# MAGOWEB – User Manual

## *Purpose of the procedure*

The procedure describes how to perform the purchase, installation, repair and configuration of MagoWeb

## *Index*

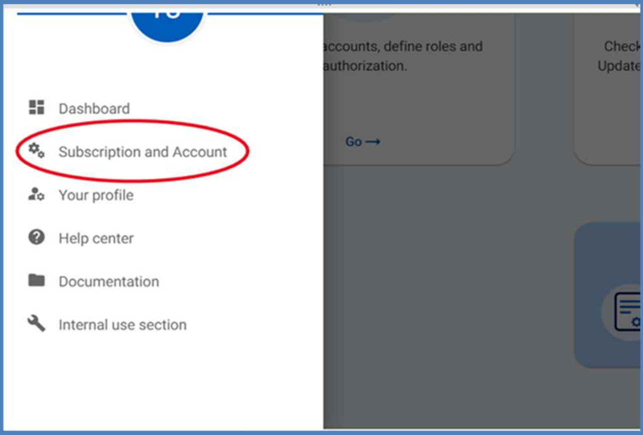
- **Purchase Magoweb** ........................................................................................ 2
- **Hardware and Software Prerequisites** ........................................................ 4
- **First Installation** ........................................................................................ 5
- **Maintenance and configuration of installation** ......................................... 15
- **Database Management** ............................................................................ 18
- **Update to another version** ........................................................................ 20
- **Uninstalling and recovery** ......................................................................... 22
- **Addendum A : Details on Microsoft application creation for Oauth** .............. 24
- **Addendum B: Magoweb online exposure** .................................................... 30
- **Addendum C: Certificate Configuration** .................................................... 31
- **Troubleshooting** ......................................................................................... 32

# PURCHASE MAGOWEB

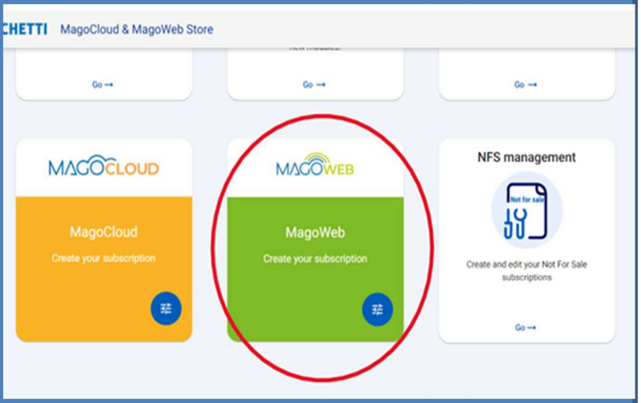
## PURCHASE MAGOWEB : STORE

○ *https://store.mago.cloud/home* : Link required for subscription activation.
(For internal developers: select the store of the test-store environment or release-store)

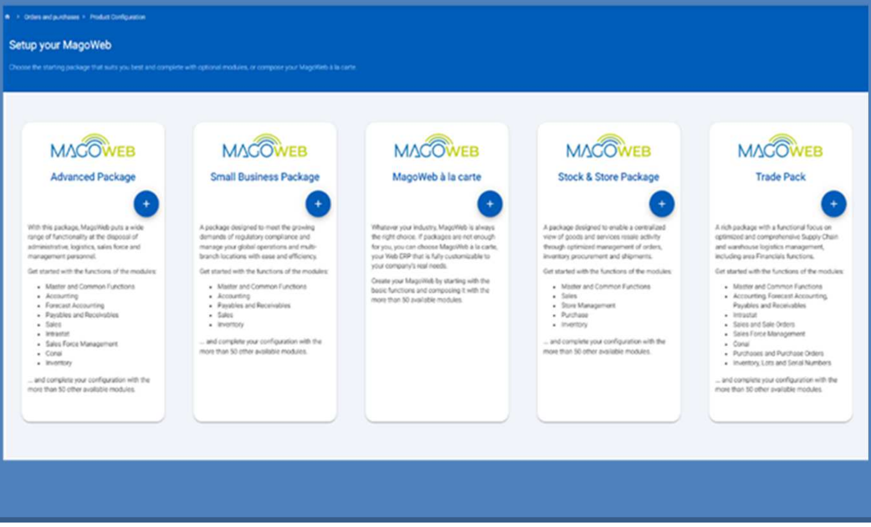
Once authenticated, in the left panel select **Subscription and Account** to activate MagoWeb.



Seleziona MagoWeb – *Create your subscription* .



Select one of the Packs
 Proposed



Setup your MagoWeb

Choose the starting package that suits you best and complete with optional modules, or compose your MagoWeb à la carte.

MAGOWEB **Advanced Package**

With this package, MagoWeb puts a wide range of functionality at the disposal of administrative, logistics, sales force and management personnel.

Get started with the functions of the modules:

- Master and Common Functions
- Accounting
- Forecast Accounting
- Payables and Receivables
- Sales
- Intrastat
- Sales Force Management
- Conai
- Inventory

... and complete your configuration with the more than 50 other available modules.

MAGOWEB **Small Business Package**

A package designed to meet the growing demands of regulatory compliance and manage your global operations and multi-branch locations with ease and efficiency.

Get started with the functions of the modules:

- Master and Common Functions
- Accounting
- Payables and Receivables
- Sales
- Inventory

... and complete your configuration with the more than 50 other available modules.

MAGOWEB **MagoWeb à la carte**

Whatever your industry, MagoWeb is always the right choice. If packages are not enough for you, you can choose MagoWeb à la carte, your Web ERP that is fully customizable to your company's real needs.

Create your MagoWeb by starting with the basic functions and composing it with the more than 50 available modules.

MAGOWEB **Stock & Store Package**

A package designed to enable a centralized view of goods and services resale activity through optimized management of orders, inventory procurement and shipments.

Get started with the functions of the modules:

- Master and Common Functions
- Sales
- Store Management
- Purchase
- Inventory

... and complete your configuration with the more than 50 other available modules.

MAGOWEB **Trade Pack**

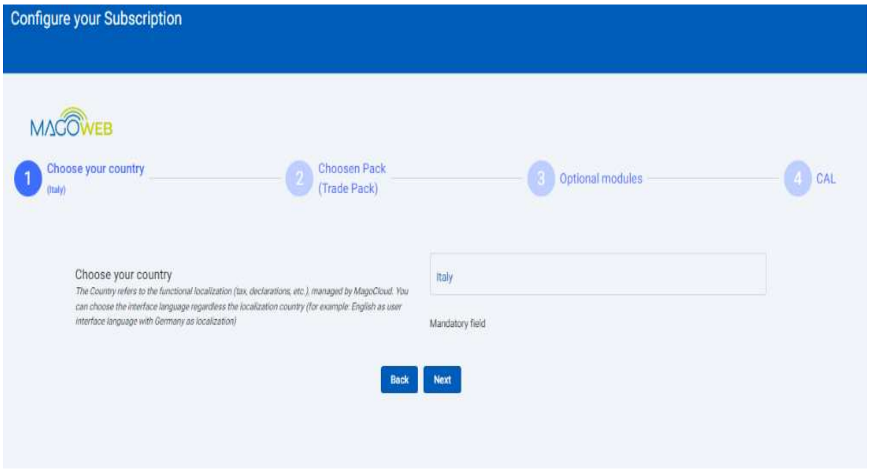
A rich package with a functional focus on optimized and comprehensive Supply Chain and warehouse logistics management, including area Financials functions.

Get started with the functions of the modules:

- Master and Common Functions
- Accounting, Forecast Accounting, Payables and Receivables
- Intrastat
- Sales and Sale Orders
- Sales Force Management
- Conai
- Purchases and Purchase Orders
- Inventory, Lots and Serial Numbers

... and complete your configuration with the more than 50 other available modules.

- This screen then appears, where you can proceed with the selection of the country and view the chosen basic packs and then the optional ones.



Configure your Subscription

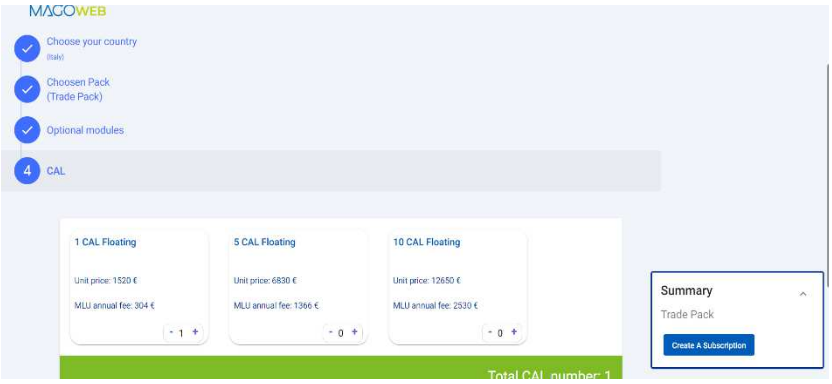
Choose your country

*The Country refers to the functional localization (tax, declarations, etc.), managed by MagoCloud. You can choose the interface language regardless the localization country (for example: English as user interface language with Germany as localization)*

Italy

Mandatory field

- At the end of the 4 steps click *Create a Subscription* to end the process.



1 CAL Floating
Unit price: 1520 €
MLU annual fee: 304 €
- 1 +

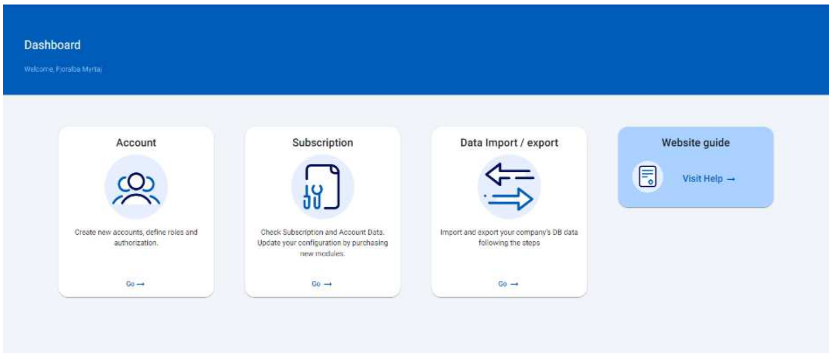
5 CAL Floating
Unit price: 6830 €
MLU annual fee: 1366 €
- 0 +

10 CAL Floating
Unit price: 12650 €
MLU annual fee: 2530 €
- 0 +

Total CAL number: 1

Summary
Trade Pack

- Finally, returning to the Dashboard, you can view your subscriptions.



Dashboard

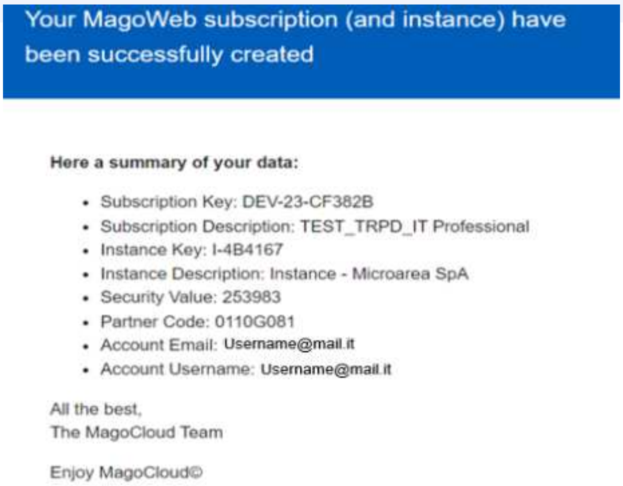
Welcome, Fioralba Myrtaj

Account
Create new accounts, define roles and authorization.

Subscription
Check Subscription and Account Data. Update your configuration by purchasing new modules.

Data Import / export
Import and export your company's DB data following the steps

- At the end of the process you will receive an email containing the information necessary for the installation, including the ***Instance Key*** and the ***Security Value***



Your MagoWeb subscription (and instance) have been successfully created

**Here a summary of your data:**

- Subscription Key: DEV-23-CF382B
- Subscription Description: TEST_TRPD_IT Professional
- Instance Key: I-4B4167
- Instance Description: Instance - Microarea SpA
- Security Value: 253983
- Partner Code: 0110G081
- Account Email: Username@mail.it
- Account Username: Username@mail.it

All the best,
The MagoCloud Team

Enjoy MagoCloud©

You will be asked to provide these details during the first installation.
Afterwards, you can proceed to create the new Database.

# HARDWARE AND SOFTWARE PREREQUISITES

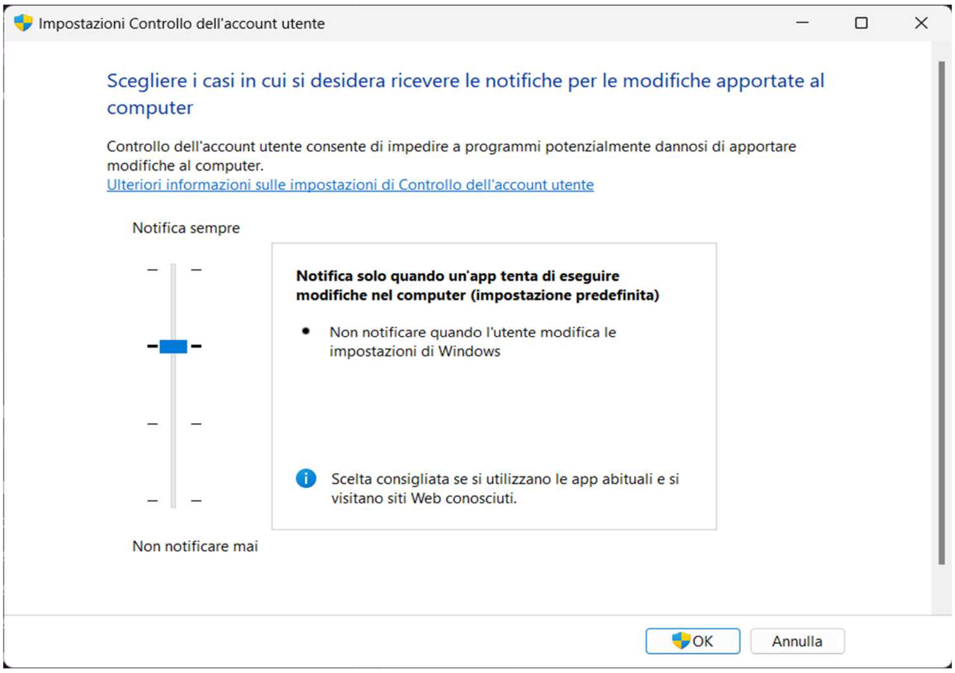
Below are the minimum requirements for a **MagoWeb** installation.
The HW requirements refer to two ranges of workstations (PDL), and relating to the scenario in which the same machine acts as both an Application and a DB server.

The HW resources indicated are deduced from load tests done by simulating interactive use of the program, and may vary based on use cases.
With the same virtual resources, performance may vary based on the type of underlying HW and the virtualization system in use. The requirements indicated should be considered as a general reference.

| PDL range | CPU | RAM | SW Prerequisites |
|---|---|---|---|
| 1-5 | 2 core | 16 GB | - Windows Server Standard (2016 or later)<br>- Postgres 14.9 or later (o MSSQL 2017 or later) |
| 6-10 | 4 core | 16 GB | - Windows Server Standard (2016 or later)<br>- Postgres 14.9 or later (o MSSQL 2017 or later) |

# FIRST INSTALLATION

Log in to the machine on which you intend to install MagoWeb with an account that has administrative permissions.
Download the installer and the .zst file for the version you intend to install from the Microarea website https://mymago.zucchetti.com
, verifying that the versions of the two files match.
Starting from version 1.4, the MagoWeb installer has been modified, it is necessary to use the setup.exe installer and it is NOT possible to use the MagoWebinstaller.exe of previous versions, doing so will cause the installation to fail and a clean reinstallation of the product will be necessary.
Verify and/or set the Windows User Account Control (UAC) security level to the default level as in the screenshot.



Impostazioni Controllo dell'account utente

Scegliere i casi in cui si desidera ricevere le notifiche per le modifiche apportate al computer

Controllo dell'account utente consente di impedire a programmi potenzialmente dannosi di apportare modifiche al computer.
Ulteriori informazioni sulle impostazioni di Controllo dell'account utente

**Notifica solo quando un'app tenta di eseguire modifiche nel computer (impostazione predefinita)**

- Non notificare quando l'utente modifica le impostazioni di Windows

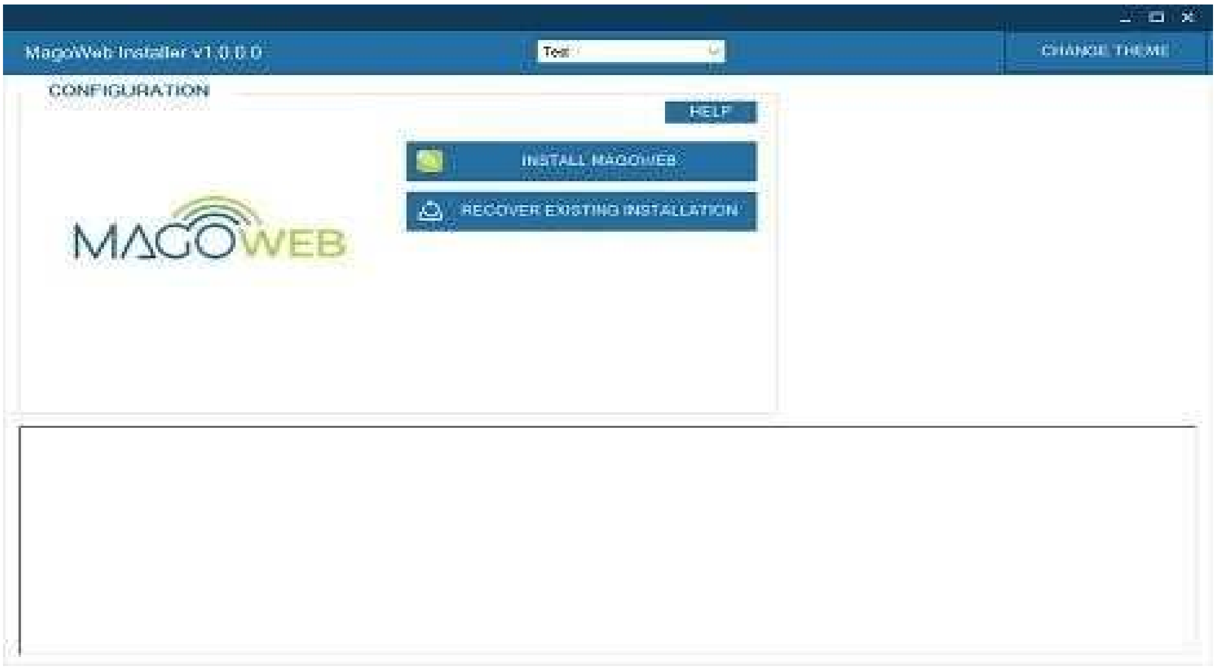
Scelta consigliata se si utilizzano le app abituali e si visitano siti Web conosciuti.

### Versions 1.3 or earlier

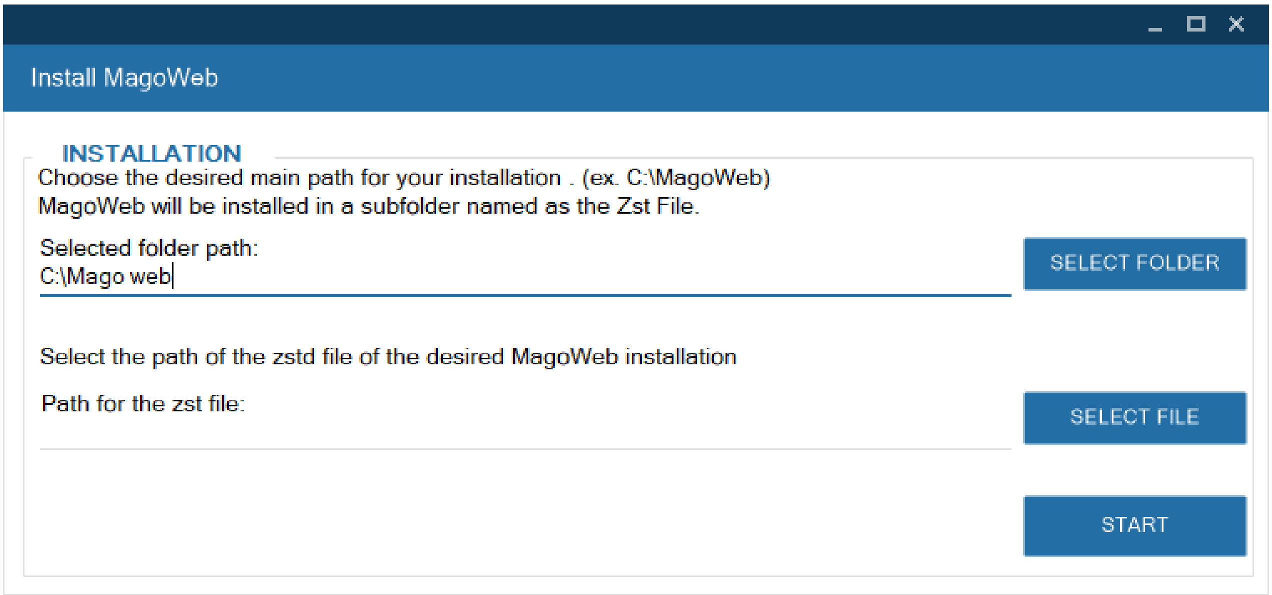
Run MagoWebInstaller.exe as administrator, if the previous step has not been performed, a warning message will alert the user.

### Versions 1.4 or later

Open an administrative command prompt and run the Setup.exe file, the setup will check and download the necessary prerequisites and, once this operation is completed, it will open the installer window. Also in this case, if the UAC permission levels are not set correctly, a message will warn the user.



Select **Install Magoweb**


Install MagoWeb

INSTALLATION

Choose the desired main path for your installation . (ex. C:\MagoWeb)
MagoWeb will be installed in a subfolder named as the Zst File.

Selected folder path:
C:\Mago web

Select the path of the zstd file of the desired MagoWeb installation

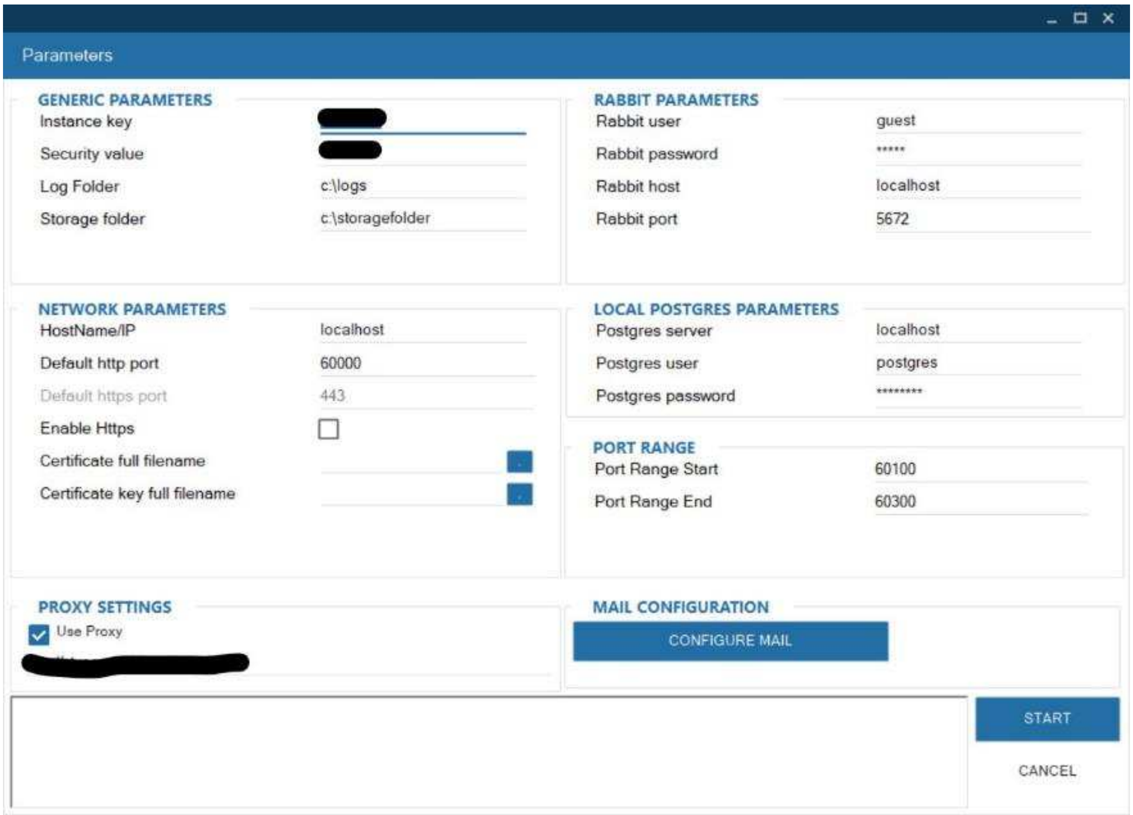
Path for the zst file:

Select the main folder where the various versions of MagoWeb and all subsequent updates will be installed.
Then select the .zst file relating to the desired MagoWeb version using the appropriate button.

Once you have entered these two pieces of information, pressing the “Start” button will start the installation.

Note: the destination folder must not already be present on the PC in order to start the installation, if it is already present the **Start** button will not be clickable, in this case close the window, manually delete the folder and press Install MagoWeb again.

At the end of the unzip, the installation parameters configuration window will appear



Parameters

GENERIC PARAMETERS

Instance key [redacted]

Security value [redacted]

Log Folder c:\logs

Storage folder c:\storagefolder

RABBIT PARAMETERS

Rabbit user guest

Rabbit password *****

Rabbit host localhost

Rabbit port 5672

NETWORK PARAMETERS

HostName/IP localhost

Default http port 60000

Default https port 443

Enable Https □

Certificate full filename

Certificate key full filename

LOCAL POSTGRES PARAMETERS

Postgres server localhost

Postgres user postgres

Postgres password ********

PORT RANGE

Port Range Start 60100

Port Range End 60300

PROXY SETTINGS

☑ Use Proxy

[redacted]

MAIL CONFIGURATION

The configuration window is divided into 5 main sections. Let's analyze them in detail::

**Generic Parameters:** in this section you will have to enter the mandatory information:

- the Instance Key and Security Value, which you should have received by email previously (see MagoWeb purchase section).
- Log Folder: folder in which the diagnostic logs produced by the various services will be stored.
- Storage folder: in this folder the various files will be temporarily parked during any Upload / Download operations..

**Network Parameters:**

- Hostname/Ip: this fields hosts the public IP address of the machine that will host the MagoWeb installation, ora a related alias set externally at DNS level
- Default http e Https port: default 60000 (http) e 443(https)
- Enable Https: specify whether to enable https management for installation (enabling this option will enable the following two fields:

- Full path to the certificate file and key: (e.g. c:\cert\certificate.crt and c:\cert\certificate.key). Specify the certificate and key files for the domain/ip you set up earlier

If https is enabled, make sure to enter the exact name of the host corresponding to the certificate you will use in the HostName field

The installer will automatically configure the various services to run in https and create rules in the Windows firewall to allow incoming traffic on the specified ports

**Proxy Settings**

If the MagoWeb installation is carried out in a proxy domain, enable the relevant flag and set the proxy URL.

**Rabbit Parameters**

In this section enter the parameters for connecting to RabbitMQ

The installer is able to use an already existing version of RabbitMQ or if it does not exist, it will be installed and configured automatically

**Postgres Parameters**

As with RabbitMQ, the installer is able to use existing versions of PostgreSql or automatically install the necessary version.

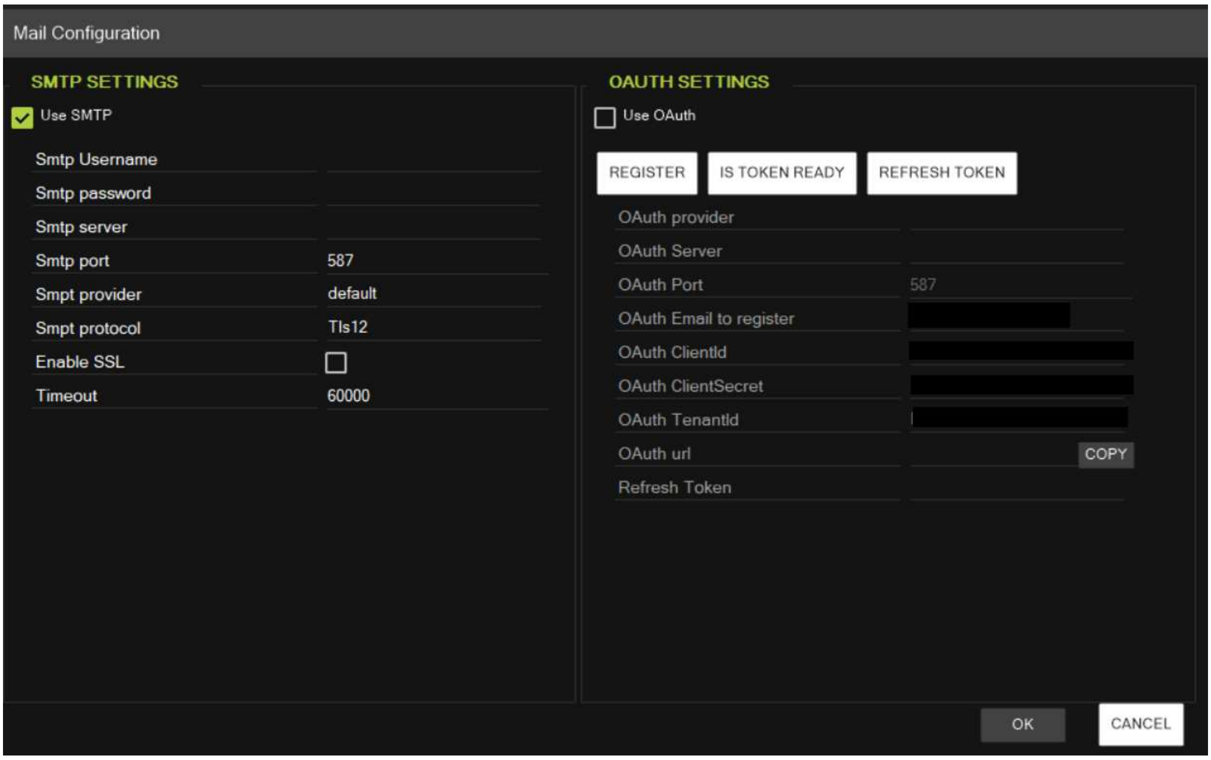
Note that PosgreSql is a prerequisite for the operation of some MagoWeb services, and is not necessarily to be considered the database server to be connected to the subscription

**Port settings**

Finally, this section highlights the range of ports on which the various MagoWeb services will listen.

## Email Configuration

The Mail Configuration button will bring up the relative config window



Mail Configuration

SMTP SETTINGS

☑ Use SMTP

| | |
|---|---|
| Smtp Username | |
| Smtp password | |
| Smtp server | |
| Smtp port | 587 |
| Smpt provider | default |
| Smpt protocol | Tls12 |
| Enable SSL | □ |
| Timeout | 60000 |

OAUTH SETTINGS

□ Use OAuth

| | |
|---|---|
| OAuth provider | |
| OAuth Server | |
| OAuth Port | 587 |
| OAuth Email to register | [redacted] |
| OAuth ClientId | [redacted] |
| OAuth ClientSecret | [redacted] |
| OAuth TenantId | [redacted] |
| OAuth url | |
| Refresh Token | |

SMTP Settings:
It’s the default choice as email provider. If you want to use this one, you need to configure the parameters (server, user, password, etc.) to set the SMTP server connection.
Il parametro Smtp Provider = default should not be changed

Oauth settings: The Use Oauth button will disable the SMTP section and enable the fields below.

Note: To use the mail features via Oauth it is necessary to create the application on the desired mail provider (Microsoft or Google), following the instructions in the providers' official guides.

*Provider Microsoft:*
Getting started: Register an app in Microsoft Identity Platform - Microsoft identity platform | Microsoft Learn

*Provider Google:*
Use OAuth 2.0 to Access Goole APIs | Authorization | Google for Developers

A. Make a note of the parameters provided by the provider to perform authentication when configuring the new OAuth2 protocol, namely::

- Client Id
- Client Secret
- Tenant Id

B. Nella schermata presente Inserire tutti i dati fino a TenantId.

1. Write the desired provider, Google or Microsoft as instructed in step A
2. For the server enter “smtp.google.com” for Google or “smtp.office365.com” for Microsoft.
3. The port is always 587
4. Indicare l’indirizzo e-mail del mittente per l’OAuth nella sezione “Email to register” in base al provider selezionato precedentemente.
5. Enter the Client ID, Client Secret, and Tenant ID: This information is to be retrieved in the application that you registered with Google or Microsoft. For authentication with Google there is no Tenant ID, however the field must not be left blank and must be filled with any text
6. At this point click "Register", the process will generate a URL (which will be transferred to the relative property in the dialog). The system will try to open on an incognito page of the Chrome browser; If it fails, it will open a page on your default browser, but not in incognito mode. In this second scenario, it is important to be careful that the email is not automatically deduced by the browser, perhaps with your Google or Microsoft account already set up. Be careful to enter the same e-mail address you entered previously. If in doubt, open an incognito page of your browser and copy the link that you will find in the box next to the COPY button.
7. Then enter the password for the email entered and accept the conditions.
8. If the process was successful, you will be returned to a page of encrypted information in your browser tab. This means that the token is ready and you can close the tab safely.
9. Proceed by clicking the “IsTokenReady” button. If the process was succesful, the “Refresh token” field should auto-populate
10. Cliccare the ‘OK’  button

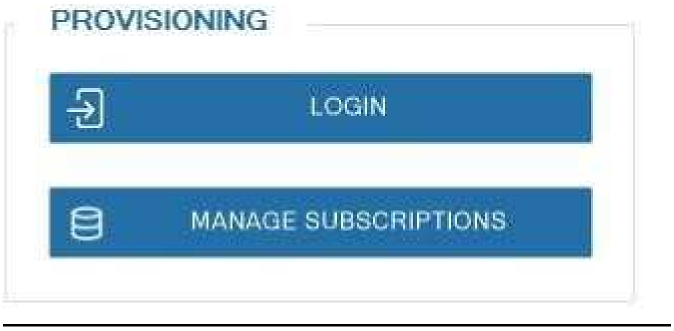
Note
The 'Refresh token' button should not be used. The received token will expire after one hour of the request, but the update request will start automatically, making this button just a precaution.
**In fact, the validity check and any refresh of the token will take place at each new login on Mago and before each email is sent.**

You are now ready to send emails with OAuth2.

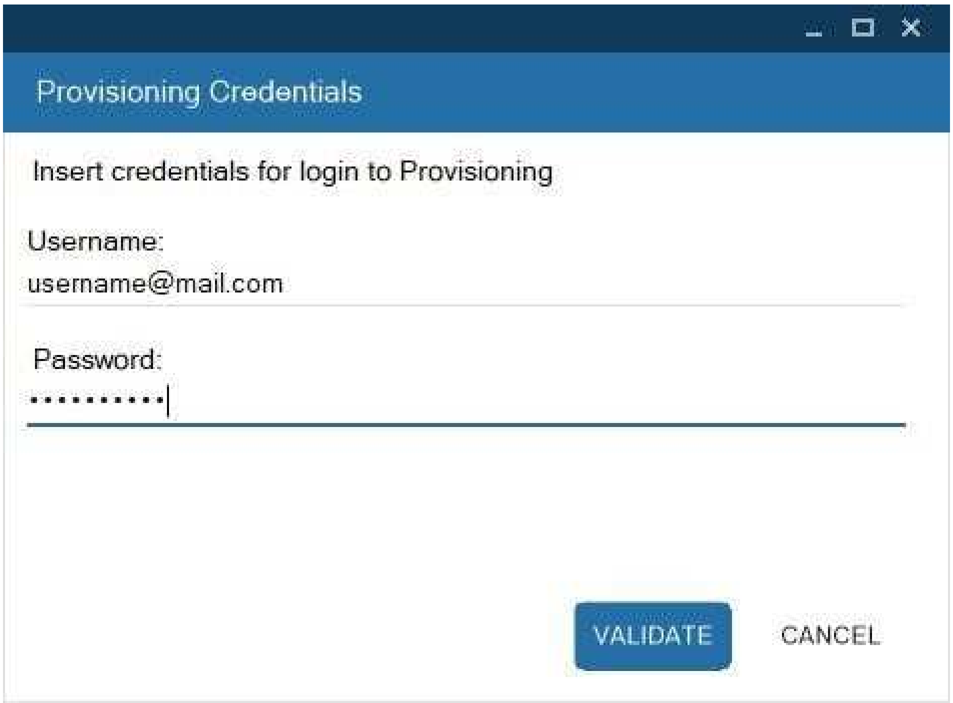
Once all the mandatory parameters have been set, the start button should be enabled.
By pressing the start button, the actual configuration and installation of MagoWeb will start

**Login**

At the end of the configuration, it will be necessary to login to the provisioning system to proceed with the creation and configuration of the database relating to the subscription purchased in the store.



Enter your username and password, using an account that has the APPLICATION-ADMIN role


Provisioning Credentials

Insert credentials for login to Provisioning

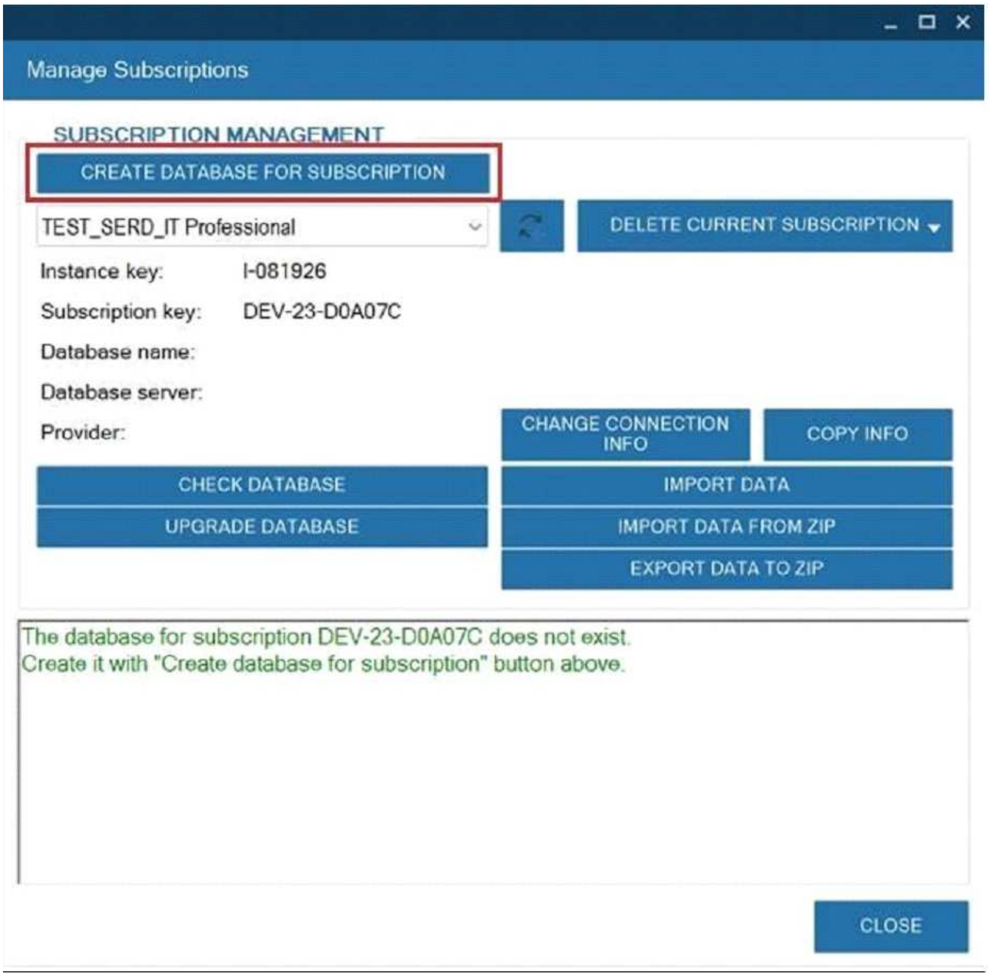
Username:
username@mail.com

Password:
•••••••••••

**Manage Subscriptions**

After authentication, the user will find the previously purchased subscription in the dropdown menu.

At this stage the installer will warn that the subscription does not yet have a database: then proceed to the creation by pressing the button "Create database for subscription”.



TEST_SERD_IT Professional

Instance key: I-081926

Subscription key: DEV-23-D0A07C

Database name:

Database server:

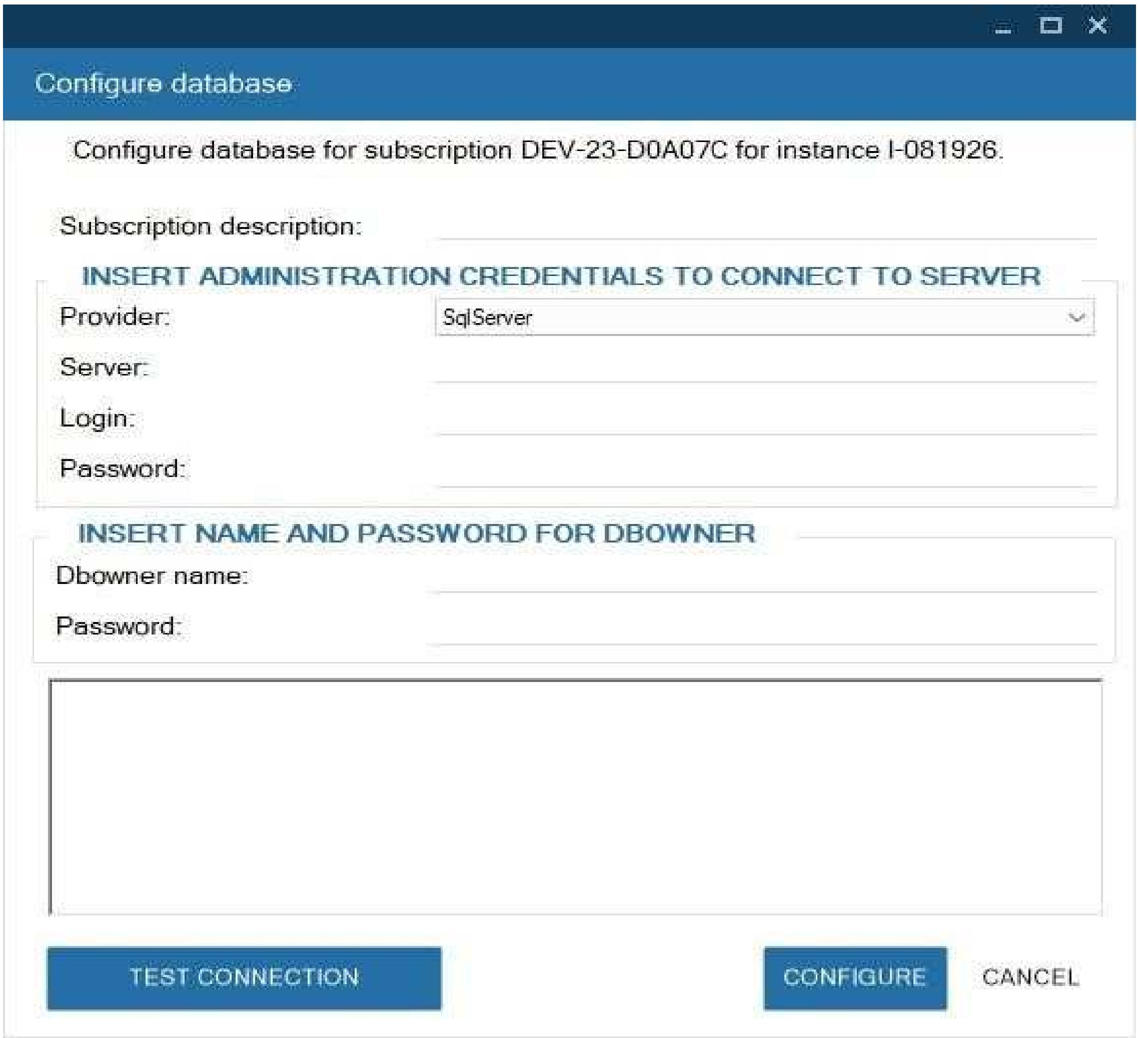
Provider:

```
The database for subscription DEV-23-D0A07C does not exist.
Create it with "Create database for subscription" button above.
```

### Configure Database

You can use both SqlServer and PostgreSQL as database servers.
Select the desired provider from the drop-down menu.
Once the provider is set up you must enter the Server, Login and Password information to connect to the database server.
You can use the "Test Connection" button to check the goodness of the information just entered.
Then you need to insert the credentials for the dbowner associated to the database
You can use an existing user/password for the dbowner, or insert credentials for a new one.

*(Note: it is not possible to use an administrator user as dbowner (e.g. sa))*



Configure database

Configure database for subscription DEV-23-D0A07C for instance I-081926.

Subscription description:

INSERT ADMINISTRATION CREDENTIALS TO CONNECT TO SERVER

Provider: SqlServer

Server:

Login:

Password:

INSERT NAME AND PASSWORD FOR DBOWNER

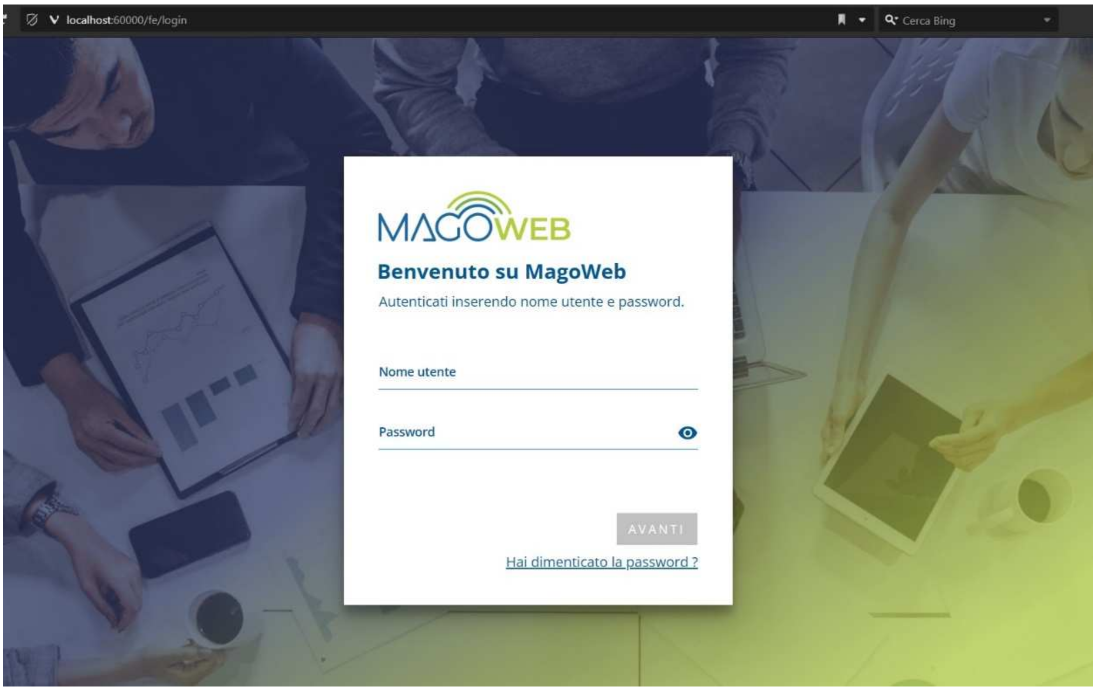
Dbowner name:

Password:

Pressing the "Configure" button will start the creation of the database associated with the subscription.
You can then proceed to import the default or example data:
**Default data** - configuration data necessary for application procedures to work. They are divided by country and configuration. Usually the choice of country refers to the one selected when purchasing the Subscription.
**Example Data** - A default data set enriched with additional values that make up a data set for illustrative purposes.
It will also be possible to use the appropriate buttons to check and upgrade the database.

At this point the installation and configuration of MagoWeb is **completed** and it will be possible to connect to the mago frontend.

To open the frontend you can use the "MagoWeb" button at the bottom right via the installer, using the "Open client" option.



localhost:60000/fe/login

Benvenuto su MagoWeb

Autenticati inserendo nome utente e password.

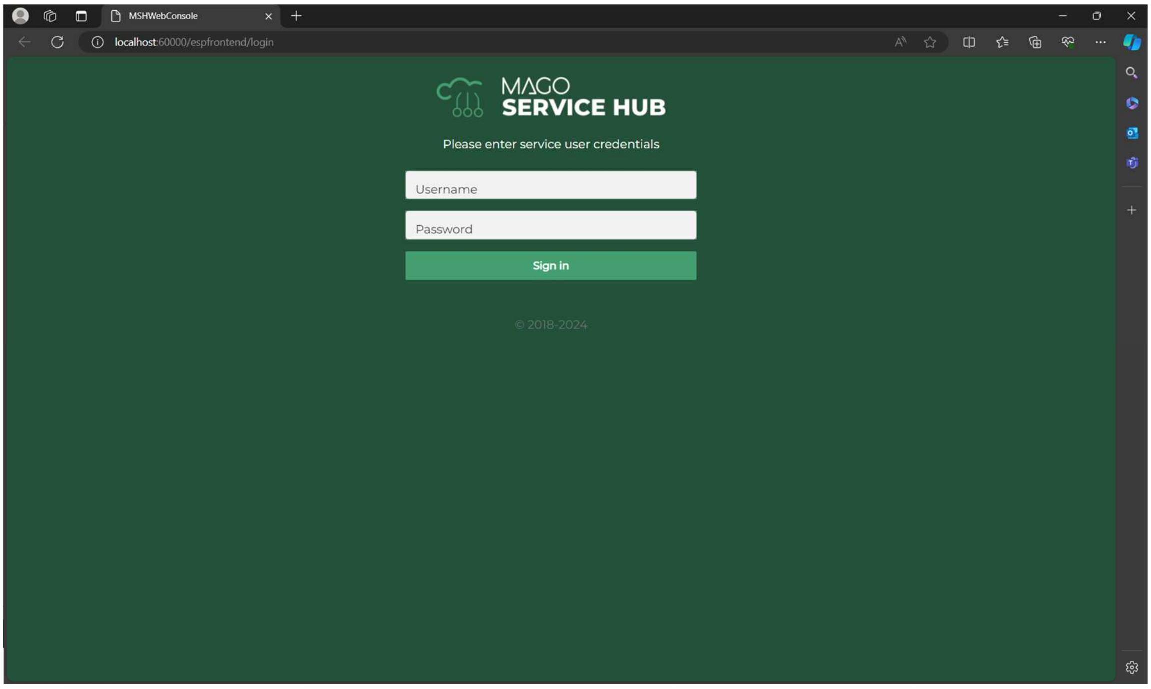
Nome utente

Password

AVANTI

Hai dimenticato la password ?

The “Open MSH frontend” option opens the MSH frontend on the default browser



localhost:60000/espfrontend/login

Please enter service user credentials

Username

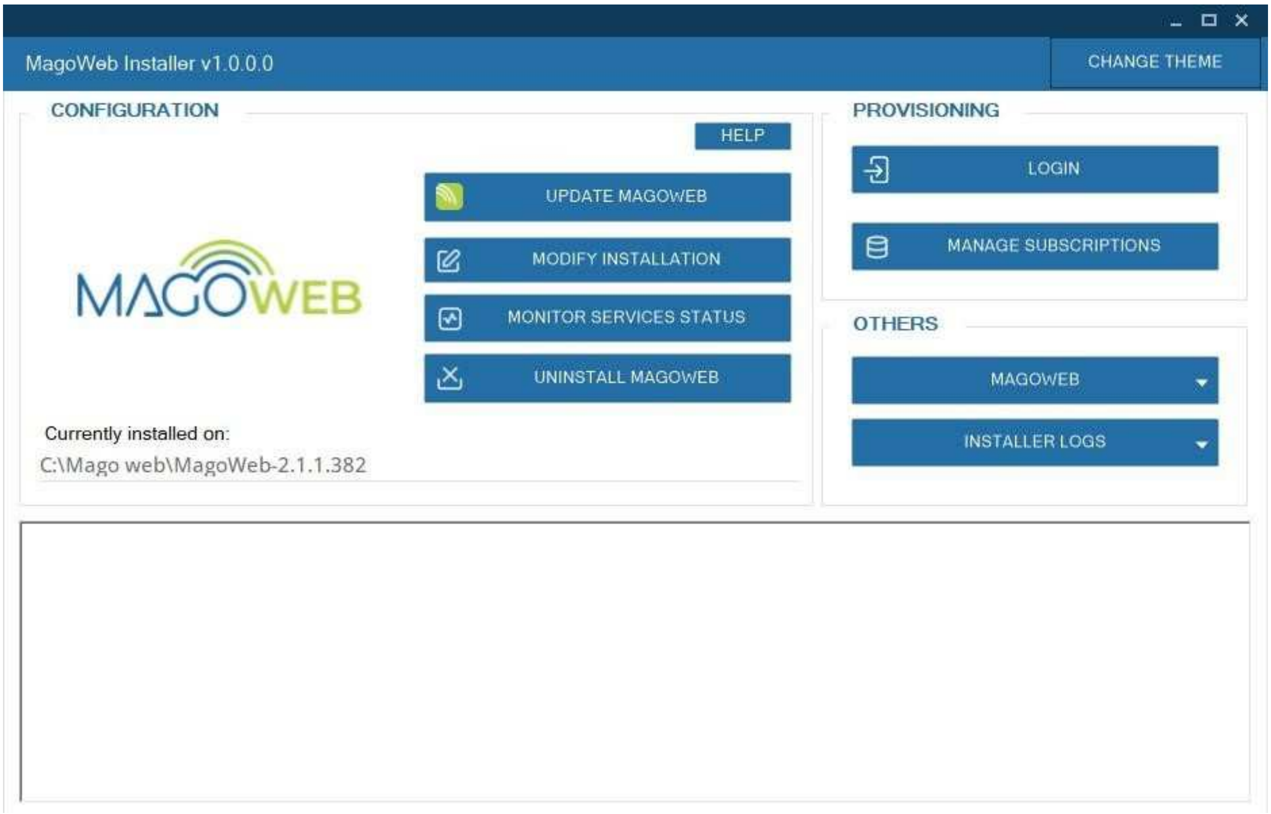
Password

Sign in

© 2018-2024

*Note: access to the MSH Frontend occurs with the same credentials used to access the Mago Store, unlike Mago4 there is no service user for MSH.*

# MAINTANANCE AND INSTALLATION CONFIGURATION



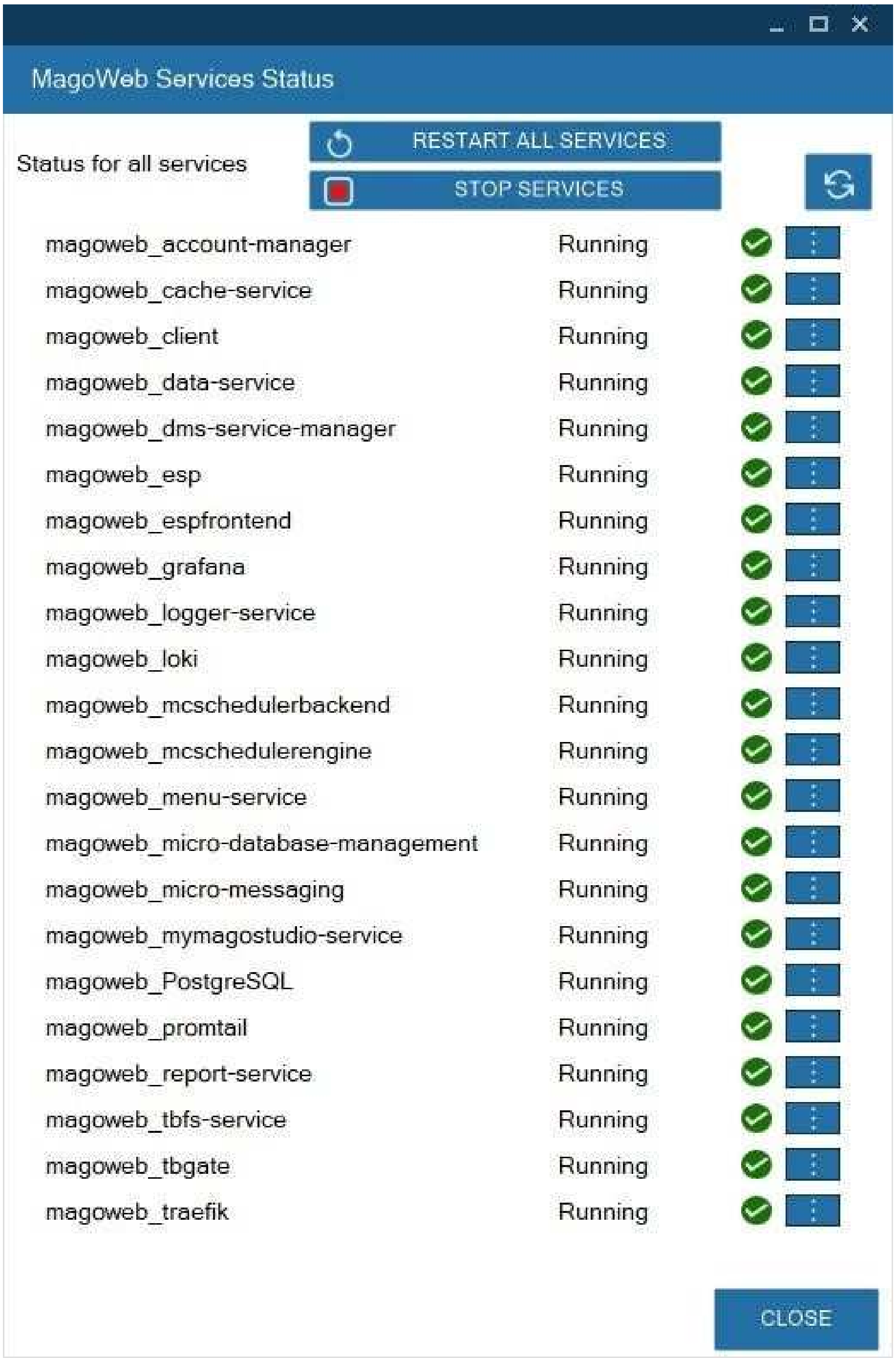
Currently installed on:

C:\Mago web\MagoWeb-2.1.1.382

*Main interface*

At any time you can perform maintenance operations of the various component services of the installation.

Through the **Monitor Services Status** button you can see the status of various microservices, with the possibility to stop and restart them individually or all together.



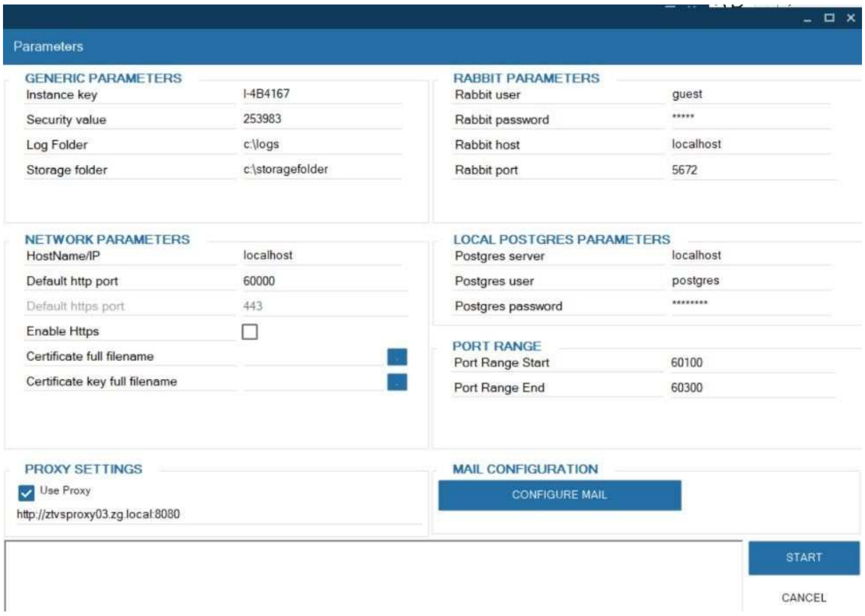
Status for all services

| | | |
|---|---|---|
| magoweb_account-manager | Running | ✓ |
| magoweb_cache-service | Running | ✓ |
| magoweb_client | Running | ✓ |
| magoweb_data-service | Running | ✓ |
| magoweb_dms-service-manager | Running | ✓ |
| magoweb_esp | Running | ✓ |
| magoweb_espfrontend | Running | ✓ |
| magoweb_grafana | Running | ✓ |
| magoweb_logger-service | Running | ✓ |
| magoweb_loki | Running | ✓ |
| magoweb_mcschedulerbackend | Running | ✓ |
| magoweb_mcschedulerengine | Running | ✓ |
| magoweb_menu-service | Running | ✓ |
| magoweb_micro-database-management | Running | ✓ |
| magoweb_micro-messaging | Running | ✓ |
| magoweb_mymagostudio-service | Running | ✓ |
| magoweb_PostgreSQL | Running | ✓ |
| magoweb_promtail | Running | ✓ |
| magoweb_report-service | Running | ✓ |
| magoweb_tbfs-service | Running | ✓ |
| magoweb_tbgate | Running | ✓ |
| magoweb_traefik | Running | ✓ |

*(Note: the magoweb_micro-dabase-management service is automatically activated and stopped as needed, during database maintenance operations. Outside of these uses, the service will be stopped to avoid unnecessary memory occupations and it will therefore be normal to see it "stopped" in typical conditions of use)*

*(Note: Some service are dependent from others: If services that depend on or are dependent on other services are manually restarted, the connected services will also be restarted accordingly)*

With the Modify Installation button, if for any reason it is necessary to change one of the parameters (for example the log folder, the rabbit user password, etc.), it will be possible to completely reconfigure your MagoWeb installation



Parameters

GENERIC PARAMETERS

| | |
|---|---|
| Instance key | I-4B4167 |
| Security value | 253983 |
| Log Folder | c:\logs |
| Storage folder | c:\storagefolder |

RABBIT PARAMETERS

| | |
|---|---|
| Rabbit user | guest |
| Rabbit password | ***** |
| Rabbit host | localhost |
| Rabbit port | 5672 |

NETWORK PARAMETERS

| | |
|---|---|
| HostName/IP | localhost |
| Default http port | 60000 |
| Default https port | 443 |
| Enable Https | □ |
| Certificate full filename | |
| Certificate key full filename | |

LOCAL POSTGRES PARAMETERS

| | |
|---|---|
| Postgres server | localhost |
| Postgres user | postgres |
| Postgres password | ******** |

PORT RANGE

| | |
|---|---|
| Port Range Start | 60100 |
| Port Range End | 60300 |

PROXY SETTINGS

☑ Use Proxy

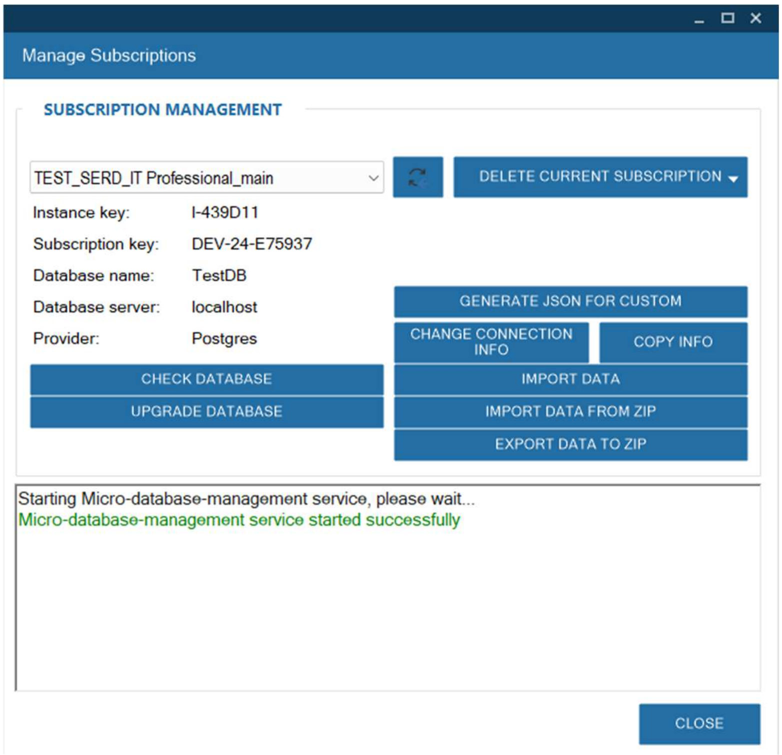
http://ztvsproxy03.zg.local:8080

MAIL CONFIGURATION

The various services will be temporarily disabled, and reinstalled shortly with the new configuration.

# DATABASE MANAGEMENT

Using the Manage Subscriptions menu, you can manage the MagoWeb database



TEST_SERD_IT Professional_main

| | |
|---|---|
| Instance key: | I-439D11 |
| Subscription key: | DEV-24-E75937 |
| Database name: | TestDB |
| Database server: | localhost |
| Provider: | Postgres |

```
Starting Micro-database-management service, please wait...
Micro-database-management service started successfully
```

The drop-down menu allows you to select the current subscription in case of multicompany, below it the information regarding the subscription is collected.

**Check Database** performs a check on the current DB of the subscription by verifying whether the table structure is aligned with the current version, if operations are necessary, this is indicated in the lower box.
The database update is performed via the button below Upgrade Database.

**Delete Current Subscription** using the two options in its menu:
*Delete Database Objects* deletes, upon confirmation, the entire table structure of MagoWeb
*Delete Data Only* deletes, upon confirmation, all the data contained in the tables leaving the table structure unchanged.

**Change Connection Info** opens the relative menu where it is possible to change the pointing for the MagoWeb database, within this it is possible to change all the necessary information in case of server or database change.
It is not currently possible to change the provider selected during the creation of the subscription DB from Postgres to SQL or vice versa from this menu, if this operation is necessary it is possible to contact technical support by opening a ticket and the current database will be unlinked from the subscription. Following this operation by opening Manage Subscription again, the Create Database for Subscription button will be shown again and you will be able to select the provider again.

Copy info copies the subscription information shown on the left into the clipboard.

**Import Data** allows you to import default data from MagoWeb:
*Default data* - configuration data needed to make the application procedures work. They are divided by country and configuration. Usually the choice of country refers to the one selected when purchasing the Subscription.
*Example data* - A set of default data enriched with additional values that make up a set of data for illustrative purposes.

**Import Data from ZIP** allows you to upload files in .xml format with data chosen by the user. It is necessary that the structure of the xml perfectly follows the structure that the system is able to read. This can be deduced by exporting the tables with the export functionality and then using them to generate the files that can then be zipped and imported correctly. The size limit is 100 MB.

**Export Data to ZIP** allows you to export all the contents of the tables in .xml format within a .zip file, the operation has a maximum database size limit of 2GB

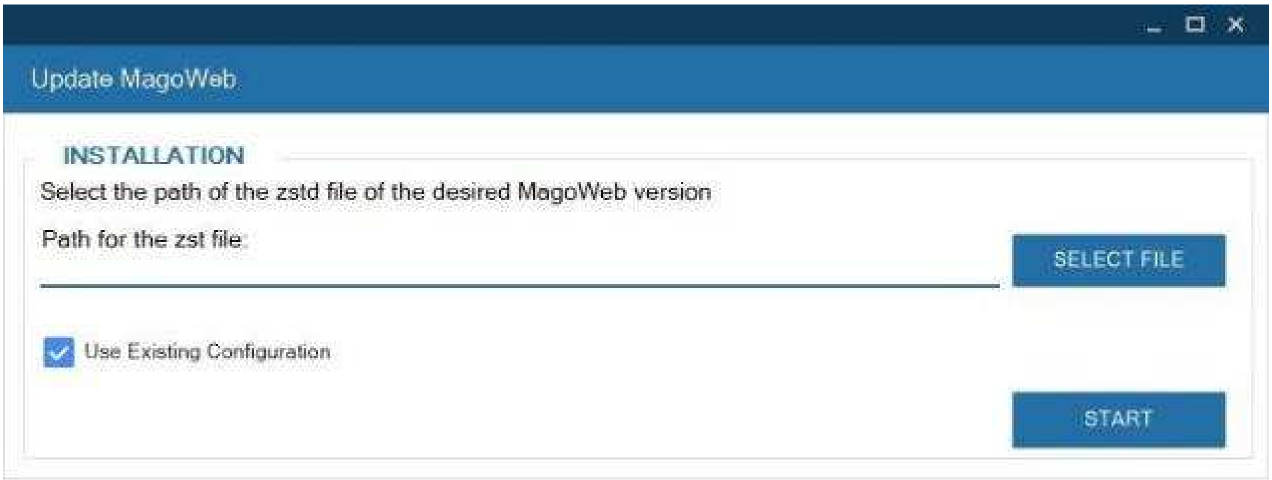
## UPDATE TO A NEW VERSION

To update MagoWeb to a later version, the steps to follow are very simple. Simply download the zip of the new version, click on the Update MagoWeb button.
Note: When updating to a new version, check that the version of the installer and its .zst match.

A window will appear in which, in a totally similar manner to the first installation, you will be asked for the path to the MagoWeb zip.

Depending on the version of Magoweb the window has some differences:

Versions <1.3



Update MagoWeb

INSTALLATION

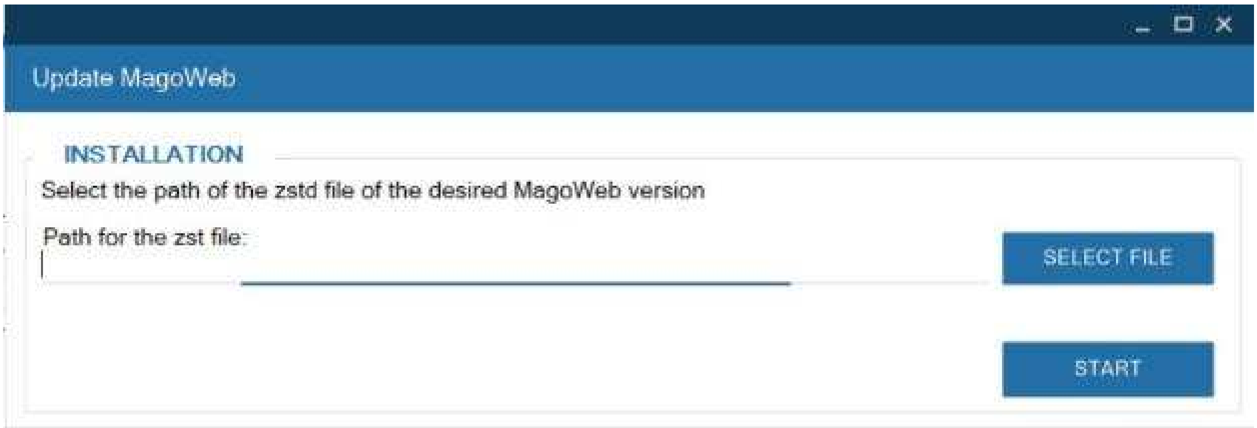
Select the path of the zstd file of the desired MagoWeb version

Path for the zst file:

☑ Use Existing Configuration

In the window you can choose whether to configure MagoWeb with the same settings as the current version, or by removing the "Use existing configuration" flag, you can set the parameters again.
Note: by upgrading from 1.2 to 1.3 the services will not start correctly. If so, you can click on modify installation and then on Start, the services will start correctly.

Versioni 1.3 or later



Update MagoWeb

INSTALLATION

Select the path of the zstd file of the desired MagoWeb version

Path for the zst file:

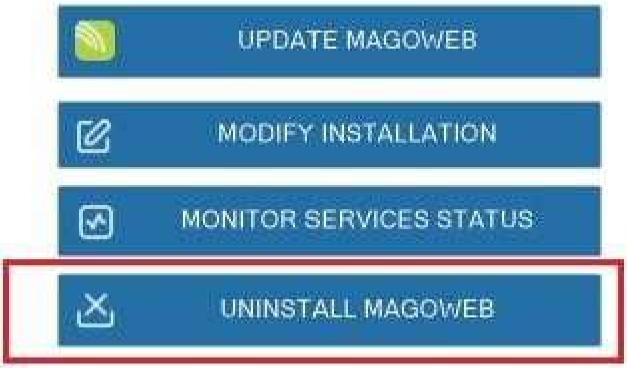
The “use existing configuration” command is not present.

The previous installation will not be affected in the slightest: the installer will take care of "turning off" the services linked to the previous version, and installing and launching those of the new version.

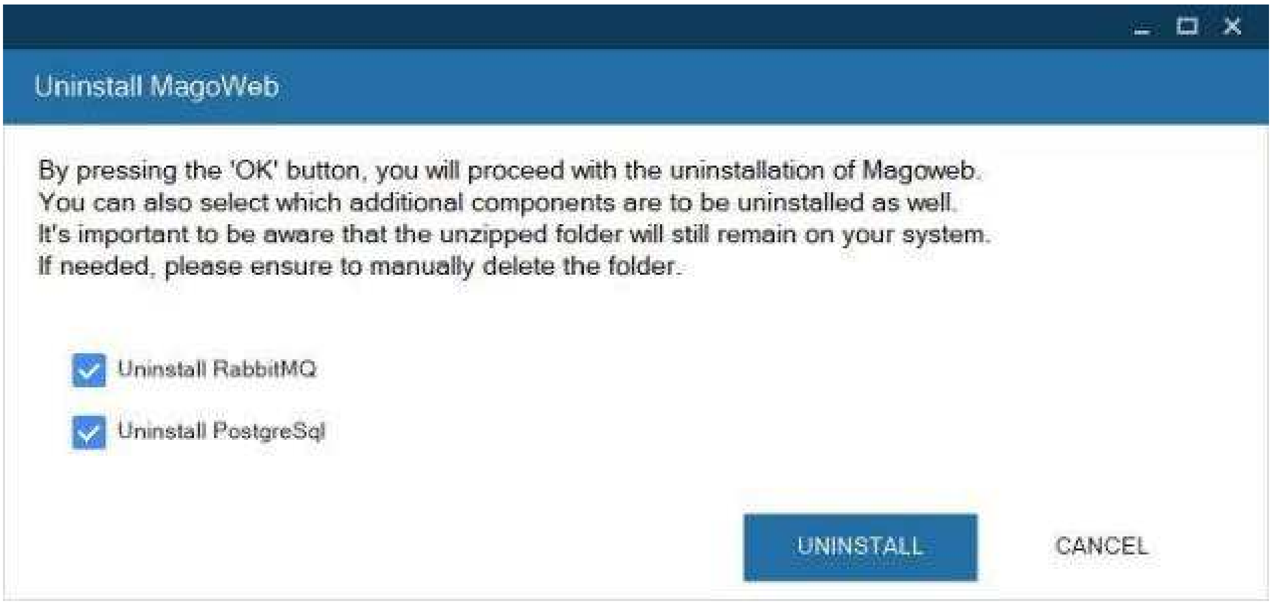
*Note: it is not possible to have multiple active installations of MagoWeb at the same time. It is necessary to update to a new version or uninstall the current one and recover an existing version.*

## UNINSTALLING THE CURRENT VERSION

Through the button highlighted in the figure, it will be possible to uninstall the current version.



All services will be uninstalled, including RabbitMQ and PostgreSQL (unless they were previously installed by the user).



By pressing the 'OK' button, you will proceed with the uninstallation of Magoweb.
You can also select which additional components are to be uninstalled as well.
It's important to be aware that the unzipped folder will still remain on your system.
If needed, please ensure to manually delete the folder.

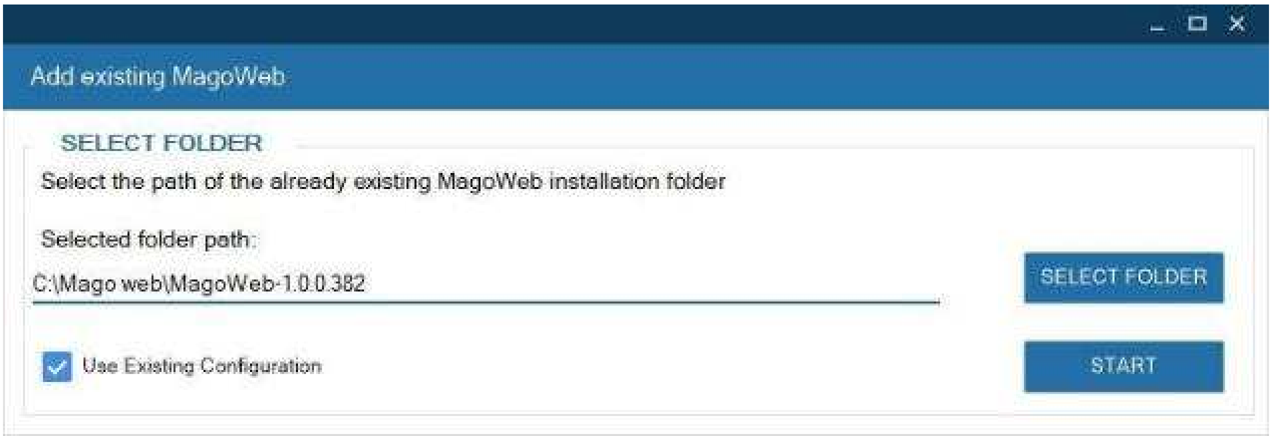
☑ Uninstall RabbitMQ

☑ Uninstall PostgreSql

Note that the installation folder will **not** be deleted: it will be the user's responsibility to delete it manually.
At any time it will be possible to recover a version of MagoWeb through the "Recover Existing Installation" button.

# RECOVERING A PREVIOUS INSTALLATION

At any time it is possible to uninstall the current version of Magoweb and recover a previously uninstalled version.
To recover a previously uninstalled version of MagoWeb, simply click on the "Recover existing installation" button.


Add existing MagoWeb

SELECT FOLDER

Select the path of the already existing MagoWeb installation folder

Selected folder path:

C:\Mago web\MagoWeb-1.0.0.382

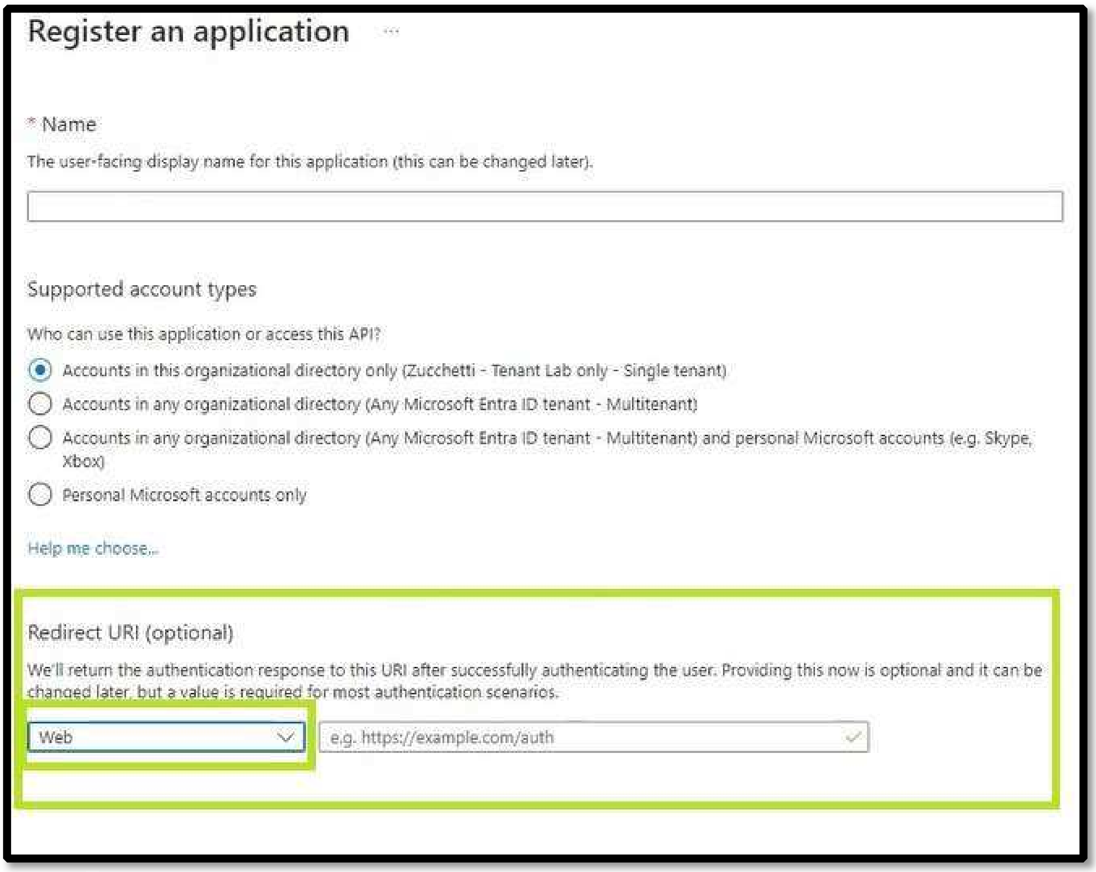
☑ Use Existing Configuration

In the window that appears, select the folder of the version you want to restore.
Pressing start will reinstall all services using the last configuration entered by the user.

# ADDENDUM A
# DETAILS ON CREATION OF MICROSOFT APPLICATION FOR OAUTH

## 1. Registration

When registering the application, you will be asked to specify a 'Redirect URI'/'Authorized redirect URI' (see Figure 1). Specify the address: https://mymago.zucchetti.com/OAuthService/OAuth2/get-token



Register an application

* Name

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

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Zucchetti - Tenant Lab only - Single tenant)

○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

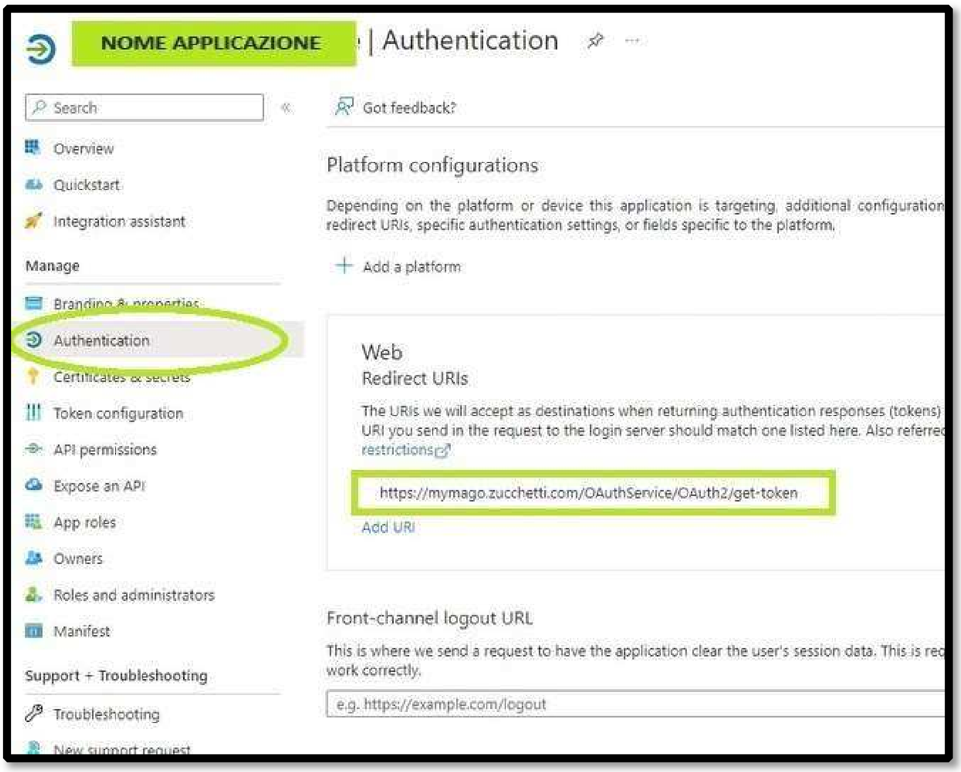
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web

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

Figura 1

If it was not set during creation, it is possible to specify the same value in the 'Authentication' section, adding a new URI (Add URI button, see Figure 2)



Platform configurations

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

Web

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) URI you send in the request to the login server should match one listed here. Also referre restrictions

https://mymago.zucchetti.com/OAuthService/OAuth2/get-token

Front-channel logout URL

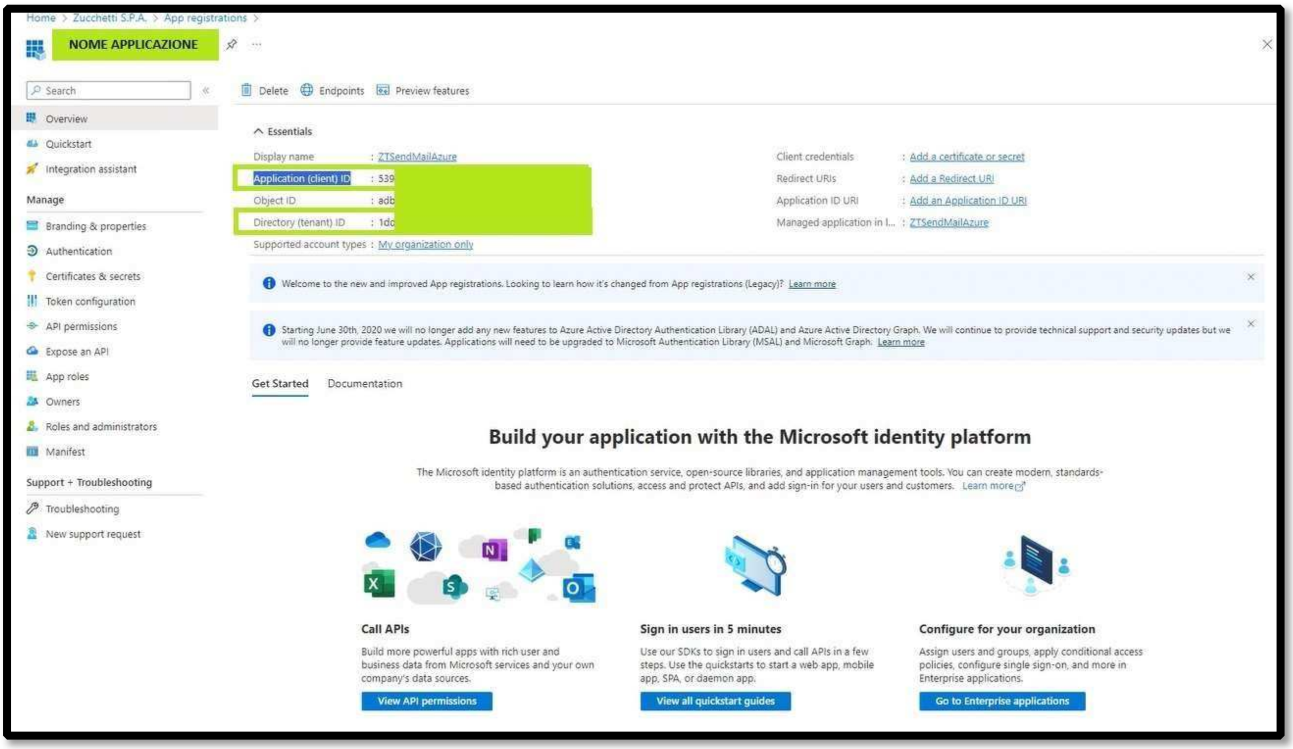
This is where we send a request to have the application clear the user's session data. This is req work correctly.

e.g. https://example.com/logout

Figura 2

## 2. Parameters to be saved

The parameters required in MagoWebInstaller are the following:
- Client ID: you may find it called Client ID, Application ID or Application ID (see Figure 3).
- Tenant ID: You may find it called Directory ID. (see Figure 3).



Display name : ZTSendMailAzure
Application (client) ID : 539[redacted]
Object ID : adb[redacted]
Directory (tenant) ID : 1dc[redacted]
Supported account types : My organization only

Client credentials : Add a certificate or secret
Redirect URIs : Add a Redirect URI
Application ID URI : Add an Application ID URI
Managed application in l... : ZTSendMailAzure

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

**Build your application with the Microsoft identity platform**

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. Learn more

**Call APIs**
Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

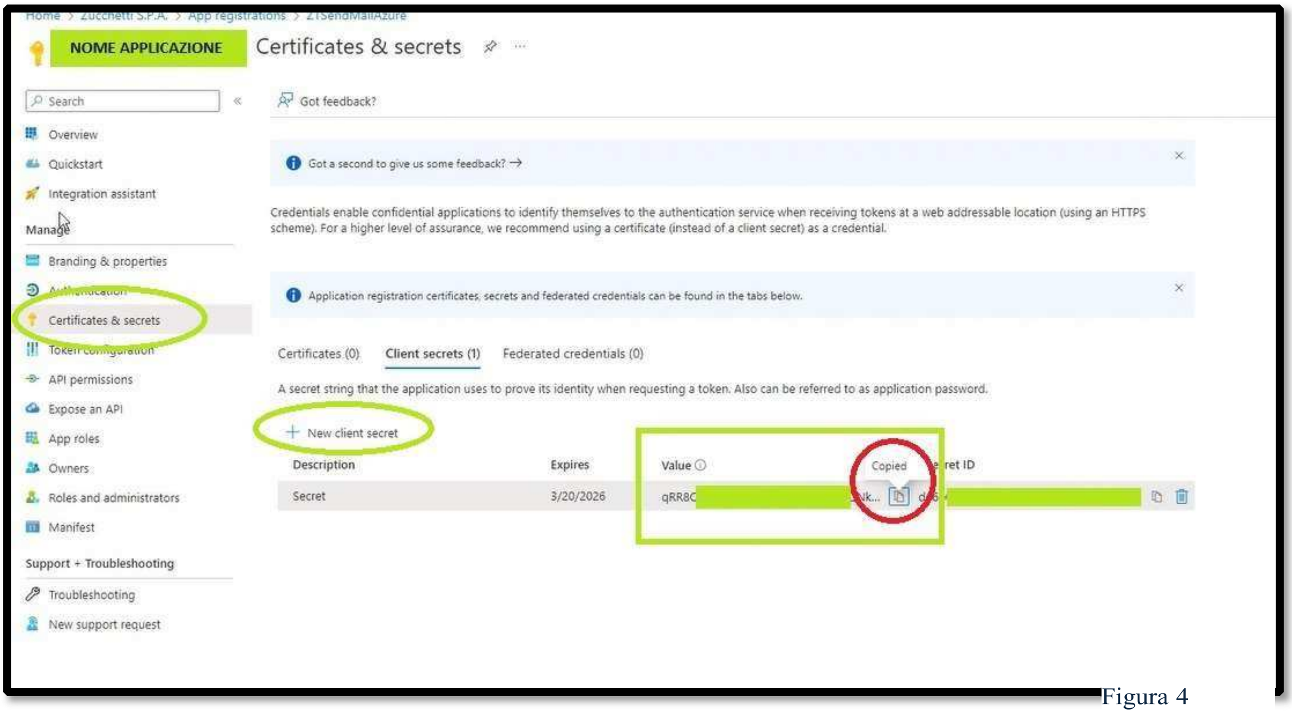
**Sign in users in 5 minutes**
Use our SDKs to sign in users and call APIs in a few steps. Use the quickstarts to start a web app, mobile app, SPA, or daemon app.

**Configure for your organization**
Assign users and groups, apply conditional access policies, configure single sign-on, and more in Enterprise applications.

Figura 3

- Client Secret: corresponds to the 'Value' framed in green.

In the 'Certificates and Secrets' section, create a new secret by clicking on the button circled in green in Figure 4. A sidebar will open in which you can specify the duration of the secret. The choice is free, being aware that at each expiration, a new secret will have to be regenerated and changed in the parameters of the MagoWebInstaller.



Got a second to give us some feedback? →

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

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

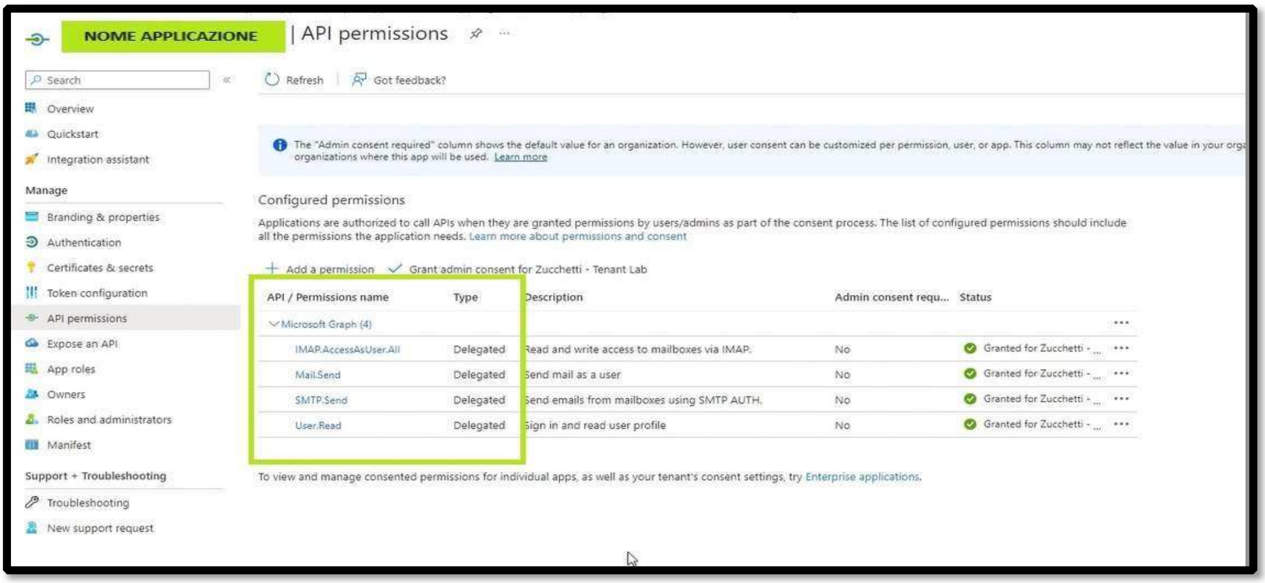
| Description | Expires | Value | Secret ID |
|---|---|---|---|
| Secret | 3/20/2026 | qRR8C[redacted]Nk... | d6[redacted] |

Figura 4

The Client Secret to be inserted in the MagoWebInstaller parameters corresponds to 'Value' framed in green. Please note that this value can only be copied once, after which it will become illegible. The only way to have a client secret will be to create a new client secret entirely.

## 3. Permissions

The complete list of necessary permissions is as follows:
- IMAP.AccessAsUSer.All
- Mail.Send
- SMTP.Send - User.Read



The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your orga organizations where this app will be used. Learn more

Configured permissions

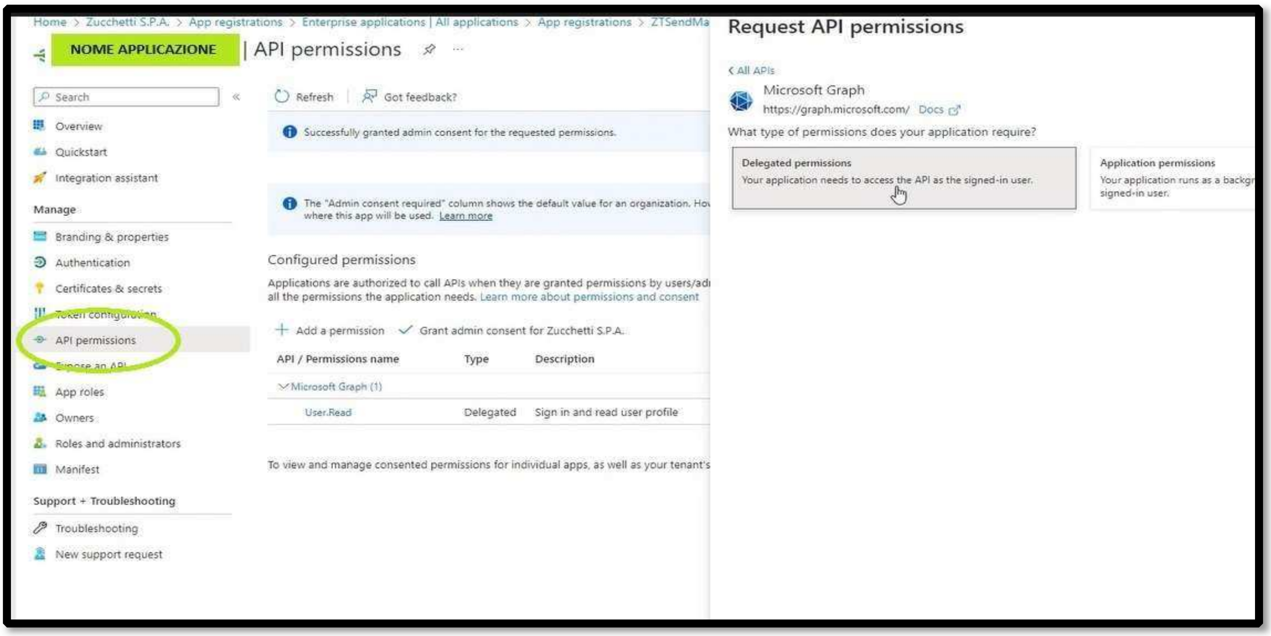
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

| API / Permissions name | Type | Description | Admin consent requ... | Status |
|---|---|---|---|---|
| Microsoft Graph (4) | | | | |
| IMAP.AccessAsUser.All | Delegated | Read and write access to mailboxes via IMAP. | No | Granted for Zucchetti - ... |
| Mail.Send | Delegated | Send mail as a user | No | Granted for Zucchetti - ... |
| SMTP.Send | Delegated | Send emails from mailboxes using SMTP AUTH. | No | Granted for Zucchetti - ... |
| User.Read | Delegated | Sign in and read user profile | No | Granted for Zucchetti - ... |

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications.

Figura 5

In the 'API permissions' section you will need to add the permissions necessary for sending emails. Click on the 'add permission' button, choose 'Microsoft Graph' and 'Delegated permissions' (see Figure 6)



Successfully granted admin consent for the requested permissions.

The "Admin consent required" column shows the default value for an organization. Ho where this app will be used. Learn more

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/ad all the permissions the application needs. Learn more about permissions and consent

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

To view and manage consented permissions for individual apps, as well as your tenant's

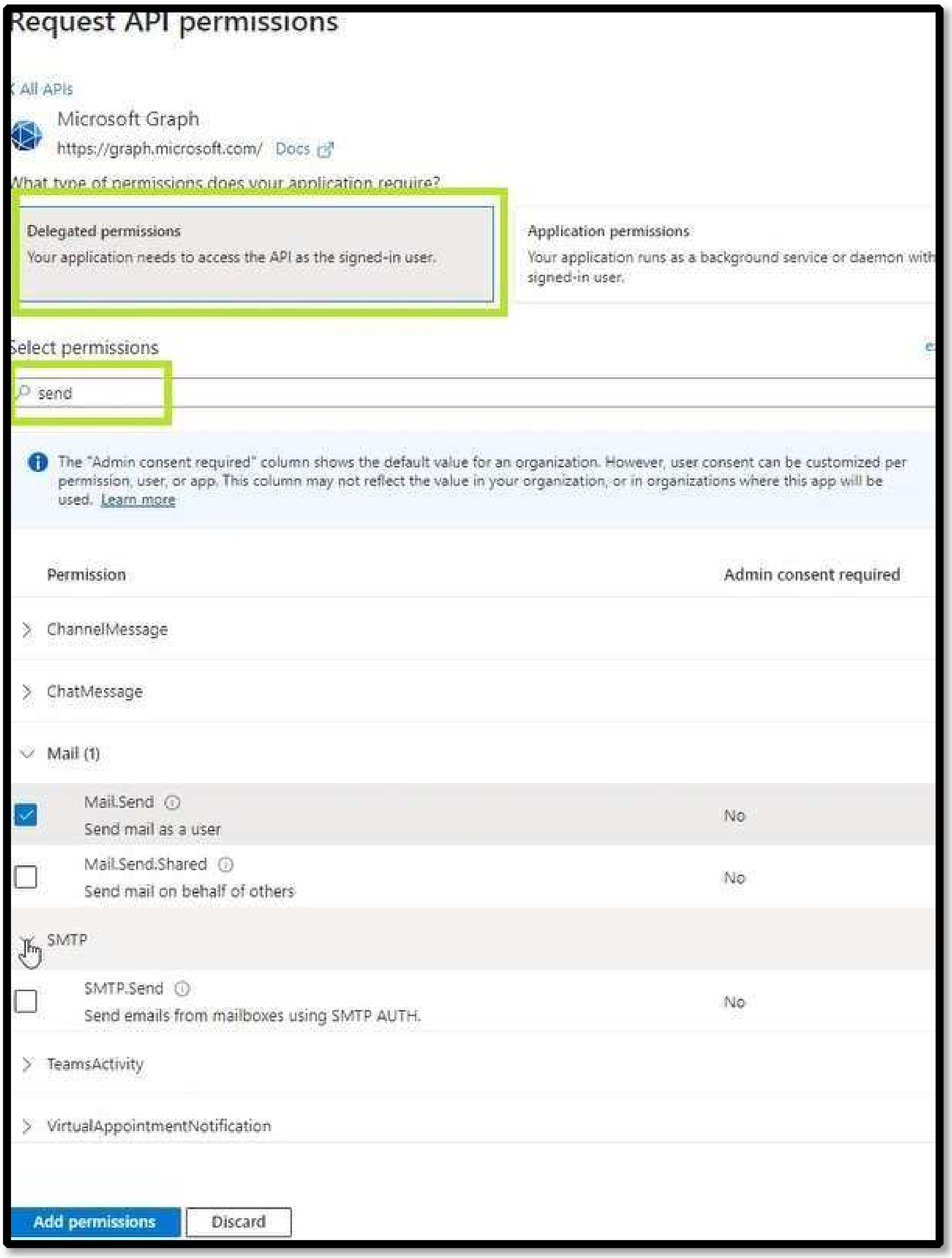
What type of permissions does your application require?

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

**Application permissions**
Your application runs as a backgr signed-in user.

Figura 6

An example of a search is Figure 7, in which the 'mail.Send' permission is searched for.



Request API permissions

< All APIs

Microsoft Graph
https://graph.microsoft.com/ Docs

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 with
signed-in user.

Select permissions

send

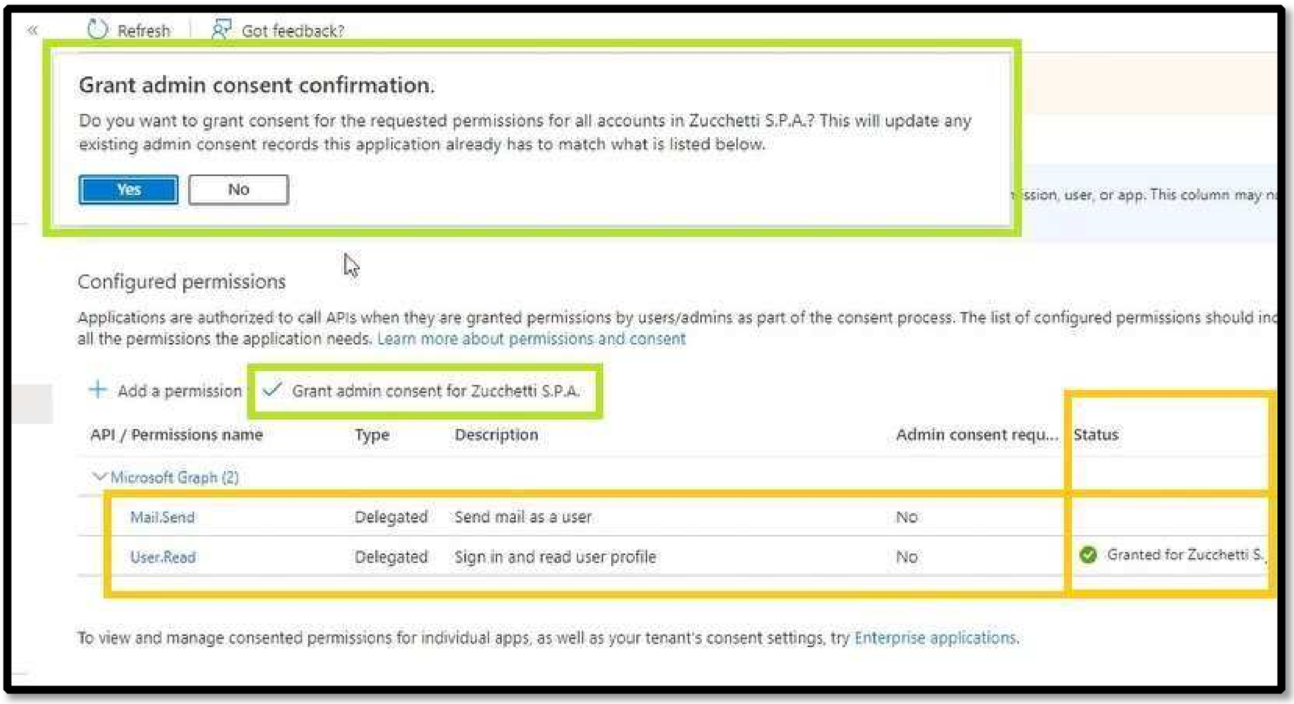
The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more

| | Permission | Admin consent required |
|---|---|---|
| > | ChannelMessage | |
| > | ChatMessage | |
| ∨ | Mail (1) | |
| ☑ | Mail.Send<br>Send mail as a user | No |
| ☐ | Mail.Send.Shared<br>Send mail on behalf of others | No |
| ∨ | SMTP | |
| ☐ | SMTP.Send<br>Send emails from mailboxes using SMTP AUTH. | No |
| > | TeamsActivity | |
| > | VirtualAppointmentNotification | |

Figura 7

Once the permission has been added, it will be necessary to give it 'consent', i.e. click on the 'Grant admin consent ...' button and confirm (see figure 8).

In the yellow boxes you can see the difference in status between a permit granted and one that has not yet been granted.



Grant admin consent confirmation.

Do you want to grant consent for the requested permissions for all accounts in Zucchetti S.P.A.? This will update any existing admin consent records this application already has to match what is listed below.

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 inc all the permissions the application needs. Learn more about permissions and consent

| API / Permissions name | Type | Description | Admin consent requ... | Status |
|---|---|---|---|---|
| Microsoft Graph (2) | | | | |
| Mail.Send | Delegated | Send mail as a user | No | |
| User.Read | Delegated | Sign in and read user profile | No | ✓ Granted for Zucchetti S. |

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications.

Figura 8

# ADDENDUM B – MAGOWEB ONLINE EXPOSURE

For the network configuration in order to publicly expose MagoWeb to reach it from the outside, these are the configurations that we generally indicate:

1. Enter the server's public ip/dns to the hostname entry of the MagoWeb installer

2. Click Start to save your changes

3. On the firewall side, enable incoming rules that accept calls to the server from clients that log in to MagoWeb, taking care to open ports in the range 60000 - 60300, with a rule like this: ES:
   - Type: All TCP Rules (or All Traffic):
   - Protocol: All Protocols
   - Port Range: 60000 – 60300
   - Origin: IP client/32

4. Outbound calls must be opened with a rule like this:
   - Type: ( or all traffic:
   - Protocol: All Protocols
   - Port Range: All
   - Target: 0.0.0.0/0

5. Set up an inbound rule that also allows calls from the server's own public/private IP:
   - Type: All TCP rules( or all traffic):
   - Protocol: All Protocols
   - Port Range: 60000 – 60300
   - Source: ip server/32

Note: These are general indications, specific parameters or configurations may vary according to the structure of the network where MagoWeb is present.

# ADDENDUM C – CERTIFICATE CONFIGURATION

In general you can use any type of certificate that falls within the supported formats (*.pem, *.crt, *.der, *.cer, *.ca-bundle, *.p7b, *.p7c, *.p7s, * .der, *.pfx, *.p12, *.key).
And non-self-signed ones generated and issued by a valid CA.
There are no "official" integrations on the MagoWeb side. The installer is only interested in ensuring that the two certificate files are loaded and that the certificate is correctly installed and validated. In general, both paid certificates and those issued by a public CA are fine.

Generally the two parameters referring to the private and public keys are separate, but if you have a single certificate that contains both the public and private parts, you can also use only the first one (if the format is among those allowed).

The two files indicated must be loaded in the first entry, however it could be that if the certificate contains both parts (public and private), not separated, only one of the two is read and therefore the error is generated. There are many possible configurations and we suggest carrying out several tests.

For example, regarding the certificates generated by Certbot/Let's Encrypt, what the customer/reseller can do, on the installer side, is obviously to select a path on the file system relating to the two certificates (for example C:\Users\Administrator\ Documents\certificate.cer and C:\Users\Administrator\Documents\certificate.key).

**Certificate format conversion**
Below are some commands to convert some certificates into supported formats

Conversion to a combined PEM file

To convert a PFX file to a PEM file that contains both the certificate and private key, the following command needs to be used:

```
openssl pkcs12 -in filename.pfx -out cert.pem -nodes
```

Conversion to separate PEM files

We can extract the private key form a PFX to a PEM file with this command:

```
openssl pkcs12 -in filename.pfx -nocerts -out key.pem
```

Exporting the certificate only:

```
openssl pkcs12 -in filename.pfx -clcerts -nokeys -out cert.pem
```

Removing the password from the extracted private key:

```
openssl rsa -in key.pem -out server.key
```

# TROUBLESHOOTING

**Where to find the logs**

The Magoweb logs are located in the path set during installation (by default c:\logs), divided into files for the different Magoweb services.

The Installer logs are in the path C:\Users\user\AppData\Roaming\MagoWebInstaller\Logs

**General guidelines:**

- It may be necessary to disable the firewall during the installation of Mago Web.

- Verify that the ports assigned to the services are not already occupied or used

- Verify that UAC is set to the Default value (2), this is necessary for the correct execution of the installation scripts, if it has not been set correctly, a warning will appear in the installer

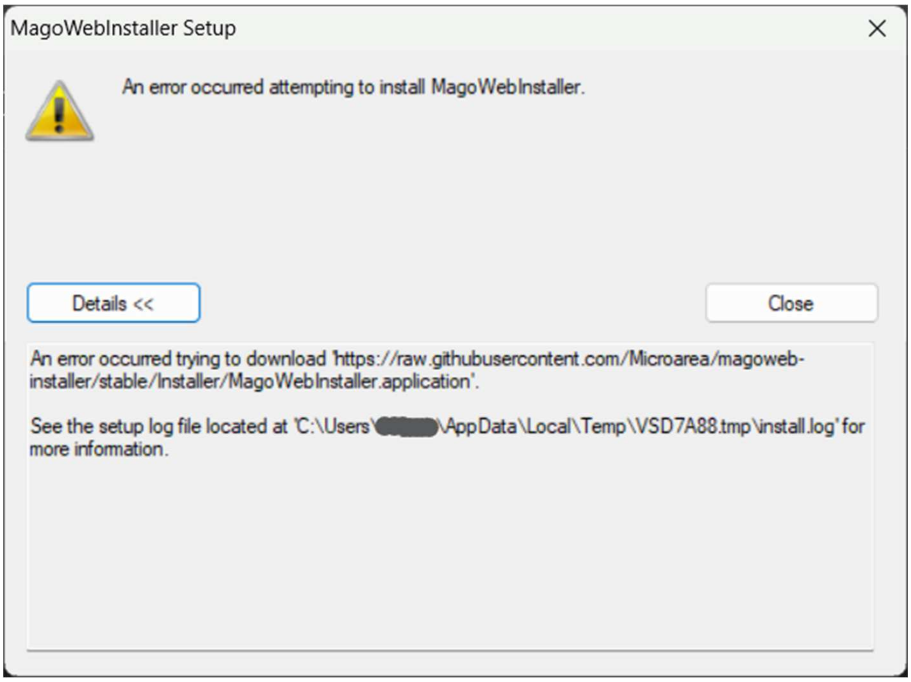
**Important** After each change made to the installer interface, press START to save the changes

**Important** When a new build is released, download both the new packages, installer and ztds, from the mymago.zucchetti.com website. To perform the upgrade procedure, always use the installer aligned with the version you are installing/upgrading.

**Important** Before upgrading from a consecutive release (e.g. from 1.2 to 1.3) make sure that the Use existing configuration item is not flagged. See anomaly 34747

**Important** When creating a new database, store and maintain the credentials for the dbowner part, these will be necessary if backup/restore operations are performed on the database server, or migrations to database providers (for example from postgres to sql, or vice versa). If credentials other than the display are entered, errors related to permissions may appear.

### (Version > 1.4) MagoWebInstaller Setup: An error occurred while downloading a required file



An error occurred attempting to install MagoWebInstaller.

An error occurred trying to download 'https://raw.githubusercontent.com/Microarea/magoweb-installer/stable/Installer/MagoWebInstaller.application'.

See the setup log file located at 'C:\Users\[redacted]\AppData\Local\Temp\VSD7A88.tmp\install.log' for more information.

Open the registry editor, go to the path HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings Check the key DisableCachingOfSSLPages if the value is 1 set it to 0

Launch the installer again.

### TestConnection exception: Response status code does not indicate success: 404 (Not Found).

Verify from the services status, from the Magoweb installer interface, that the *traefik* microservice has arrived correctly and that the port used is not already in use.
Restart the corresponding service and try to access again. If the problem persists, modify the installation and restart Start.

### Verify dotnet installation

In order for MagoWeb to work correctly, dotnet and its tools must be installed correctly. To verify that this is the case, you can do the following:

- open powershell and go to the folder containing the MagoWeb installer exe (and therefore Psexec)
- run: .\psexec -s -i powershell
- a second powershell window will open, here run: dotnet ef

If the shell draws the image of a unicorn (https://learn.microsoft.com/en-us/ef/core/cli/dotnet#verify-installation), the installation was successful. In case of error, follow the workaround indicated in anomaly 34337.

### Promtail does not start

Delete the positions.yaml file in C:\ProgramData\scoop\apps\promtail\current\positions.yaml
Restart the Promtail service

### Error: I cannot find any subscriptions associated with this account.

This error occurs when during the initialization of your MagoWeb instance, in the interface, under the item modify installation, an incorrect instance key or security value has been entered. Re-enter the correct security value from modify installation and click **START**.

### Frontend loading problem for versions prior to 1.4

On versions prior to 1.4, a frontend loading problem may occur, with the following error: net::ERR_CONTENT_LENGTH_MISMATCH 200 (OK). Even by refreshing the page, it may continue to reappear. The problem has been fixed from version 1.4 onwards and is solved by updating to this version of MagoWeb. If the partner cannot perform the upgrade soon, but only on schedule with the customer, while waiting for the resolving upgrade, there is a temporary workaround with specific instructions that solve the problem. Contact support for further information