MAGOWEB – User Manual

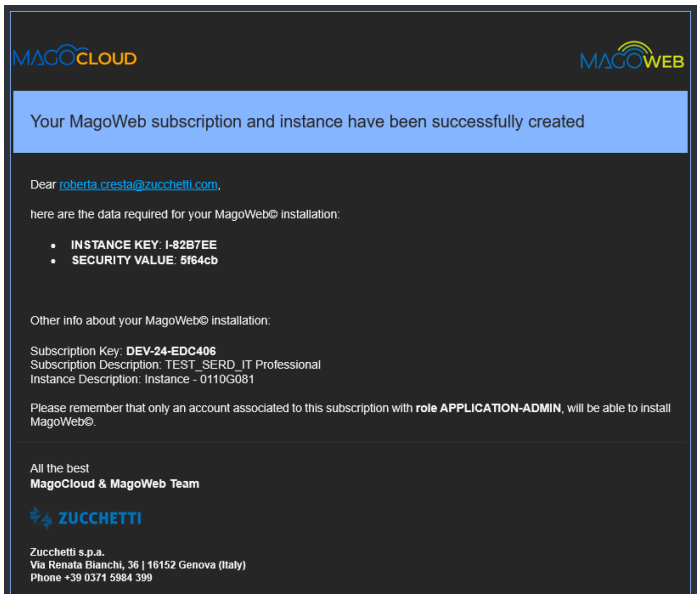
Summary

Purchase MagoWeb

The purchase of MagoWeb subscriptions is done through the dedicated Zucchetti Portal, following the standard procedure.

• Once the order is placed, it is necessary to activate the subscription via the appropriate activation button in the "My Clients" section of the Mago Store screen.

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



You need to provide these details during the initial installation.
Afterward, you will be able to proceed with the creation of the new database.

Hardware and software prerequisites

Below are the minimum requirements for a MagoWeb installation.
The hardware requirements refer to two ranges of workstations (PDL) and are related to the scenario where the same machine acts as both the Application and DB server.

The indicated hardware resources are based on load tests conducted by simulating interactive use of the program and may vary depending on the use cases.

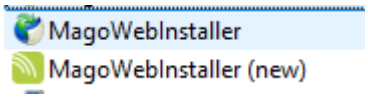
With the same virtual resources, performance may vary depending on the underlying hardware and the virtualization system in use. The specified requirements should be considered as a general reference.

Range PDL	CPU	RAM	Requisiti SW
1-5	2 core	16 GB	- Windows Server Standard (2016 or later - Postgres 14.9 or later (o MSSQL 2017 or later)
6-10	4 core	16 GB	- Windows Server Standard (2016 or later - Postgres 14.9 or later (o MSSQL 2017 or later)

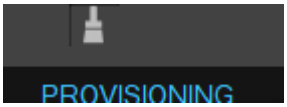
Updating to versione 5.1.0

Starting by version 5.1, the MagowebInstaller tool will change installation tecnology from “clikonce” to a proprietary tecnology.
The new installer will be placed at the following url:

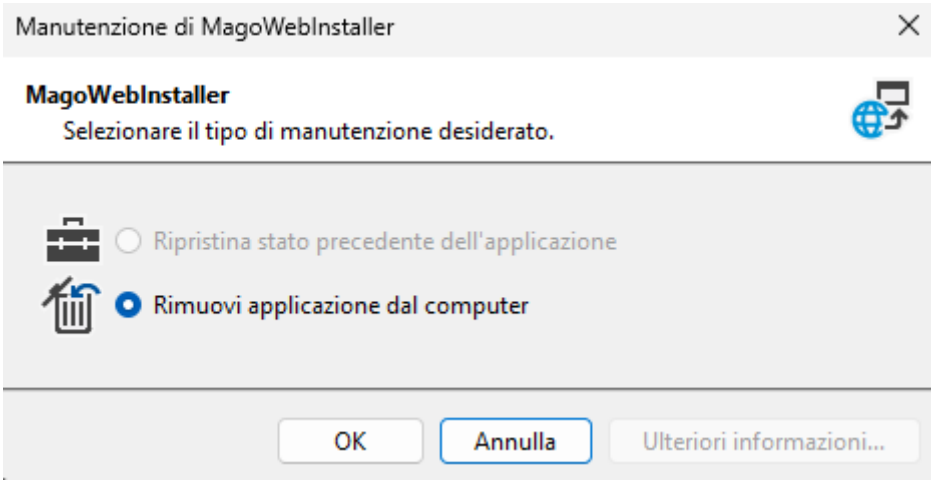
https://raw.githubusercontent.com/Microarea/magoweb-installer/stable/setup.exe
The old “clickonce” version will be able to automatically update to the new tecnology.
Due to a limitation in the clickonce uninstallation procedure, the old version cannot be automatically uninstalled.
The user need to manually remove the old versione from the control panel: in order to differenciate the two version, the new one will be listed as “MagowebInstaller (new)”



In order to simplify the uninstallation process of the old version, a button will be added to the main window of the Magowebinstaller



The user need onlyt to confirm the “removal” of the old version.

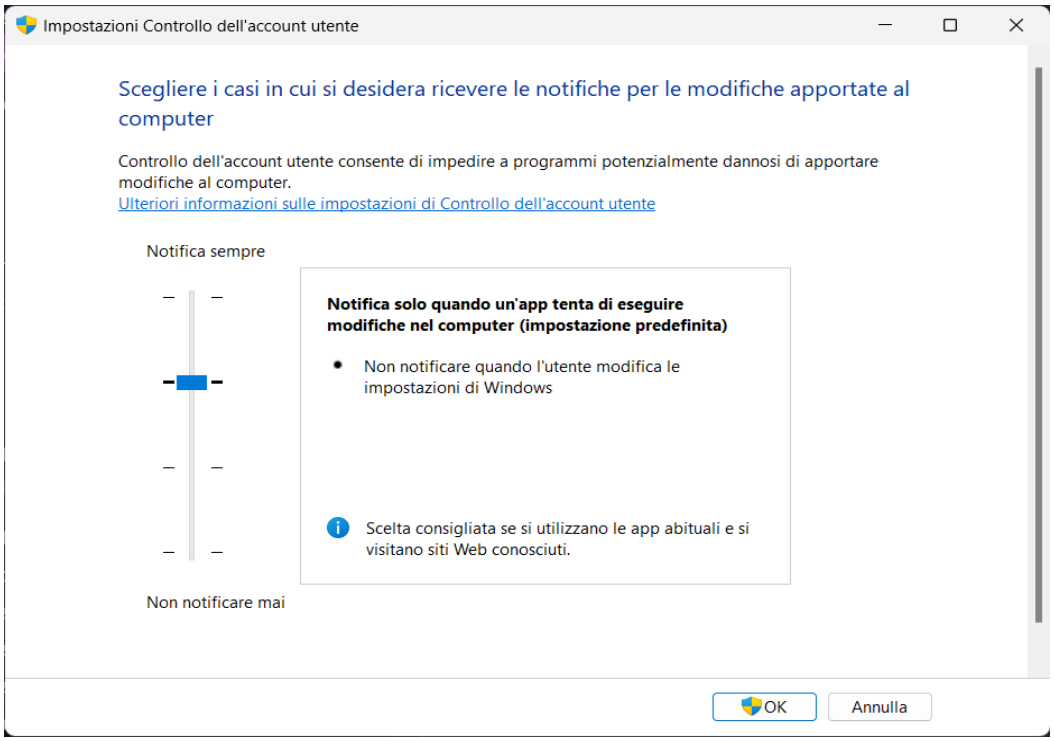


Installation and first Configuration

Log in to the machine where MagoWeb will be installed using an account with administrative privileges.
Download the installer and the .zst file for the version you intend to install from the Microarea website at https://mymago.zucchetti.com, ensuring that the versions of the two files match.

Starting from version 1.4, the MagoWeb installer has been modified. You must use the setup.exe installer, and it is NOT possible to use the MagoWebinstaller.exe from previous versions. Doing so will cause the installation to fail, and a clean reinstall of the product will be required.

Check and/or set the Windows User Account Control (UAC) security level to the default level as shown in the screenshot.



Versions 1.3 or earlier

Run MagoWebInstaller.exe as an administrator. If the previous step is not completed, a warning message will notify the user.

Versions 1.4 or later

Open an administrative command prompt and run the Setup.exe file. The setup will verify and download the necessary prerequisites, and once this operation is complete, it will open the installer window. Again, if the UAC permission levels are not set correctly, a message will notify the user.

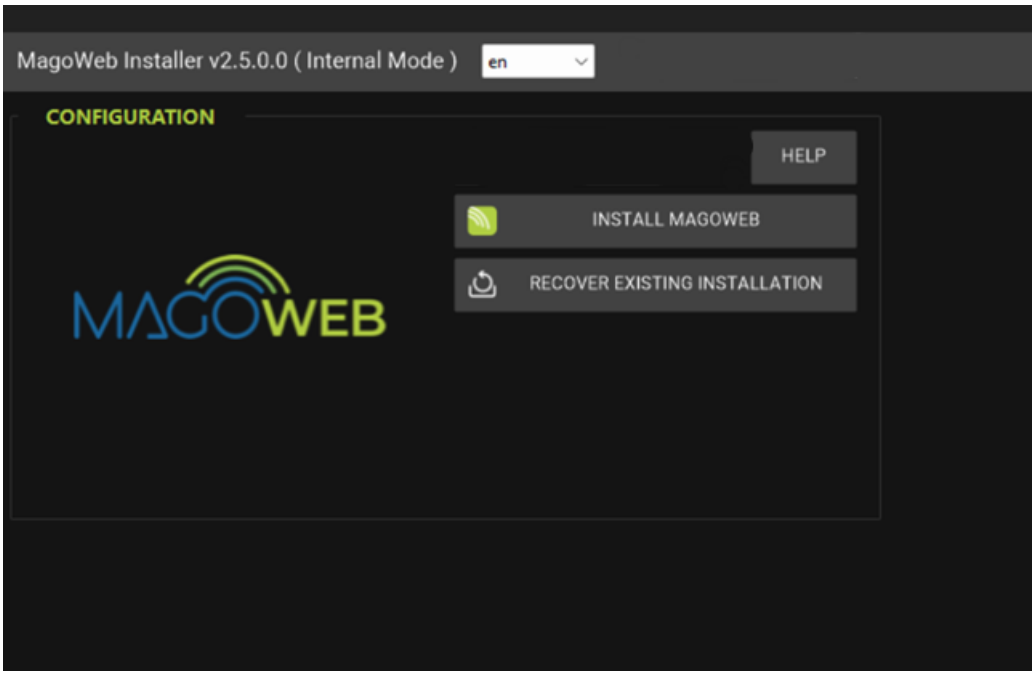
Starting the Installer

Run the file MagoWebInstaller.exe

If the system has never been configured before, a configuration wizard will automatically start, guiding you step by step through the process.

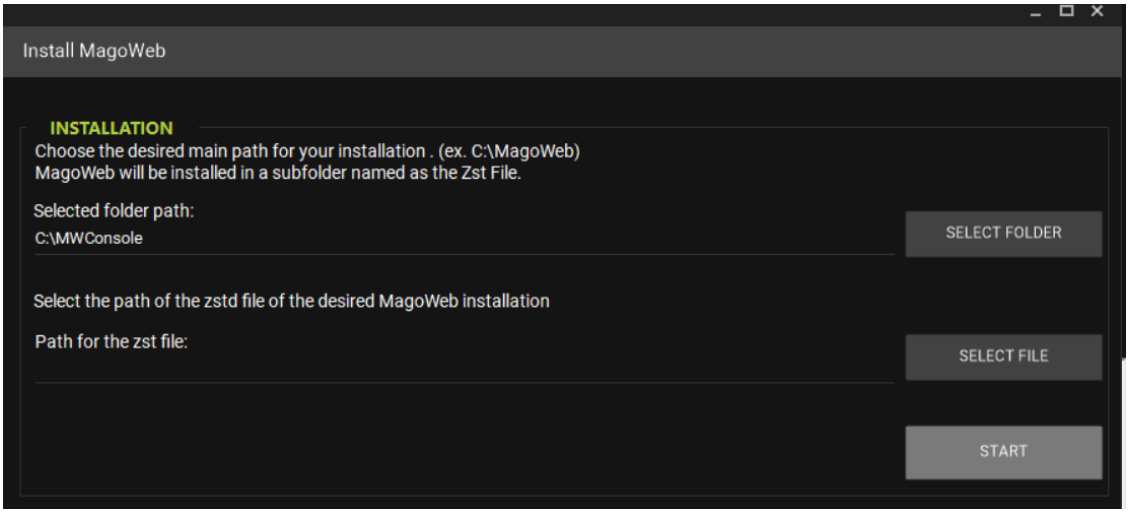
Installation Mode

- New Installation (Install MagoWeb): If this is your first time installing MagoWeb.
- Restore an Existing Installation (Recovery existing installation): If you wish to use a previously existing configuration.



Select Installation Path

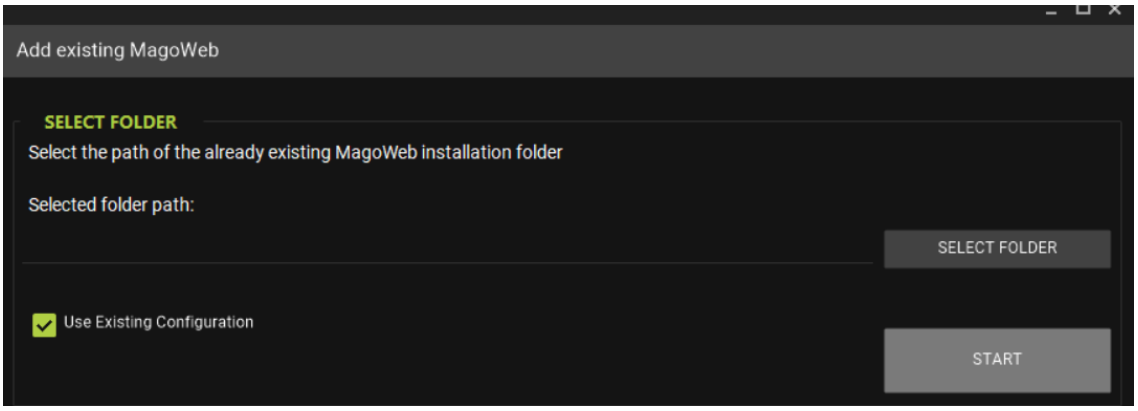
- By clicking INSTALL MAGOWEB, you need to select the folder where you wish to install MagoWeb. During the installation, MagoWeb will be created in a subfolder named "Zst file."
- Zstd file path: Enter the path of the Zst file associated with the MagoWeb installation (the downloaded file).



Start the installation

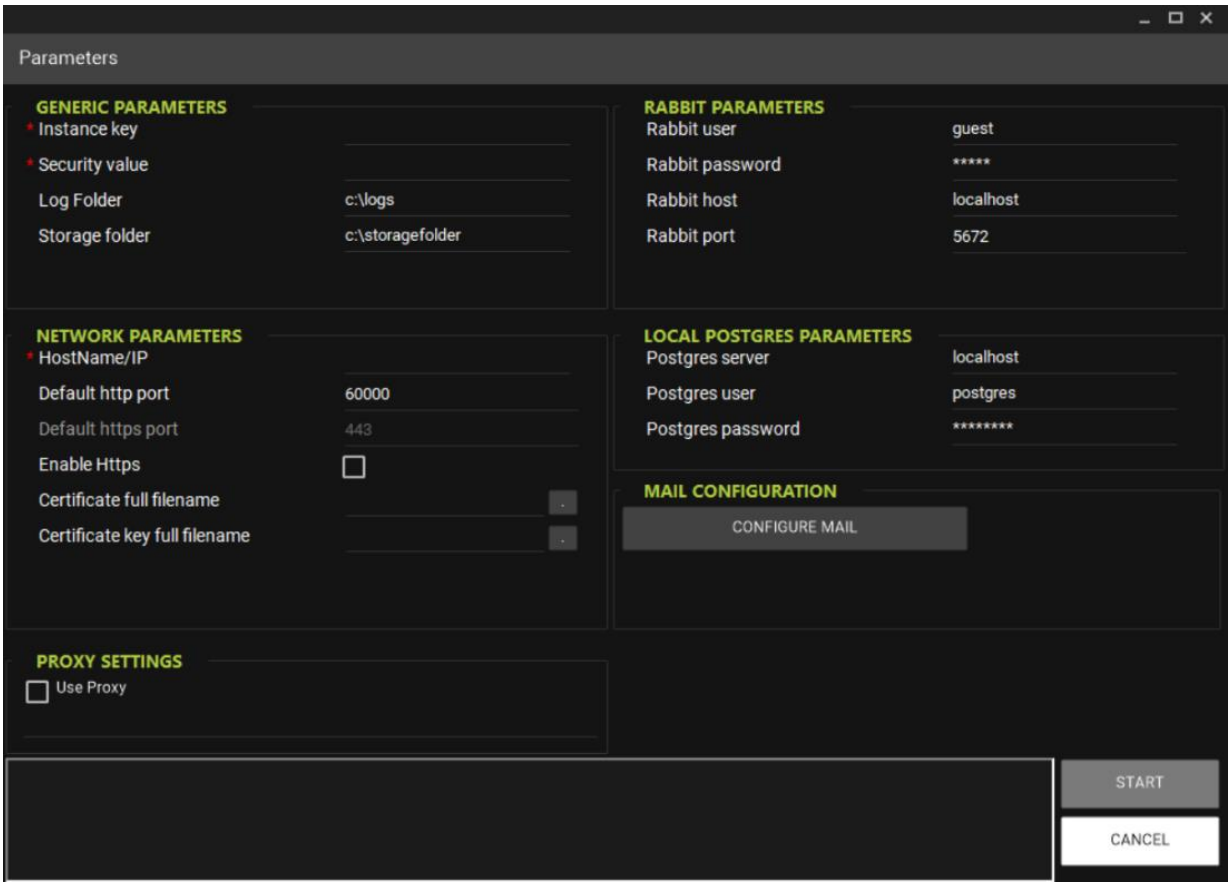
- After selecting the path, click Start to begin the installation.
- The system will proceed with downloading and installing the necessary files.

Alternatively, you can proceed with Recovery existing installation. In this case, the system will prompt you to select the path of the already existing MagoWeb installation folder. Once selected, click Start to begin the recovery procedure.



Initial configuration of parameters

The configuration window is divided into five main sections:



General parameters:

- The Instance Key and Security Value, which you should have received via email earlier (see the MagoWeb Purchase section).
- Log folder: The folder where the diagnostic logs produced by the various services will be stored.
- Storage folder: This folder will temporarily store the various files during any Upload/Download operations.

Network parameters:

- Hostname/Ip: This field hosts the public IP address of the machine that will host the MagoWeb installation, or a related alias set externally at the DNS level.
- Default http e Https port: default 60000 (http) e 443 (https)
- Enable Https: Specifies whether to enable HTTPS management for the installation. Enabling this option will activate the parameters related to certificates.
- Full path of the certificate file and the key:(es. c:\cert\certificate.crt e c:\cert\certificate.key). Specify the certificate and key files related to the domain/IP set previously.

If HTTPS is enabled, ensure that the exact hostname corresponding to the certificate you will be using is entered in the HostName field.

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

Proxy settings

If the MagoWeb installation is performed in a domain behind a proxy, enable the corresponding flag and set the proxy URL.

Rabbit parameters

In this section, enter the parameters for the RabbitMQ connection. The installer can use an existing version of RabbitMQ, or if it doesn't exist, it will be automatically installed and configured.

Postgres parameters

As with RabbitMQ, the installer can use existing versions of PostgreSQL or automatically install the necessary version.

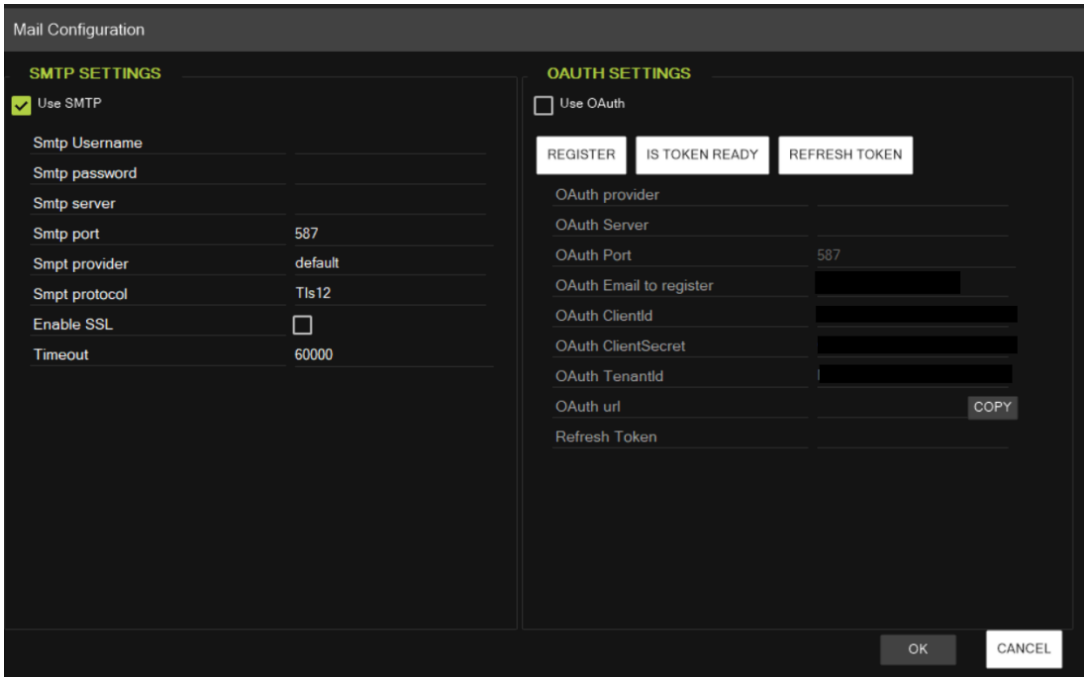
Note: PostgreSQL is a prerequisite for the operation of certain MagoWeb services and is not necessarily the database server is connected to the subscription.

Port settings

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

Email configuration

The Configure Mail button will open the corresponding configuration window.



SMTP Settings: In this section, which is selected by default, if you have a mail service, you need to configure the various parameters (server, user, password, etc.) for the connection to the SMTP server. The parameter "Smtp Provider = default" should not be modified.

OAuth Settings: The Use OAuth button will disable the SMTP section and enable the fields below.

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

Provider Microsoft:
Guida introduttiva: Registrare un'app in Microsoft Identity Platform - Microsoft identity platform
Provider Google:
Utilizzare OAuth 2.0 per accedere alle API di Google | Authorization | Google for Developers

- Note the parameters provided by the provider for authentication during the configuration of the new OAuth2 protocol, namely:
- Client Id
- Client Secret
- Tenant Id

- In the current screen, enter all the data up to TenantId.
  1. Enter the desired provider, Google or Microsoft, as indicated in point A.
  2. For the server, enter "smtp.google.com" for Google or "smtp.office365.com" for Microsoft.
  3. The port is always 587.
  4. Specify the sender's email address for OAuth in the "Email to register" section based on the provider previously selected.
  5. Enter the Client ID, Client Secret, and Tenant ID: these details can be retrieved from the application registered with Google or Microsoft. For Google authentication, there is no Tenant ID; however, the field should not be left empty and should be filled with any text.
  6. At this point, click "Register." The process will generate a URL (which will be transferred to the corresponding property in the dialog). The system will attempt to open in an incognito page of the Chrome browser; if it fails, it will open a page in your default browser, but not in incognito mode. In this second scenario, be careful that the email is not automatically deduced by the browser, with your Google or Microsoft account already set up. Ensure that the same email previously entered is used. If in doubt, open an incognito window in your browser and copy the link found in the box next to the COPY button.
  7. Enter the password for the email entered and accept the terms.
  8. If the process is successful, a page with encrypted information will be returned in the browser tab. This means the token is ready, and you can safely close the tab.
  9. Proceed by clicking the "IsTokenReady" button. If the process is successful, the "Refresh token" field should auto-fill.
  10. Click the "OK" button.

Note: The 'Refresh token' button should not be used. The received token will expire one hour after the request, but the update request will be triggered automatically, making this button just a precaution. In fact, the validity check, and token refresh will occur with each new login to Mago and before sending any email.

It is now possible to send emails using OAuth2.

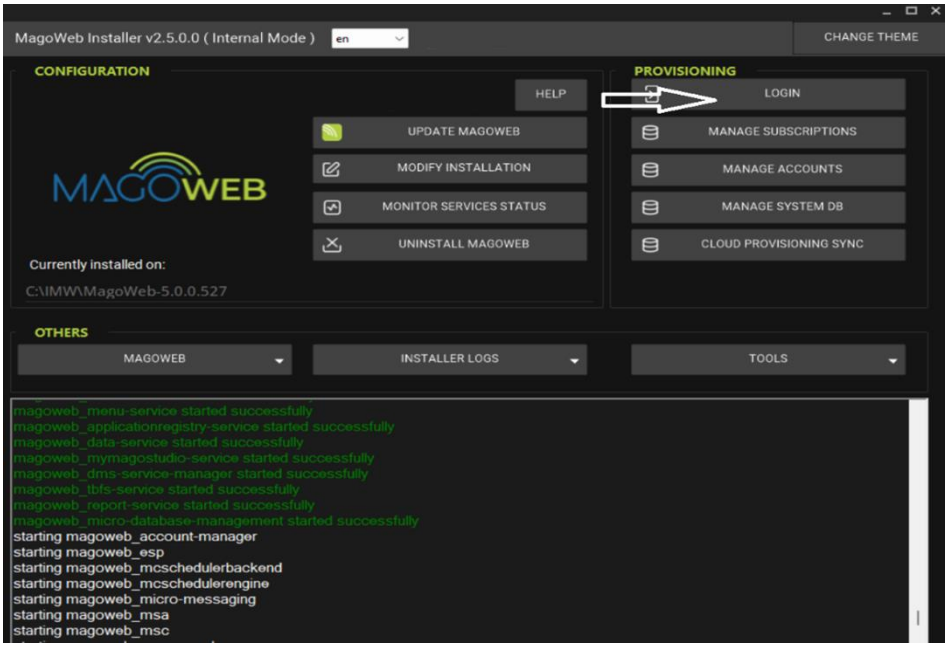
Once all mandatory parameters are set, the start button will be enabled.

Pressing the Start button will initiate the actual configuration and installation of MagoWeb.

Creation of the SYS-ADMIN user

Access to the system

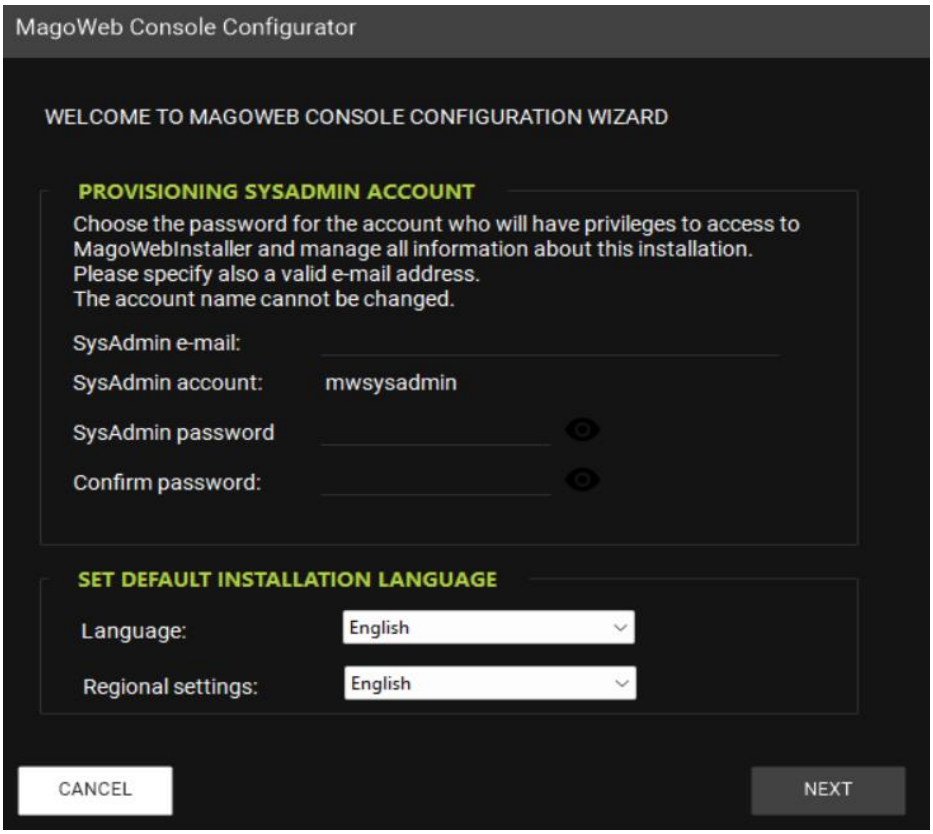
- Once the installation is complete, it will be necessary to create a SYS-ADMIN account.
- In the Provisioning section, click on Login to start the SYS-ADMIN account configuration wizard.
-



Configuration of the SYS-ADMIN account

- Password: Choose a password for the SYS-ADMIN account.
- Email address: Enter a valid email address for account recovery and notifications.
- Account name: This field is not editable and will be pre-filled with the SYS-ADMIN account name, which is mwsysadmin.

You can also choose your preferred language for the user interface.



Click Next to proceed.

Configuration of the System Database

- Before configuring the database for MagoWeb Console, administrative database credentials will be required.

Selection of the Database Provider

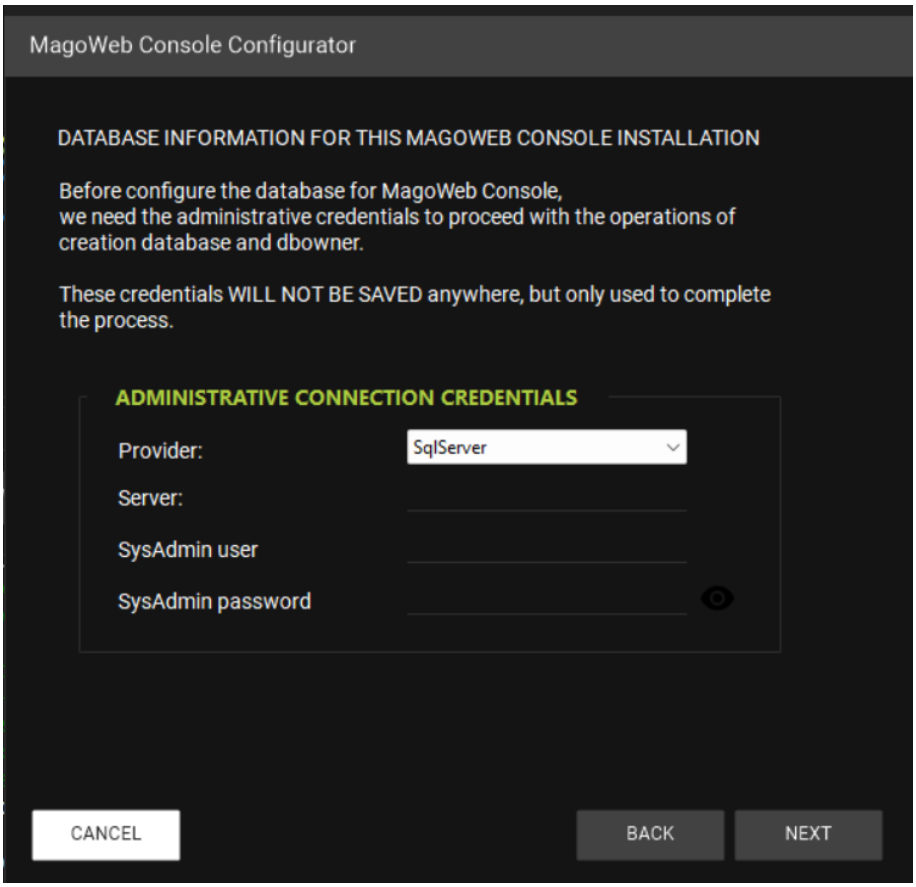
Select the database provider to use:

- SQL Server or PostgreSQL.

Enter the database server details:

- Reference server: Enter the address of the SQL or PostgreSQL server.
- SysAdmin User: The username for administrative access (e.g., 'sa' for SQLServer / 'postgres' for PostgreSQL).
- SysAdmin Password: The password for the administrative user.

Note: The provided administrative credentials are used only for system database management operations and will NOT be saved locally.



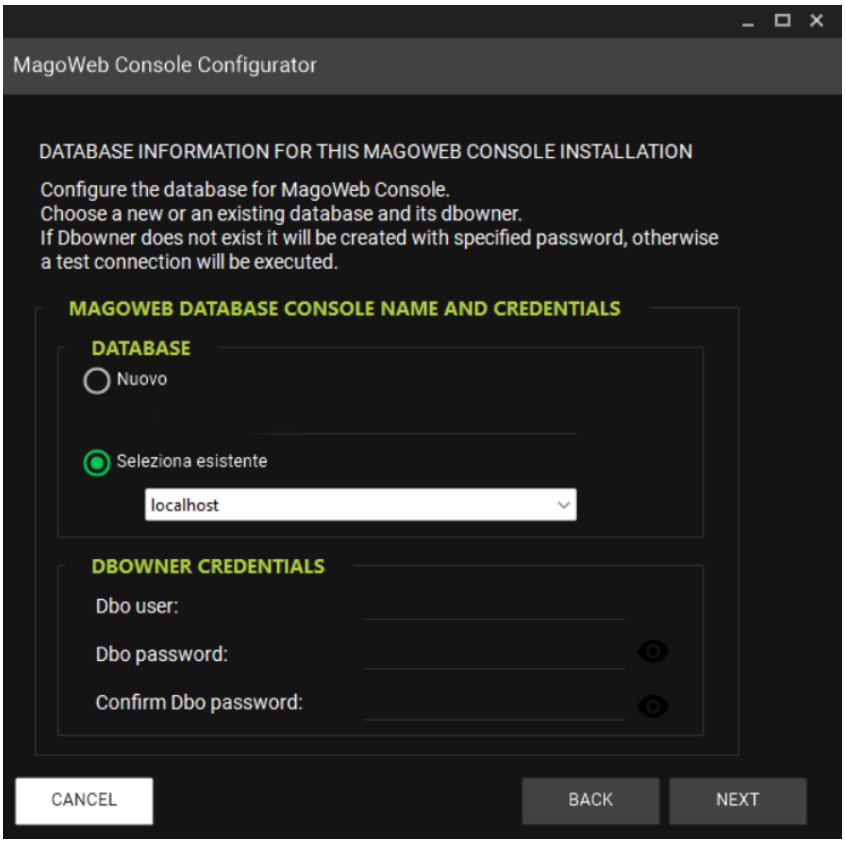
Click Next to proceed.

Creation or Selection of the System Database

- New Database: You can choose to create a new database.
- Existing Database: Select an existing database.
- Dbowner: Credentials of the user who will become the dbowner for the system database.

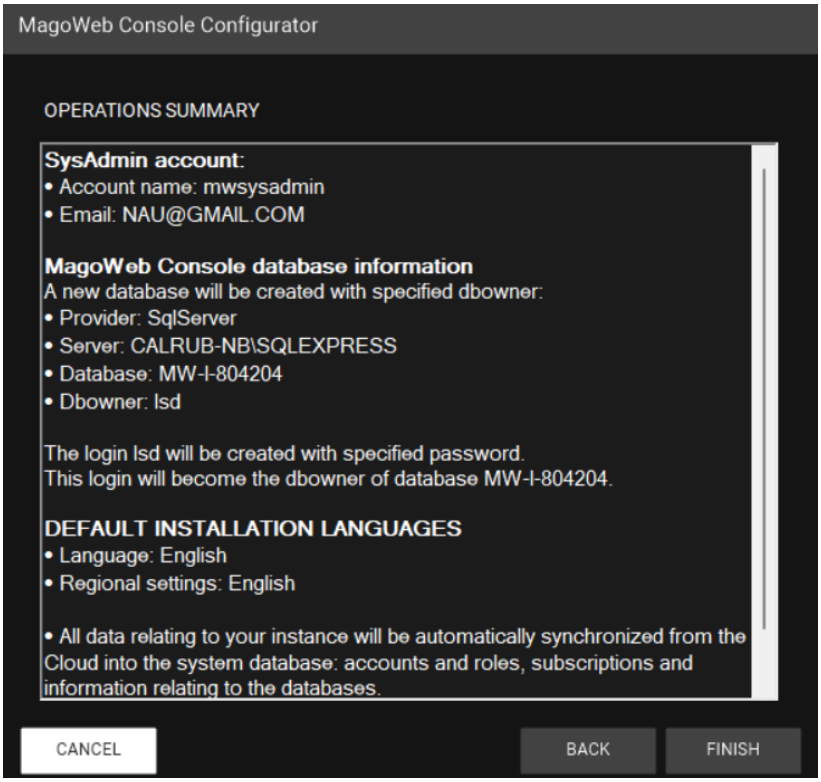
If the dbowner does not exist, it will be created automatically with the specified password. If it already exists, a test connection will be made to verify its validity. The chosen dbowner will be applied to all objects in the system database.

Note: If the password of an existing dbowner cannot be retrieved, manual intervention will be required by connecting to the server and modifying it using the provider's administration tools.



Summary of Operations

- Once all the data has been entered, a summary of the configuration operations will be displayed.



- Click on Finish to complete the configuration.

Installation completion.

- After clicking on Finish, the system will perform the final configuration operations, starting the necessary services for the proper functioning of MagoWeb Console.

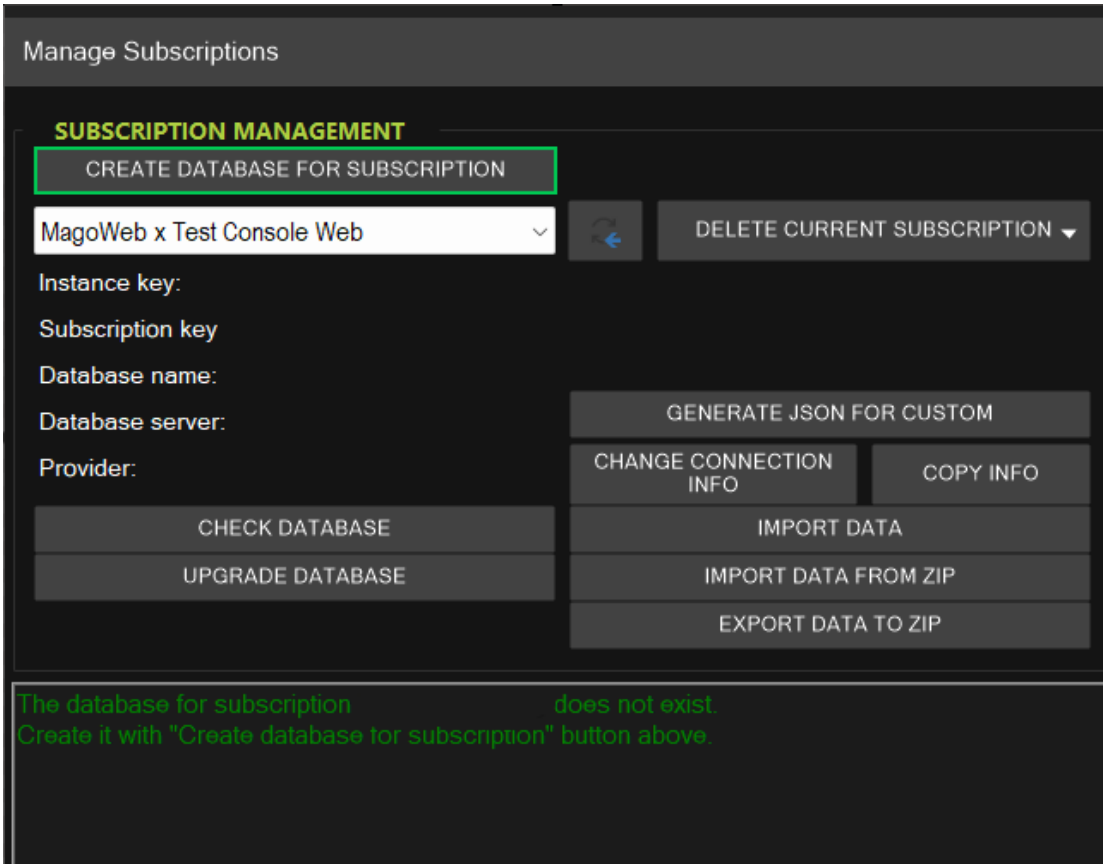
Note: It is reminded that at the end of the Wizard, data synchronization from Provisioning Cloud is performed. Please refer to the details in the dedicated section.

Creation of Subscription Database

After authentication, you will find your subscriptions in the dropdown menu.

At this stage, the installer will notify you that the subscription does not yet have a database.

Proceed with creating the database by clicking the "Create database for the subscription" button.



Database Configuration

It is possible to use either SqlServer or PostgreSQL as the database provider.

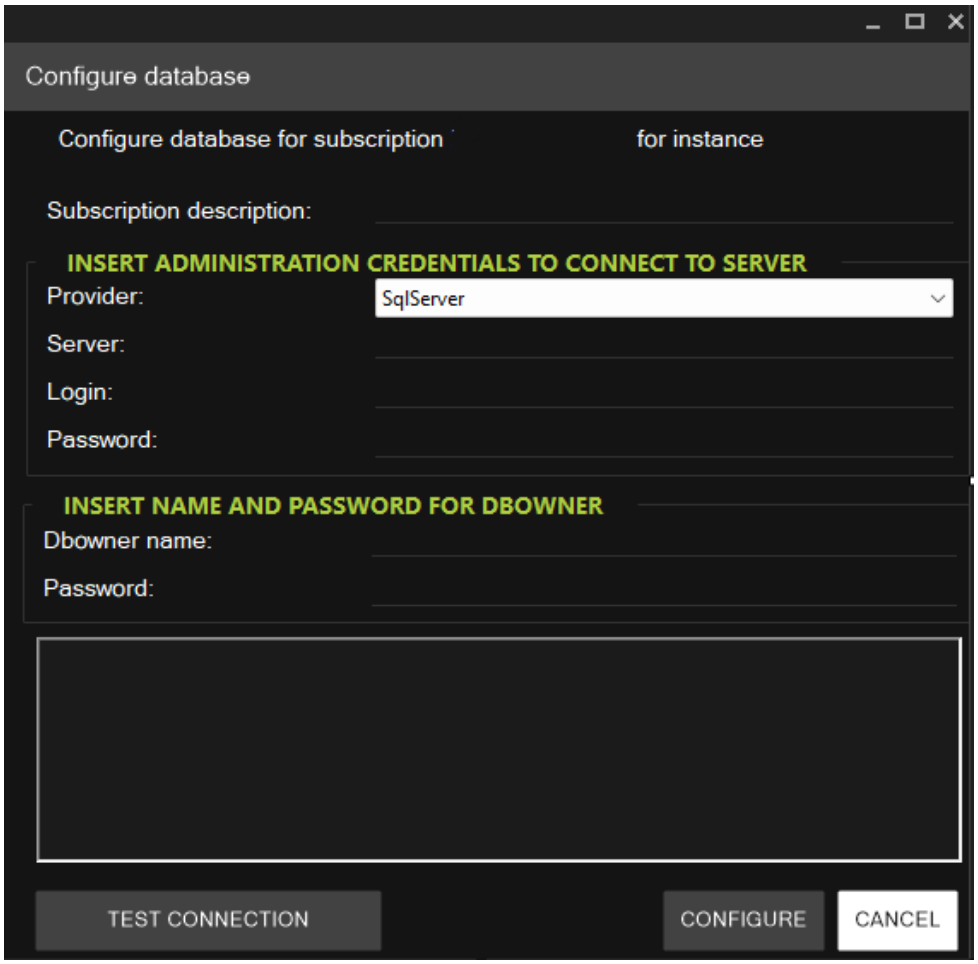
Select the desired provider from the appropriate dropdown menu.

Once the provider is set, you will need to enter the Server, Login, and Password information for the connection.

You can use the "Test Connection" button to verify the validity of the information you just entered.

You will need to enter the credentials of the dbowner to be associated with the database. You can enter the credentials of an existing dbowner or a new user; the installer will automatically create it.

Nota: non è possibile indicare come dbowner un utente amministratore (e.g. sa / postgres)



By pressing the "Configure" button, the database creation will begin.

Afterwards, you can proceed with importing a default or sample dataset.

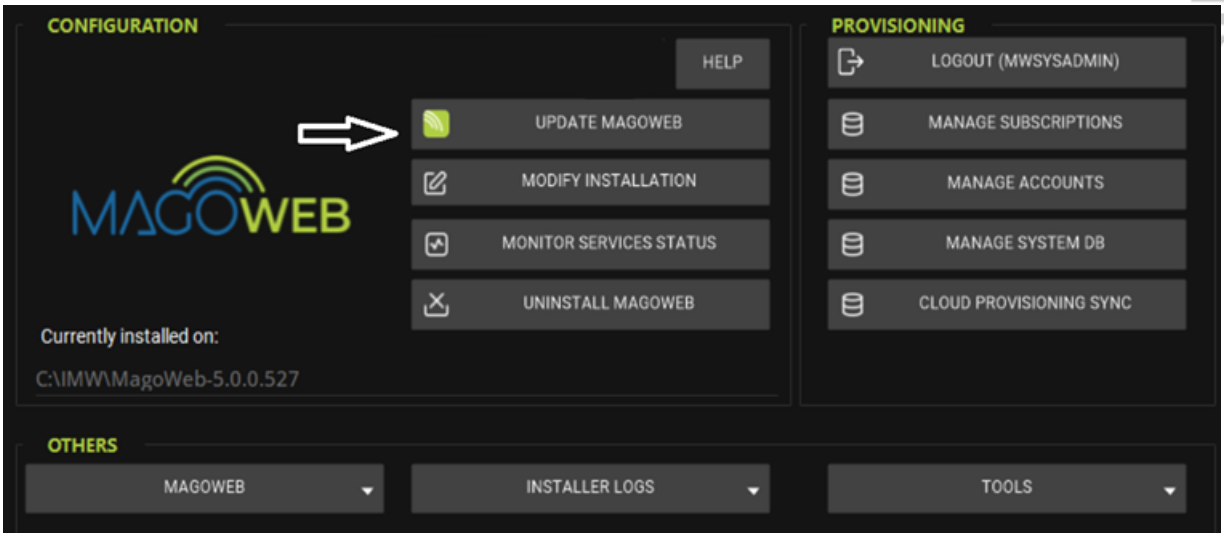
Changes to the Initial Configuration

Once the initial configuration is complete, it will still be possible to make changes to the configuration.

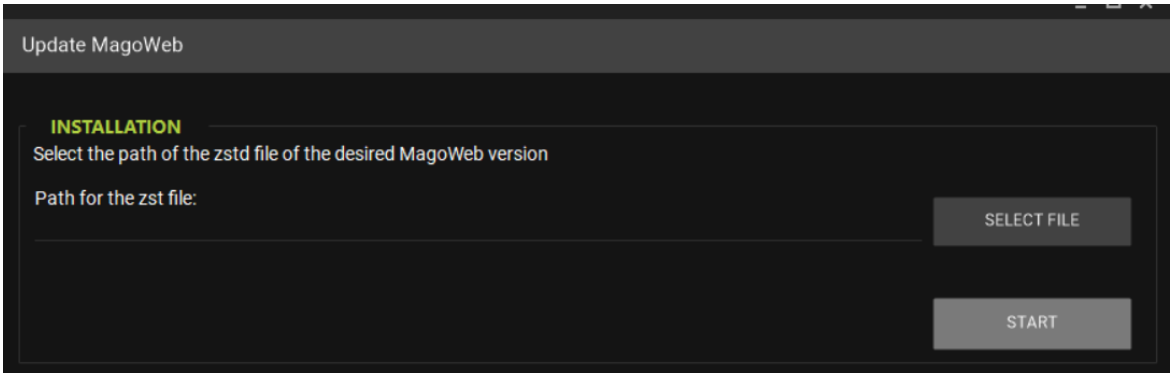
MagoWeb Update

To update MagoWeb:

1. In the Configuration section, select Update MagoWeb.



2. You will be prompted to select the path of the zst file for the version of MagoWeb you wish to install.



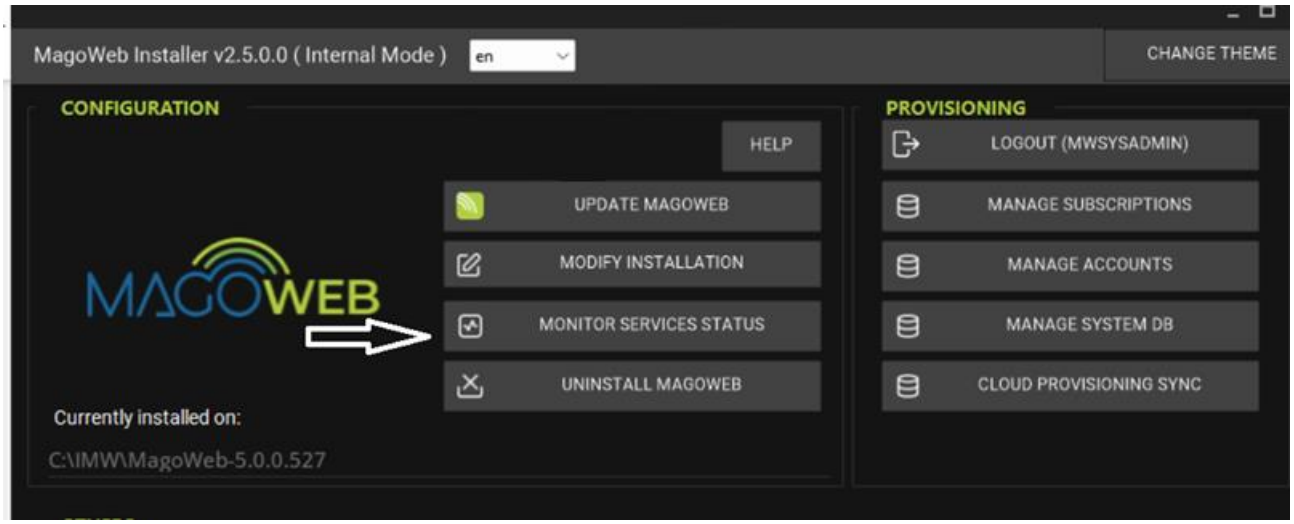
3. After selecting the file and clicking on Start, the system will automatically proceed with the update.

Note: It is not possible to have multiple active MagoWeb installations at the same time. You must either update to a recent version or uninstall the current version and restore an existing one.

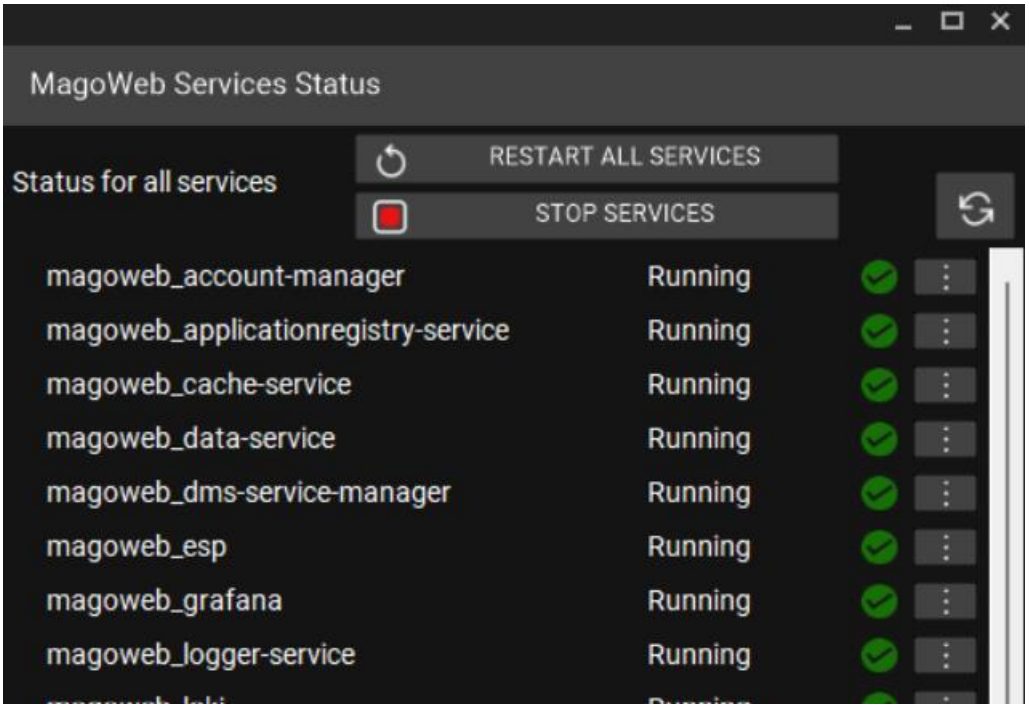
Service Monitoring

To monitor the service status and manage them:

1. Go to the Monitor Service Status section.



2. Here, you can view the status of the running services.
3. To restart a service, click on Restart.
4. To stop a service, click on Stop.



Note: The magoweb micro-database-management service is automatically started and stopped as needed during database maintenance operations.
Outside of these uses, the service will be stopped to prevent unnecessary memory usage, so it will be normal to see it as "stopped" under typical usage conditions.

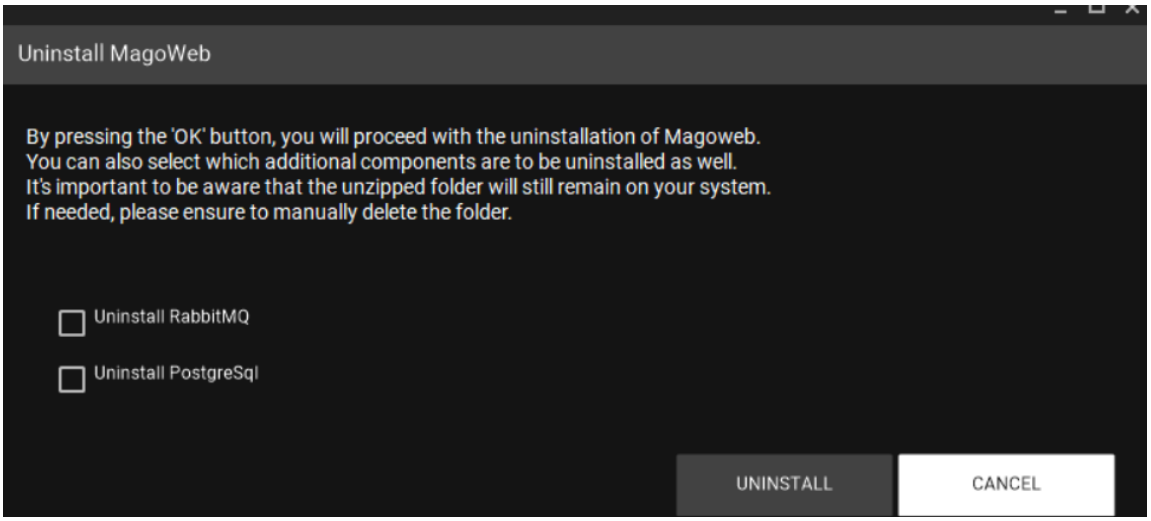
Note: Some services depend on others. If services that depend on or are dependencies of other services are manually restarted, the connected services will also be restarted accordingly.

Uninstallation of MagoWeb

To uninstall MagoWeb and its additional components:

1. Go to the UNINSTALL MAGOWEB section.

2. All services will be "stopped" and removed, except for RabbitMQ and PostgreSQL (unless the user has chosen not to remove them, as shown in the next image).
3. Click on UNINSTALL to start the uninstallation process.

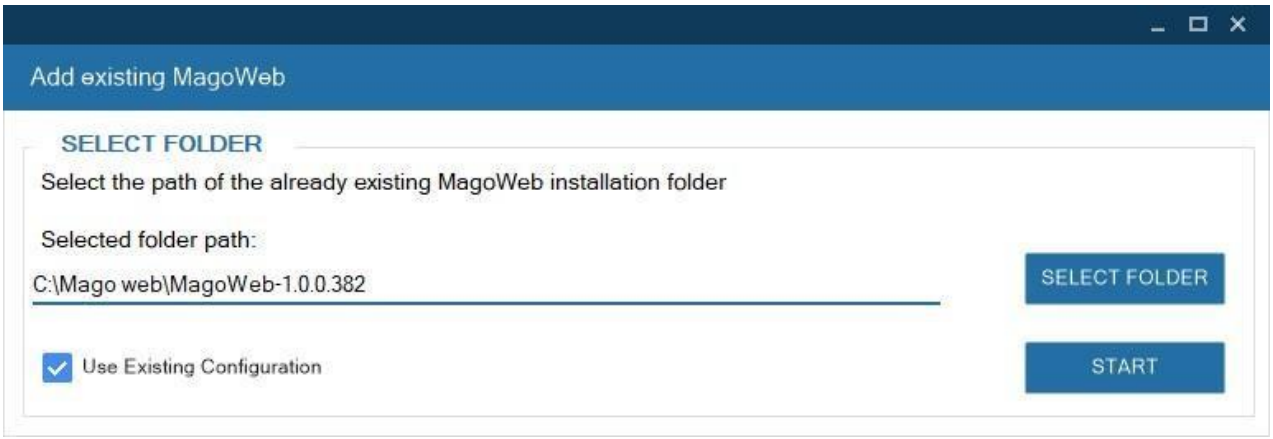


4. The system will proceed with the removal of MagoWeb and the selected components.

Note: The installation folder will not be deleted; it is the user's responsibility to remove it manually. At any time, it will be possible to recover a version of MagoWeb using the Recover Existing Installation button.

Recovery of 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 Previous Installation button.



In the window that appears, select the folder of the version you want to restore. By pressing Start, all services will be reinstalled using the last configuration entered by the user.

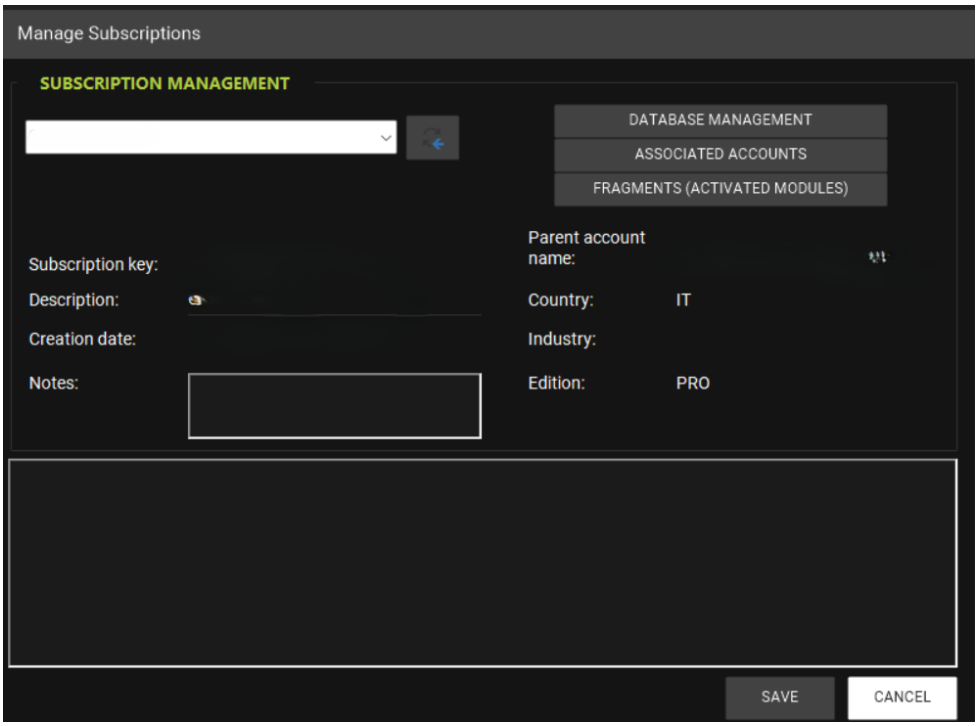
User and Subscription Management

After logging in as SYS-ADMIN, go to the Provisioning section.

Subscription Management

In the Provisioning section, click on Manage Subscriptions.

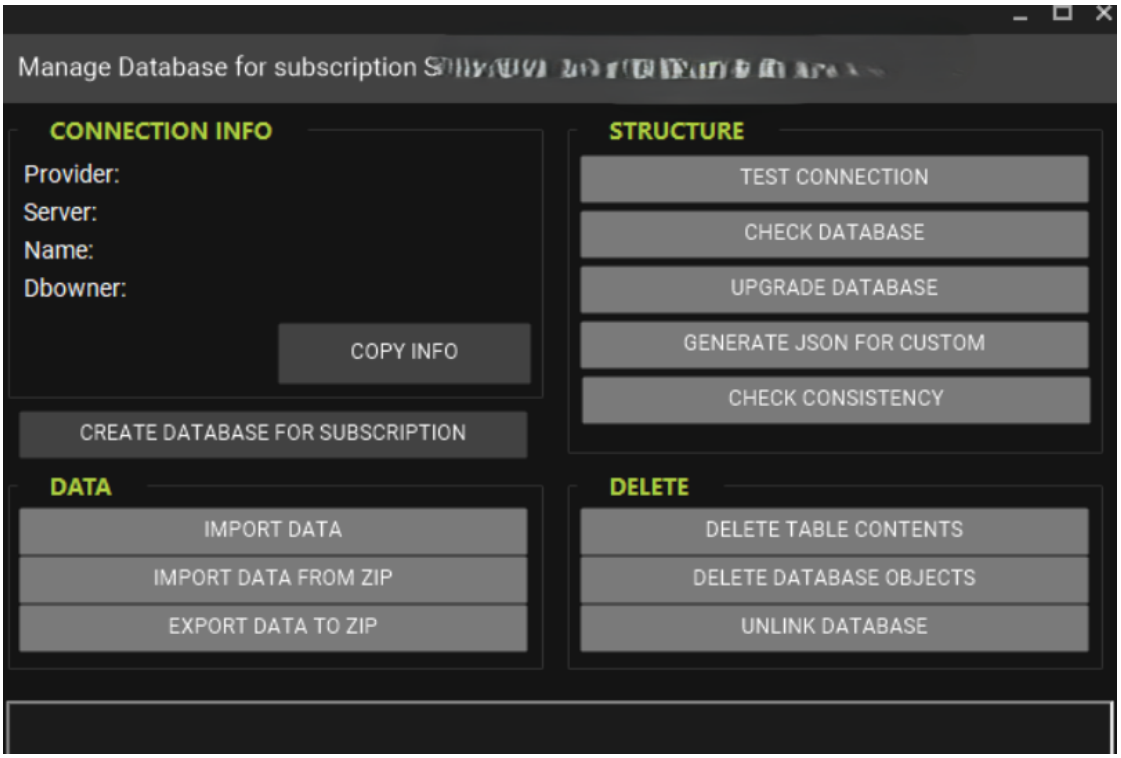
From this section, it will be possible to manage Databases, Associated Accounts, and Modules.



Database Management

By clicking on Database Management, information related to the database connection will be displayed.

From this screen, you can perform the following operations:



- In the CONNECTION INFO section:
- **Change connection info** allows you to modify the database connection information (e.g., in case of a server or database name change).
- **Copy info** copies the subscription information to the clipboard.

- In the STRUCTURE section:
  - Test Connection performs a test to check the reachability of the database.
  - Check Database runs a check on the current database of the subscription to verify if the table structure is aligned with the current version.
  - Upgrade Database triggers the database upgrade for the subscription.
  - Generate JSON for Custom creates a JSON file, which will be saved in the tb_customtbfs table, containing the entire current structure of the database. This information is used by Reporting Studio and MyMagoStudio.
  - Check Consistency initiates a check between the database structure of the subscription and the objects (tables, columns) declared in the EFSchemaObjects.xml files, highlighting any differences.

- In the **DATA** section:
  - **Import Data** allows you to import the default data for MagoWeb:
    - **Default data**: Configuration data necessary for the application procedures to function. These are divided by country and configuration. Usually, the country selection corresponds to the one chosen during the subscription purchase.
    - **Sample data**: A set of default data enriched with additional values that create a dataset for illustrative purposes.

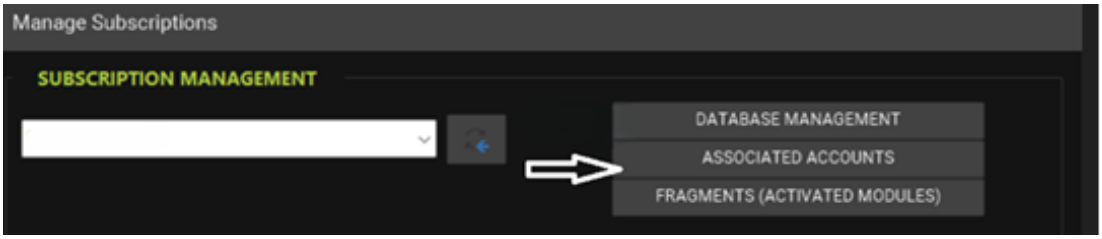
- **Import Data from ZIP** allows you to upload `.xml` files containing user-defined data. The XML structure must strictly follow the format that the system can read. This can be determined by exporting tables using the export function and then using them to generate the files, which can be zipped and imported correctly. The size limit is **100 MB**.

- **Export Data to ZIP** allows you to export the entire content of the tables in `.xml` format within a `.zip` file. This operation has a maximum database size limit of **2 GB**.

- In the DELETE section:
  - Delete Table Contents deletes, after confirmation, all data contained in the tables while leaving the table structure unchanged.
  - Delete Database Objects deletes, after confirmation, the entire table structure of the MagoWeb subscription.
  - Unlink Database removes the link between the subscription and the database without altering the database itself, which will remain available on the designated server.

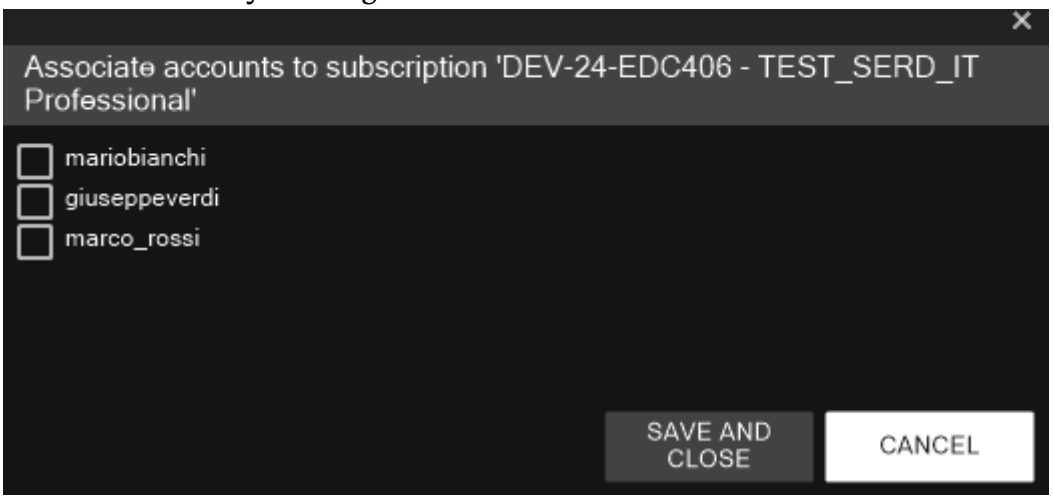
Associated Account Management

By selecting Associated Accounts, a new screen will open displaying the list of all accounts associated with the subscription.



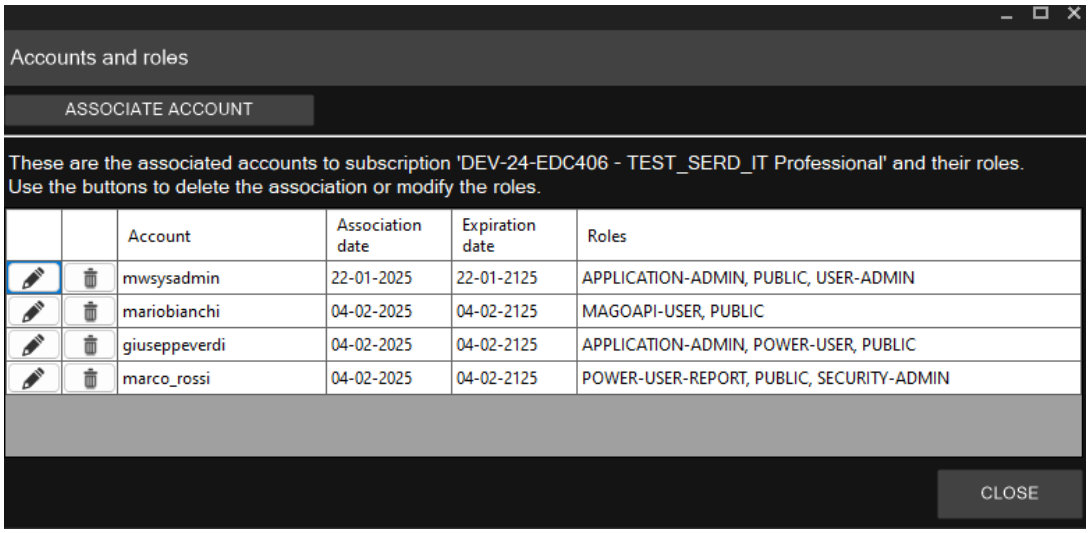
In this section, you can:

- Associate a new account: Click on the Associate Account button, select the desired account, and confirm by clicking Save.



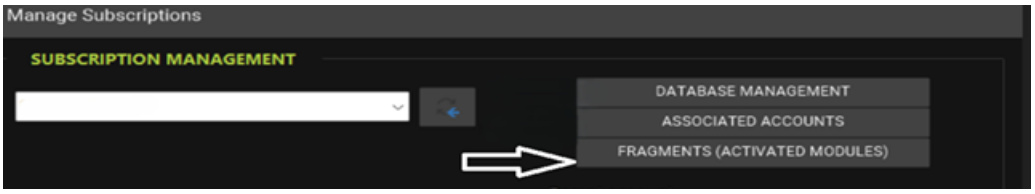
- **Modify an account's role**: Click on the pencil icon next to the account to edit its role.

- Remove an account association: To delete an account linked to the subscription, click on the trash bin icon.



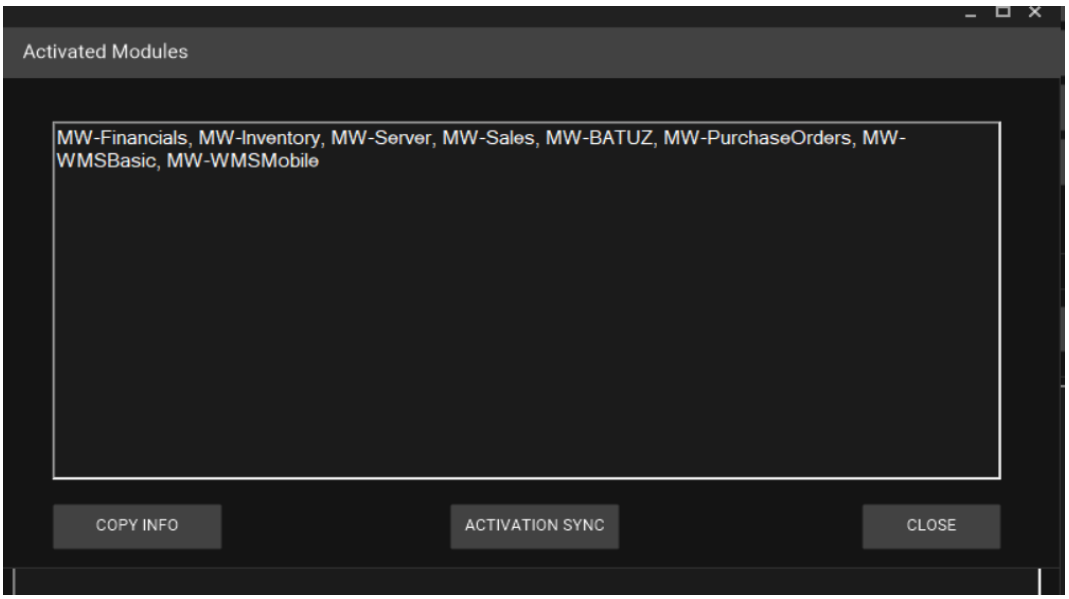
-

Clicking on the Fragments (Activated Modules) button will display all the modules associated with the subscription.



Module Synchronization

If new modules are added to the subscription in the future via the Infinity portal or the store, a local synchronization will be required for the new modules to become visible. To do this, click on the Activation Sync button to complete the synchronization process.

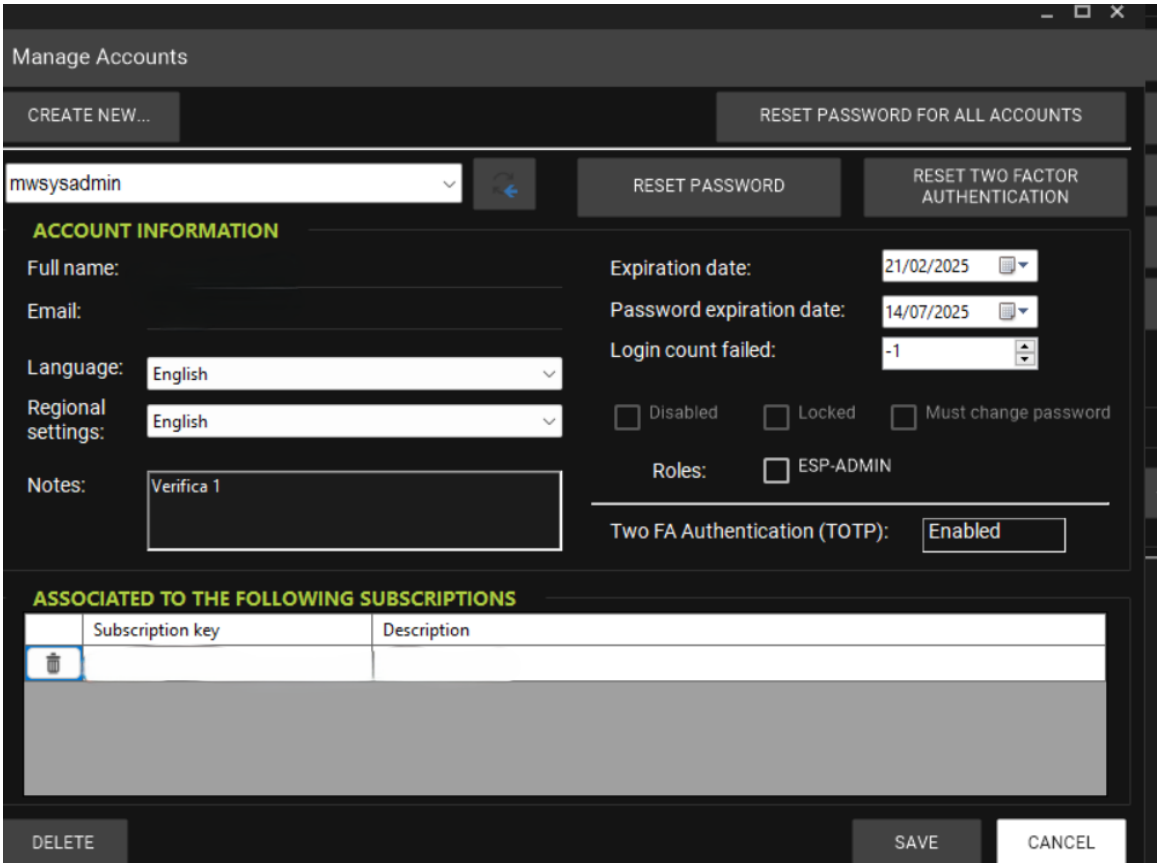


Note: Make sure to perform synchronization every time new modules are added to your subscription to ensure proper information updates.

Account Management

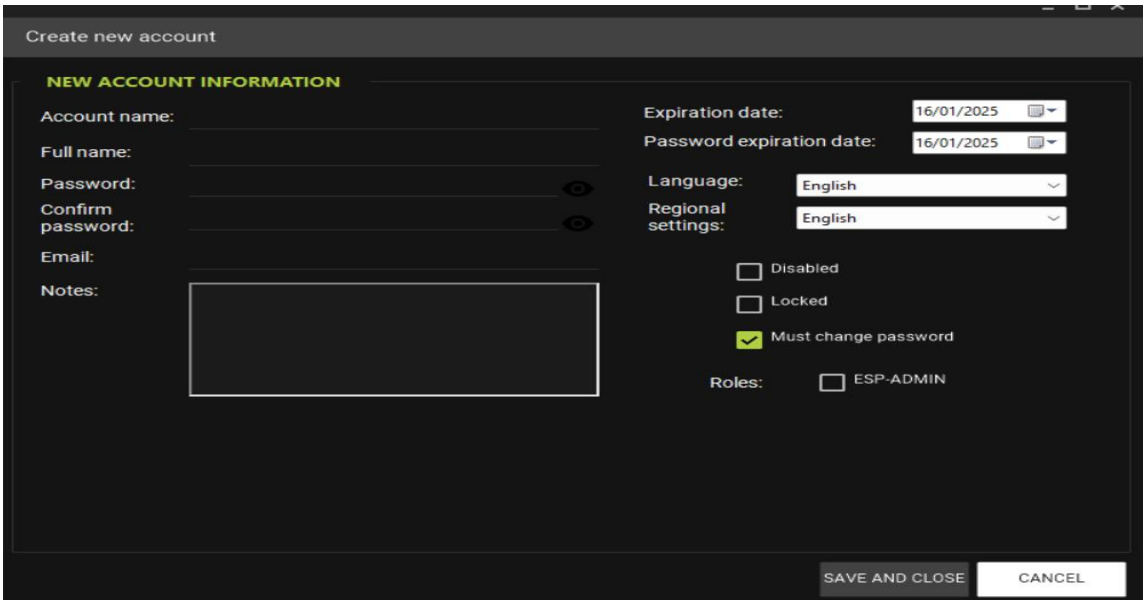
In the Provisioning section, click on Manage Accounts.

In this section, the SYS-ADMIN can view the list of current accounts and access the creation and management functionalities.



Creating a New Account

Click on Create new.



Then, fill in all the required fields:

- Account Name: The identifying name of the account.
- Full Name: The full name of the user.
- Password: Enter a secure password for the user.
- E-mail: The email address associated with the account.
- Note (Optional): You can add supplementary notes for the account (this field is optional).

Click on Save and close to complete the account creation.

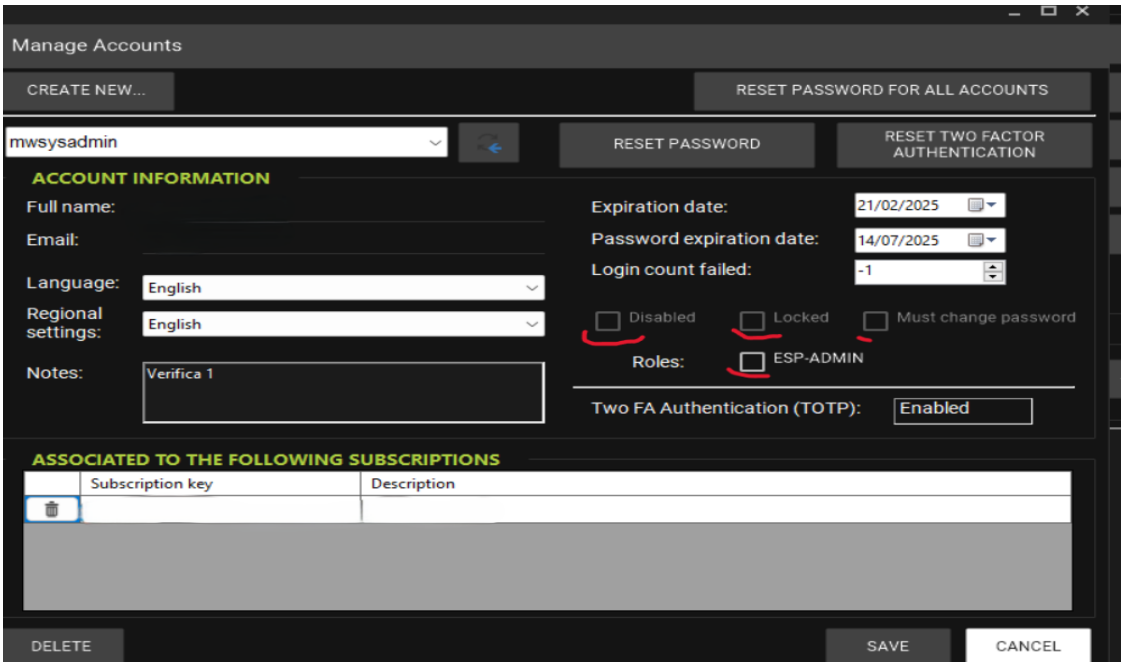
After creating the account, upon first login, the user will be required to change the password using the Change Password functionality.

Management of Existing Accounts

The Sys-Admin can manage all accounts present in the console directly from the Manage Accounts screen.

The available actions include:

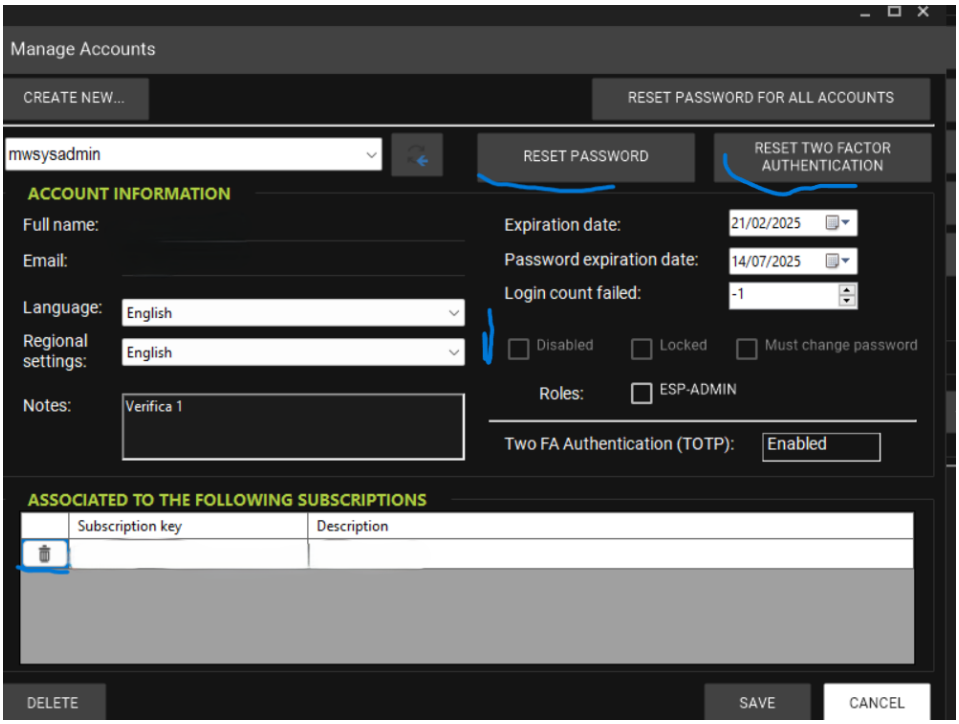
- Disable Account: Click on the appropriate icon to disable the account, preventing access.
- Lock Account: Click on the icon to lock the account, preventing access without fully disabling it.
- Assign ESP-ADMIN Role: If necessary, you can assign this role to the selected account.



- Modify Password Expiration Date: If necessary, you can set or update the password expiration date for the user.
- Modify Language: You can also change the preferred language for the user.

In the account management screen, the Sys-Admin can also perform the following actions:

- Remove Association to Subscription: Click on the trash bin icon to remove the account's association to the subscription.
- Reset Password: If required, the Sys-Admin can reset the password by setting a new temporary password for the user, who will be required to change it on their first login.
- Enable/Disable Two-Factor Authentication (2FA): If the account has Two-Factor Authentication (2FA) enabled, the status will be displayed as Enabled. If necessary, the Sys-Admin can disable 2FA by clicking the corresponding button.
-



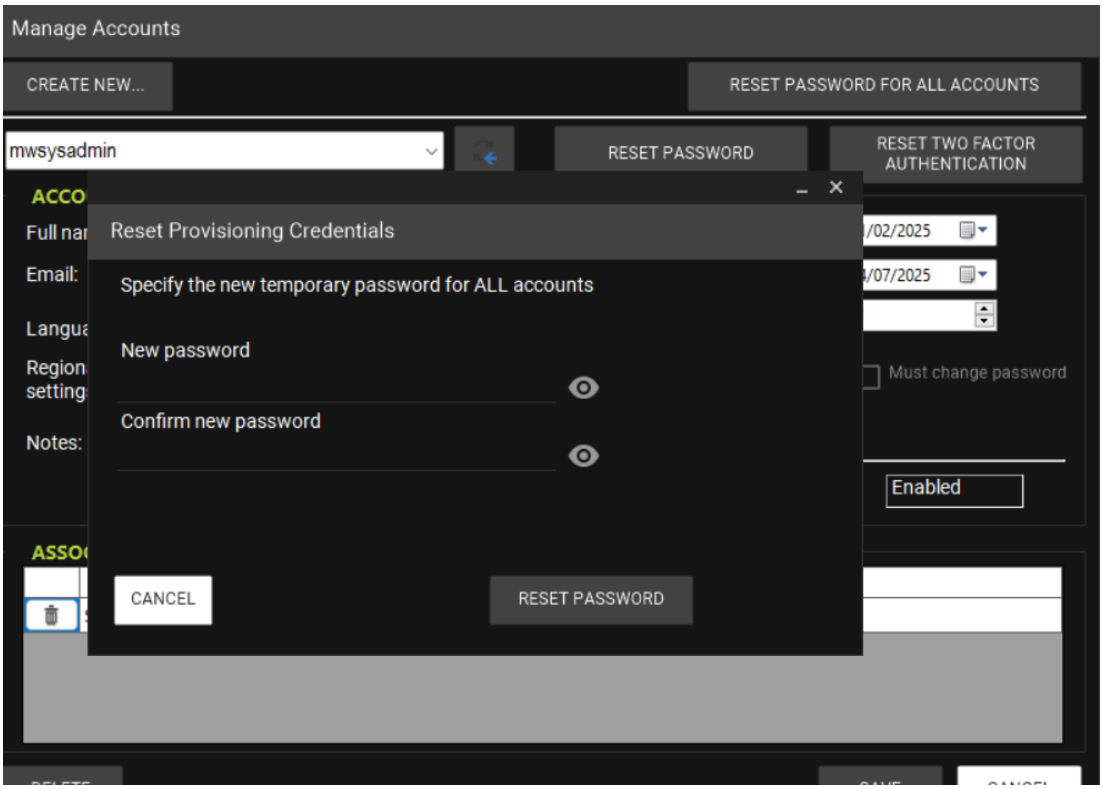
In the account list, the Sys-Admin can view the following information for each account:

- Account Name
- Account E-mail
- Two-Factor Authentication (2FA) Status: If enabled, it will be shown as active.
- Password Expiration Date: The date when the account's password will expire.

If necessary, the Sys-Admin can update account information, such as the name and email, directly from the management screen.

Additionally, the Sys-Admin can quickly update the passwords for all accounts at once, without having to manually change each account individually, by using the Reset Password for all accounts button.

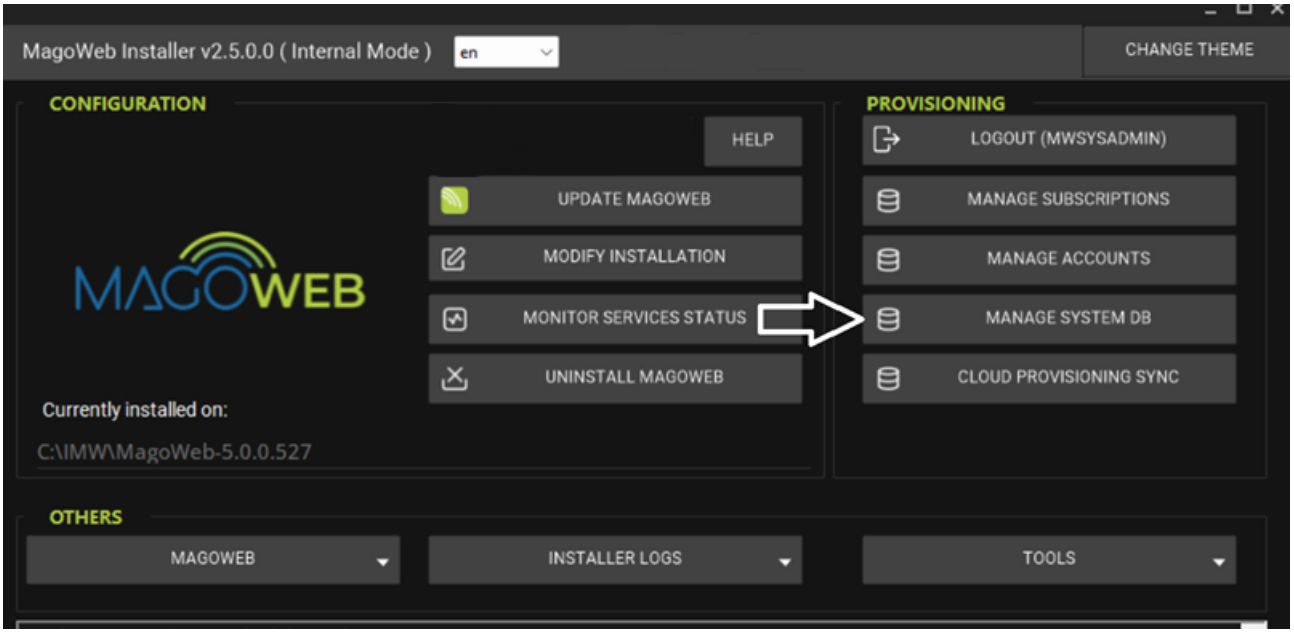
It will be possible to set a temporary password for all accounts without meeting complexity requirements, which must be changed upon the first login to the system. The Sys-Admin is automatically excluded from this mass reset operation.



Note: The "Reset password for all accounts" functionality is particularly useful after the initial system configuration phase. In fact, account synchronization from the Provisioning Cloud removes certain sensitive data, such as email, full name, and password. With this mass reset option, it is possible to set a temporary password for all accounts in a single step.

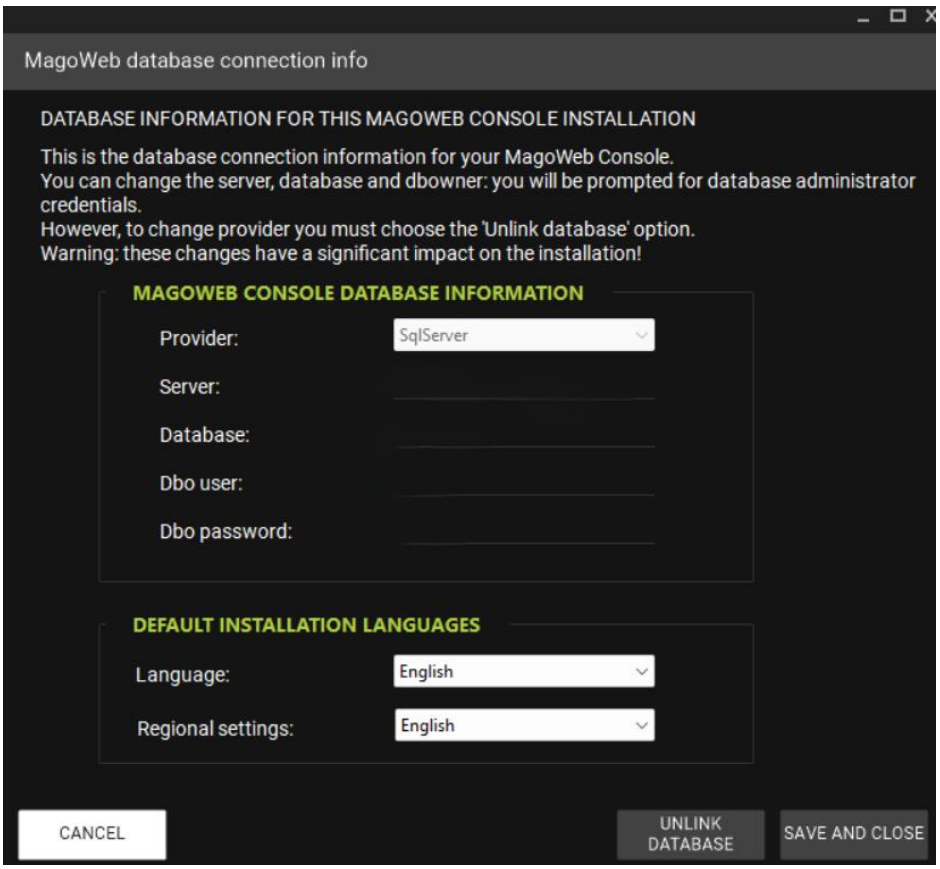
System DB Management

In the Provisioning section, by clicking on Manage System DB, the MagoWeb Installer will take you to a screen displaying all the information related to the connection to the MagoWeb system database.



In this screen, you will find the following data:

- Server: Indicates the address of the server hosting the database.
- Database: The name of the system database that the application connects to.
- Dbo user: Identifies the database owner (dbowner).



It will be possible to modify the database connection credentials. To perform this operation, you will be prompted to enter the database administrator's credentials. These credentials are necessary to authorize the modification of settings and ensure correct access to the database.

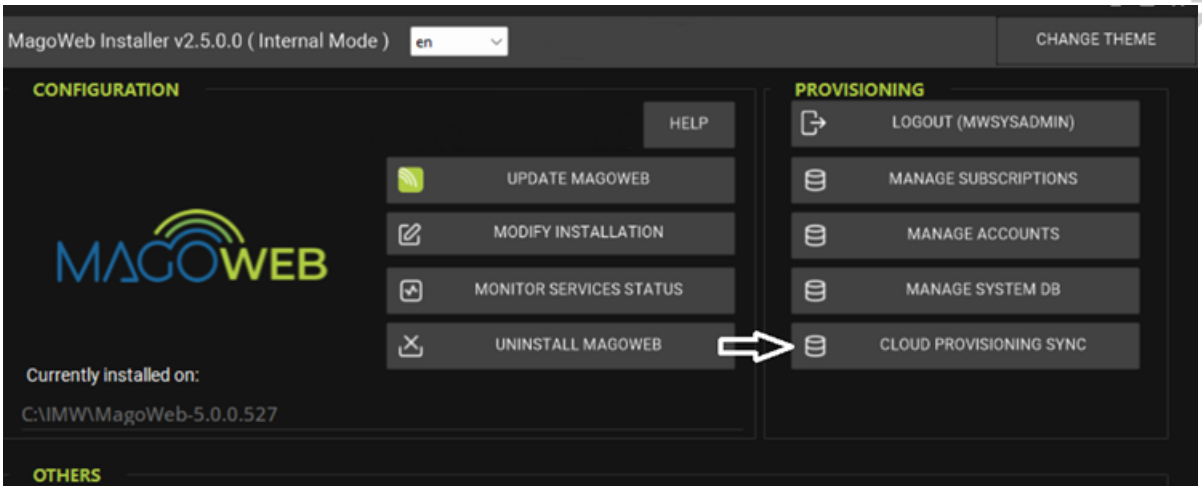
If it is necessary to change the connection provider, you must choose the Unlink DB option. This operation will unlink the current database and allow you to configure a new connection with a different provider.

Data Synchronization from Cloud Provisioning

If you are using a MagoWeb instance with a version earlier than 5.0, it will be necessary to synchronize all the related data that is currently stored in the Provisioning Cloud archives.

Note: It is important to remember that the data synchronization from the Provisioning Cloud is automatically performed at the end of the system database configuration wizard.

Data synchronization can be repeated using the "Cloud Provisioning SYNC" option.



This operation is useful when you want to update local data with those in the Provisioning system in the Cloud.

If conflicts with existing data occur during the synchronization process, the Sync action will prevent overwriting to avoid losing essential information.

Accounts are synchronized after the deletion of certain sensitive data, such as email, full name, and password.

Through the "Reset password for all accounts" functionality, the Sys-Admin can set a temporary password for all accounts in one step, ensuring that users can access the program smoothly.

Access to MagoWeb and Two-Factor Authentication Configuration

Access to MagoWeb

From the console, by selecting Others-MagoWeb, a dropdown menu will appear. By clicking on Open Client, the browser will open for MagoWeb authentication.

Authentication

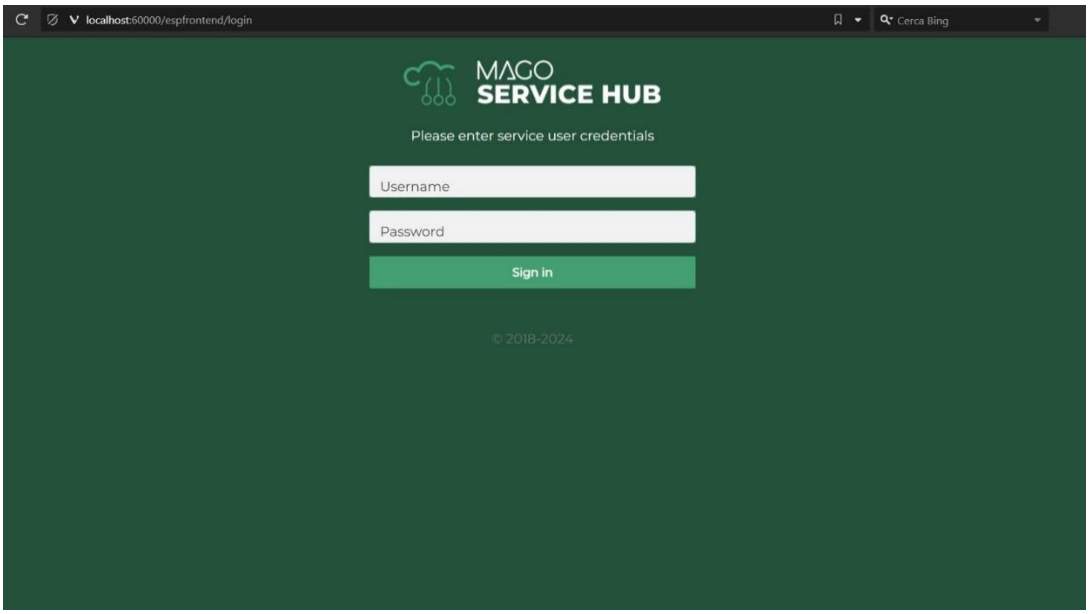
Once the MagoWeb browser is opened, you will be prompted to enter the username and password.

After entering the credentials, the system will prompt you to select the subscription you wish to access.

After selecting the subscription, click on "Accedi" to enter the system.

Access to MSH

The "Open MSH Frontend" option opens the MSH frontend in the default browser.

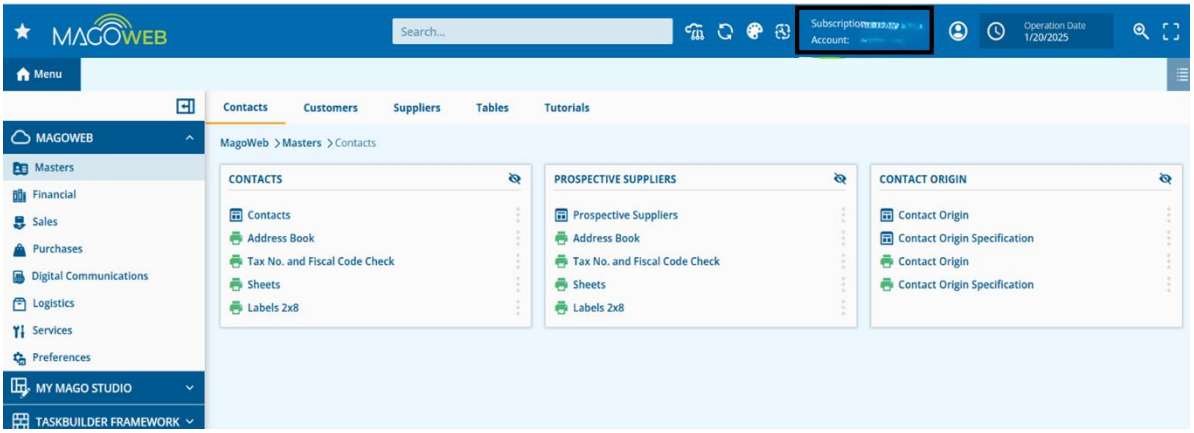


Note: Access to the MSH Frontend is done using the same credentials used for logging into the Mago Store. Unlike Mago4, there is no service account for MSH.

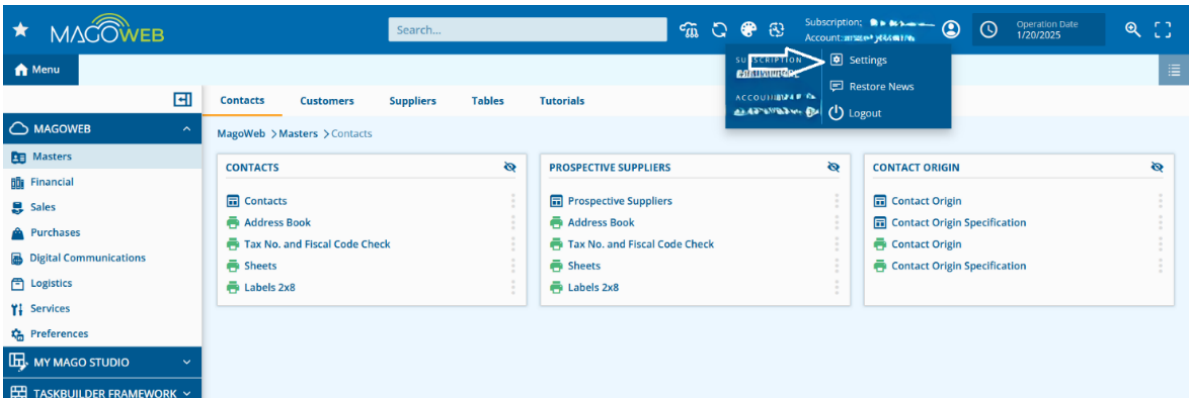
Account Settings Management

Viewing and Editing Settings:

Once logged into MagoWeb, the details related to your subscription and user will be displayed.

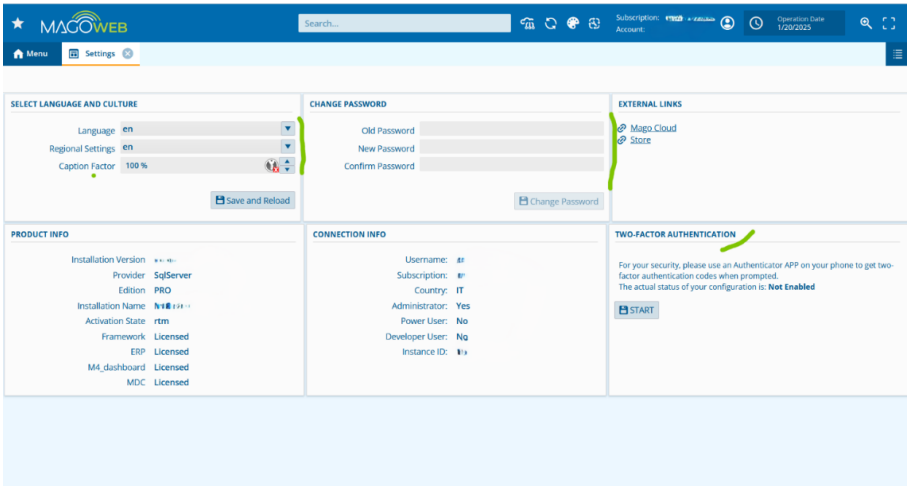


To access your account settings, click on Account Information and then on Settings.



In this section, you can:

- Change the system language.
- Modify the account password.
- Enable Two-Factor Authentication (2FA).

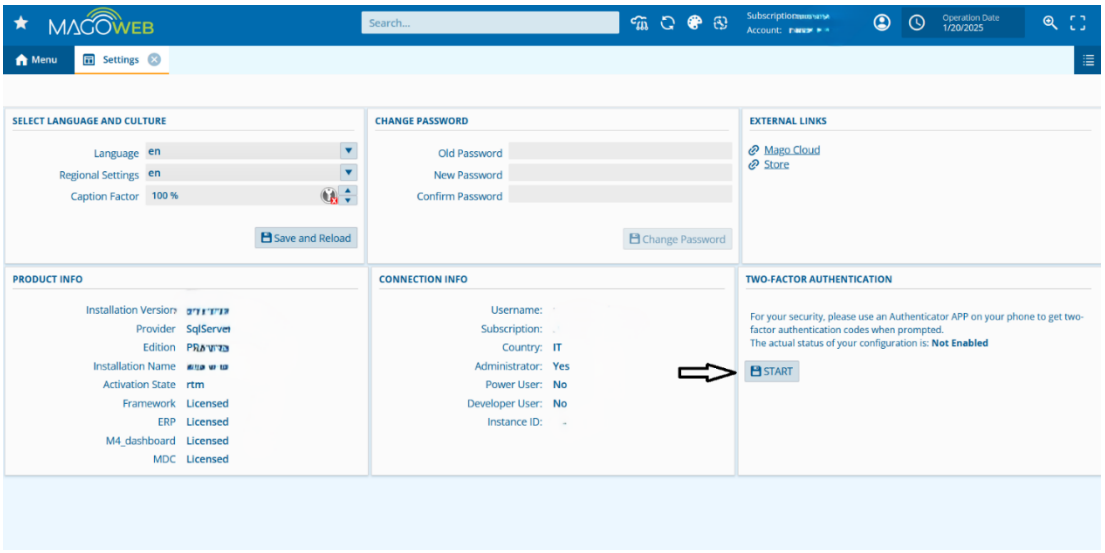


Enabling Two-Factor Authentication (2FA)

Note: In MagoWeb, the only type of authentication allowed for 2FA is via TOTP, meaning by an authentication app.

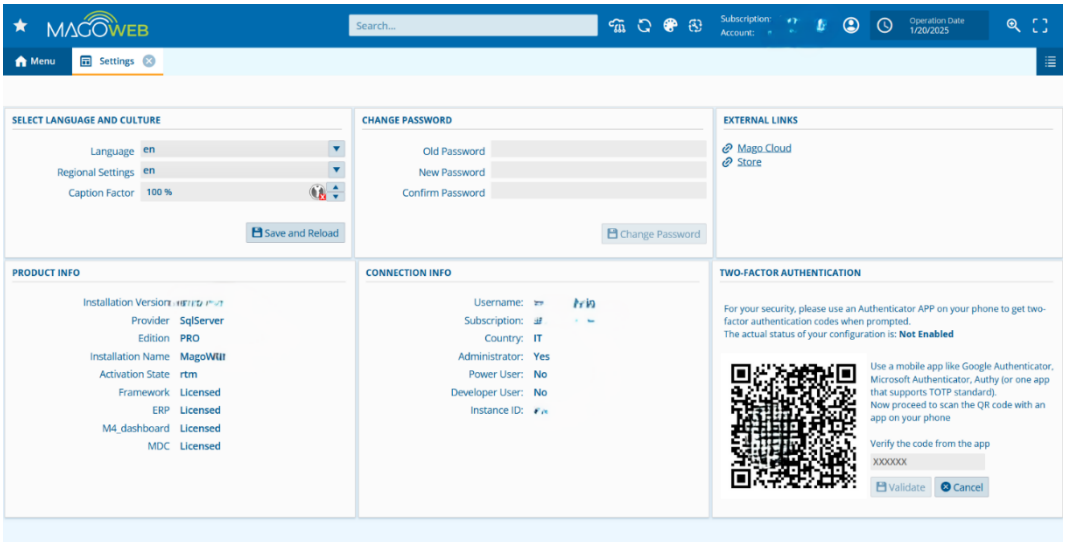
To start the activation process:

In the account settings screen, click "Start" to begin the 2FA setup process.



Scan the QR code:

Once the process is started, a QR code will appear on the screen. Use an authentication app (such as Google Authenticator, Microsoft Authenticator, Authy, or other apps compatible with the TOTP system) to scan the QR code.



Verification of the OTP code:

After scanning the QR code, the mobile app will generate a temporary code (OTP - One Time Password).

Enter the code displayed in the app and click "Validate" to complete the activation of Two-Factor Authentication.

Future Access with Two-Factor Authentication Enabled

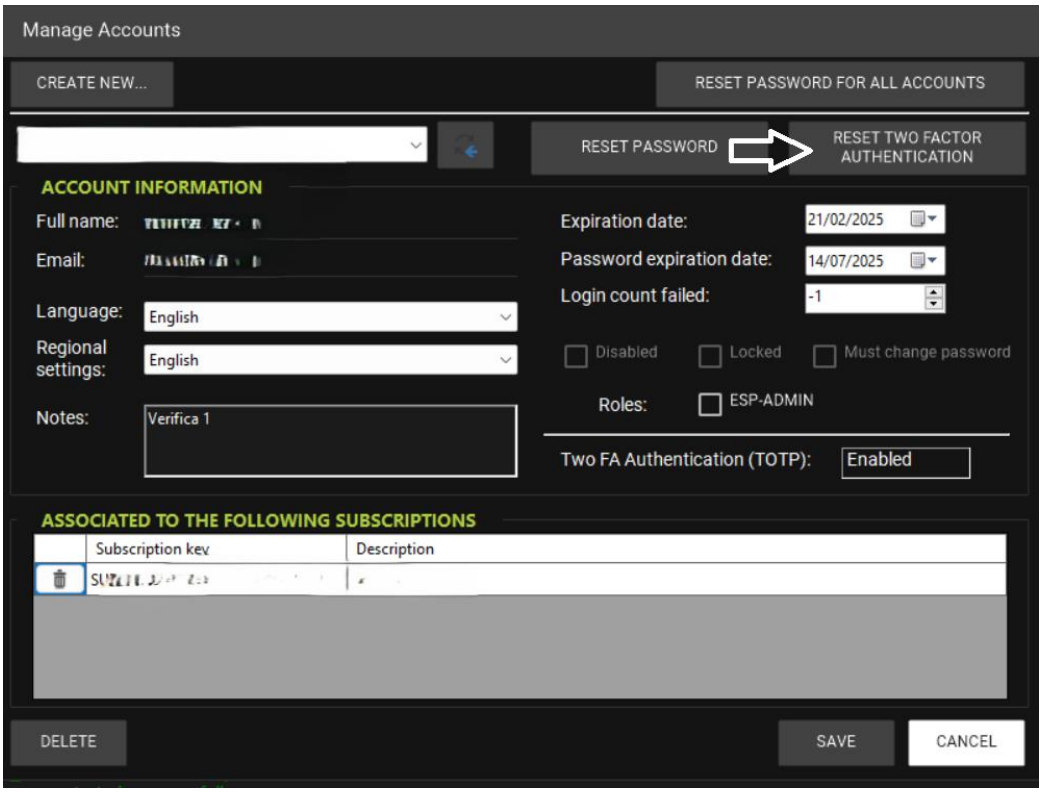
After enabling 2FA, the next time you log in to MagoWeb, in addition to entering your username and password, you will also need to enter the OTP code generated by the authentication app.

This temporary code will change every 30 seconds and will be automatically generated by the app you have configured, providing an extra layer of protection for your account.

Disabling Two-Factor Authentication (2FA)

Deactivation of 2FA:

If you later wish to disable Two-Factor Authentication, the Sys-Admin (system administrator) will have the ability to deactivate it for you, if necessary.



This step must be conducted by the Sys-Admin, who has the necessary privileges to modify the account's security settings.

Appendix A

Details on creating a Microsoft application for OAuth.

1. Registration

During the application registration process, you need to specify an "Authorized Redirect URI" (see Figure 1).

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

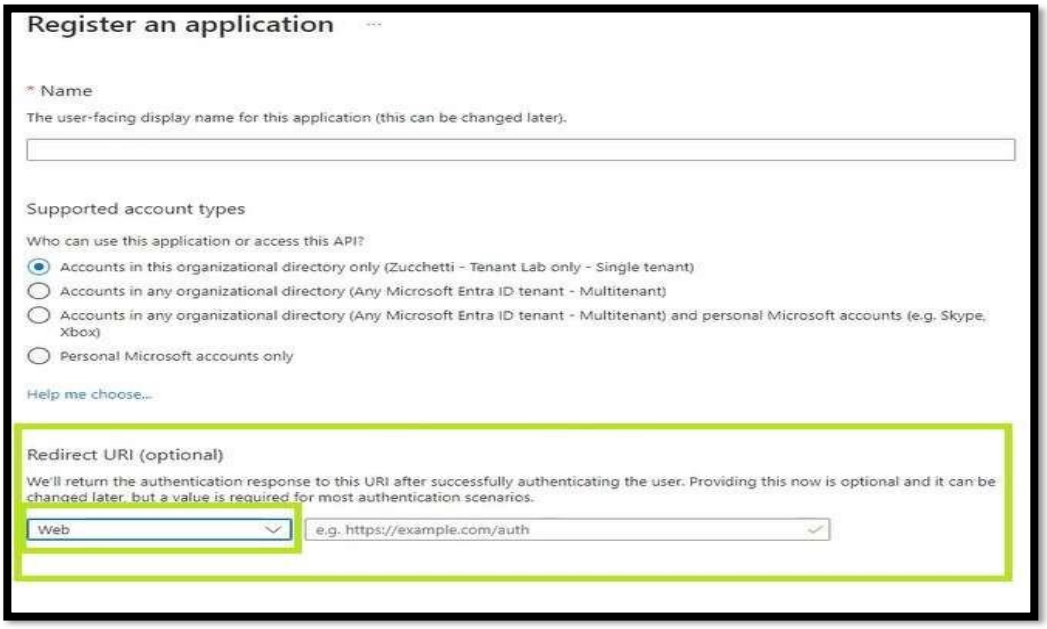


Figura 1

If you did not set it during creation, you can specify the same value in the 'Authentication' section by adding a new URI (click the Add URI button, see Figure 2).

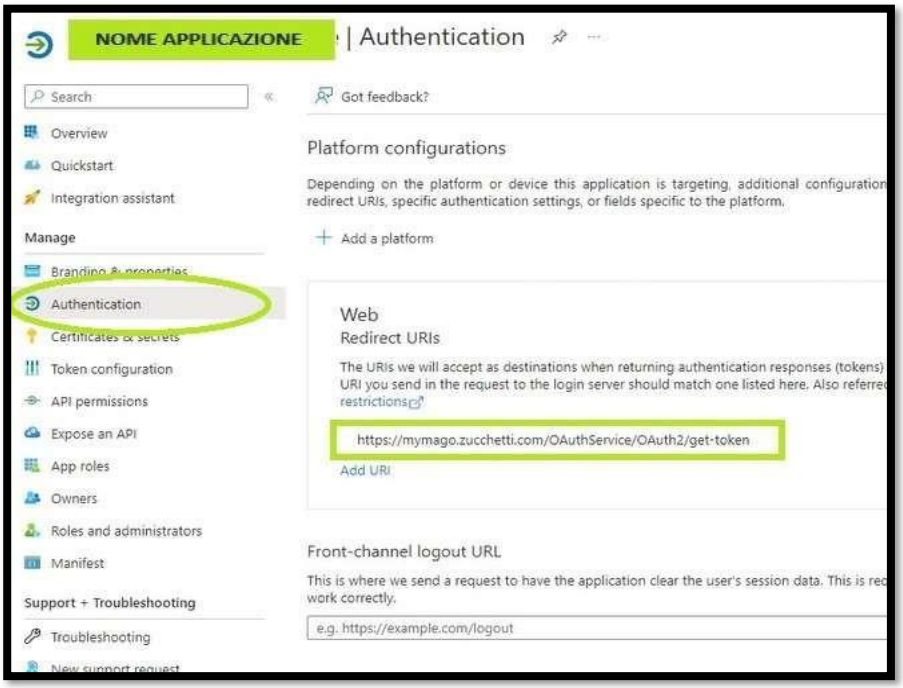


Figura 2

2. Parameters to Save: parameters required in the MagoWebInstaller are as follows:
   - Client ID: You may find it referred to as Client ID, Application ID, or Application Identifier (see Figure 3).
   - Tenant ID: You may find it referred to as Directory ID (see Figure 3).

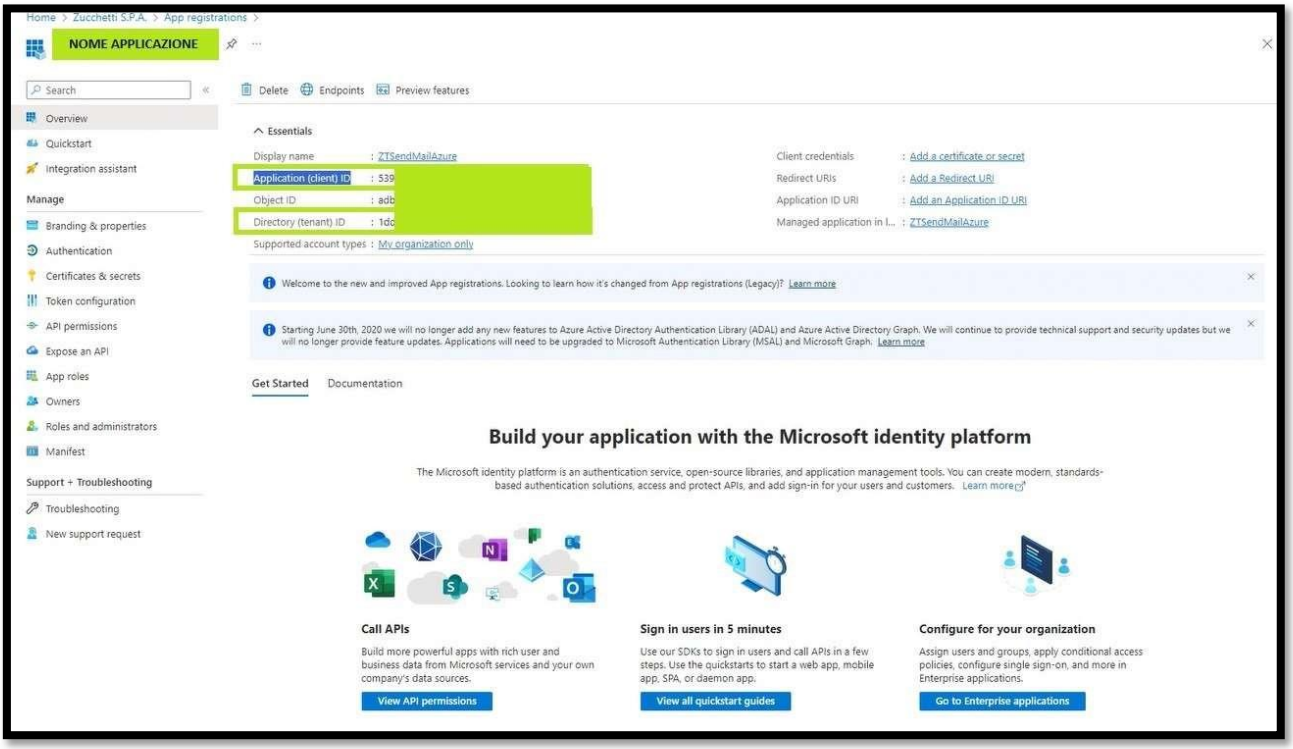


Figura 3

- Client Secret: This corresponds to the 'Value' highlighted in green.
- In the Certificates and Secrets section, create a new secret by clicking the button circled in green in Figure 4. A sidebar will appear where you can specify the duration of the secret. The choice is flexible, but keep in mind that each time the secret expires, a new one will need to be generated and updated in the MagoWebInstaller parameters.

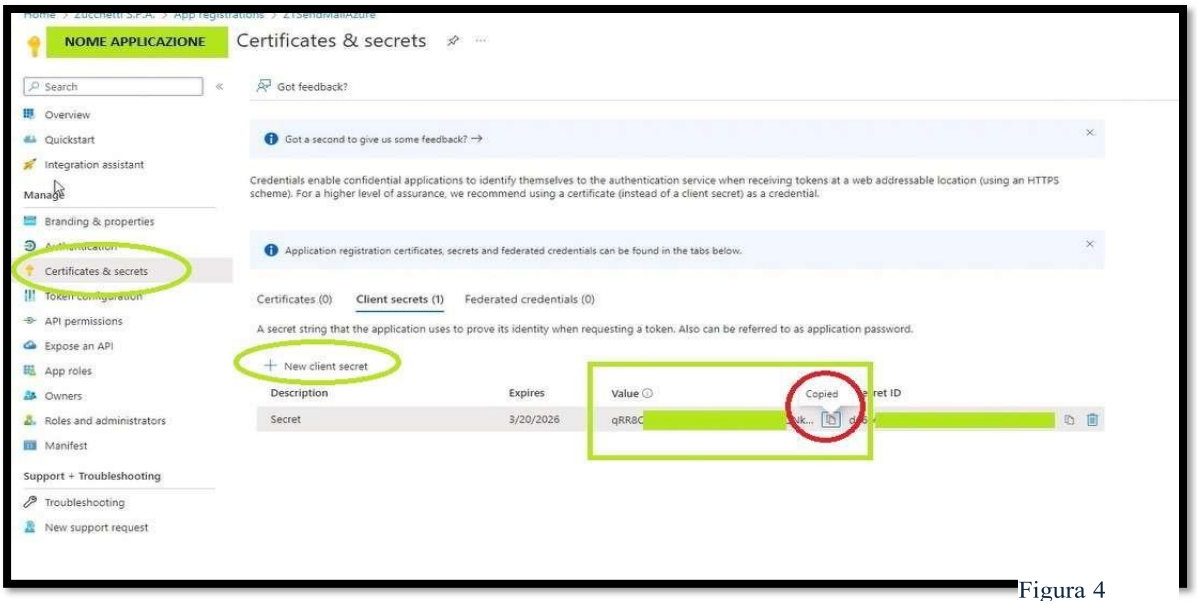


Figura 4

The Client Secret to be entered in the MagoWebInstaller parameters corresponds to the Value highlighted in green. Be cautious, as this value can only be copied once; after that, it will become unreadable. The only way to obtain a new client secret will be to create a new one entirely.

3. Permissions

The complete list of required permissions is as follows:

- Mail.Send
- IMAP.AccessAsUSer.All
- SMTP.Send
- User.Read

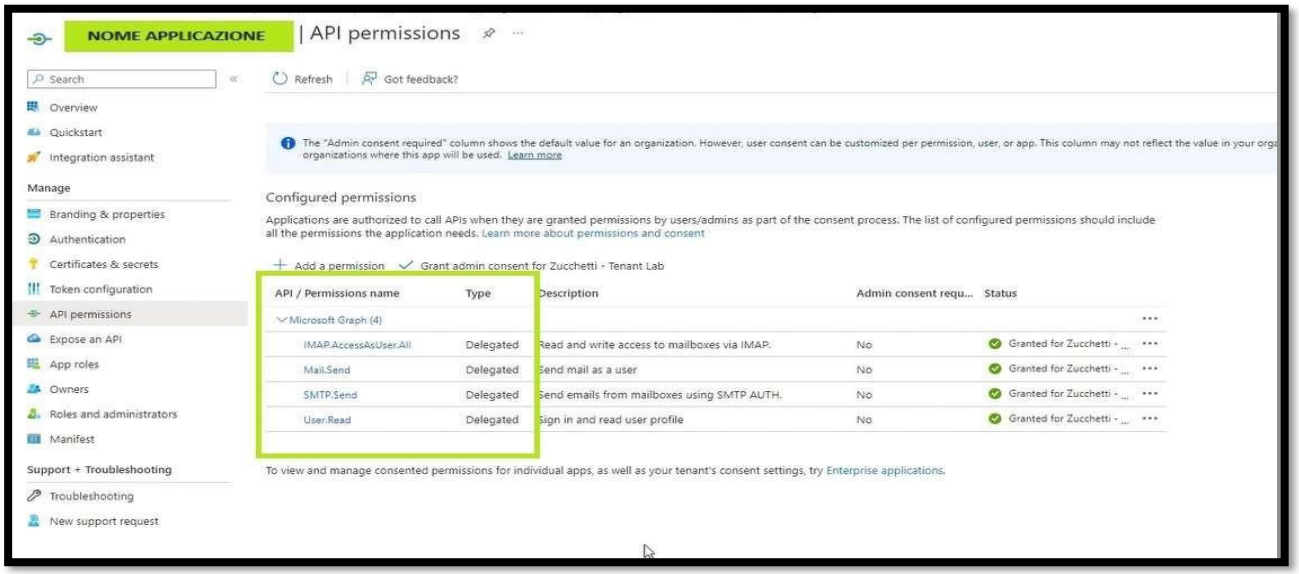


Figura 5

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

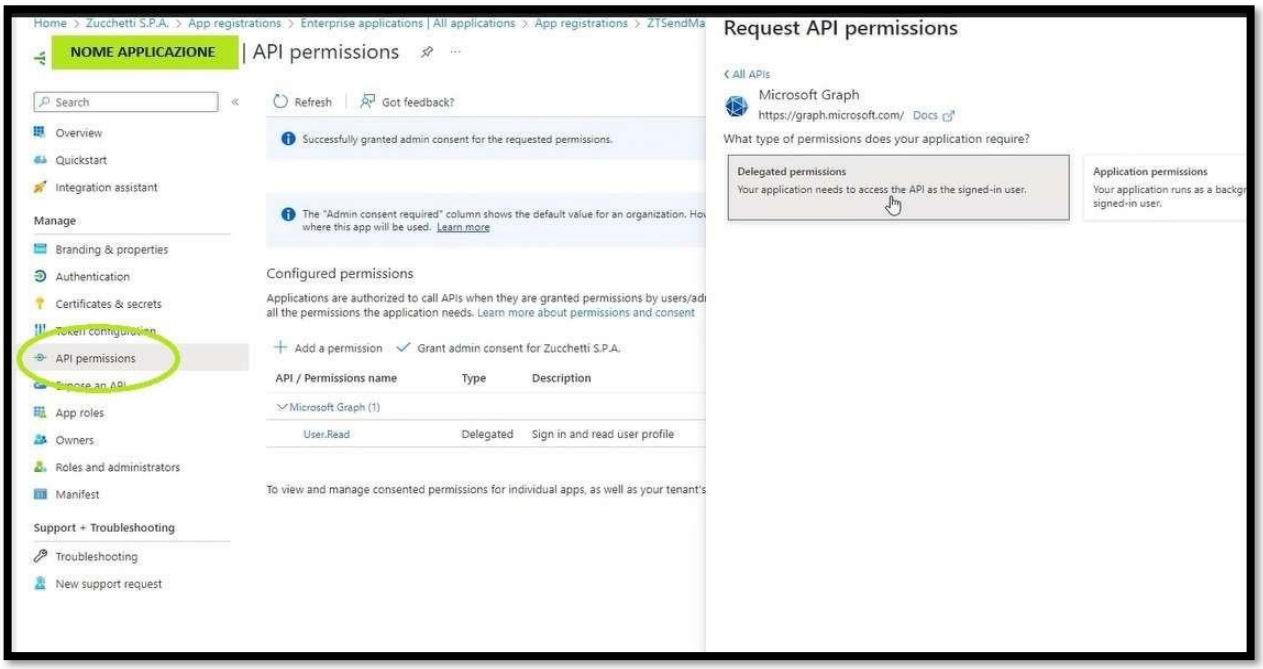

Home > Zucchetti S.P.A. > App registrations > Enterprise applications | All applications > App registrations > ZTSendMa
NOME APPLICAZIONE | API permissions
Search
Overview
Quickstart
Integration assistant
Manage
Branding & properties
Authentication
Certificates & secrets
API permissions
App roles
Owners
Roles and administrators
Manifest
Support + Troubleshooting
Troubleshooting
New support request
Refresh
Got feedback?
Successfully granted admin consent for the requested permissions.
The "Admin consent required" column shows the default value for an organization.
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
Add a permission
Grant admin consent for Zucchetti S.P.A.
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
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
signed-in user.

Figura 6

An example of the search shown in Figure 7, where the permission 'mail.Send' is being searched for.

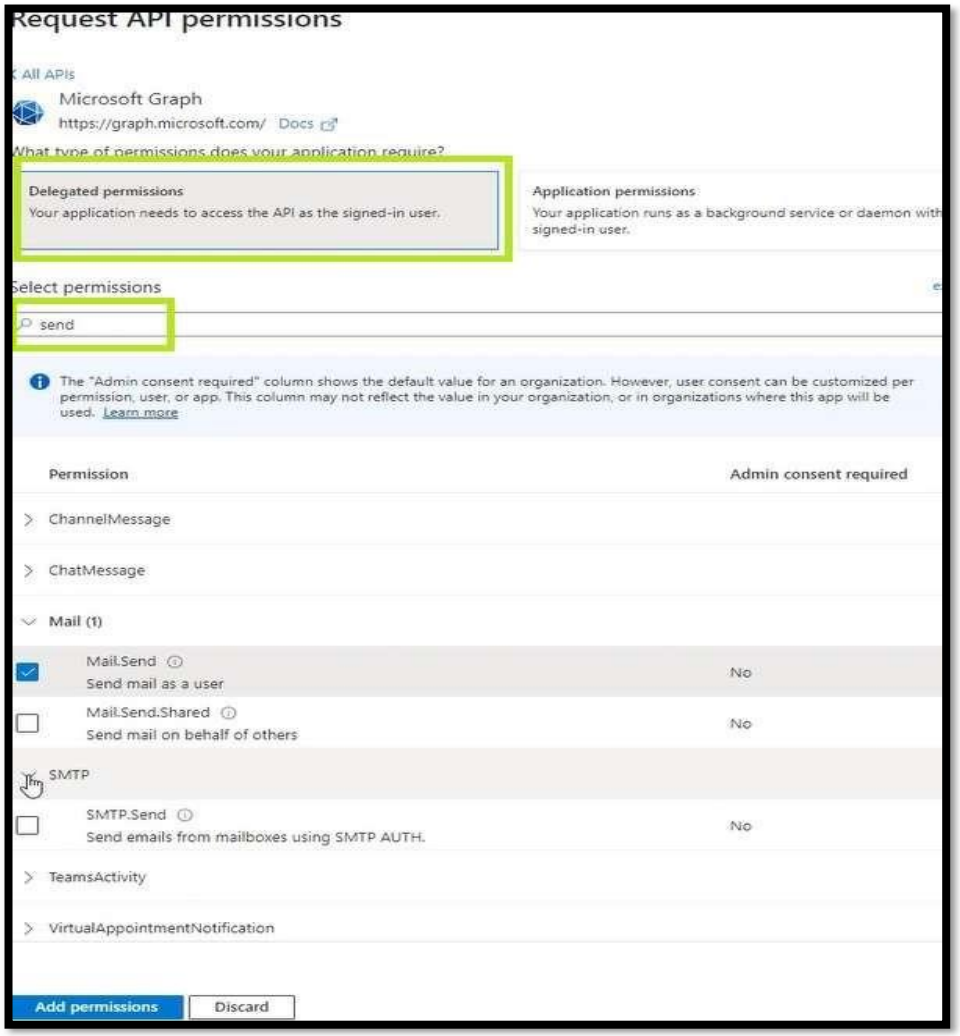


image 7

Once the permission has been added, you will need to grant consent by clicking the button labelled "Grant admin consent..." and confirming the action (see Figure 8).

In the yellow-highlighted boxes, you will notice the difference in status between a granted permission and one that has not been granted yet.

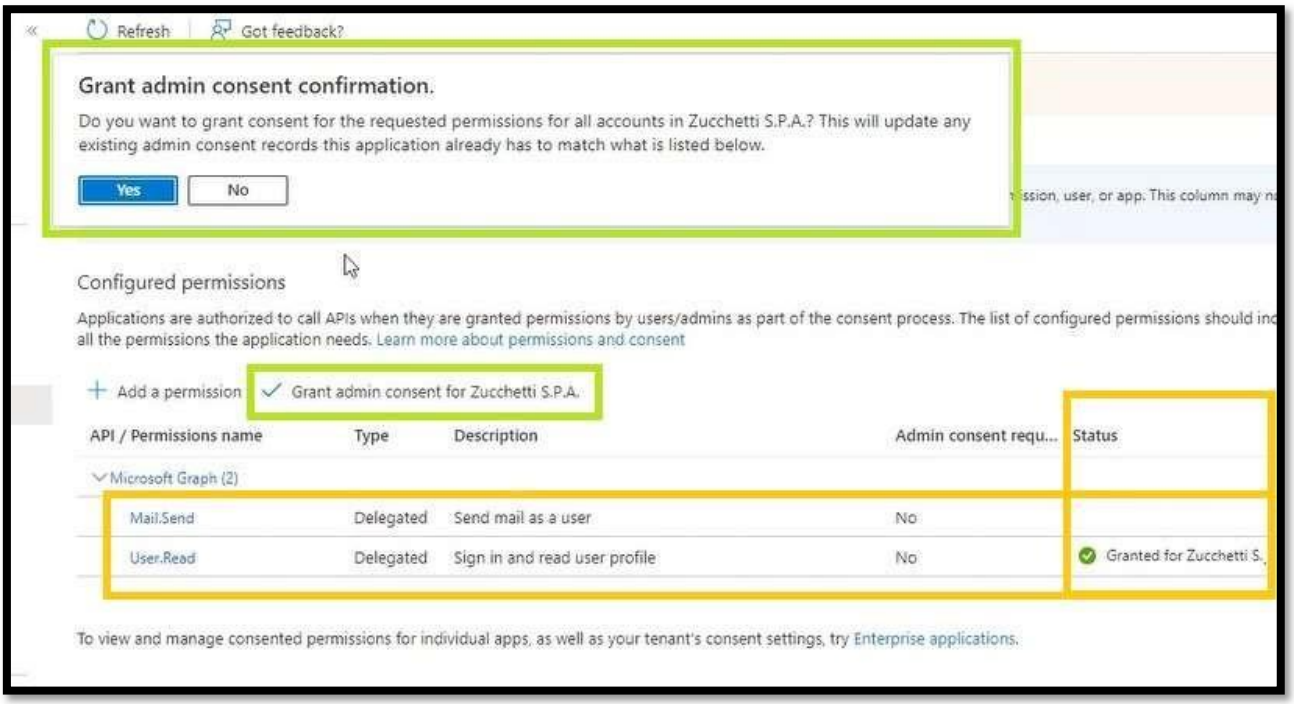

Refresh
Got feedback?
Grant admin consent confirmation.
Do you want to grant consent for the requested permissions for all accounts in Zucchetti S.P.A.? This will update any existing admin consent records this application already has to match what is listed below.
Yes
No
Configured permissions
Applications 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
Add a permission
Grant admin consent for Zucchetti S.P.A.
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

Appendix B
Exposure of MagoWeb on the network

For the network configuration to expose MagoWeb publicly and allow access from the outside, the following general configurations are recommended:

1. Insert Public IP/DNS of the Server in the hostname field of the MagoWeb installer.
2. Firewall Configuration:
    - Enable incoming rules to accept calls to the server from clients logging into MagoWeb, ensuring that ports between 60000 - 60300 are open. A sample rule might look like this:
        - Type: All TCP rules (or all traffic)
        - Protocol: All protocols
        - Port Range: 60000 - 60300
        - Source: client IP/32

3. Outgoing Calls:
    - All outgoing calls should be allowed with a rule like this:
        - Type: All TCP rules (or all traffic)
        - Protocol: All protocols
        - Port Range: All
        - Destination: 0.0.0.0/0

4. Incoming Rule for Server's Public/Private IP:
    - Set an incoming rule to allow calls from the server's own public/private IP:
        - Type: All TCP rules (or all traffic)
        - Protocol: All protocols
        - Port Range: 60000 - 60300
        - Source: server IP/32

An alternative option is to register an internal and external DNS. Specifically, you can define the private IP and registered DNS name in the server's hosts file, and in the external DNS server, you would map the same DNS name to the public IP of the host.

Note: These are general guidelines, and specific parameters or configurations may vary depending on the network structure where MagoWeb is located.

Appendix 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).

Additionally, non-self-signed certificates generated and issued by a valid Certificate Authority (CA) can also be used.

There are no "official" integrations on the MagoWeb side. The installer only requires the two certificate files to be uploaded and ensures that the certificate is correctly installed and validated. Both paid certificates and those issued by a public CA work.

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

The two indicated files must be uploaded in the first field. However, if the certificate contains both parts (public and private) without separation, only one of the two may be read, resulting in an error. There are many configurations, and we suggest conducting several tests.

For example, for certificates generated by Certbot/Let's Encrypt, the client/reseller can select a file path for the two certificates on the file system (e.g., `C:\Users\Administrator\Documents\certificate.cer` and `C:\Users\Administrator\Documents\certificate.key`).

Certificate Format Conversion

Di seguito alcuni comandi per effettuare la conversione di alcuni certificati in formati supportati:

- 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 in the path set during installation (by default c:\logs), divided into files for the different MagoWeb services.

The logs of the Installer are located at C:\Users\user\AppData\Roaming\MagoWebInstaller\Logs

General guide Lines:

- It may be necessary to disable the firewall during the Mago Web installation.
- Check that the ports assigned to the services are not already occupied or in use.
- Ensure that UAC is set to the default value (2), as this is necessary for the correct execution of installation scripts. If it is not set correctly, a warning will appear in the installer.

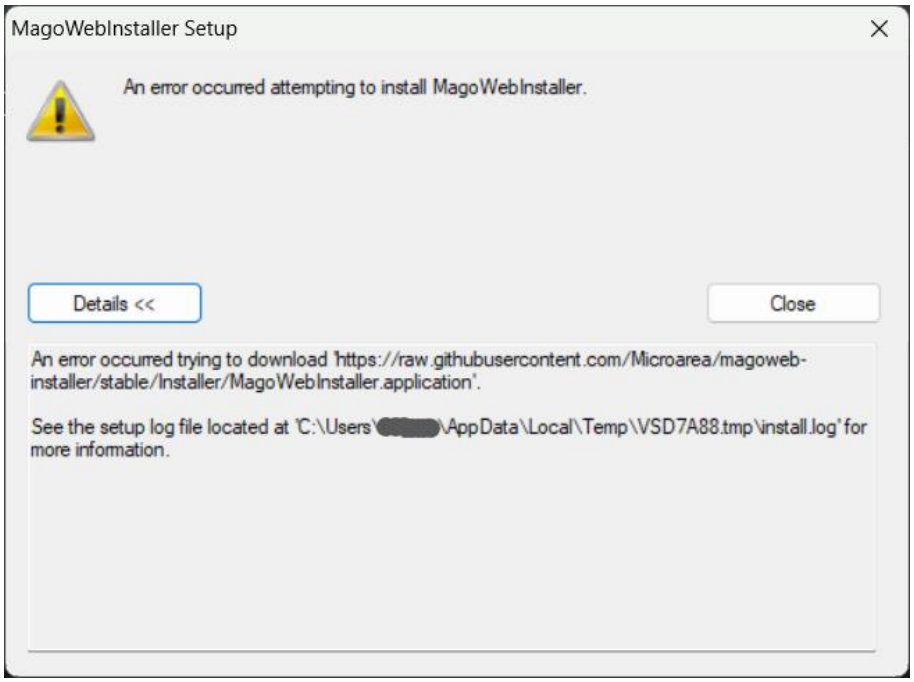
Important: After making any changes in the installer interface, press START to save the changes.
Important: When a new build is released, download both the new installer and ztds packages from mymago.zucchetti.com. To perform the upgrade procedure, always use the installer aligned with the version you are installing/upgrading.

Important: Before performing an upgrade from a consecutive release (e.g., from 1.2 to 1.3), ensure that the "Use existing configuration" box is not checked. See anomaly 34747.

Important: When creating a new database, save and keep the credentials related to the dbowner part. These will be required if backup/restore operations are performed on the database server or migrations to a different database provider (e.g., from PostgreSQL to SQL or vice versa).

If credentials different from the ones displayed are entered, permission-related errors may occur.

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



Open the Registry Editor, navigate to the path

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings, and check the key DisableCachingOfSSLPages. If the value is 1, set it to 0. Then, relaunch the installer.
TestConnection exception: Response status code does not indicate success: 404 (Not Found).
Check the status of the services from the MagoWeb installer interface, ensuring that the Traefik microservice has started correctly and that the port used is not already in use. Restart the corresponding service and try accessing again. If the problem persists, modify the installation and restart Start.

Verify .NET installation
For MagoWeb to function correctly, .NET and its tools must be installed properly. To verify this:

- Open PowerShell and navigate to the folder containing the MagoWeb installer exe (and thus Psexec).
- Run: .\psexec -s -i powershell
- A second PowerShell window will open, run: dotnet ef

If the shell displays a unicorn image (https://learn.microsoft.com/en-us/ef/core/cli/dotnet#verify-installation), the installation is successful. If an error occurs, follow the workaround indicated in anomaly 34337.
Promtail not starting

Delete the positions.yaml file

Delete the positions.yaml file located in
C:\ProgramData\scoop\apps\promtail\current\positions.yaml.
Then, restart the Promtail service.

Error: I cannot find any subscriptions associated with this account.
This error occurs when, during the initialization of the MagoWeb instance, an incorrect instance key or security value was entered in the "Modify Installation" section of the interface.
Re-enter the correct security value under "Modify Installation" and click Start.

Frontend loading issue for versions prior to 1.4
In versions prior to 1.4, a frontend loading issue may occur with the following error: net::ERR_CONTENT_LENGTH_MISMATCH 200 (OK). Even after refreshing the page, this issue may continue. This problem was fixed in version 1.4 and can be resolved by upgrading to this version of MagoWeb.

If the partner cannot upgrade soon but only as scheduled with the customer, there is a temporary workaround with specific instructions to resolve the issue until the upgrade is applied. Contact support for further assistance.