issues.

## Tuning and customizations

The monitoring service can run external processes if needed; its behavior can be fine-tuned and customized through XML files. Please ask Imagicle Technical Support team if you have specific needs.

## SNMP configuration

The SNMP configuration web page allows you to easily add the UCX Suite server to a SNMP monitor.

The Simple Network Monitoring Protocol **monitor** is a third party software able to receive the notifications, installed somewhere on your network. Optionally, the software may include a **master agent** which receives the notifications and makes them available to the monitor.

Imagicle MAM acts as a **monitored device**. There is no need to install a third party agent on the UCX Suite server to monitor it through SNMP.

**Warning:** Imagicle monitoring services only sends SNMP trap services. It does not respond to SNMP inquiries.

Here are the steps to activate the SNMP trap generation and receive them on a SNMP manager:

- **SNMP trap servers:** enter the SNMP manager IP address; if more than one manager must be reached, enter the ip addresses separated by commas. If your system includes a master agent, enter the master agent ip address.
- **SNMP trap community:** it is a common practice to put monitored devices in groups called *communities*. If this parameter does not match the configured community on the monitor, the trap messages could be discarded.

Press Save after the changes.

## imagicle

To enable the third party SNMP monitor to receive the SNMP trap messages from the MAM, you should download the Imagicle MIB file by pressing "Download SNMP MIB" button, then load it to the SNMP monitor software. Please refer to your SNMP monitor documentation to know how to load the UCX Suite MIB file.

After configuration, whenever an alarm is raised, a SNMP trap is also sent to the SNMP monitor. SNMP traps can be selectively disabled from the Events history web page

Note: if the UCX Suite server fails (for example because of a power outage), no SNMP trap will be generated, because the MAM won't be running.

**Warning:** SNMP traps are sent towards UDP port 162. Please ensure the SNMP manager IP address and port can be reached over the network, and no firewall is blocking the communication.

### Technical details

SNMP OID used for TRAP messages associated to Imagicle alerts are located in the Imagicle branch:

.1.3.6.1.4.1.39801 (.iso.org.dod.internet.private.enterprise.imagicle)

Events are identified as follows, through SNMPv2 OIDs:

39801.2.0.[eventid] (imagicle.suiteEventNotifs.[enterprise-specific].[eventid])

Events include the following additional variables:

39801.1.1 (imagicle.types.eventText) (with a short text description of the events).

### Troubleshooting SNMP trap messages

- When you sent the test TRAP, the result displayed can be misleading. Check that you can actually ping the configured SNMP manager or master agent IP addresses from the UCX Suite server
- Verify that no firewall is blocking outgoing UDP connections FROM the IAS server towards port 162 of the SNMP monitor server
- To generate an actual alarm, please stop one of the licensed Imagicle services (e.g. Imagicle Attendant Console)