System Parameters

20 Apr 2024

Table of Contents

System Parameters...1/30

Cisco IP Telephony System Parameters...1/30

Outgoing Email Shared Parameters...2/30

Microsoft OAuth2 Authentication for email sending...6/30

Numbering Plan...17/30

Users Authentication Settings...18/30

CuCM CTI Configuration...19/30

Enable AXL access to Cisco UCM...22/30

Proxy settings...23/30

Secure Communications Certificate...25/30

Imagicle Cloud services authentication data...27/30

Web Server setting...29/30

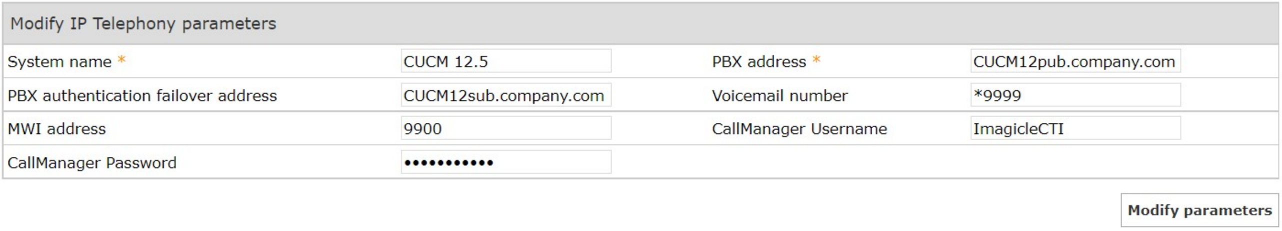
System Parameters

System Parameters

Cisco IP Telephony System Parameters

You can edit Cisco IP telephony system shared parameters by accessing **System parameters** link in the **Main** menu. Some of these parameters are mandatory for the applications to work.

- **System name**: a label to identify the system. This parameter is **mandatory** but can be arbitrary
- **PBX Address**: IP or DNS name of Cisco UCM "Publisher" node in your network. Please make sure that "Cisco Call Manager" service is active on this Primary node, otherwise please choose a "Subscriber" node. This parameter is **mandatory**
- **PBX authentication failover Address**: IP or DNS name of an alternative Cisco UCM node in your network, handling users' authentication in case above Primary node does not answer or it answers with an error message. Failover PBX address is only engaged when authentication fails on primary Cisco node due to application problem (user with insufficient permissions or wrong credentials).
- **Voicemail number**: this is the pilot number of the voicemail. It is used only by Imagicle VoiceMail application and must match Cisco UCM configuration
- **MWI Address**: Prefix of the pattern you configured in Cisco UCM to turn on or off IP Phones' Message Waiting Indicator. See VoiceMail configuration here.
- **CallManager Username**: This is the CUCM Application User's username to establish AXL communications. Typically, the value is "ImagicleCTI". See here for more details.
- **CallManager Password**: This is the CUCM Application User's password to establish AXL communications. Typically, the value is "ImagicleCTI". See here for more details.



Modify IP Telephony parameters

System name *	CUCM 12.5	PBX address *	CUCM12pub.company.com
PBX authentication failover address	CUCM12sub.company.com	Voicemail number	*9999
MWI address	9900	CallManager Username	ImagicleCTI
CallManager Password	•••••••••••		

Limitations

If you configure PBX address (Primary Cisco UCM node) with a Subscriber's IP address/FQDN, please choose the Subscriber node with lowest RTT against Publisher node, to avoid AXL communications timeout.

Alternative failover PBX address is **only** used for **authentication purposes.**

If **Imagicle AXL Client** service is started while Primary Cisco UCM node is unreachable or its AXL Service is disabled, it won't be possible to authenticate against the alternative CUCM node, until Primary node establishes AXL communications with Imagicle UC Suite.

If Primary node stops working while Imagicle AXL Client service is already running, authentication is automatically routed to alternative node, without any OOS.

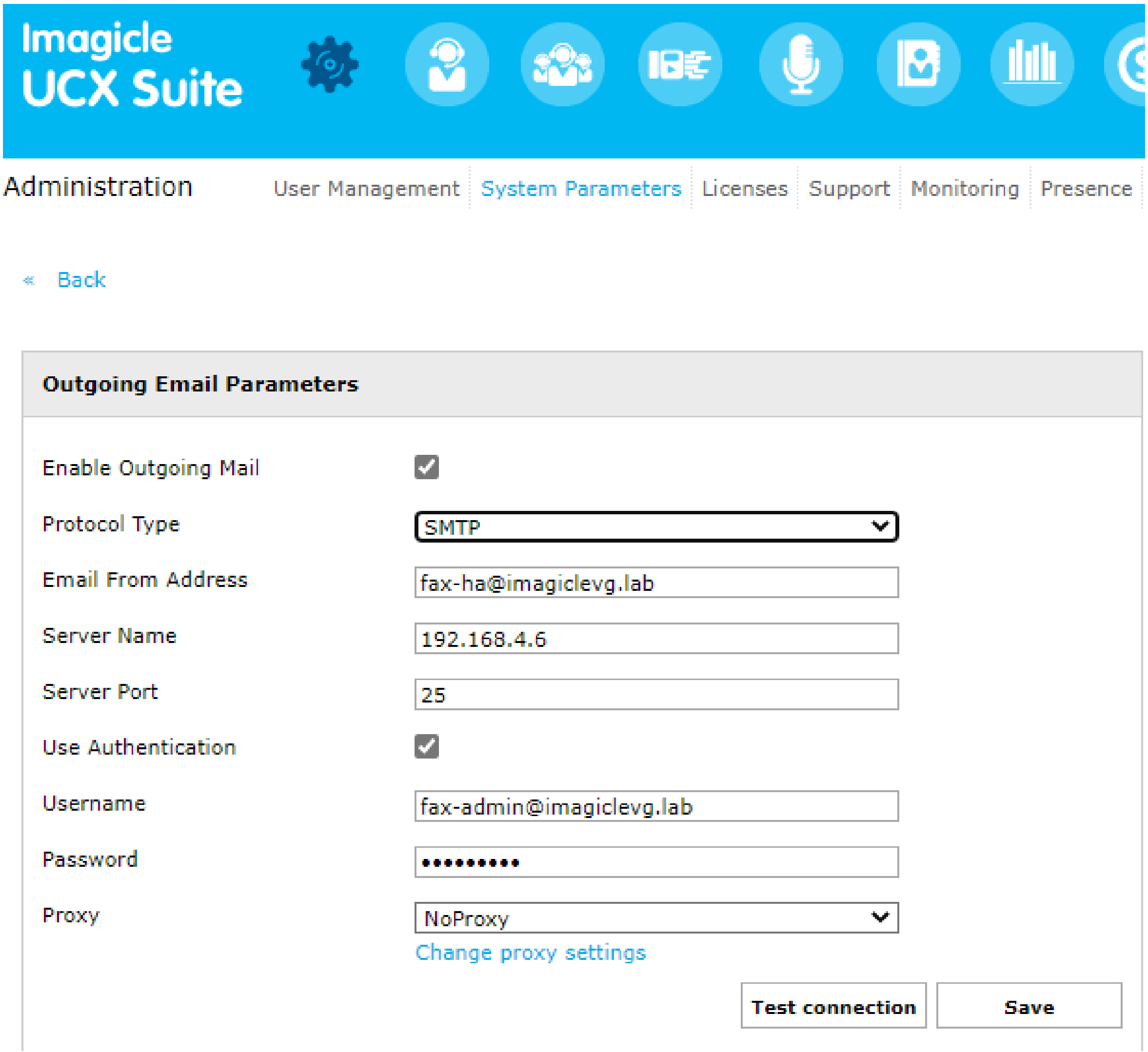
Outgoing Email Shared Parameters

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:



Outgoing Email Parameters

Enable Outgoing Mail	☑
Protocol Type	SMTP
Email From Address	fax-ha@imagiclevg.lab
Server Name	192.168.4.6
Server Port	25
Use Authentication	☑
Username	fax-admin@imagiclevg.lab
Password	•••••••••
Proxy	NoProxy

- 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
- 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.

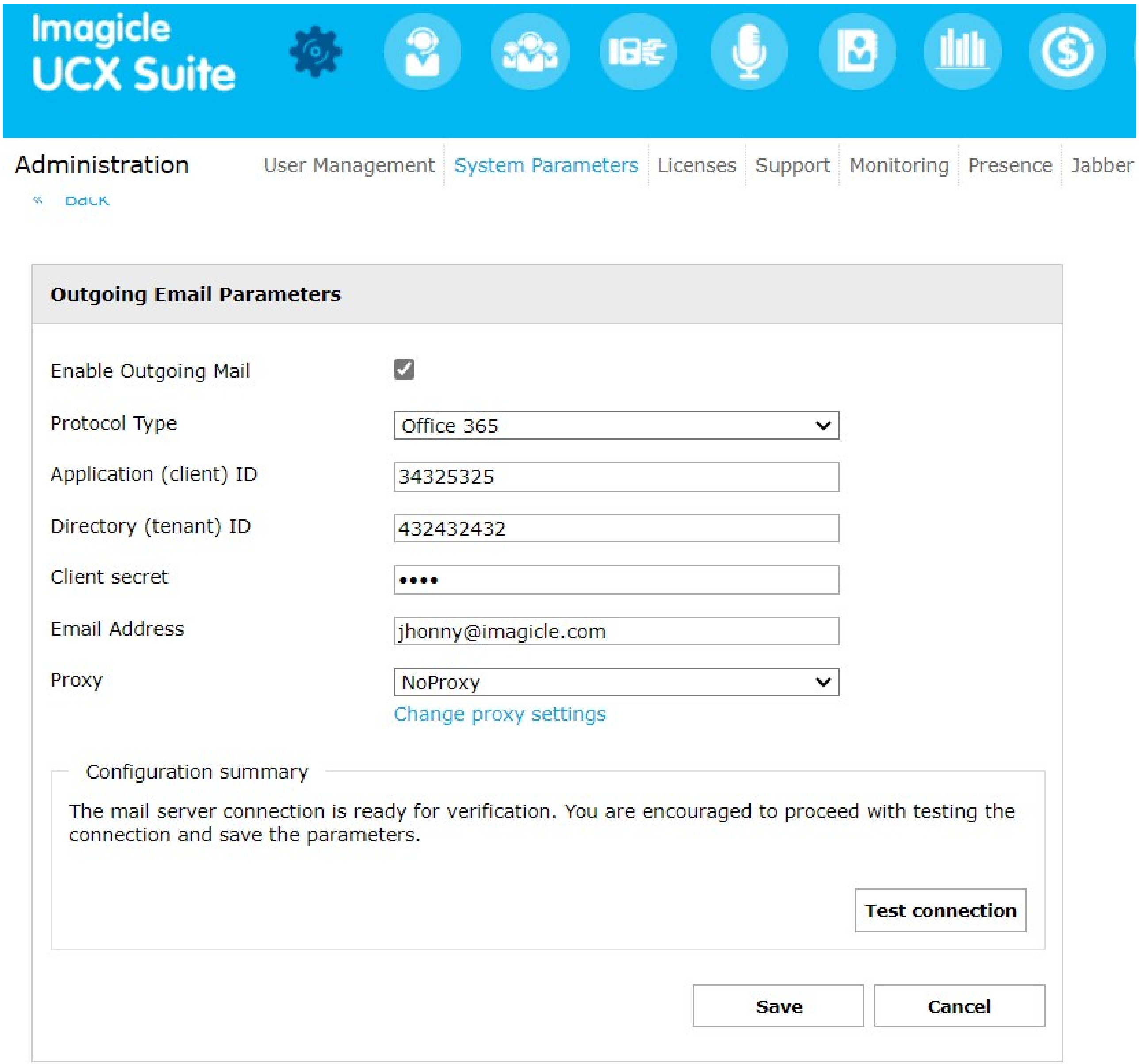
Warning: even if the connection test succeeds, some email server might reject the "email from" address at the moment the email message is sent. Please check your email server configuration.

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	☑
Protocol Type	Office 365
Application (client) ID	34325325
Directory (tenant) ID	432432432
Client secret	••••
Email Address	jhonny@imagicle.com
Proxy	NoProxy

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_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

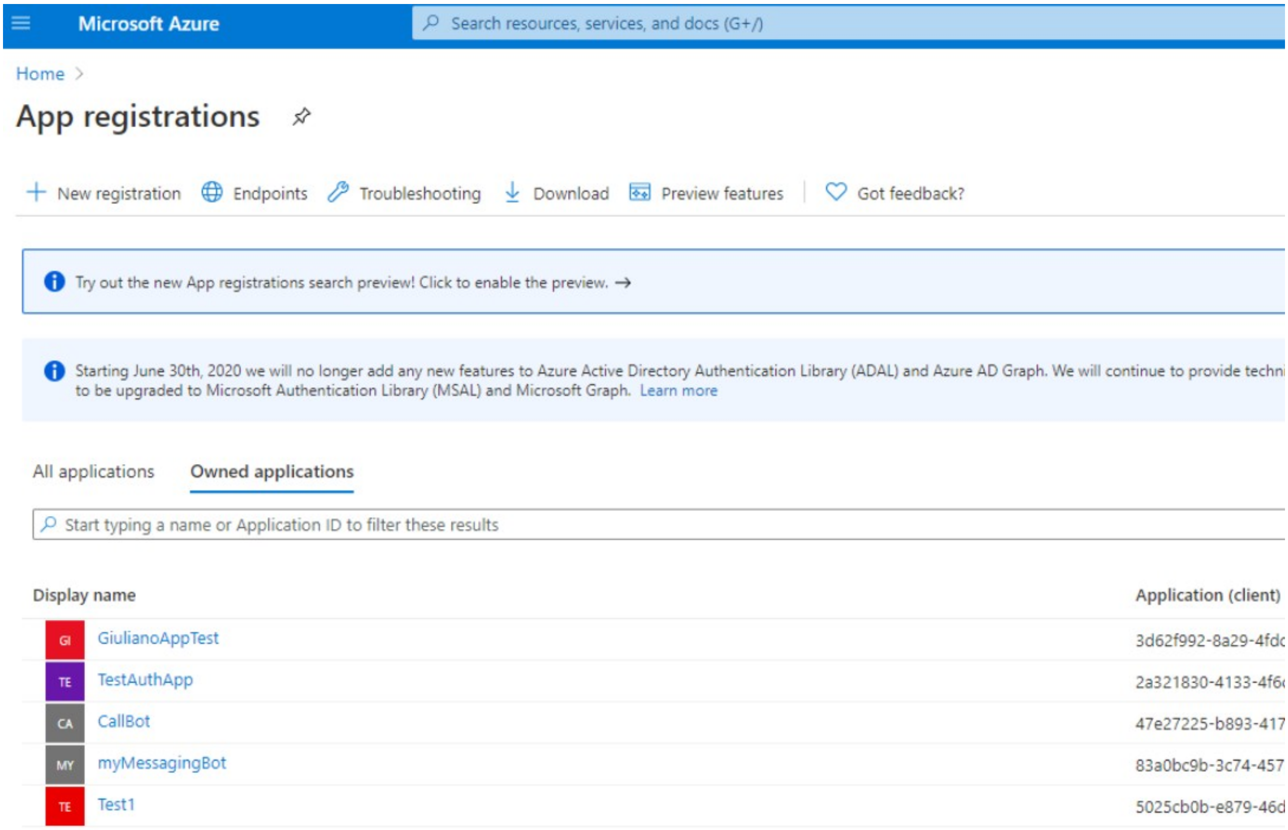
This authentication method is supported by Imagicle UC Suite, starting from 2021.Winter.2 release, and it relays on advanced OAuth2 authentication available for cloud-based Office 365 email service. Previous Imagicle releases are supporting OAuth2 basic authentication, which is dismissed by Microsoft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

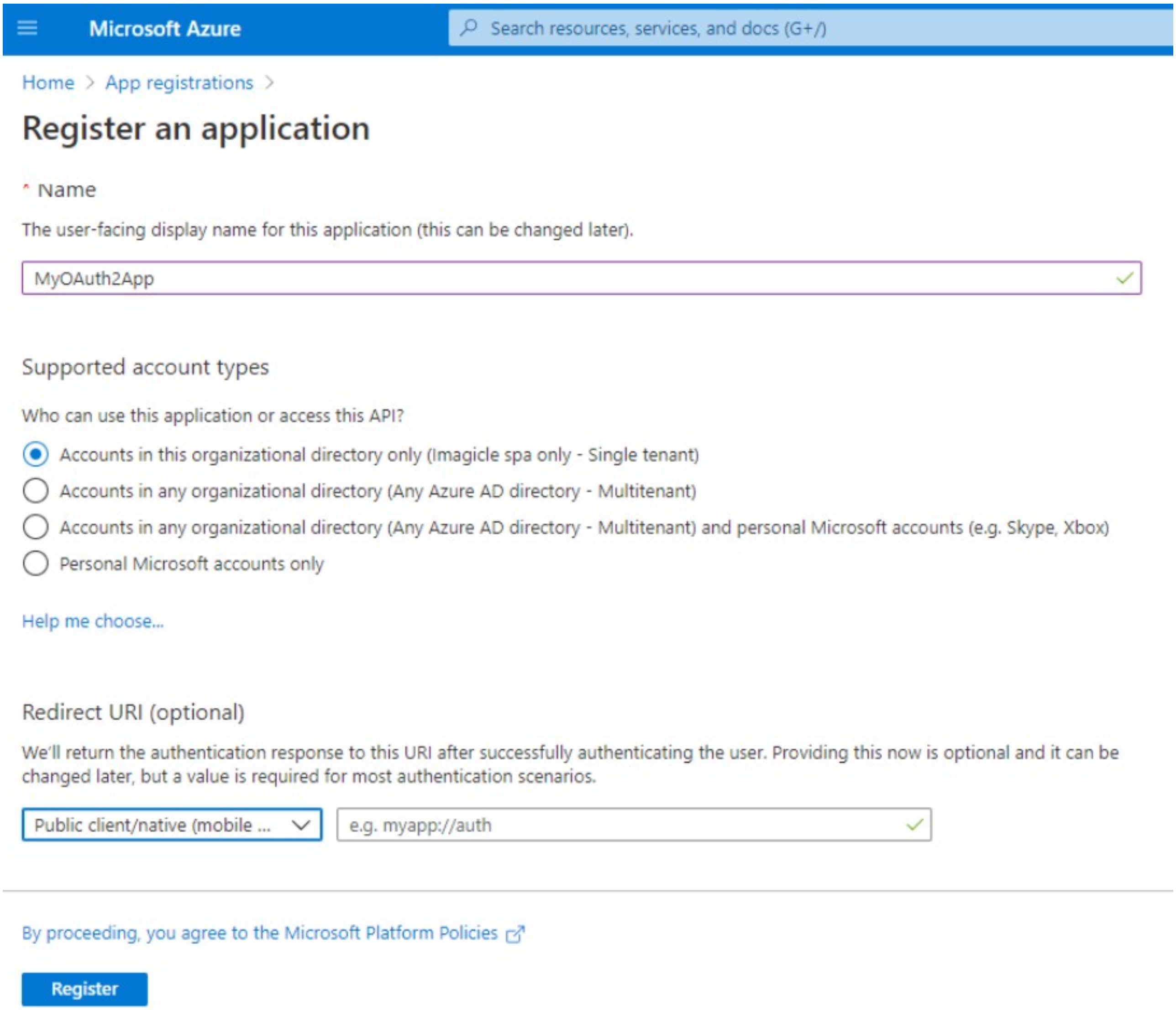


Try out the new App registrations search preview! Click to enable the preview. →

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide techni
to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Display name	Application (client)
GI GiulianoAppTest	3d62f992-8a29-4fdc
TE TestAuthApp	2a321830-4133-4f6
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...

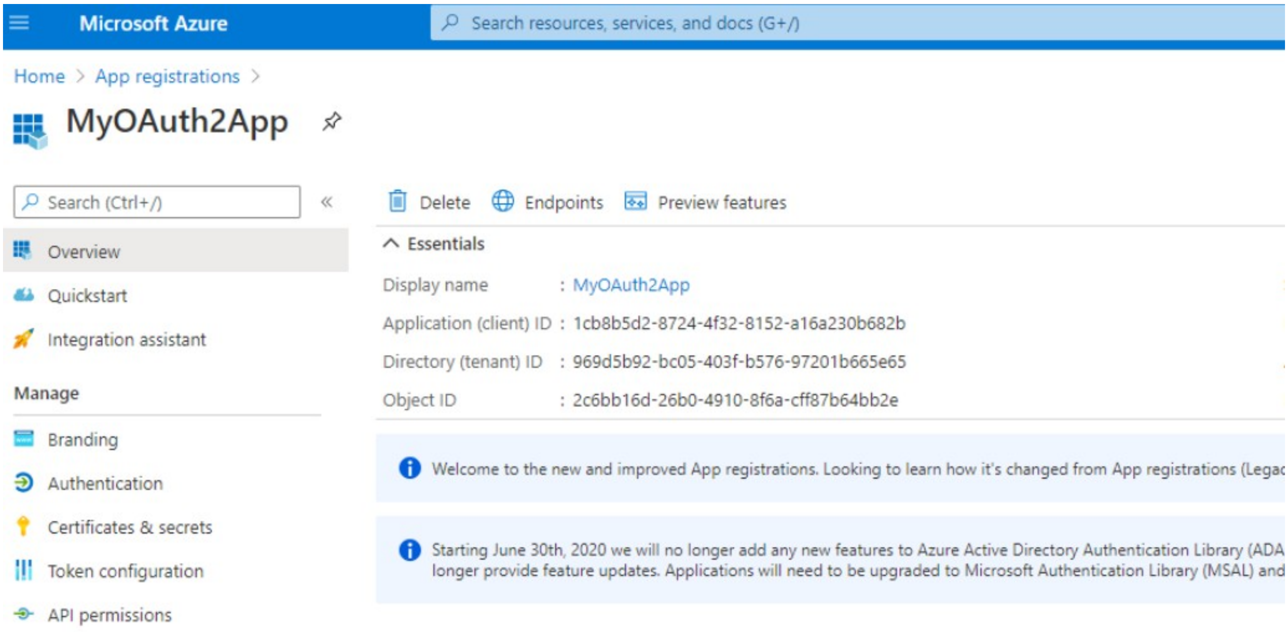
Redirect URI (optional)

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

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

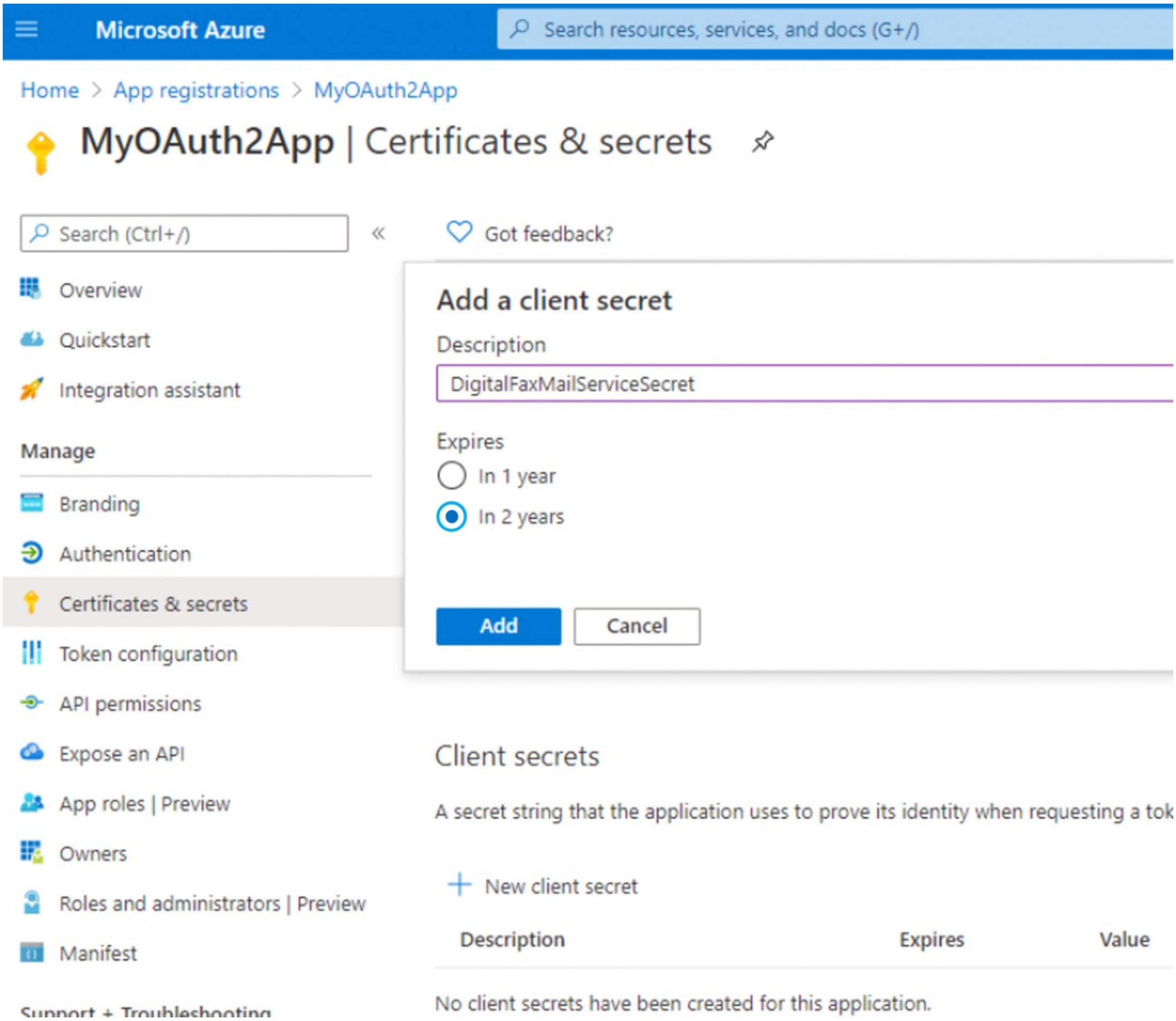


Display name : MyOAuth2App
Application (client) ID : 1cb8b5d2-8724-4f32-8152-a16a230b682b
Directory (tenant) ID : 969d5b92-bc05-403f-b576-97201b665e65
Object ID : 2c6bb16d-26b0-4910-8f6a-cff87b64bb2e

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legac

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADA longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and

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

Add a client secret

Description: DigitalFaxMailServiceSecret

Expires

○ In 1 year

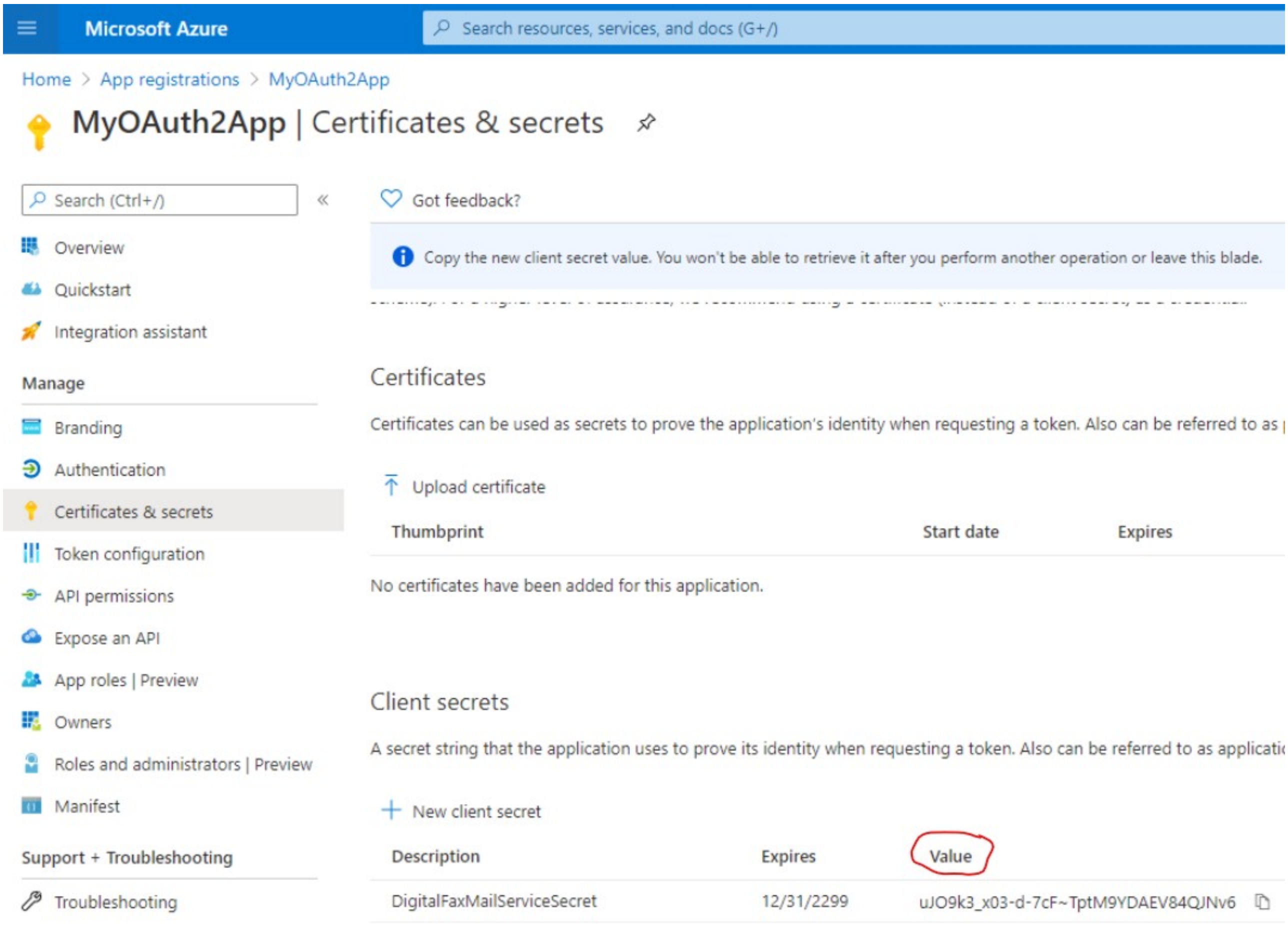
● In 2 years

Client secrets

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

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.



MyOAuth2App | Certificates & secrets

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

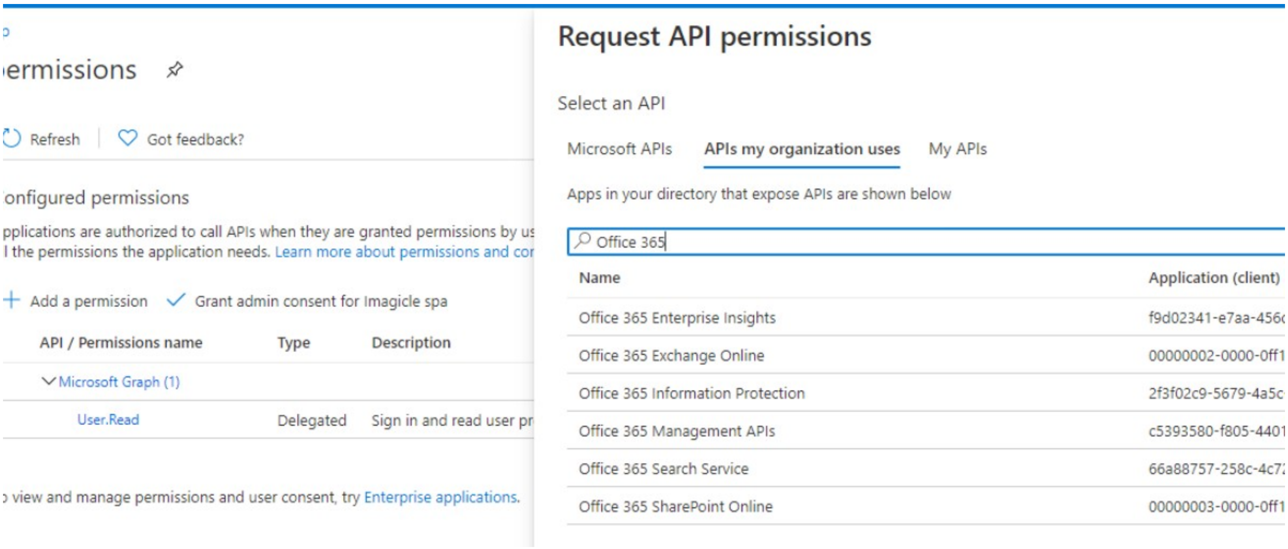
Thumbprint	Start date	Expires
No certificates have been added for this application.		

Client secrets

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

Description	Expires	Value
DigitalFaxMailServiceSecret	12/31/2299	uJO9k3_x03-d-7cF~TptM9YDAEV84QJNv6

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



onfigured permissions

pplications are authorized to call APIs when they are granted permissions by us
l the permissions the application needs. Learn more about permissions and con

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.

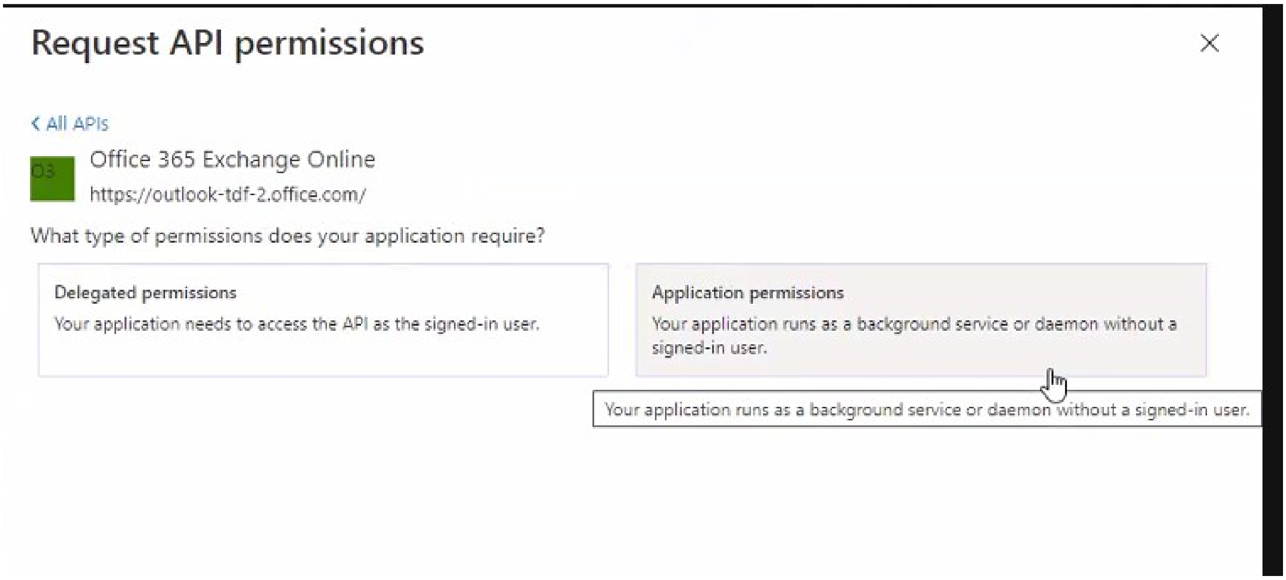
Request API permissions

Select an API

Apps in your directory that expose APIs are shown below

Name	Application (client)
Office 365 Enterprise Insights	f9d02341-e7aa-456
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 Exhange online" and then select "Application Permissions"



Request API permissions

< All APIs

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

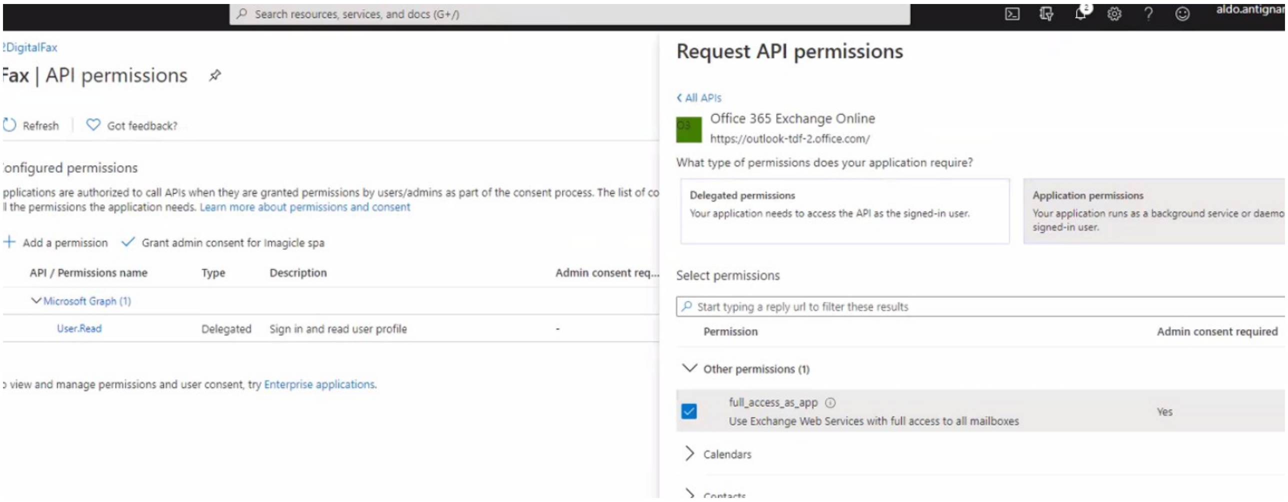
What type of permissions does your application require?

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.



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

aldo.antignar

:DigitalFax

Fax | API permissions

Refresh | Got feedback?

onfigured permissions

pplications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of co
l 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.

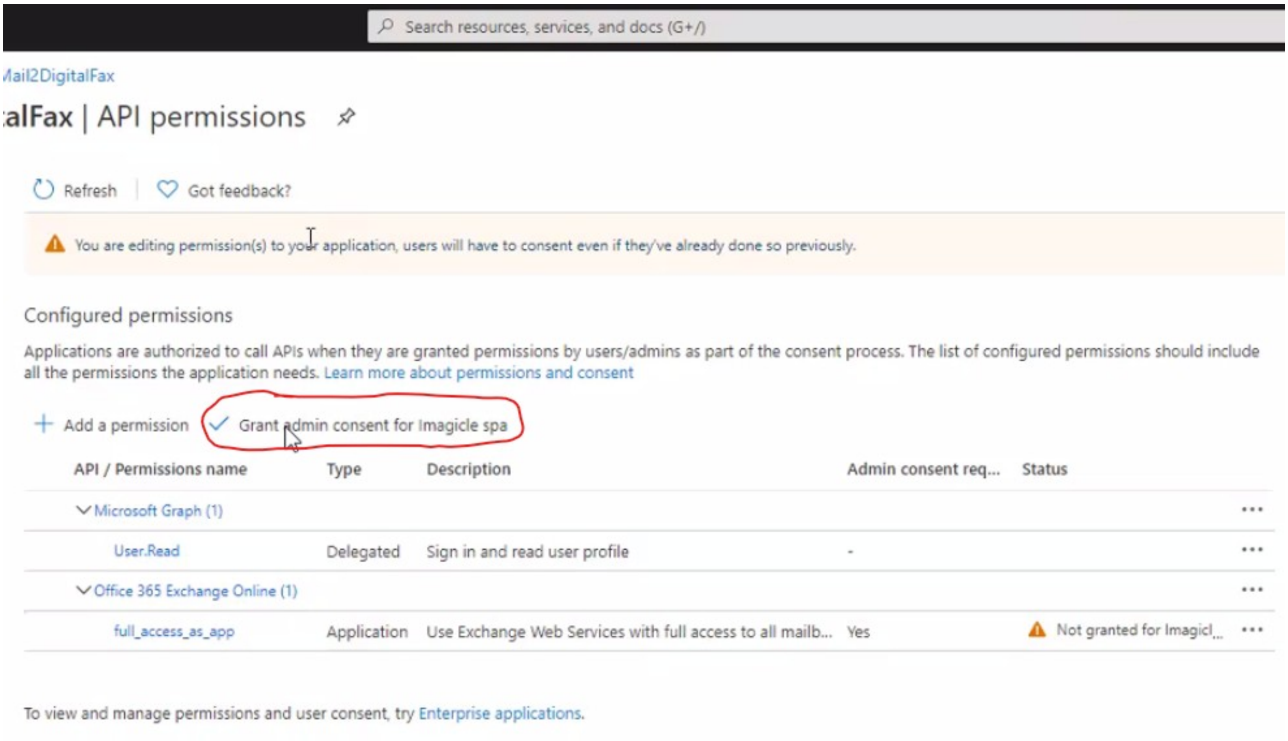
Application permissions
Your application runs as a background service or daemo
signed-in user.

Select permissions

Start typing a reply url to filter these results

	Permission	Admin consent required
	Other permissions (1)	
☑	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>".



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

/ail2DigitalFax

alFax | 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

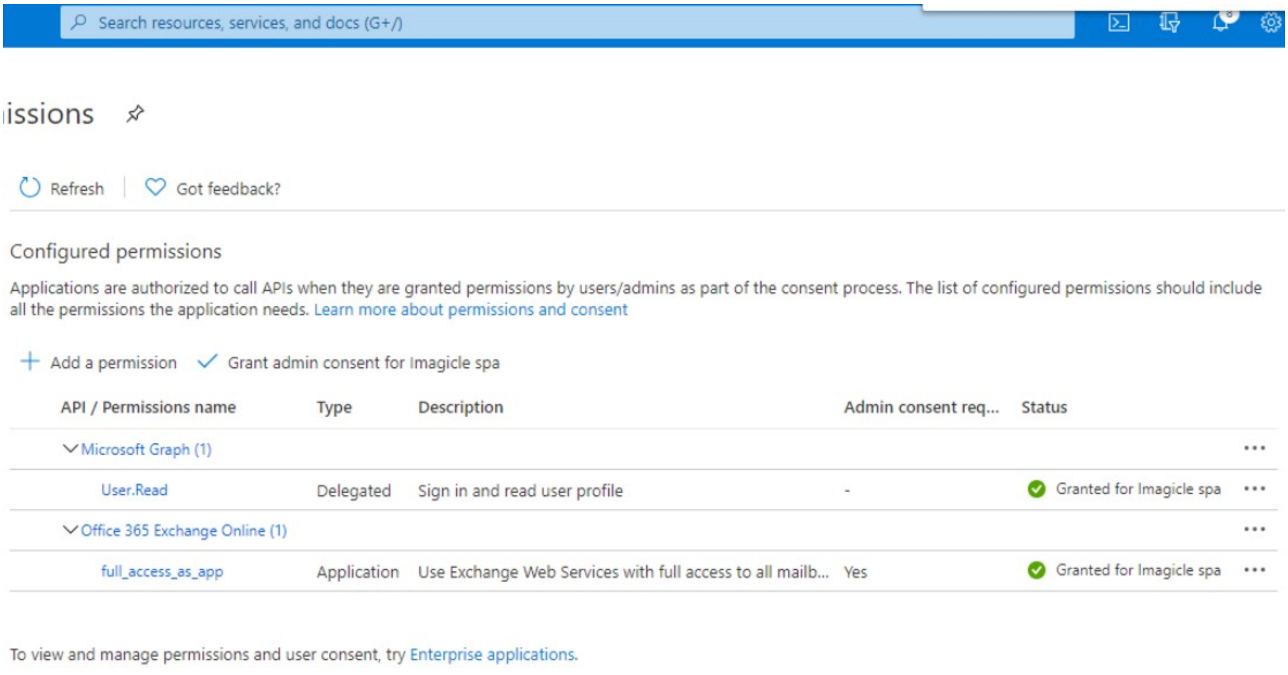
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

+ 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	Not granted for Imagicl...	•••

To view and manage permissions and user consent, try Enterprise applications.

This is the resulting page.



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

issions

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	-	✓ 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	✓ Granted for Imagicle spa	•••

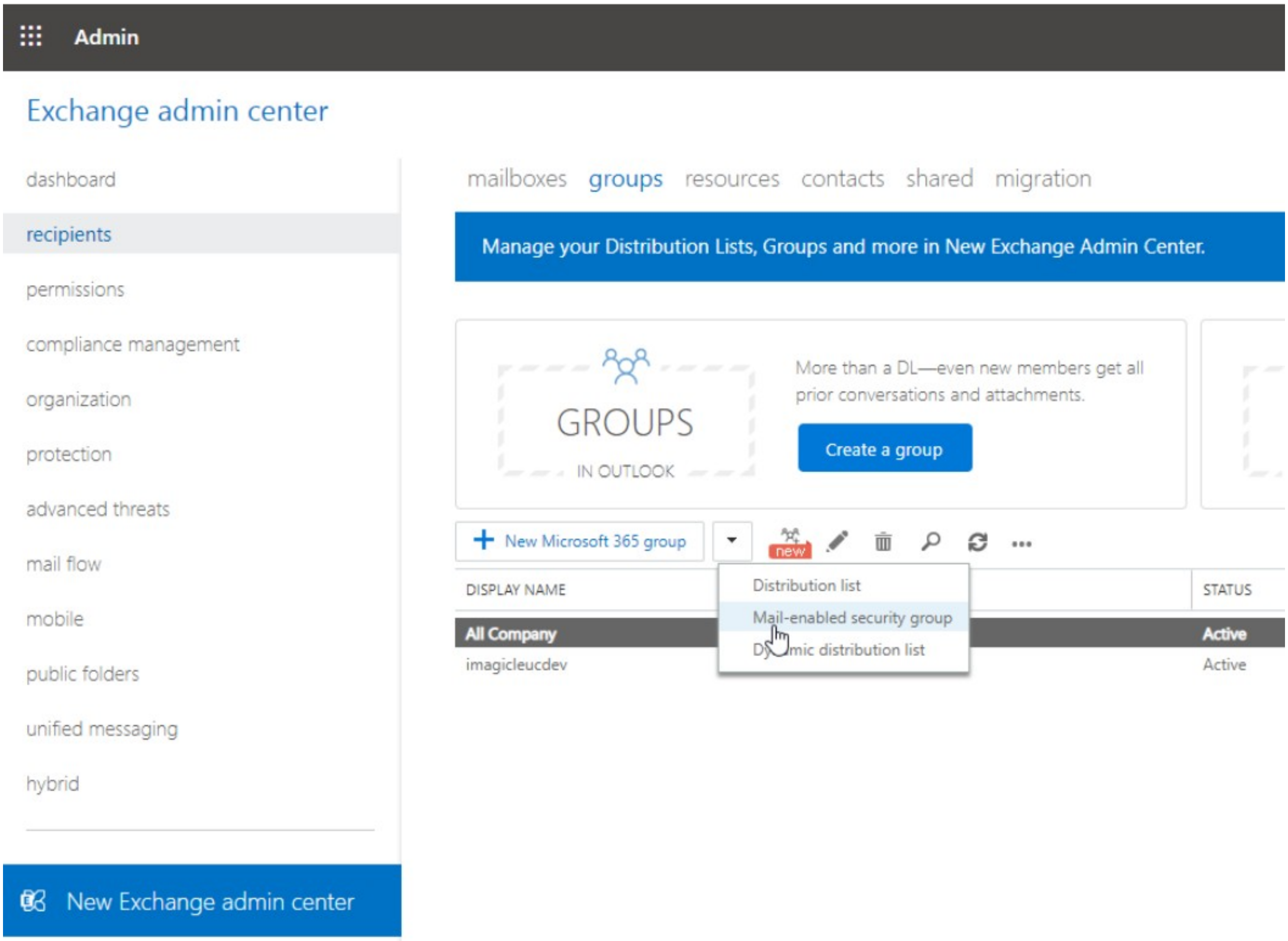
To view and manage permissions and user consent, try Enterprise applications.

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** â **Groups** â **New mail-enabled security group**

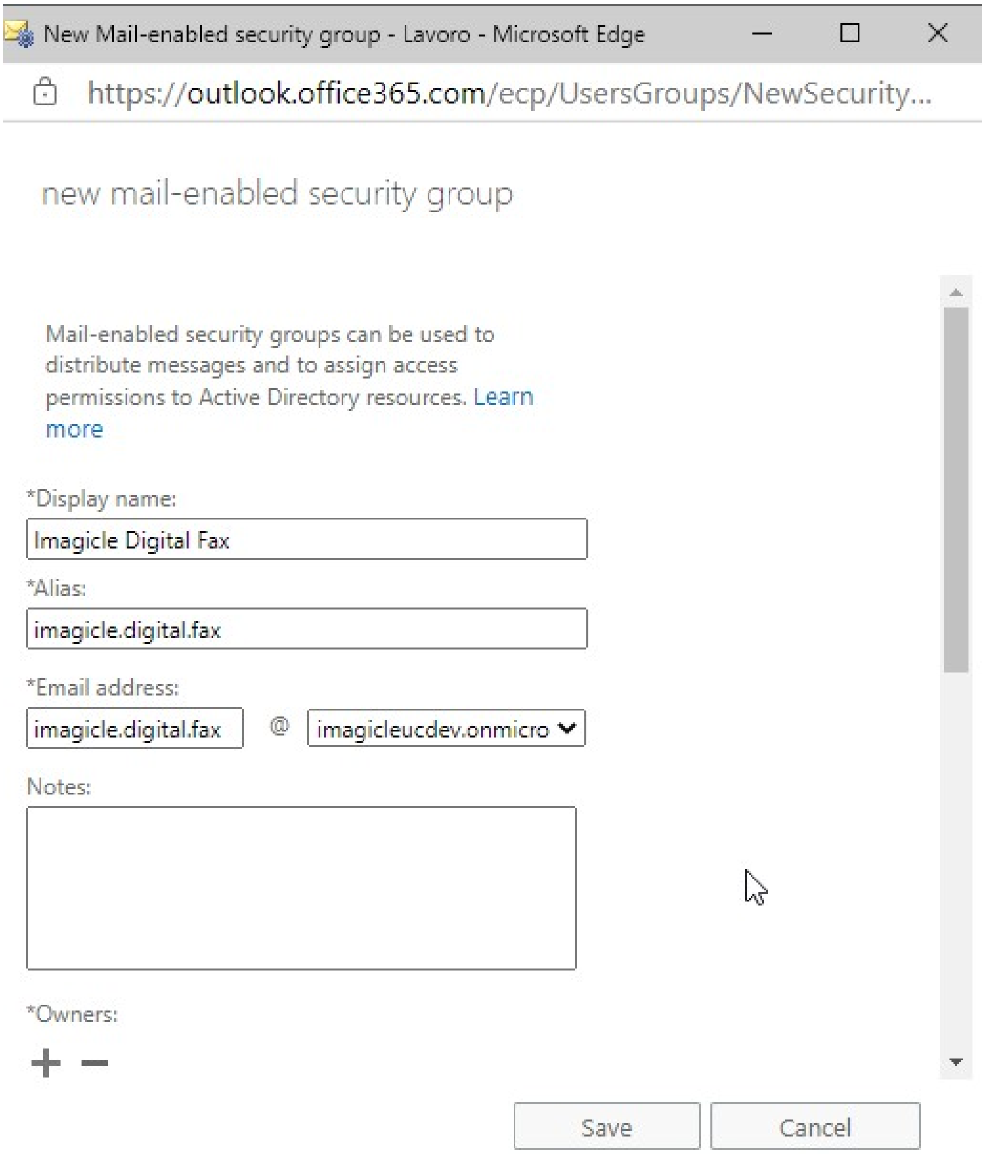


Manage your Distribution Lists, Groups and more in New Exchange Admin Center.

More than a DL—even new members get all prior conversations and attachments.

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 - Lavoro - Microsoft Edge

https://outlook.office365.com/ecp/UsersGroups/NewSecurity...

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: Imagicle Digital Fax

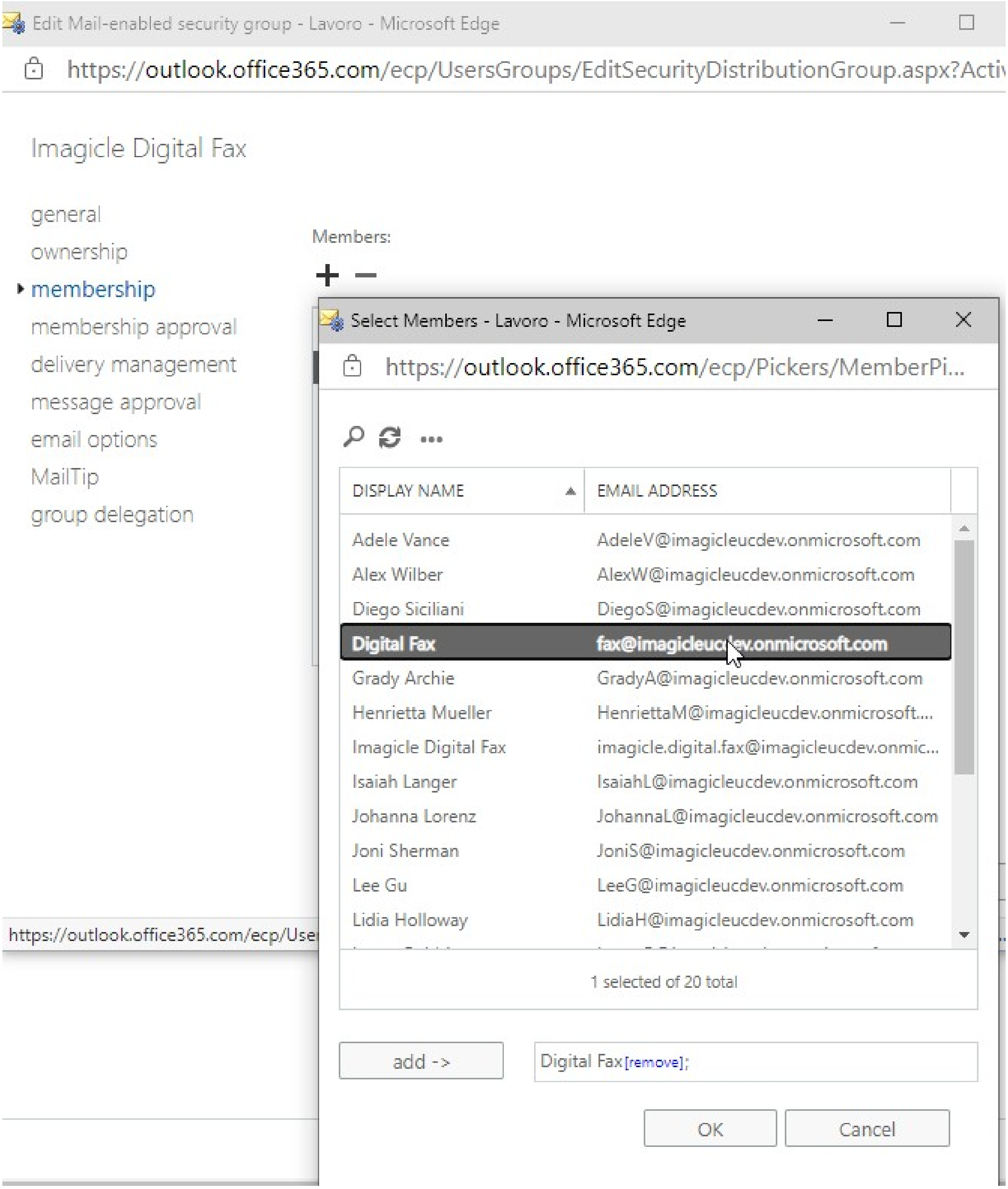
*Alias: imagicle.digital.fax

*Email address: imagicle.digital.fax @ imagicleucdev.onmicro

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:


Edit Mail-enabled security group - Lavoro - Microsoft Edge
https://outlook.office365.com/ecp/UsersGroups/EditSecurityDistributionGroup.aspx?Acti
Imagicle Digital Fax
general
ownership
membership
membership approval
delivery management
message approval
email options
MailTip
group delegation
Members:
Select Members - Lavoro - Microsoft Edge
https://outlook.office365.com/ecp/Pickers/MemberPi...
https://outlook.office365.com/ecp/Use
add ->
OK
Cancel

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....
Imagicle Digital Fax	imagicle.digital.fax@imagicleucdev.onmic...
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

Digital Fax [remove];

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
- **ECC-CURRI callbacks include prefix**: Enable this option if incoming calls notified by ECC do include the "prefix for incoming calls". If you are unsure, check the Blocked calls history in StoneLock administration after having configured ECC. This setting affects the lookup in Speedy directories for the **called** numbers of incoming calls.

Outgoing calls

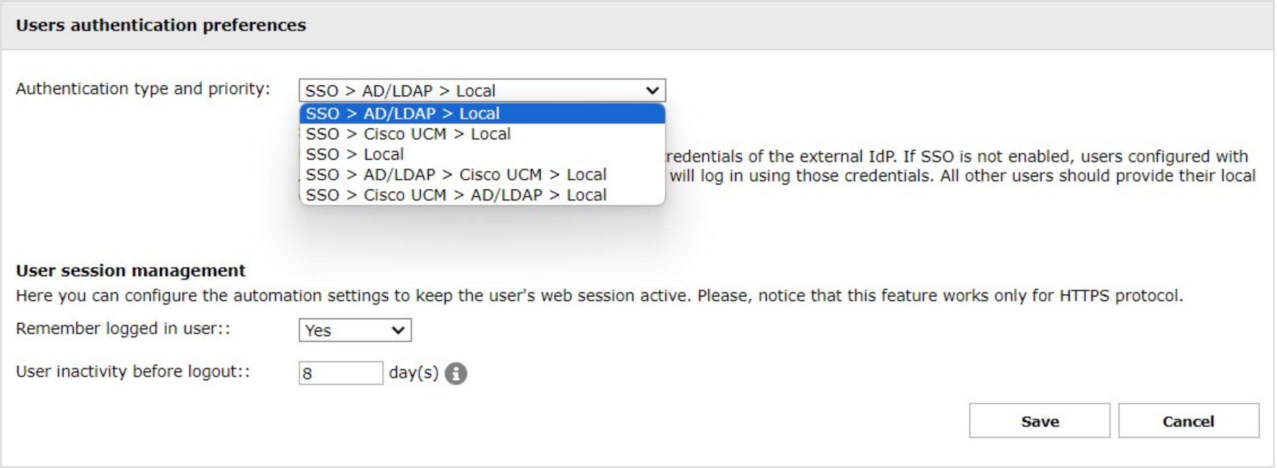
- **Prefix** for outgoing calls: This prefix will be automatically added to outgoing calls, e.g. to calls placed by Speedy towards external numbers. This prefix won't be added to internal calls nor to calls towards the users' primary extension configured in the users list
- **Suffix** for outgoing calls: 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.
- **ECC-CURRI callbacks include prefix**: Enable this option if incoming calls notified by ECC do include the "prefix for outgoing calls". If you are unsure, check the Blocked calls history in StoneLock administration after having configured ECC. 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 â   System Parameters â   Users authentication settings.

Users authentication preferences



Users authentication preferences

Authentication type and priority: SSO > AD/LDAP > Local

SSO > AD/LDAP > Local
SSO > Cisco UCM > Local
SSO > Local
SSO > AD/LDAP > Cisco UCM > Local
SSO > Cisco UCM > AD/LDAP > Local

redentials of the external IdP. If SSO is not enabled, users configured with will log in using those credentials. All other users should provide their local

User session management

Here you can configure the automation settings to keep the user's web session active. Please, notice that this feature works only for HTTPS protocol.

Remember logged in user:: Yes

User inactivity before logout:: 8 day(s)

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 loosing 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 an increase this parameter up to 30 days.

CuCM CTI Configuration

To allow Imagicle applications to monitor and control IP phones trough TAPI, the Cisco TSP must be installed on the UC Suite server. Please follow the procedure in the **Installation** chapter. Once the TSP is configured, you need to associate the devices to a new application user, reserved to Imagicle applications.

Create a dedicated Application User on Cisco UCM

Log on to Cisco Call Manager web interface and select from the menu: **User Management** -> **Application User**. Press the **Add new** button.

Enter a UserID and a password (e.g. **ImagicleCTI/ImagicleCTI**).

This user will be used by Imagicle applications to:

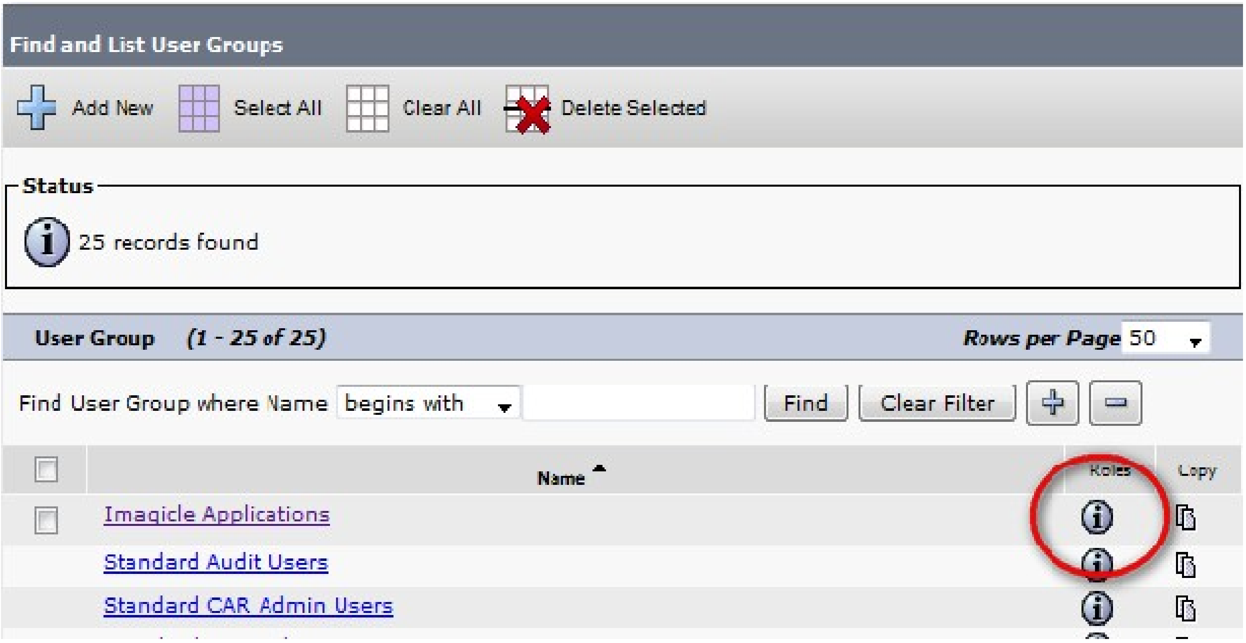
- Monitor and control devices through CTI
- Execute AXL queries
- Trigger On-Demand recording from Imagicle Attendant Console, gadget for Finesse and gadget for Jabber
- Leverage park ports to allow call park from Imagicle Attendant Console

Application User Permissions

Required permissions vary application by application. The following procedure allows you to add the minimal list of permissions to let all the Imagicle applications run as expected.

1. From the "User Management" menu select "User Settings", then "Access Control Group". Press "Add". Enter "Imagicle Applications" and press Save.

2. Edit the list of roles associated to the Access Control Group by clicking the little grey button to the right.



25 records found

User Group (1 - 25 of 25) Rows per Page 50

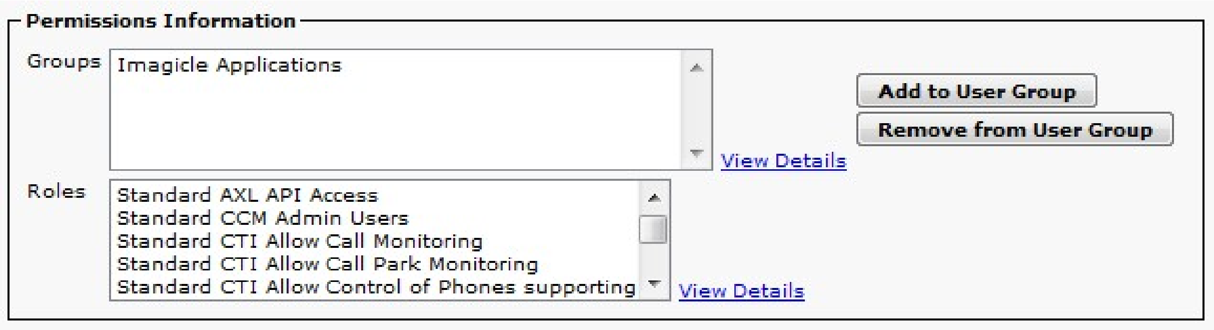
Find User Group where Name begins with

□	Name	Roles	Copy
□	Imagicle Applications	ⓘ	⎘
	Standard Audit Users	ⓘ	⎘
	Standard CAR Admin Users	ⓘ	⎘

Press "Assign Role to Group" and select:

- Standard AXL API Access
- Standard CCM Admin Users
- Standard CTI Allow Call Monitoring
- Standard CTI Allow Call Park Monitoring

- Standard CTI Allow Call Recording
- Standard CTI Enabled
- Standard CTI Allow Control of Phones supporting Connected Xfer and conf
- Standard CTI Allow Control of Phones supporting Rollover Mode
- Standard SERVICEABILITY Read Only


Permissions Information

Groups: Imagicle Applications

Roles:
Standard AXL API Access
Standard CCM Admin Users
Standard CTI Allow Call Monitoring
Standard CTI Allow Call Park Monitoring
Standard CTI Allow Control of Phones supporting

Permissions details

â ¢ Standard AXL API Access
 This role is used to access to AXL API for getting the list of users and devices using AXL protocol

â ¢ Standard CCM Admin Users
This role is needed to log in to Cisco Unified Communications Manager Administration (For AXL API access)

â ¢ Standard CTI Allow Call Monitoring
It allows our CTI application to monitor the status of the CUCM device using CTI (needed for Attendant Console, ACD, Phonelock, recording and for getting information shared among all the Imagicle applications)

â ¢ Standard CTI Allow Call Park Monitoring
It allows our CTI application to monitor the status of the CUCM park resources (showing these info in the attendant console). Please make sure to configure no more than 500 park ports on CUCM, to avoid CTI service overload.

â ¢ Standard CTI Allow Call Recording
It allows our Call Recording application to record calls

â ¢ Standard CTI Enabled
It enables CTI application control for our applications, needed by attendant console, recorder, ACD, phone lock

â ¢ Standard CTI Allow Control of Phones supporting Connected Xfer and conf
Same as standard CTI enabled, but for devices that supported Rollover mode

â ¢ Standard CTI Allow Control of Phones supporting Rollover Mode
Same as standard CTI enabled, but for devices that supported connected transfer and conferencing

â ¢ Standard SERVICEABILITY Read Only
It allows Imagicle applications to view all SOAP Serviceability AXL APIs, the SOAP Call Record APIs, and the SOAP Diagnostic Portal (Analysis Manager) Database Service, used for getting info about phone and devices in real time.

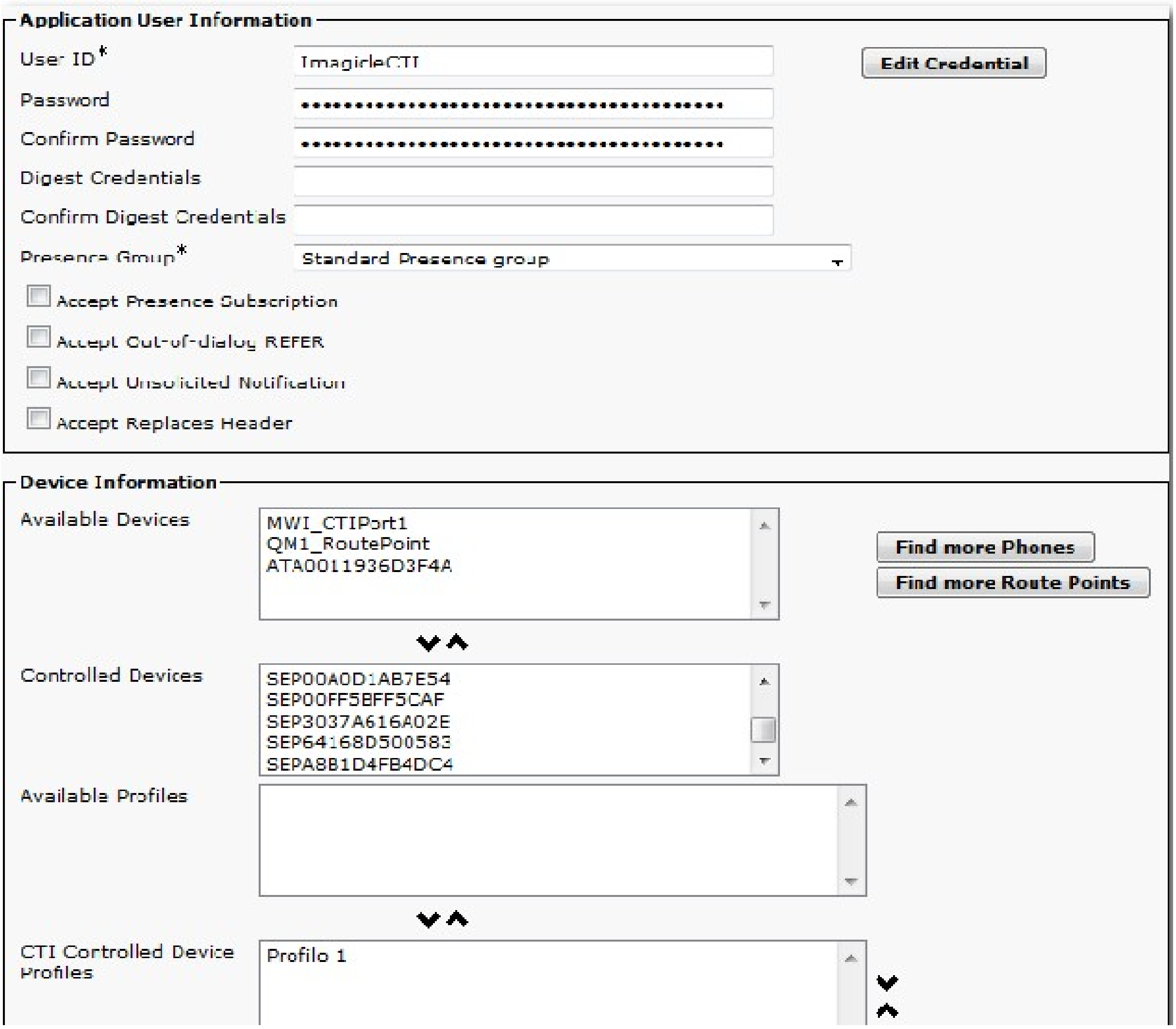
Device Association

When the Imagicle Applications has been created, and the ImagicleCTI user has been added to it, you have to associate to this user all the devices you want to be monitored or controlled. Supported devices are:

- SEPxxxxxxx = Cisco IP Phones
- CSFxxxxxxx = Jabber and Webex desktop clients

If Extension Mobility is enabled, associate the relevant profiles AND the devices. Please bear in mind that some Imagicle apps don't leverage TAPI, like Digital Fax and Call Analytics. For the Attendant console, all operators' phones need to be associated.

Real-time BLF status display on Attendant Console might be retrieved from the Presence Server. If not available, then you need to add all phones to this Application User. Please refer to the specific application PBX configuration section for details.



Application User Information

User ID*	ImagicleCTI
Password	•••
Confirm Password	•••
Digest Credentials	
Confirm Digest Credentials	
Presence Group*	Standard Presence group

☐ Accept Presence Subscription

☐ Accept Out-of-dialog REFER

☐ Accept Unsolicited Notification

☐ Accept Replaces Header

Device Information

Available Devices
MWI_CTIPort1
QM1_RoutePoint
ATA0011936D3F4A

Controlled Devices
SEP00A0D1AB7E54
SEP00FF5BFF5CAF
SEP3037A616A02E
SEP64168D500583
SEPA8B1D4FB4DC4

Available Profiles

CTI Controlled Device Profiles
Profilo 1

Enable AXL access to Cisco UCM

AXL is a Cisco legacy protocol based on SOAP and XML which Imagicle Application Suite leverages to retrieve the IP addresses of Cisco IP Phones, extension mobility login status and user device association. If AXL queries are disabled, many features of the Imagicle Application Suite won't be available.

Cisco Unified CallManager

Three steps are required for the Imagicle Application Suite to be able to make AXL queries to the CallManager:

- Create an Application user with the rights to execute AXL queries
- Set Imagicle AXL/CTI user credentials in the Telephony Service parameters page of the Imagicle Application Suite
- Ensure that the AXL service is enabled in the Application Suite server

Axl Service authenticates by the credentials you enter in the **Administration - System Parameters - IP Telephony Service** parameters.

You can either use the ImagicleCTI user you created to control IP phones, or the main CallManager administrator credentials.

Please make sure you also entered the CuCm the IP address. For CuCm clusters, this is the address of the node running the AXL service (which usually is the Publisher).

The Imagicle Axl client service can be started from the web interface through the **Directory - Manage Service** page. Ensure Speedy service is operational. If not, press Start.

You can also start the service by the Windows Services management console. Ensure the "Imagicle AXL Client" service status is "started".

Cisco Unified CallManager Express

Add the following commands to enable the AXL support and to set the AXL password:

```
(configure terminal)
  ip http server
  ip http path flash
  !
  ixi transport http
  no shutdown
  !
  ixi application cme
  no shutdown

(telephony-service)
  log password cisco
  xmltest
  xml user YourUsername password YourPassword 15
```

The username and password must match the one you entered in the Telephony services web page.

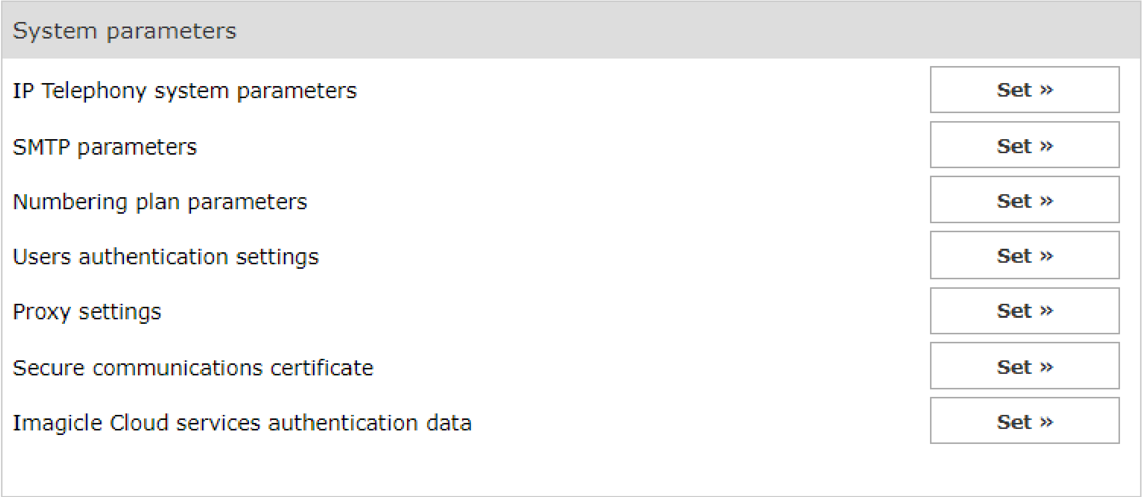
Then ensure Speedy services are operational (see above).

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
- 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 â   System parameters link in the App Suite menu, hitting "Proxy settings" button.

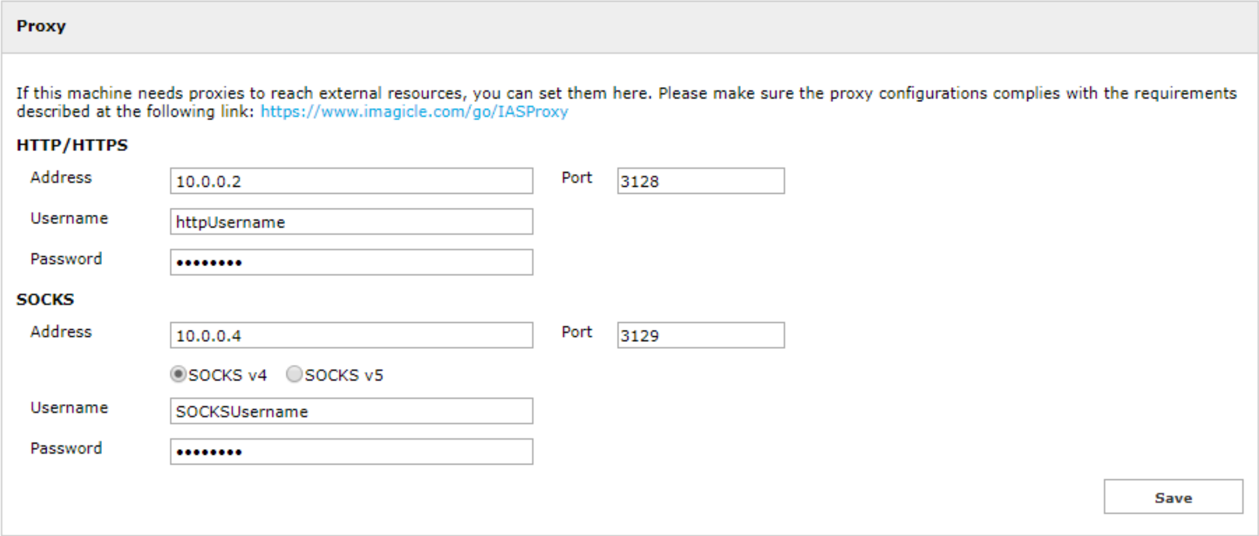


System parameters	
IP Telephony system parameters	Set »
SMTP parameters	Set »
Numbering plan parameters	Set »
Users authentication settings	Set »
Proxy settings	Set »
Secure communications certificate	Set »
Imagicle Cloud services authentication data	Set »

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: 10.0.0.2 Port: 3128

Username: httpUsername

Password: ••••••••

SOCKS

Address: 10.0.0.4 Port: 3129

● SOCKS v4 ○ SOCKS v5

Username: SOCKSUsername

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.

Secure Communications Certificate

This article is applicable to Imagicle ApplicationSuite 2020.Spring.1 or later and it allows to download the Digital Certificate, required to enable Secure SIP and Secure RDP communications for both Imagicle Call Recording and Queue Manager Enterprise applications.

Loading the Imagicle Certificate on CallManager

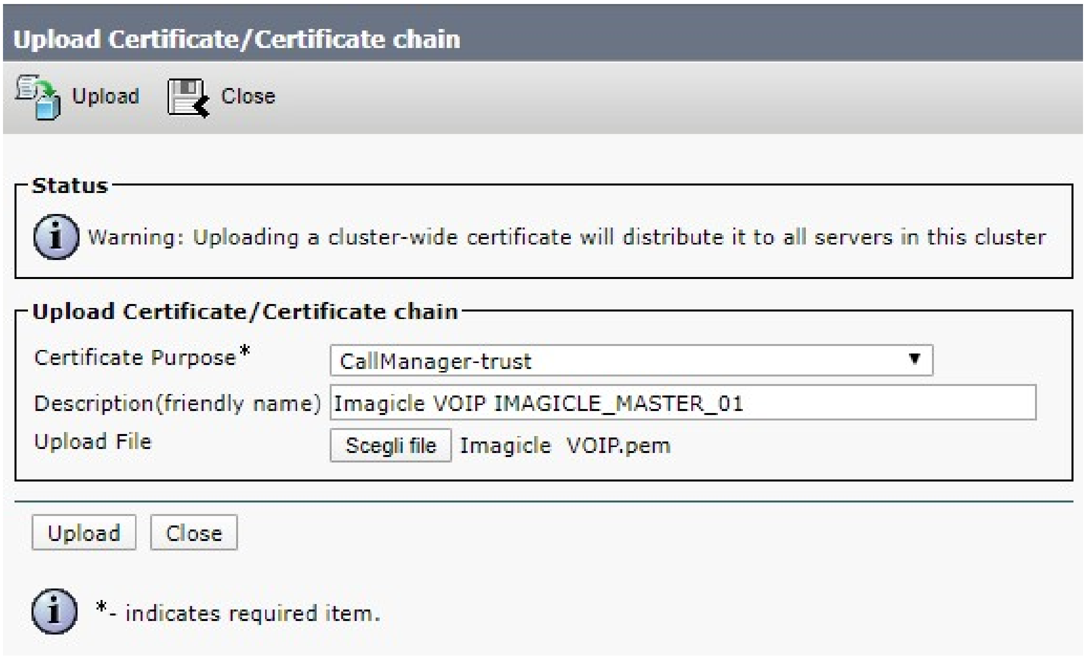
When Imagicle Server boots up, it creates a security certificate which is valid for the IAS server on which it was generated. It must be downloaded from the web interface, and loaded onto CuCM.

To get the Imagicle certificate:

- Login to the IAS web interface as Administrator
- Click on Admin â System Parameters â Secure communications certificate
- Click on the **Download** button to download the communal Imagicle digital certificate and save it to your PC. The file extension is .pem.

To load the certificate on CuCM:

- Log on CuCM as Administrator
- Select OS Administration
- From the menu, choose Security, Certificate Management
- Press the "Upload Certificate / Certificate chain" button
- As certificate purpose, choose "Callmanager-trust"
- Enter a description and then select Imagicle certificate from your PC and upload it
- Press "Close" to go back to the certificate list



Upload Certificate/Certificate chain

Status

Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

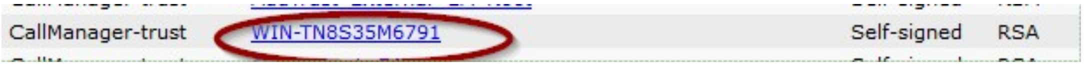
Certificate Purpose* CallManager-trust

Description(friendly name) Imagicle VOIP IMAGICLE_MASTER_01

Upload File Scegli file Imagicle VOIP.pem

*- indicates required item.

- Press "Find" to list the certificates. Locate the Imagicle certificate you just uploaded.
- Take note of the certificate Common Name for later use. By default, the certificate Common Name will match the computer name of the machine on which it was generated.



CallManager-trust	WIN-TN8S35M6791	Self-signed	RSA

Warning: Changing the Computer Name will invalidate the certificate. If you change the IAS server computer name, you need to regenerate the digital certificate.

Warning: The digital certificate will last 5 years from the day it was generated, which is the day the product was installed. If required, the certificate can be re-generated for additional 5 years, by following this procedure.

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

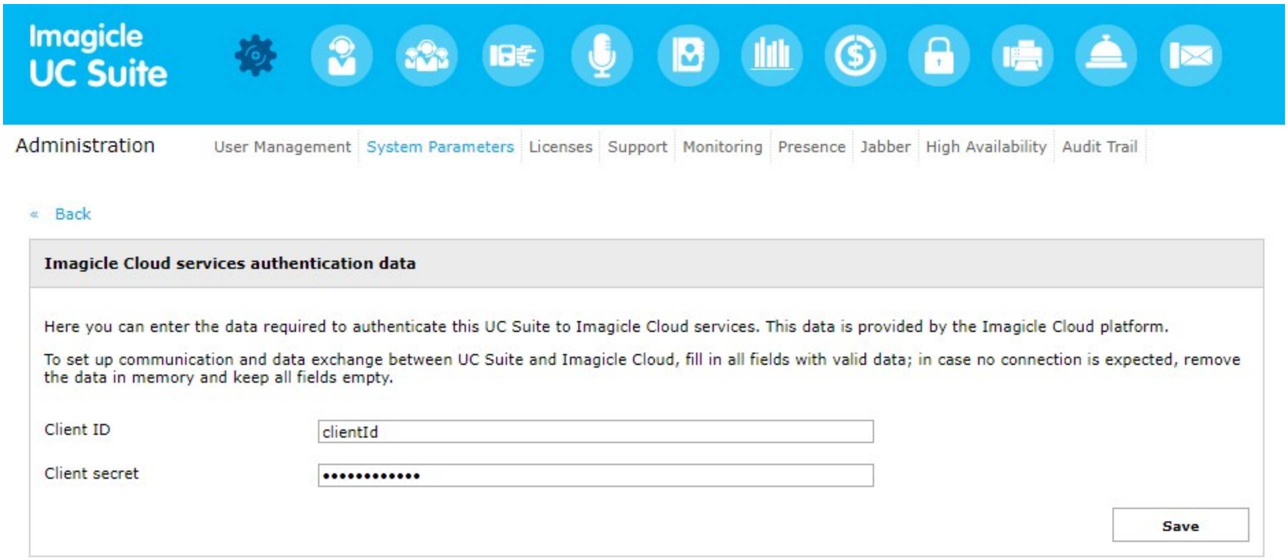
Please send above data to Imagicle Support Team.

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:



Imagicle Cloud services authentication data

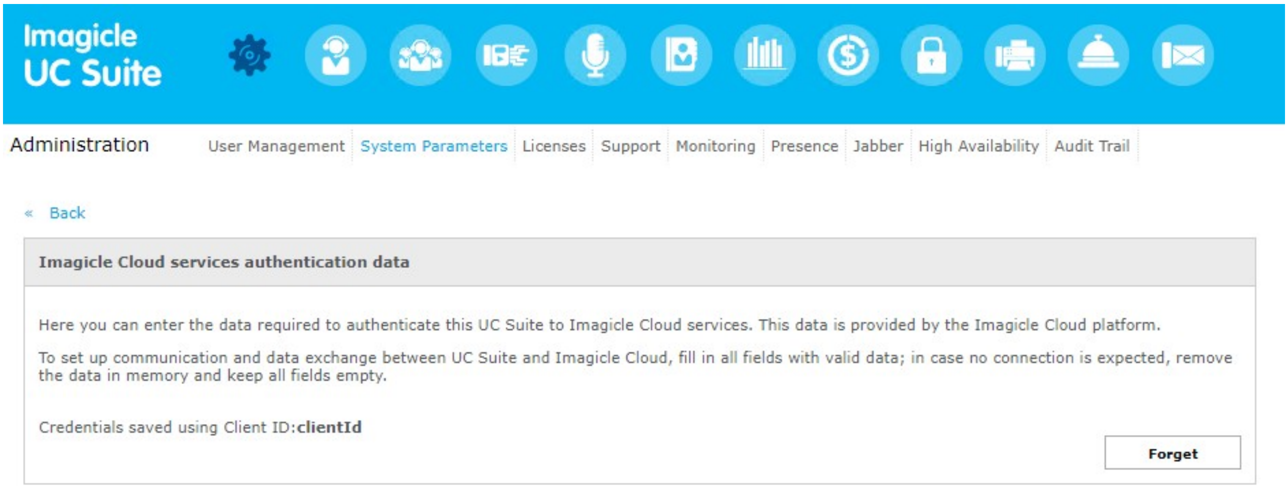
Here you can enter the data required to authenticate this UC Suite to Imagicle Cloud services. This data is provided by the Imagicle Cloud platform.

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.

Client ID: clientId

Client secret: ••••••••••••

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



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:

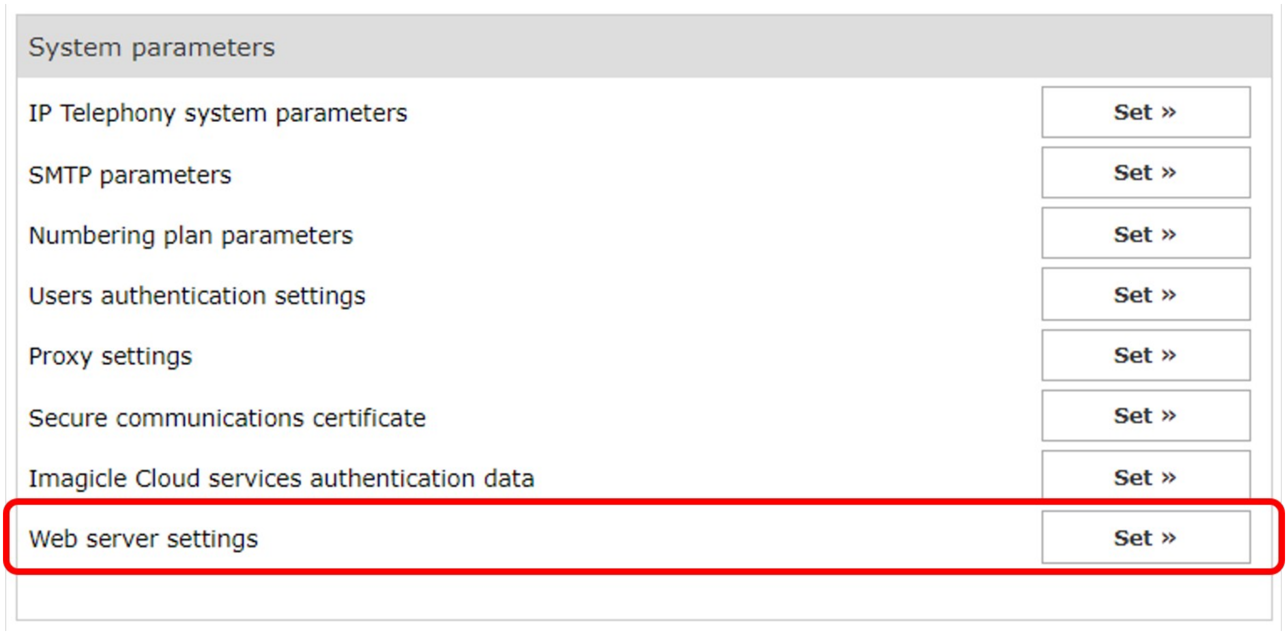
```
C:\Program Files (x86)\StonevoiceAS\Var\Log\w3wp\ApplicationSuite.log
```

Web Server setting

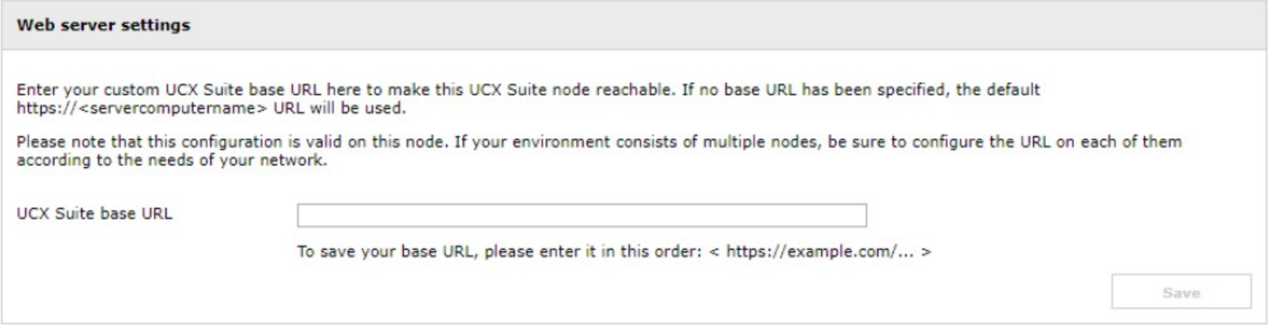
This article is applicable to Imagicle UCX Suite 2023.Spring.1 or later and it allows to change the embedded web server's URL to reach Imagicle web portal and leverage Imagicle APIs.

How to change web server's URL

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


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 »
Web server settings
Set »

The following window pops-up:



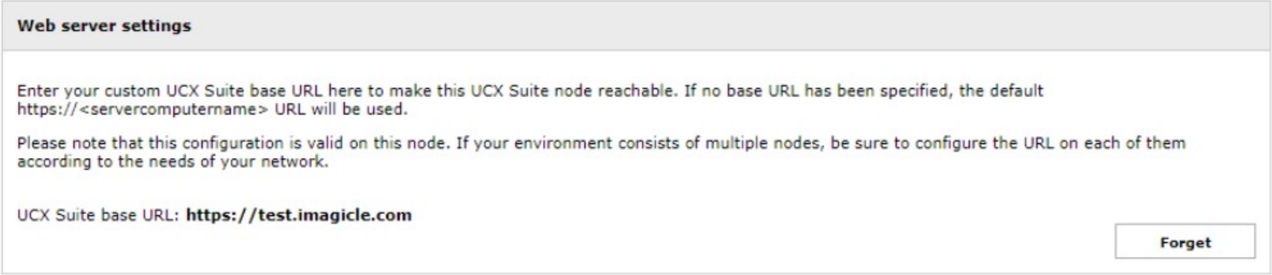
Enter your custom UCX Suite base URL here to make this UCX Suite node reachable. If no base URL has been specified, the default https://<servercomputername> URL will be used.

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.

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

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