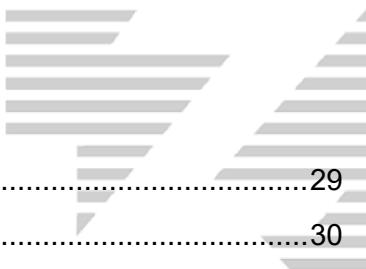




MAGOWEB – Manuale Utente

Sommario

Acquisto MagoWeb.....	3
Prerequisiti hardware e software	4
Installazione e Configurazione Iniziale	5
Avvio dell'Installer	6
Modalità di installazione.....	6
Selezione del percorso di installazione	7
Avvio dell'installazione	7
Configurazione iniziale dei parametri.....	8
Creazione dell'utente SYS-ADMIN.....	11
Accesso al sistema.....	11
Configurazione dell'account SYS-ADMIN	11
Configurazione del Database di Sistema.....	12
Scelta del provider di database.....	12
Creazione o selezione del database di sistema	13
Riepilogo delle operazioni	14
Creazione Database Sottoscrizione	15
Modifiche alla Configurazione Iniziale	16
Aggiornamento di MagoWeb.....	16
Monitoraggio dei Servizi	18
Disinstallazione di MagoWeb	19
Recupero di una installazione precedente	20
Amministrazione Utenti e Subscription.....	20
Gestione Subscriptions.....	20
Gestione Database	21
Gestione Moduli Attivati	24
Sincronizzazione dei Moduli	24
Gestione Account	25
Creazione di un Nuovo Account	25
Gestione Accounts Esistenti.....	26



Gestione System DB.....	29
Sincronizzazione dati dal Cloud Provisioning	30
Accesso a MagoWeb e configurazione del Two-Factor Authentication	31
Accesso a MagoWeb.....	31
Accesso a MSH	33
Gestione delle impostazioni dell'account	34
Abilitazione della Two-Factor Authentication (2FA)	35
Disabilitazione della Two-Factor Authentication	36
Appendice A.....	37
Dettagli su creazione applicazione Microsoft per Oauth.....	37
Appendice B.....	44
Esposizione in rete di MagoWeb.....	44
Appendice C.....	44
Configurazione certificati	44
Troubleshooting	45



Prerequisiti hardware e software

Di seguito sono riportati i requisiti minimi per un'installazione di MagoWeb.

I requisiti HW sono riferiti a due range di postazioni di lavoro (PDL), e relativi allo scenario in cui la stessa macchina faccia sia da Application che da DB server.

Le risorse HW indicate sono dedotte da test di carico fatti simulando un uso interattivo del programma, e possono variare in base ai casi d'uso.

A parità di risorse virtuali, le prestazioni possono variare in base al tipo di HW sottostante e al sistema di virtualizzazione in uso. I requisiti indicati vanno considerati come un riferimento di massima.

Range PDL	CPU	RAM	Requisiti SW
1-5	2 core	16 GB	<ul style="list-style-type: none">- Windows Server Standard (2016 or later)- Postgres 14.9 or later (o MSSQL 2017 or later)
6-10	4 core	16 GB	<ul style="list-style-type: none">- Windows Server Standard (2016 or later)- Postgres 14.9 or later (o MSSQL 2017 or later)



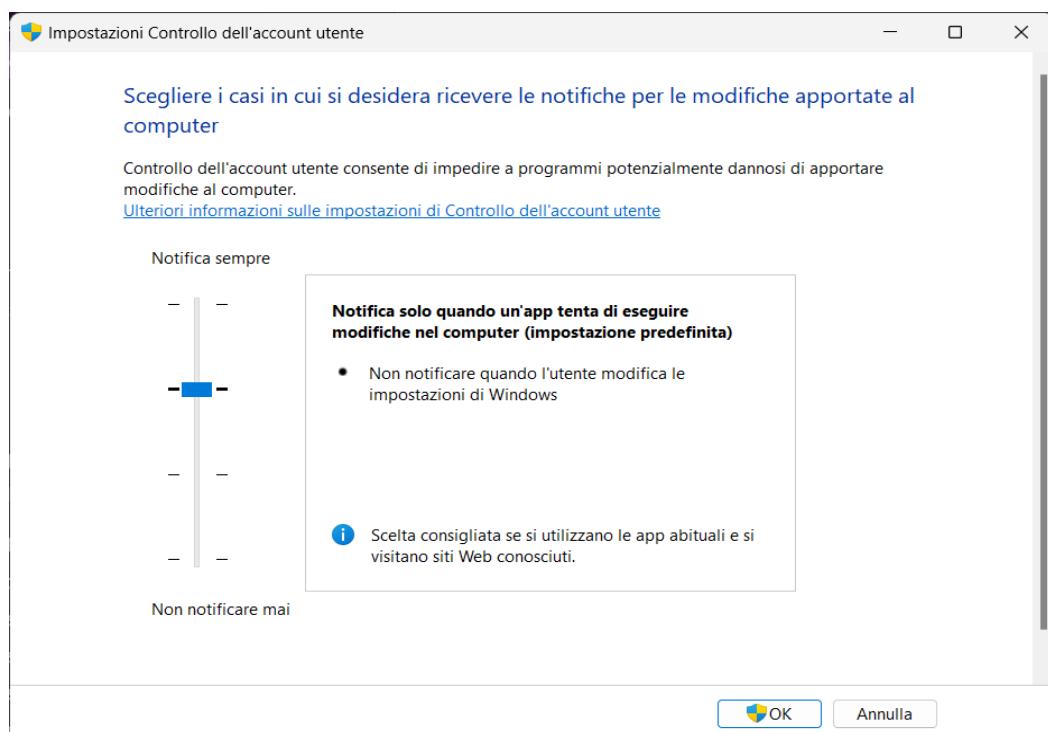
Installazione e Configurazione Iniziale

Eseguire l'accesso alla macchina, su cui si intende installare MagoWeb, con un account che dispone dei permessi amministrativi.

Scaricare dal sito Microarea <https://mymago.zucchetti.com>, l'installer e il file.zst per la versione che si intende installare, verificando che le versioni dei due file corrispondano.

A partire dalla versione 1.4 è stato modificato l'installer di MagoWeb, è necessario utilizzare l'installer setup.exe e NON è possibile utilizzare il MagoWebinstaller.exe delle versioni precedenti, facendolo l'installazione fallirà e sarà necessaria una reinstallazione clean del prodotto.

Verificare e\o impostare il livello di sicurezza del Controllo Account utente di Windows (UAC) al livello default come nello screenshot.



Versioni 1.3 o precedenti

Eseguire MagoWebInstaller.exe come amministratore, nel caso il passaggio precedente non sia stato eseguito, un messaggio di warning avviserà l'utente.

Versioni 1.4 o successive

Aprire un prompt dei comandi amministrativo ed eseguire il file Setup.exe, il setup verificherà e scaricherà i necessari prerequisiti e, conclusa questa operazione aprirà la finestra dell'installer. Anche in questo caso se i livelli di permission UAC non sono impostati correttamente un messaggio avviserà l'utente.



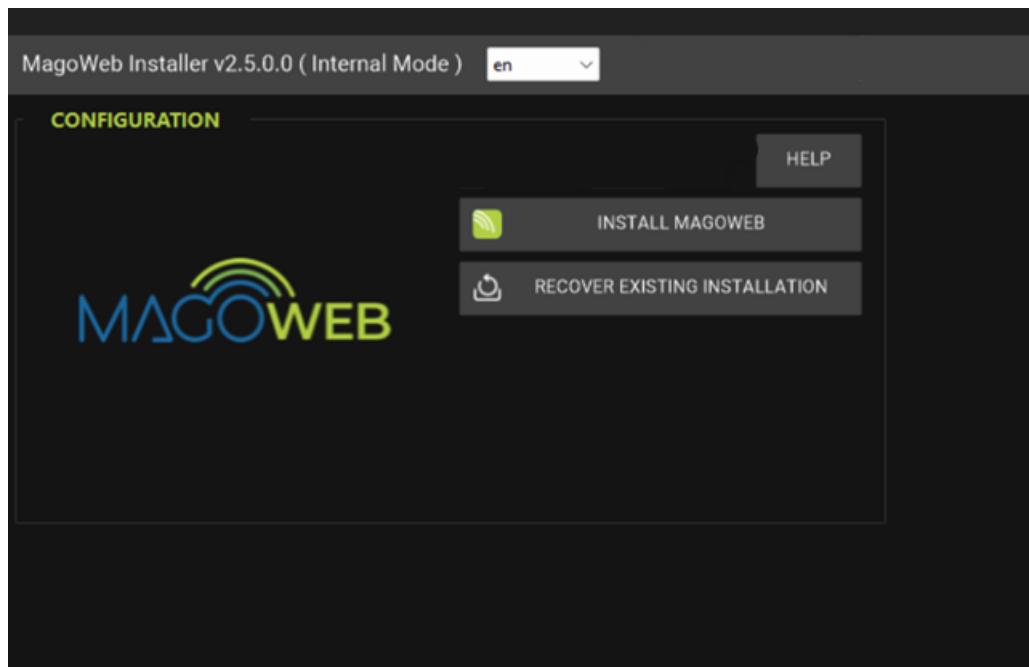
Avvio dell'Installer

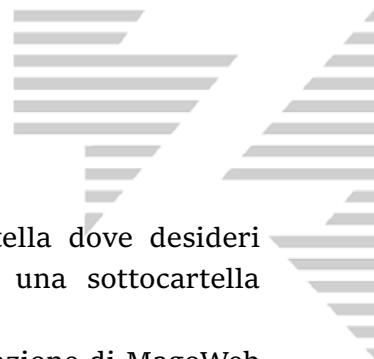
Esegui il file MagoWebInstaller.exe

Se non è mai stato configurato il sistema prima, verrà avviato automaticamente un wizard di configurazione che ti guiderà passo dopo passo nel processo.

Modalità di installazione

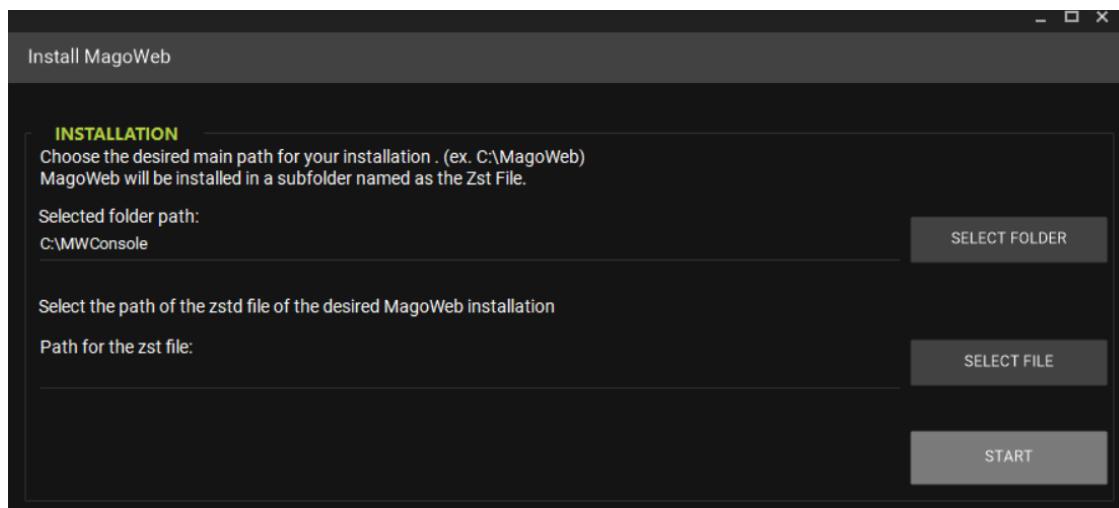
- Installazione Nuova (Install MagoWeb): Se è la prima volta che installi MagoWeb.
- Ripristino di un'installazione esistente (Recovery existing installation): Se desideri utilizzare una configurazione già presente.





Selezione del percorso di installazione

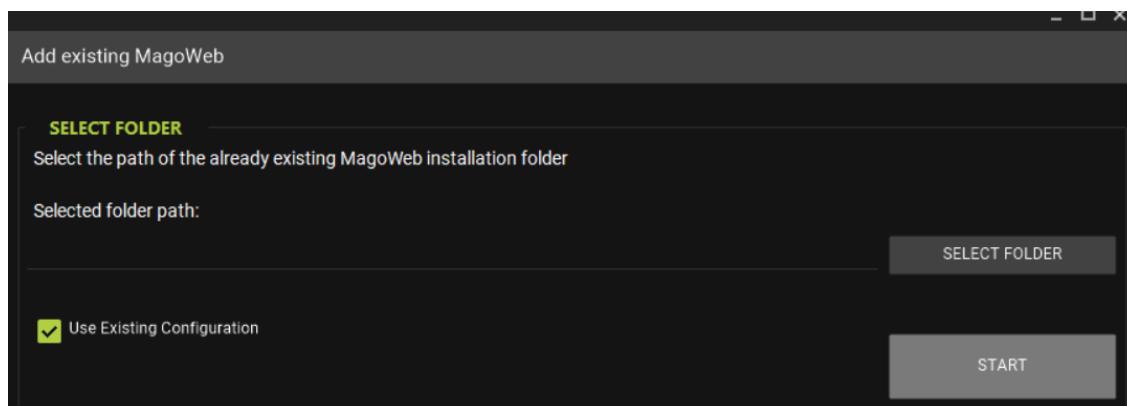
- Cliccando su INSTALL MAGOWEB verrà richiesto di selezionare la cartella dove desideri installare MagoWeb. Durante l'installazione, MagoWeb verrà creato in una sottocartella denominata "Zst file".
- Percorso del file Zstd: Inserisci il percorso del file Zst associato all'installazione di MagoWeb (il file scaricato).



Avvio dell'installazione

- Dopo aver selezionato il percorso, clicca su Start per avviare l'installazione.
- Il sistema procederà con il download e l'installazione dei file necessari.

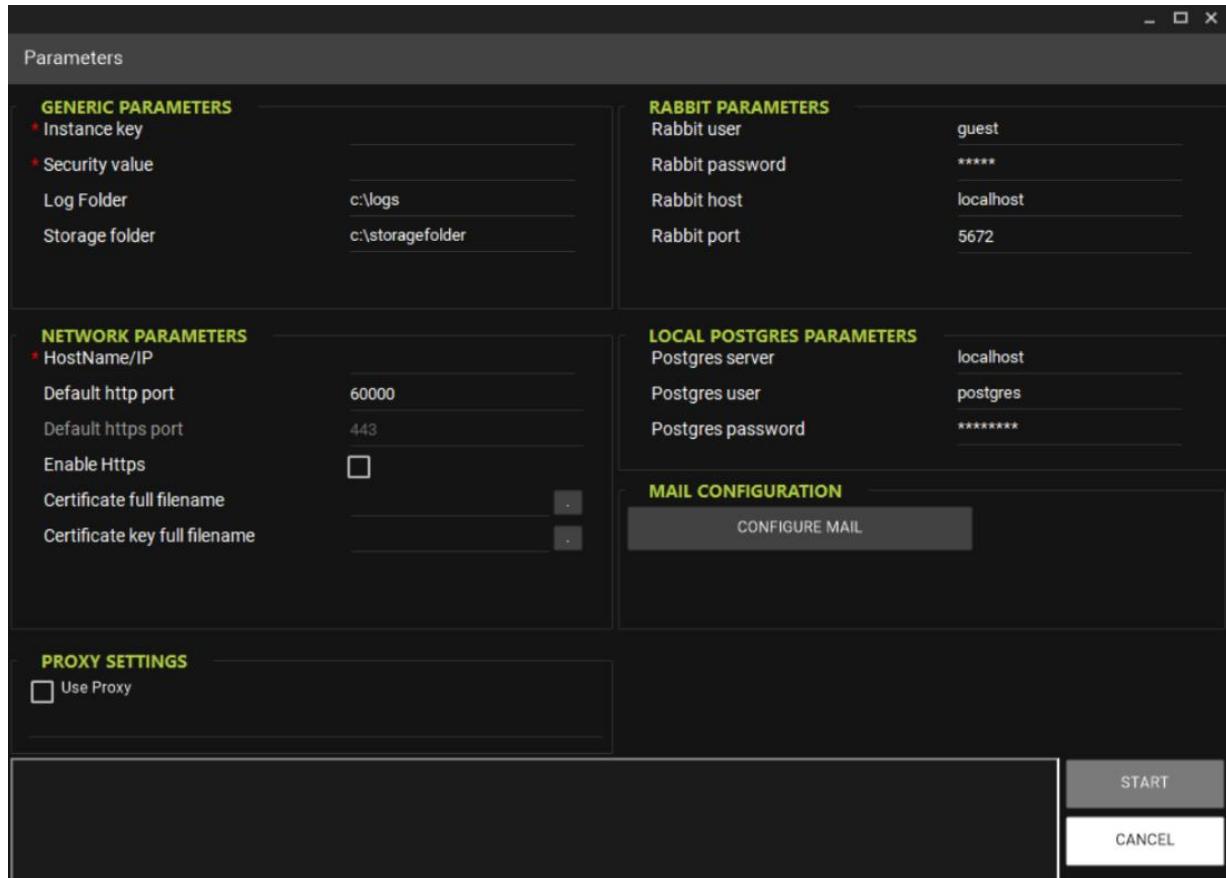
In alternativa si può procedere con Recovery existing installation, il sistema in questo caso richiederà di selezionare il percorso della cartella di installazione di MagoWeb già esistente, una volta selezionato cliccare su start per avviare la procedura di recovery.





Configurazione iniziale dei parametri

La finestra di configurazione è divisa in cinque sezioni principali:



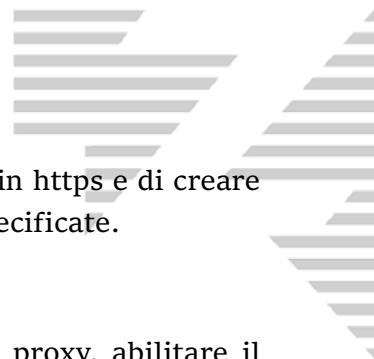
Parametri generali:

- l'Instance Key e Security Value, che dovreste aver ricevuto via mail in precedenza (vedi sezione Acquisto MagoWeb)
- Log folder: folder in cui verranno immagazzinati i log diagnostici prodotti dai vari servizi.
- Storage folder: in questa folder verranno parcheggiati temporaneamente i vari file durante le eventuali operazioni di Upload/Download.

Parametri di rete:

- Hostname/Ip: questo campo ospita l'indirizzo IP pubblico della macchina che ospiterà l'installazione di magoweb, o un relativo alias impostato esternamente a livello di DNS
- Default http e Https port: default 60000 (http) e 443 (https)
- Enable Https: specifica se abilitare la gestione https per l'installazione (abilitando questa opzione verranno abilitati i parametri relativi ai certificati).
- Percorso completo del file di certificato e della chiave: (es. c:\cert\certificate.crt e c:\cert\certificate.key). Specificare i file di certificato e di chiave relativi al dominio/ip impostato in precedenza.

Nel caso venga abilitato https, assicurarsi di inserire nel campo HostName l'esatto nome dell'host corrispondente al certificato che si andrà ad usare.



L'installer si occuperà di configurare automaticamente i vari servizi per girare in https e di creare regole nel firewall di windows per permettere il traffico in arrivo sulle porte specificate.

Impostazioni Proxy

In caso l'installazione di MagoWeb sia effettuata in un dominio sottoposto a proxy, abilitare il relativo flag e impostare l'url del proxy.

Parametri Rabbit

In questa sezione inserire i parametri per la connessione a RabbitMQ.

L'installer è in grado di utilizzare una versione già esistente di RabbitMQ o nel caso non esista, verrà installata e configurata automaticamente.

Parametri Postgres

Come per RabbitMQ, l'installer è in grado di utilizzare versioni già esistenti di PostgreSql o di installare automaticamente la versione necessaria.

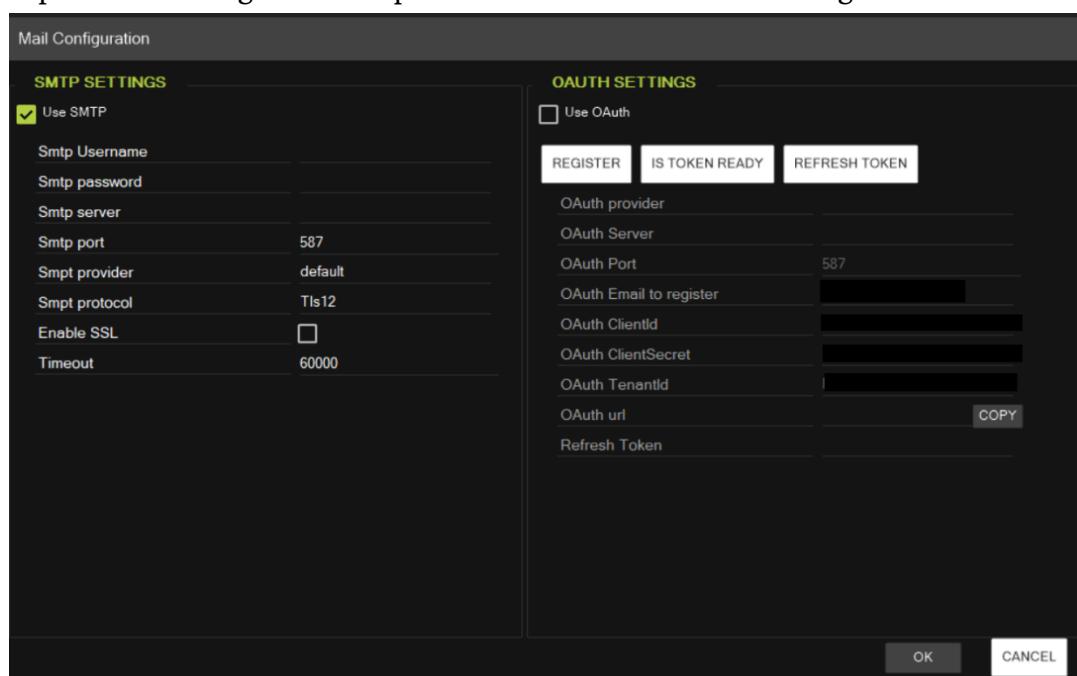
Nota: PostgreSQL è un prerequisito per il funzionamento di alcuni servizi di MagoWeb, e non è necessariamente da considerarsi il server di database da collegare alla subscription.

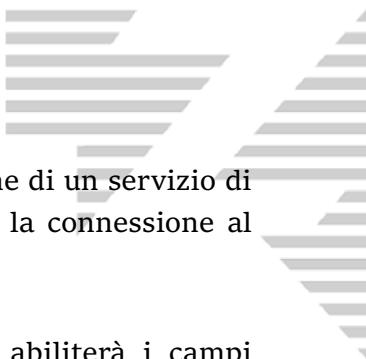
Impostazioni porte

Per finire, in questa sezione sono evidenziate le porte di default su cui i vari servizi di MagoWeb si metteranno in ascolto.

Configurazione mail

Il pulsante Configura Mail aprirà la relativa finestra di configurazione





Impostazioni SMTP: In questa sezione, che di default è selezionata, se si dispone di un servizio di posta, andranno configurati i vari parametri (server, user, password, ecc) per la connessione al server SMTP. Il parametro Smtplib Provider = default non va modificato.

Impostazioni Oauth: Il pulsante Usa Oauth disabiliterà la sezione SMTP e abiliterà i campi sottostanti.

Nota: Per l'utilizzo delle funzionalità di posta tramite Oauth è necessario creare l'applicazione sul provider di posta desiderato (Microsoft o Google), seguendo le istruzioni delle guide ufficiali dei provider.

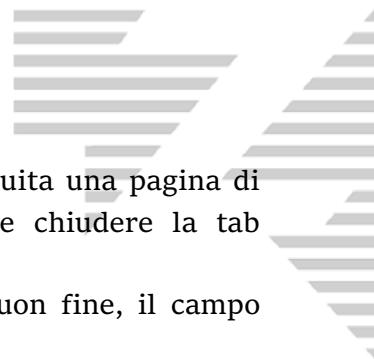
Provider Microsoft:

[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](#)

- Annotare i parametri forniti dal provider per eseguire l'autenticazione in fase di configurazione del nuovo protocollo OAuth2, ovvero:
 - Client Id
 - Client Secret
 - Tenant Id
- Nella schermata presente Inserire tutti i dati fino a TenantId.
 1. Scrivere il provider desiderato, Google o Microsoft come indicato nel punto A
 2. Per il server, inserire “smtp.google.com” per Google oppure “smtp.office365.com” per Microsoft.
 3. La porta è sempre 587.
 4. Indicare l'indirizzo e-mail del mittente per l'OAuth nella sezione “Email to register” in base al provider selezionato precedentemente.
 5. Inserire il Client ID, Client Secret e Tenant ID: queste informazioni sono da recuperare nell'applicazione che si è registrata su Google o Microsoft. Per l'autenticazione con Google non vi è un Tenant ID; tuttavia, il campo non deve essere lasciato vuoto e va valorizzato con un qualsiasi testo.
 6. A questo punto cliccare “Register”, il processo genererà un URL (che verrà travasato nella proprietà relativa nella dialog). Il sistema proverà ad aprirsi su una pagina in incognito del browser Chrome; nel caso non ci riuscisse, si aprirà una pagina sul vostro browser predefinito, ma non in modalità incognito. In questo secondo scenario è importante fare attenzione che l'e-mail non venga dedotta in automatico dal browser, magari col vostro account Google o Microsoft già predisposto. Fare attenzione ad inserire la stessa e-mail inserita precedentemente. Nel dubbio, aprire una pagina in incognito del vostro browser e copiare il link che troverete nella casella a fianco al tasto COPY.
 7. Inserire quindi la password relativa all'email inserita ed accettare le condizioni.



8. Se il processo è andato a buon fine, nella tab del browser vi verrà restituita una pagina di informazioni criptate. Questo significa che il token è pronto e potete chiudere la tab tranquillamente.
9. Procedere cliccando il tasto “IsTokenReady”. Se il processo andasse a buon fine, il campo “Refresh token” dovrebbe auto-compilarsi.
10. Cliccare il tasto ‘OK’

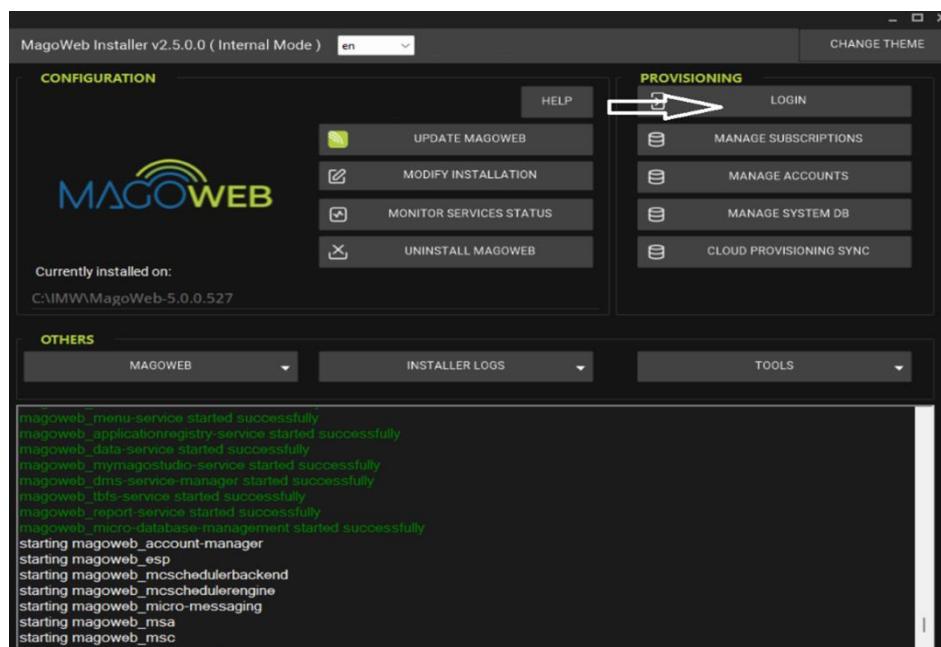
Nota: Il tasto ‘Refresh token’ invece non dovrebbe essere utilizzato. Il token ricevuto scadrà dopo un’ora dalla richiesta, ma la richiesta di aggiornamento partì in automatico, rendendo questo pulsante solo una precauzione. Infatti, il controllo di validità e l’eventuale refresh del token avverrà ad ogni nuova login su Mago e prima dell’invio di ogni mail. È ora possibile l’invio e-mail con OAuth2. Una volta impostati tutti i parametri obbligatori, si abiliterà il bottone start.

Premendo il bottone Start partì la vera e propria configurazione ed installazione di MagoWeb.

Creazione dell'utente SYS-ADMIN

Accesso al sistema

- Una volta terminata l'installazione, sarà necessario creare un account SYS-ADMIN.
- Nella sezione Provisioning, clicca su Login per avviare il wizard di configurazione dell'account SYS-ADMIN.



Configurazione dell'account SYS-ADMIN

- Password: Scegli una password per l'account SYS-ADMIN
- Indirizzo e-mail: Inserisci un indirizzo e-mail valido per il recupero dell'account e per le notifiche.
- Nome dell'account: Questo campo non è modificabile e verrà precompilato con il nome dell'account SYS-ADMIN, ovvero mwsysadmin.



Puoi anche scegliere la lingua di preferenza per l'interfaccia utente.

MagoWeb Console Configurator

WELCOME TO MAGOWEB CONSOLE CONFIGURATION WIZARD

PROVISIONING SYSADMIN ACCOUNT

Choose the password for the account who will have privileges to access to MagoWebInstaller and manage all information about this installation.
Please specify also a valid e-mail address.
The account name cannot be changed.

SysAdmin e-mail:

SysAdmin account: **mwsysadmin**

SysAdmin password

Confirm password:

SET DEFAULT INSTALLATION LANGUAGE

Language: **English**

Regional settings: **English**

CANCEL **NEXT**

Clicca su Next per procedere.

Configurazione del Database di Sistema

- Prima di configurare il database per MagoWeb Console, verranno richieste le credenziali amministrative del database.

Scelta del provider di database

Seleziona il database provider da utilizzare:

- SQL Server o PostgreSQL.

Inserisci i dati relativi al server di database:

- Server di riferimento: Inserisci l'indirizzo del server SQL o PostgreSQL.
- SysAdmin User: Il nome utente per l'accesso amministrativo (e.g. 'sa' per SQLServer / 'postgres' per PostgreSQL).
- SysAdmin Password: La password dell'utente amministrativo.

Nota: Le credenziali di amministrazione fornite sono utilizzate solo per le operazioni di gestione del database di sistema e NON verranno salvate localmente.



MagoWeb Console Configurator

DATABASE INFORMATION FOR THIS MAGOWEB CONSOLE INSTALLATION

Before configure the database for MagoWeb Console, we need the administrative credentials to proceed with the operations of creation database and dbowner.

These credentials WILL NOT BE SAVED anywhere, but only used to complete the process.

ADMINISTRATIVE CONNECTION CREDENTIALS

Provider:	SqlServer
Server:	<input type="text"/>
SysAdmin user	<input type="text"/>
SysAdmin password	<input type="password"/> 

CANCEL **BACK** **NEXT**

Clicca su Next per procedere.

Creazione o selezione del database di sistema

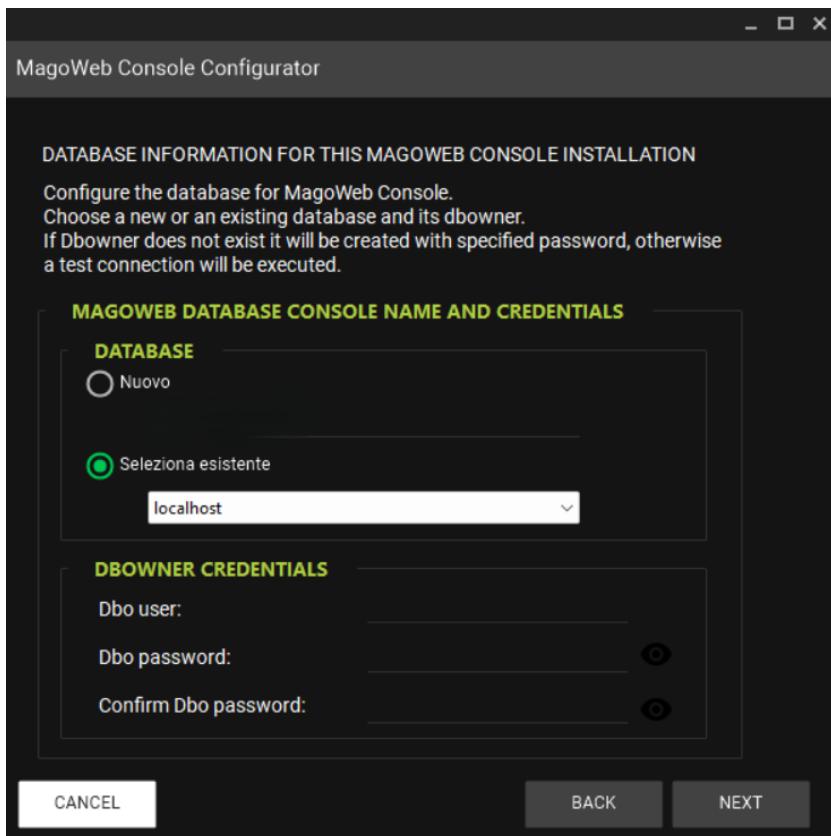
- Nuovo Database: Puoi scegliere di creare un nuovo database.
- Database Esistente: Seleziona un database esistente
- Dbowner: credenziali dell'utente che diventerà dbowner per il database di sistema.

Se il dbowner non esiste, verrà creato automaticamente con la password specificata.

Se esiste già, verrà eseguita una connessione di prova per verificarne la validità.

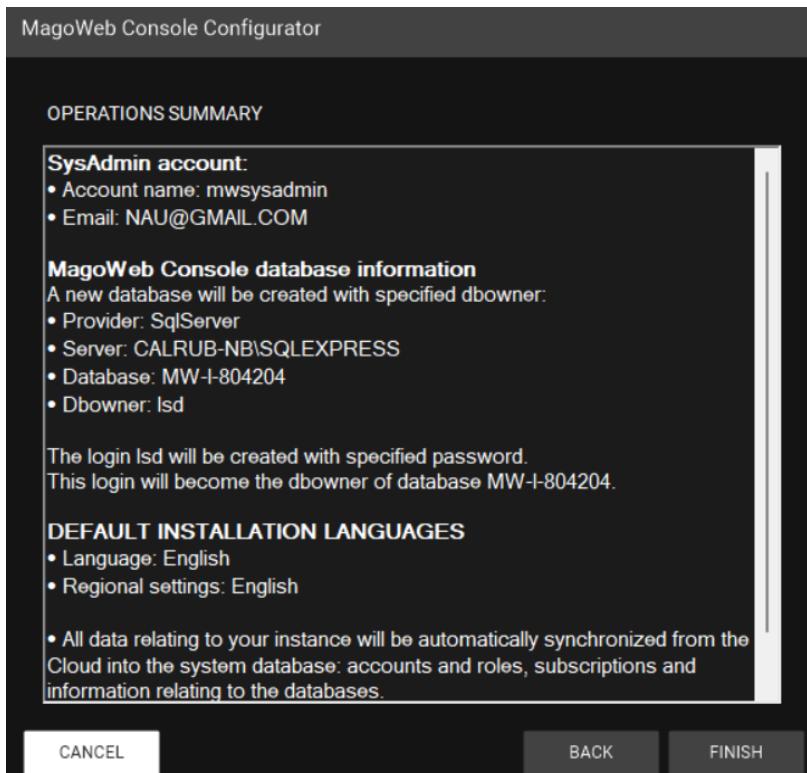
Il dbowner scelto sarà applicato a tutti gli oggetti del database di sistema

Nota: Nell'impossibilità di recuperare la password di un dbowner esistente, sarà necessario agire manualmente collegandosi al server e modificarla tramite gli strumenti amministrazione del provider.



Riepilogo delle operazioni

- Una volta inseriti tutti i dati, verrà mostrato un riepilogo delle operazioni di configurazione.



- Clicca su Finish per completare la configurazione.

Completamento dell'installazione



- Dopo aver cliccato su Finish, il sistema eseguirà le ultime operazioni di configurazione, avviando i servizi necessari per la corretta esecuzione di MagoWeb Console.

Nota: si ricorda che in coda al Wizard viene eseguita la sincronizzazione dati dal Provisioning Cloud. Si rimanda ai dettagli nella sezione dedicata.

Creazione Database Sottoscrizione

Dopo l'autenticazione troverete, nel menu a tendina, le vostre sottoscrizioni.

In questa fase l'installer avviserà che la sottoscrizione non ha ancora un database: procedere quindi alla creazione premendo il bottone “Crea database per la subscription”.

Configurazione database

È possibile utilizzare, come provider database, sia SqlServer che PostgreSql.

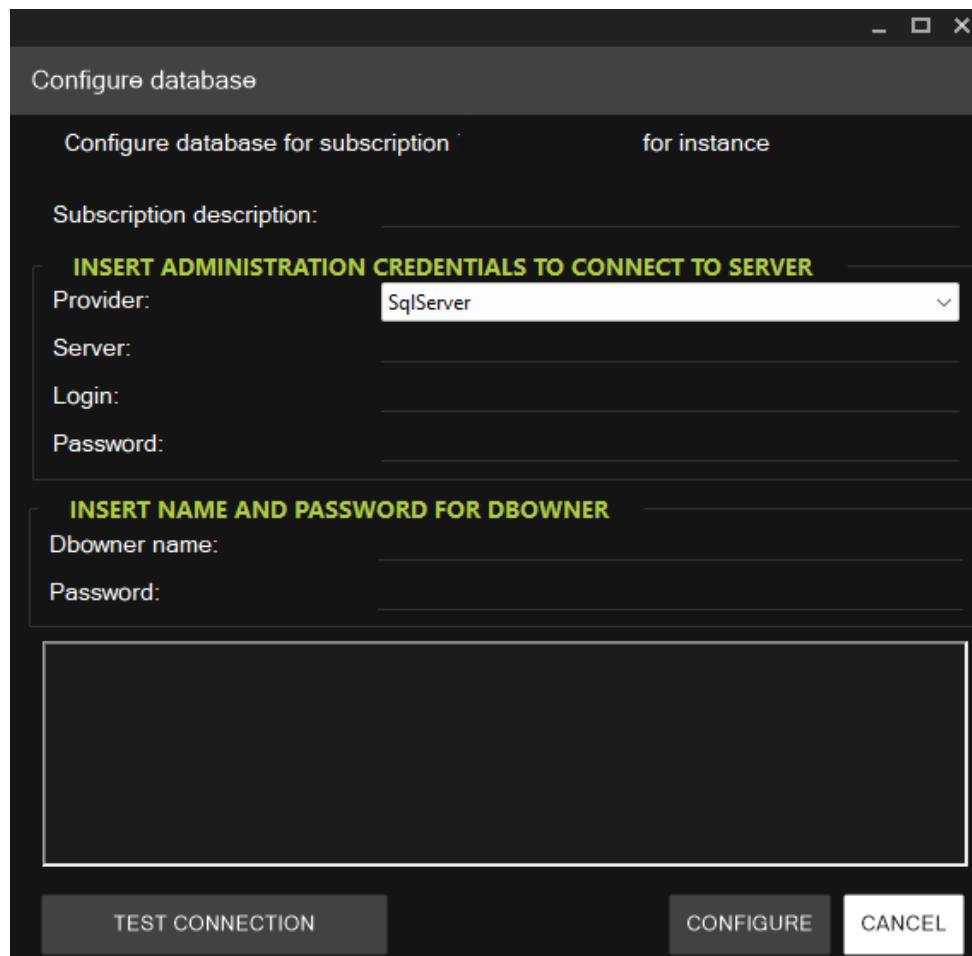
Selezionare dall'apposito menu a tendina il provider desiderato.

Una volta impostato il provider è necessario inserire le informazioni Server, Login e Password per il collegamento.

È possibile utilizzare il bottone “Test Connection” per verificare la bontà delle informazioni appena inserite.

Andranno inserite le credenziali del dbowner da associare al database. È possibile inserire credenziali di un dbowner esistente o di un utente nuovo, l'installer provvederà a crearlo automaticamente.

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



Premendo il tasto “Configura” partirà la creazione del database.

Successivamente si potrà procedere all’importazione di un set di dati di default o di esempio.

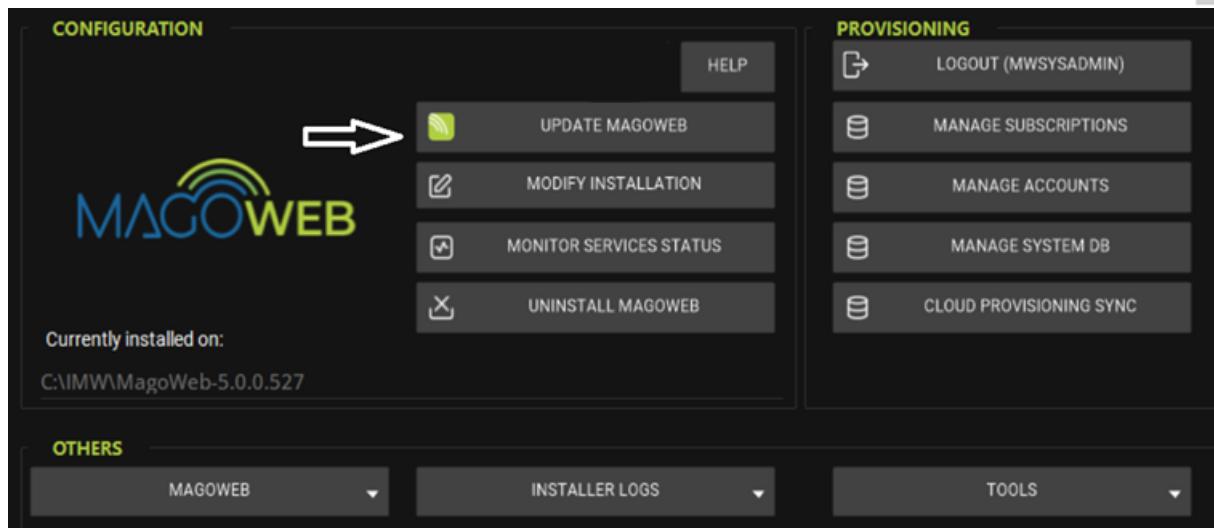
Modifiche alla Configurazione Iniziale

Una volta terminata la configurazione iniziale sarà tuttavia possibile eseguire delle modifiche inerenti alla configurazione.

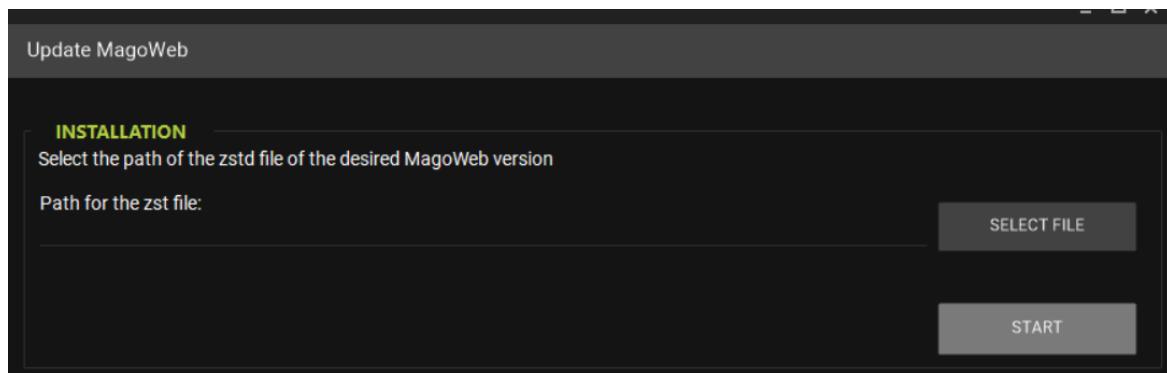
Aggiornamento di MagoWeb

Per eseguire l’aggiornamento di MagoWeb

1. Nella sezione Configurazione, seleziona Update MagoWeb.



2. Verrà richiesto di selezionare il percorso del file zst della versione di MagoWeb che si vuole installare.



3. Dopo aver selezionato il file cliccando su start, il sistema procederà automaticamente all'aggiornamento.

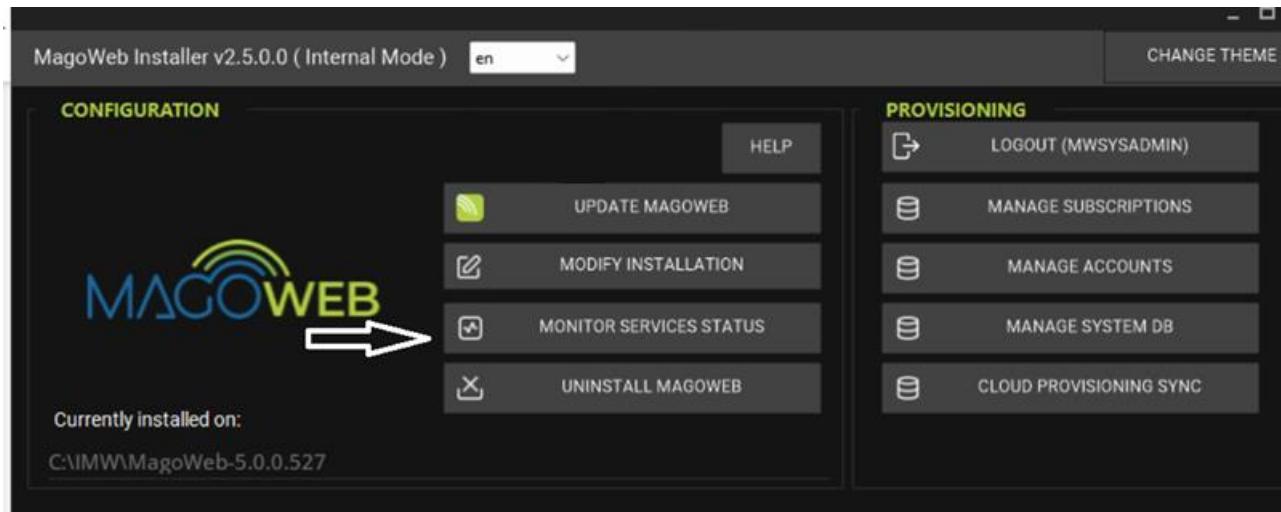
Nota: non è possibile avere più installazioni attive di MagoWeb contemporanee. È necessario aggiornare ad una nuova versione oppure effettuare una disininstallazione dell'attuale e un recupero di una versione esistente.



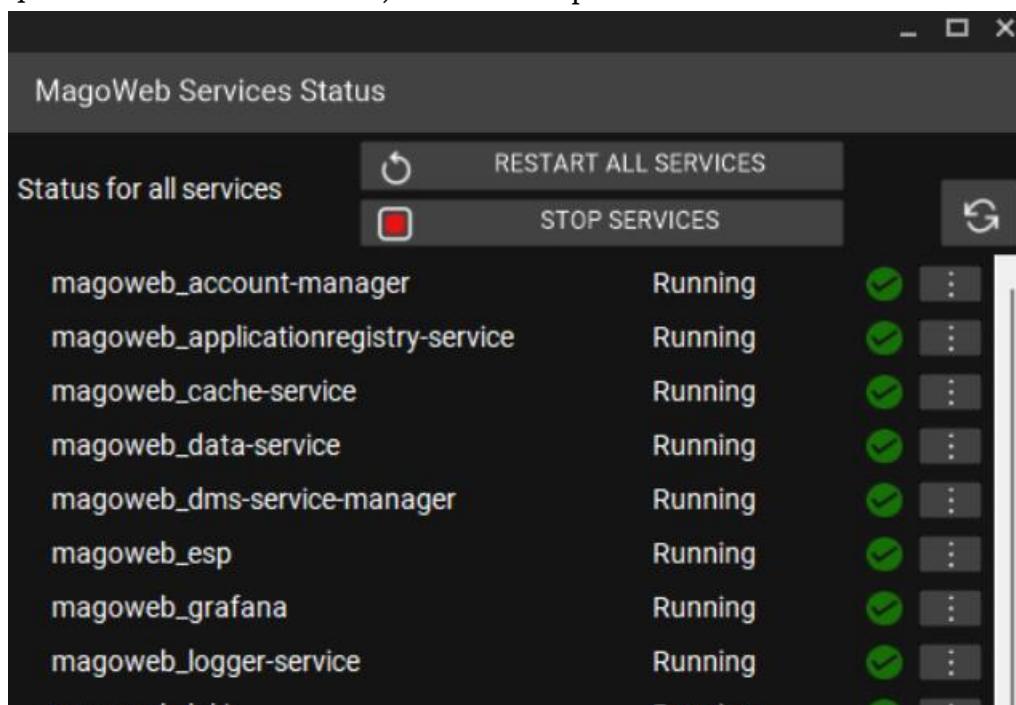
Monitoraggio dei Servizi

Per monitorare lo stato dei servizi e gestirli:

1. Vai alla sezione Monitor Service Status.



2. Qui potrai visualizzare lo stato dei servizi in esecuzione.
3. Per riavviare un servizio, clicca su Restart.
4. Per fermare un servizio, clicca su Stop.



Nota: il servizio magoweb_micro-database-management viene attivato e stoppato automaticamente a seconda delle necessità, durante le operazioni di manutenzione del database.

Al di fuori di questi utilizzi, il servizio verrà stoppato per evitare inutili occupazioni di memoria e sarà quindi normale vederlo "stopped" nelle tipiche condizioni di utilizzo

Nota: Alcuni servizi dipendono da altri: nel caso vengano riavviati manualmente servizi che dipendono o sono dipendenza di altri servizi, verranno riavviati di conseguenza anche i servizi collegati.



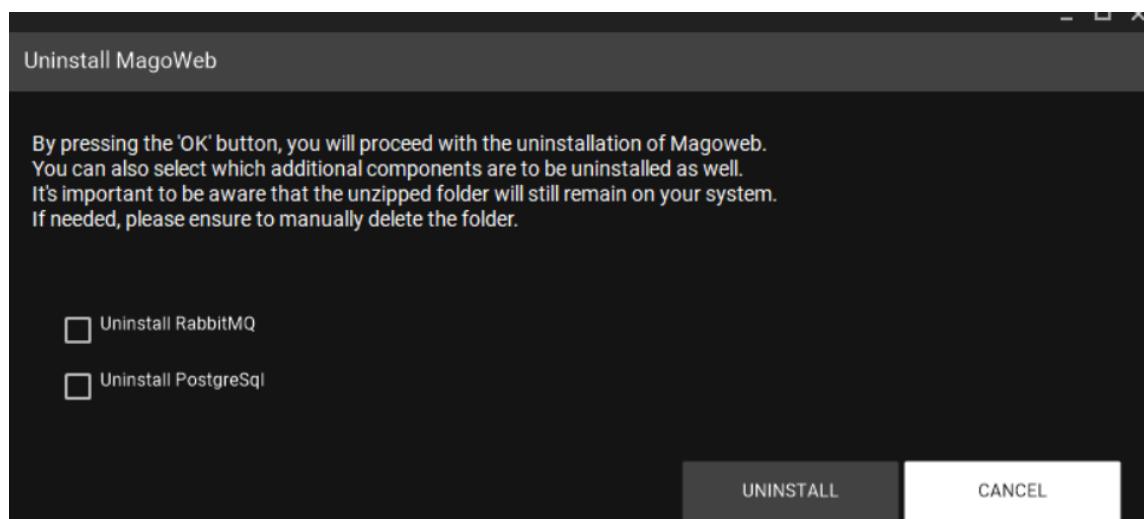
Disinstallazione di MagoWeb

Per disinstallare MagoWeb e i suoi componenti aggiuntivi:

1. Vai alla sezione UNINSTALL MAGOWEB.



2. Tutti i servizi verranno “spenti” e rimossi, ad esclusione di RabbitMQ e PostgreSQL (a meno che l’utente non abbia deciso di non rimuoverli come da immagine successiva).
3. Clicca su UNINSTALL per avviare il processo di disinstallazione.



4. Il sistema procederà con la rimozione di MagoWeb e dei componenti selezionati.

Nota: la cartella di installazione non verrà cancellata: sarà onere dell’utente cancellarla manualmente. In qualsiasi momento sarà possibile recuperare una versione di MagoWeb tramite il bottone “Recupera Installazione esistente”.



Recupero di una installazione precedente

In qualsiasi momento è possibile disinstallare l'attuale versione di Magoweb e recuperarne una disinstallata in precedenza.

Per recuperare una versione di MagoWeb disinstallata in precedenza, sarà sufficiente cliccare sul bottone “Recupera installazione precedente”.



Nella finestra che appare, selezionare la cartella della versione che si vuole ripristinare.

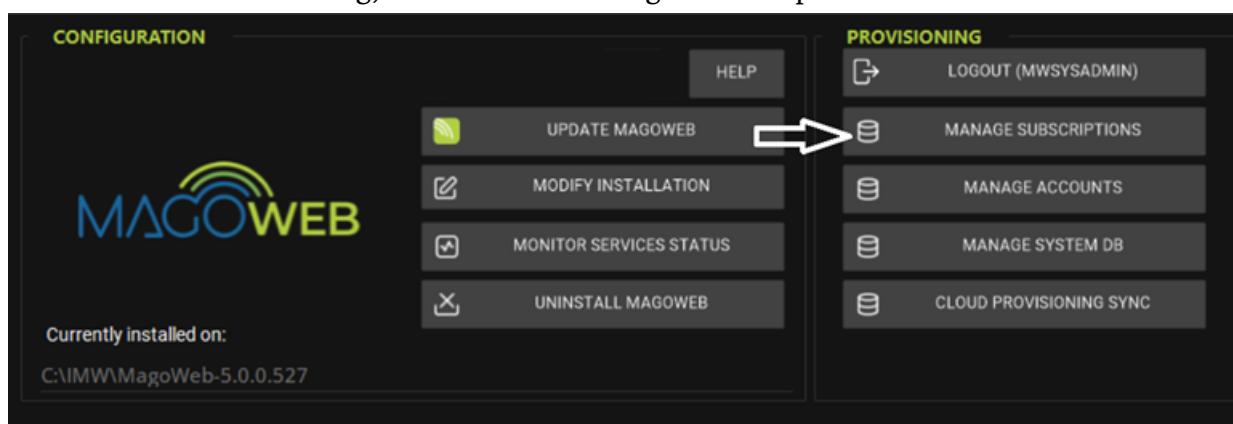
Premendo start verranno reinstallati tutti i servizi utilizzando l'ultima configurazione inserita dall'utente.

Amministrazione Utenti e Subscription

Dopo aver effettuato il login come SYS-ADMIN, accedere alla sezione Provisioning.

Gestione Subscriptions

Nella sezione Provisioning, cliccando su Manage Subscriptions



Da questa sezione sarà possibile gestire Database/Account associati/Moduli.



Manage Subscriptions

SUBSCRIPTION MANAGEMENT

Subscription key:	Parent account name:
Description:	Country: IT
Creation date:	Industry:
Notes:	Edition: PRO

DATABASE MANAGEMENT

ASSOCIATED ACCOUNTS

FRAGMENTS (ACTIVATED MODULES)

SAVE **CANCEL**

Gestione Database

Cliccando su Database Management verranno visualizzate le informazioni relative alla connessione al database.

Manage Subscriptions

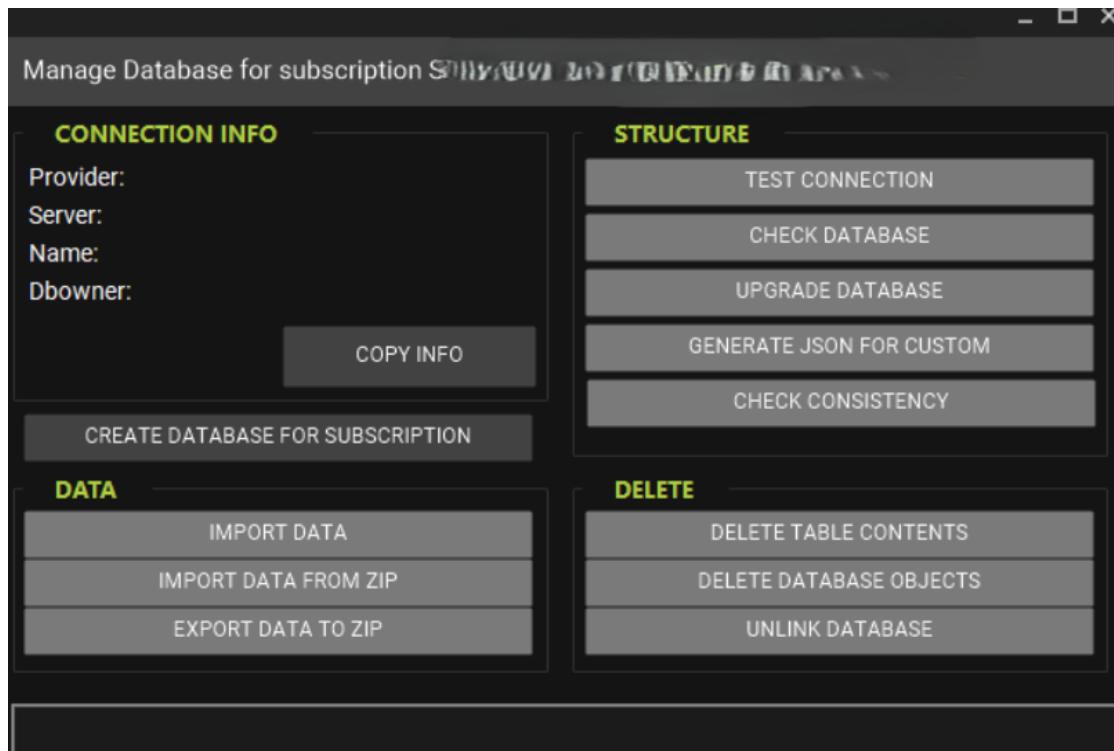
SUBSCRIPTION MANAGEMENT

DATABASE MANAGEMENT 

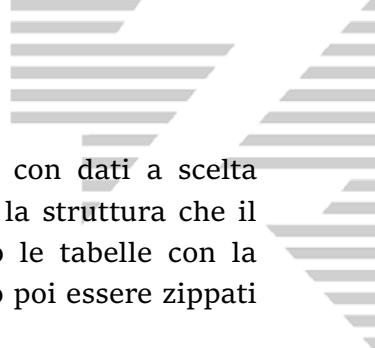
ASSOCIATED ACCOUNTS

FRAGMENTS (ACTIVATED MODULES)

Da questa schermata, è possibile eseguire le seguenti operazioni:



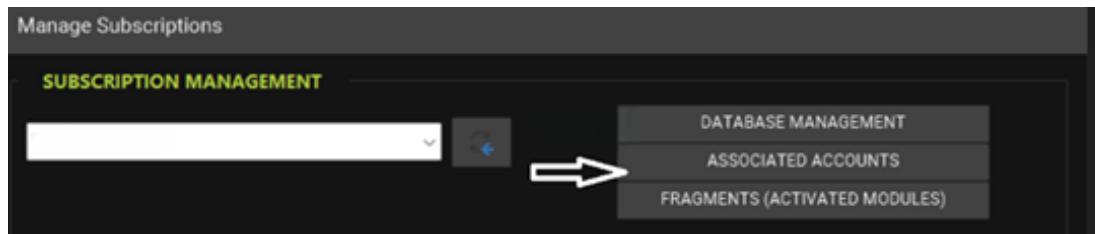
- Nella sezione di CONNECTION INFO:
 - o *Change connection info* consente di modificare le informazioni di connessione al database (e.g. in caso di cambio nome del server o del database).
 - o *Copy info* copia le informazioni della subscription nella clipboard.
- Nella sezione di STRUCTURE:
 - o Un test di connessione (*Test Connection*) per verificare la raggiungibilità del database
 - o Un *Check Database* che esegue una verifica sul DB corrente della subscription verificando se la struttura tabellare sia allineata alla versione corrente
 - o Il tasto di *Upgrade Database* che scatena appunto l'aggiornamento del database della subscription
 - o Il tasto di *Generate JSON for Custom* crea un json, che sarà salvato nella tabella tb_customtbfs, contenente tutta la struttura attuale del database. Queste informazioni sono utilizzate da Reporting Studio e MyMagoStudio.
 - o Il tasto di *Check consistency* avvia un controllo tra la struttura del database della sottoscrizione e gli oggetti (tabelle, colonne) dichiarati nei file EFSchemaObjects.xml, segnalando le eventuali differenze.
- Nella sezione di DATA:
 - o *Import Data* consente di effettuare l'import di dati di default di MagoWeb:
 - *Dati di default*: dati di configurazione necessari per far funzionare le procedure applicative. Sono divisi per paese e configurazione. Solitamente la scelta del paese fa riferimento a quella selezionata in fase di acquisto della sottoscrizione.
 - *Dati di esempio*: Un set di dati di default arricchiti di valori addizionali che vanno a comporre un insieme di dati con scopo illustrativo.



- *Import Data from ZIP* permette di caricare dei file in formato .xml con dati a scelta dell'utente. È necessario che la struttura dell'xml segua perfettamente la struttura che il sistema è in grado di leggere. Questo può essere desunto esportando le tabelle con la funzionalità di export per poi utilizzarle per generare i file che potranno poi essere zippati ed importati correttamente. Il limite di dimensione è di 100 MB.
- *Export Data to ZIP* permette di esportare tutto il contenuto delle tabelle in formato .xml all'interno di un file .zip, l'operazione ha un limite massimo di dimensione del database di 2GB.
- Nella sezione di DELETE:
 - *Delete Table Contents* elimina, previa conferma, tutti i dati contenuti nelle tabelle lasciando inalterata la struttura tabellare.
 - *Delete Database Objects* elimina, previa conferma, l'intera struttura tabellare della sottoscrizione MagoWeb.
 - *Unlink Database* elimina il collegamento tra la sottoscrizione e il database, ma SENZA alterare il database stesso, che sarà sempre disponibile nel server di riferimento.

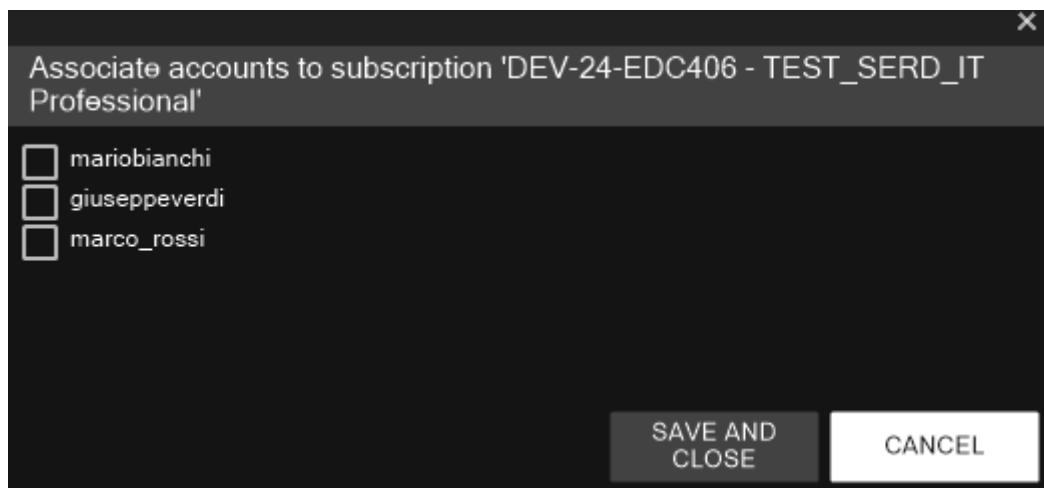
Gestione Account Associati

Selezionando la voce Accounts Associati, verrà aperta una nuova schermata con l'elenco di tutti gli accounts associati alla Subscription.



In questa sezione è possibile:

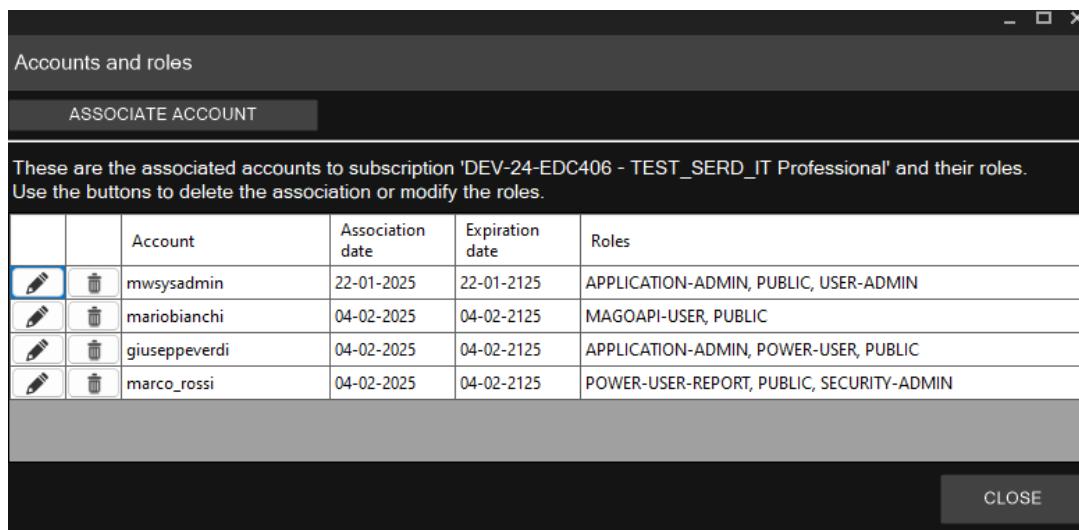
- Associare un nuovo account: cliccare sul pulsante Associa Account, selezionare l'account desiderato e confermare cliccando su Save.



- Modificare il ruolo di un account: cliccare sull'icona della matita accanto all'account per modificare il suo ruolo.



- Eliminare l'associazione di un account: per rimuovere un account associato alla sottoscrizione, cliccare sull'icona del cestino



Accounts and roles

ASSOCIATE ACCOUNT

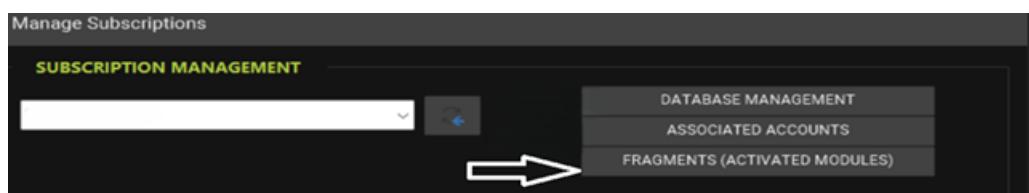
These are the associated accounts to subscription 'DEV-24-EDC406 - TEST_SERD_IT Professional' and their roles. Use the buttons to delete the association or modify the roles.

	Account	Association date	Expiration date	Roles
	mwsysadmin	22-01-2025	22-01-2125	APPLICATION-ADMIN, PUBLIC, USER-ADMIN
	mariobianchi	04-02-2025	04-02-2125	MAGOAPI-USER, PUBLIC
	giuseppeverdi	04-02-2025	04-02-2125	APPLICATION-ADMIN, POWER-USER, PUBLIC
	marco_rossi	04-02-2025	04-02-2125	POWER-USER-REPORT, PUBLIC, SECURITY-ADMIN

CLOSE

Gestione Moduli Attivati

Cliccando sul pulsante Fragments (Activated Modules) verranno visualizzati tutti i moduli associati alla sottoscrizione.



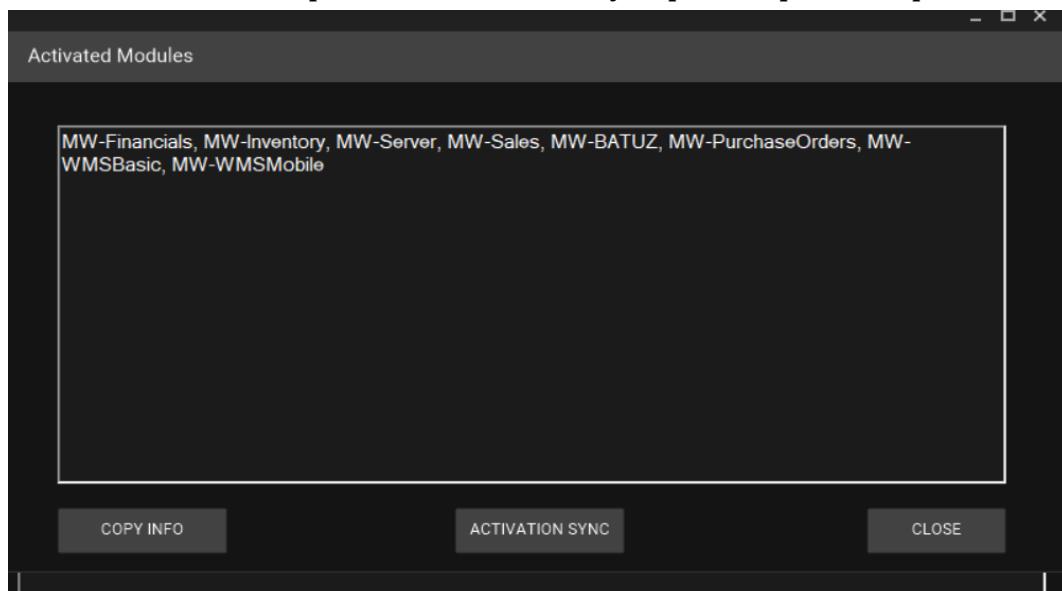
Manage Subscriptions

SUBSCRIPTION MANAGEMENT

FRAGMENTS (ACTIVATED MODULES)

Sincronizzazione dei Moduli

Se in futuro verranno aggiunti nuovi moduli alla sottoscrizione tramite il portale Infinity o dallo store, sarà necessario eseguire una sincronizzazione locale affinché i nuovi moduli siano visibili. Per farlo, cliccare sul pulsante Activation Sync per completare il processo di sincronizzazione.



Activated Modules

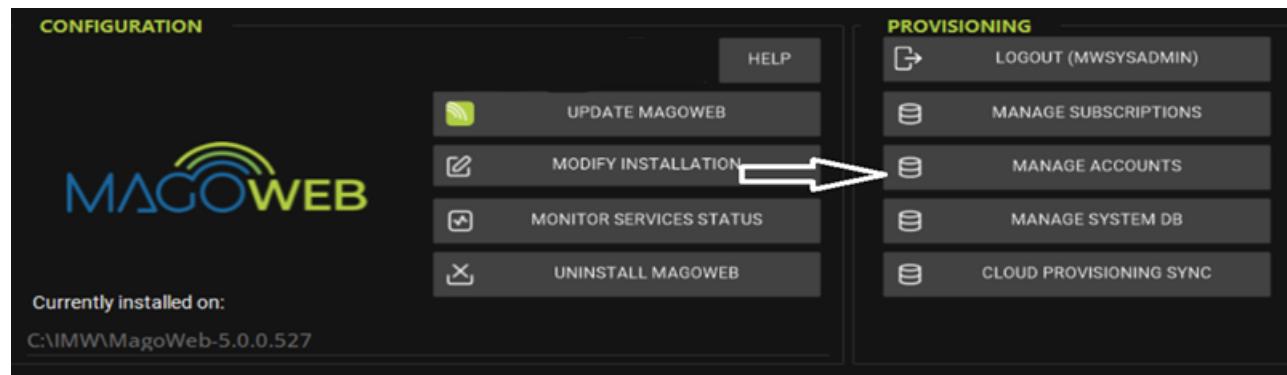
MW-Financials, MW-Inventory, MW-Server, MW-Sales, MW-BATUZ, MW-PurchaseOrders, MW-WMSBasic, MW-WMSMobile

COPY INFO ACTIVATION SYNC CLOSE

Nota: Assicurarsi di eseguire la sincronizzazione ogni volta che nuovi moduli vengono aggiunti alla propria sottoscrizione per garantire un corretto aggiornamento delle informazioni.

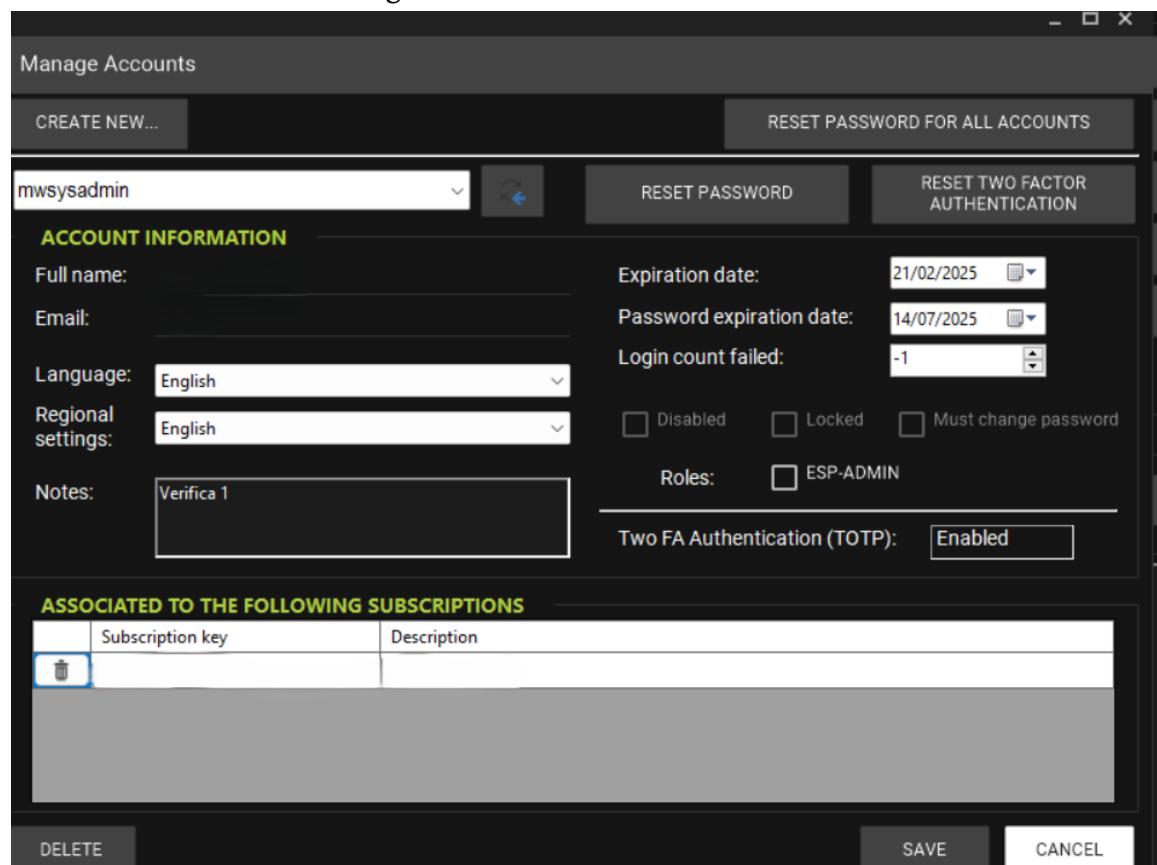
Gestione Account

Nella sezione Provisioning, cliccando su Manage accounts



The screenshot shows the MAGOWEB Configuration interface. On the left, there's a 'CONFIGURATION' sidebar with options like 'UPDATE MAGOWEB', 'MODIFY INSTALLATION' (which has a white arrow pointing to it), 'MONITOR SERVICES STATUS', and 'UNINSTALL MAGOWEB'. On the right, under 'PROVISIONING', there are links for 'LOGOUT (MWSYSADMIN)', 'MANAGE SUBSCRIPTIONS', 'MANAGE ACCOUNTS' (highlighted with a white arrow), 'MANAGE SYSTEM DB', and 'CLOUD PROVISIONING SYNC'.

in questa sezione il SYS-ADMIN potrà visualizzare la lista degli accounts attuali e accedere alla funzionalità di creazione e gestione.



The screenshot shows the 'Manage Accounts' interface. At the top, there are buttons for 'CREATE NEW...', 'RESET PASSWORD FOR ALL ACCOUNTS', and 'RESET TWO FACTOR AUTHENTICATION'. Below that, a user 'mwsysadmin' is selected. The 'ACCOUNT INFORMATION' section includes fields for 'Full name', 'Email', 'Language' (set to 'English'), 'Regional settings' (set to 'English'), 'Notes' ('Verifica 1'), and 'Roles' ('ESP-ADMIN'). It also shows 'Expiration date' (21/02/2025), 'Password expiration date' (14/07/2025), 'Login count failed' (-1), and checkboxes for 'Disabled', 'Locked', and 'Must change password'. A 'Two FA Authentication (TOTP)' section shows 'Enabled'. The 'ASSOCIATED TO THE FOLLOWING SUBSCRIPTIONS' section is empty, showing a table with columns 'Subscription key' and 'Description'. At the bottom are 'DELETE', 'SAVE', and 'CANCEL' buttons.

Creazione di un Nuovo Account

Cliccare su Create new,

Create new account

NEW ACCOUNT INFORMATION

Account name:	Expiration date:	16/01/2025
Full name:	Password expiration date:	16/01/2025
Password:	Language:	English
Confirm password:	Regional settings:	English
Email:	<input type="checkbox"/> Disabled <input type="checkbox"/> Locked <input checked="" type="checkbox"/> Must change password	
Notes:	Roles: <input type="checkbox"/> ESP-ADMIN	

successivamente compilare tutti i campi richiesti:

- Account Name: Nome identificativo dell'account.
- Full Name: Nome completo dell'utente.
- Password: Inserisci una password sicura per l'utente.
- E-mail: Indirizzo e-mail associato all'account.
- Note (Facoltativo): Puoi aggiungere delle note supplementari per l'account (questo campo è opzionale).
- Clicca su Save and close per completare la creazione dell'account.

Dopo aver creato l'account, al primo accesso, l'utente sarà obbligato a cambiare la password attraverso la funzionalità Cambia Password.

Gestione Accounts Esistenti

Il Sys-Admin può gestire tutti gli account presenti in console direttamente dalla schermata di Manage Accounts.

Le azioni disponibili includono:

- Disabilitare Account: Clicca sull'icona appropriata per disabilitare l'account, impedendone l'accesso.
- Bloccare Account: Clicca sull'icona per bloccare l'account, impedendo l'accesso ma senza disabilitarlo completamente.
- Assegnare Ruolo ESP-ADMIN: Se necessario, puoi assegnare tale ruolo all'account selezionato.

Manage Accounts

CREATE NEW... RESET PASSWORD FOR ALL ACCOUNTS

mwsysadmin RESET PASSWORD RESET TWO FACTOR AUTHENTICATION

ACCOUNT INFORMATION

Full name: Expiration date:

Email: Password expiration date:

Language: Login count failed:

Regional settings: Disabled Locked Must change password

Notes: Roles: **ESP-ADMIN**

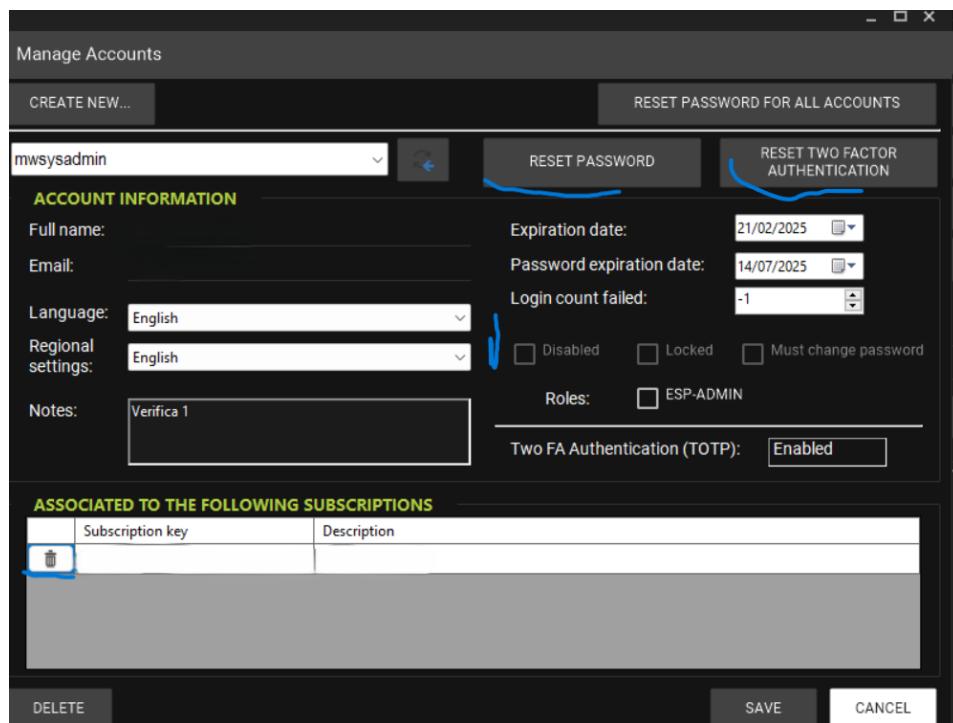
Two FA Authentication (TOTP):

ASSOCIATED TO THE FOLLOWING SUBSCRIPTIONS

	Subscription key	Description
<input type="button" value="Delete"/>		

DELETE SAVE CANCEL

- Modificare la Data di Scadenza della Password: Se necessario, puoi impostare o aggiornare la data di scadenza della password dell'utente.
- Modificare la Lingua: Puoi anche modificare la lingua preferita per l'utente.
- Nella schermata di gestione degli accounts, il Sys-Admin può eseguire anche le seguenti azioni:
 - o Rimuovere l'Associazione alla Sottoscrizione: clicca sull'icona del cestino per rimuovere l'associazione dell'account alla sottoscrizione.
 - o Reset della Password: Se richiesto, il Sys-Admin può eseguire un reset della password, inserendo una nuova password temporanea per l'utente, che sarà obbligato a cambiarla al primo accesso.
 - o Abilitare/Disabilitare Two-Factor Authentication (2FA): Se l'account ha la Two-Factor Authentication (2FA) abilitata, lo stato verrà visualizzato come Abilitato. Se necessario, il Sys-Admin può rimuovere l'abilitazione del TWO FACTOR AUTHENTICATION, cliccando sull'apposito tasto.



Nella lista degli accounts, il Sys-Admin può visualizzare le seguenti informazioni per ciascun account:

- Nome dell'Account
- E-mail dell'Account
- Stato di Two-Factor Authentication (2FA): Se abilitato, verrà mostrato come attivo.
- Data di Scadenza della Password: Viene visualizzata la data in cui la password dell'account scadrà.

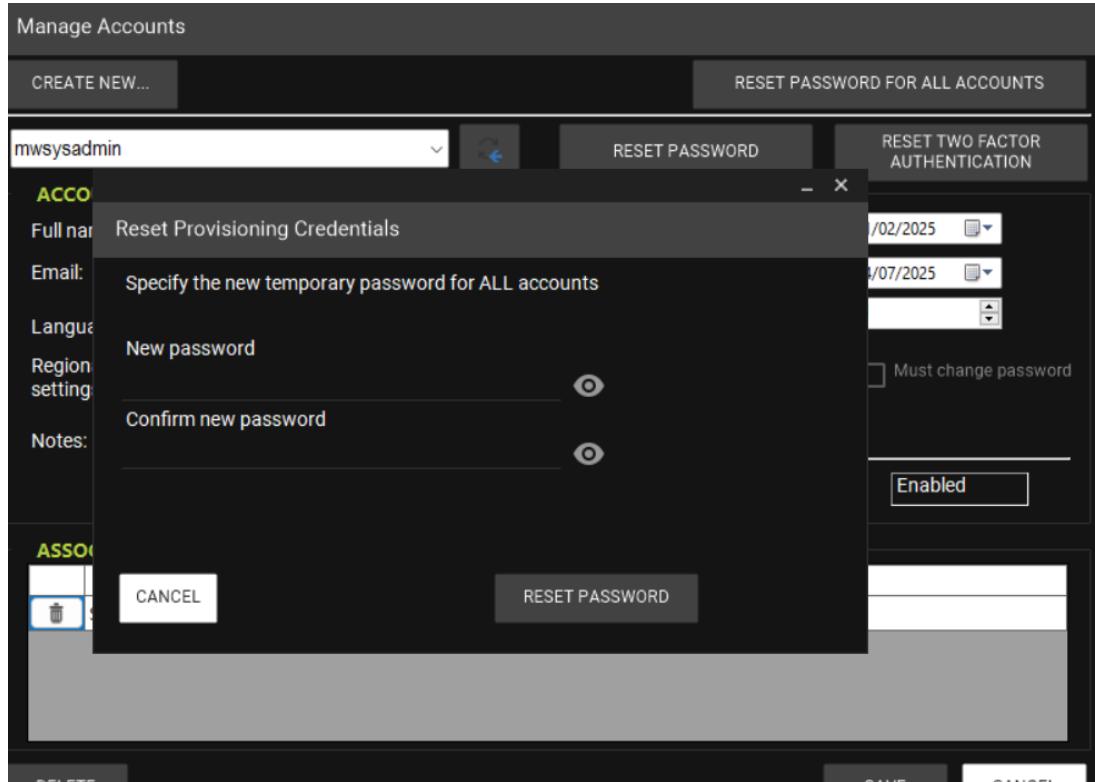
Se necessario, il Sys-Admin può aggiornare le informazioni relative all'account, come nome ed e-mail, direttamente dalla schermata di gestione.

Inoltre, il SysAdmin può aggiornare rapidamente le password di tutti gli accounts, evitando di dover modificare manualmente ciascun account individualmente, tramite l'apposito tasto Reset Password for all accounts.



Sarà quindi possibile impostare una password temporanea per tutti gli accounts senza soddisfare i criteri di complessità), che dovranno cambiare al primo accesso al programma.

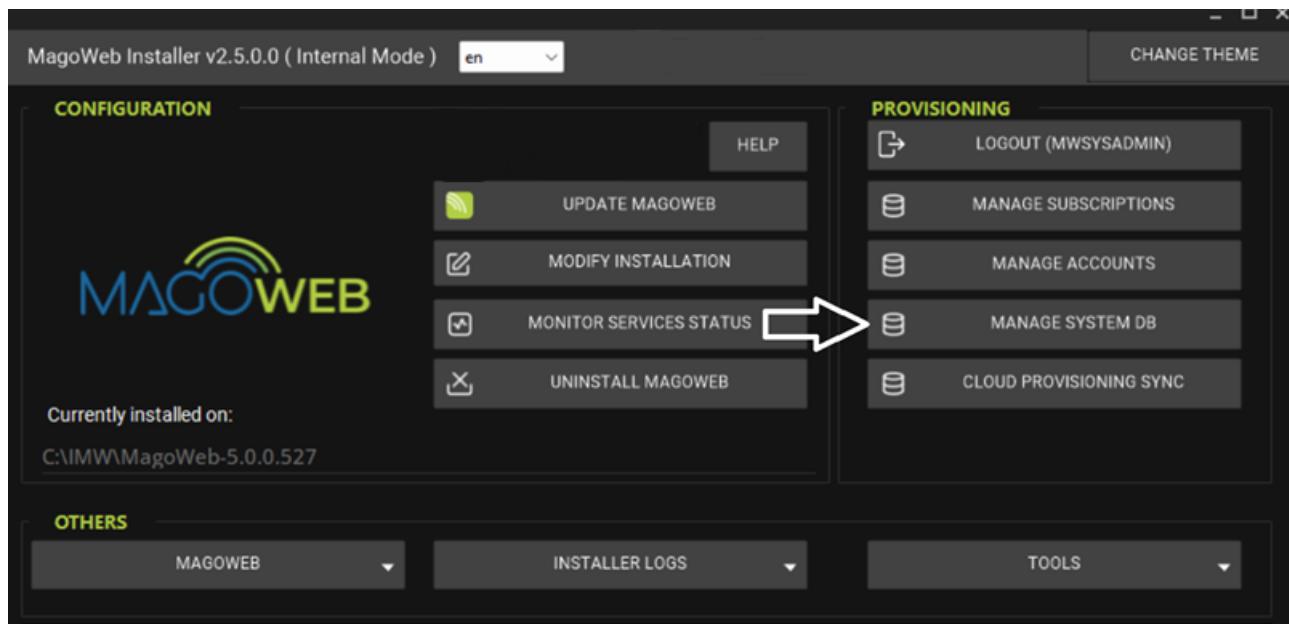
Il Sys-Admin è automaticamente escluso da questa operazione di reset massivo.



Nota: la funzionalità di “Reset password per tutti gli accounts” si rende particolarmente utile dopo la prima fase di configurazione del sistema. Infatti, la sincronizzazione degli accounts dal Provisioning Cloud elimina alcuni dati ritenuti sensibili, quali e-mail, full name e password. Con quest’opzione di Reset massivo è possibile impostare con un solo passaggio una password temporanea per tutti.

Gestione System DB

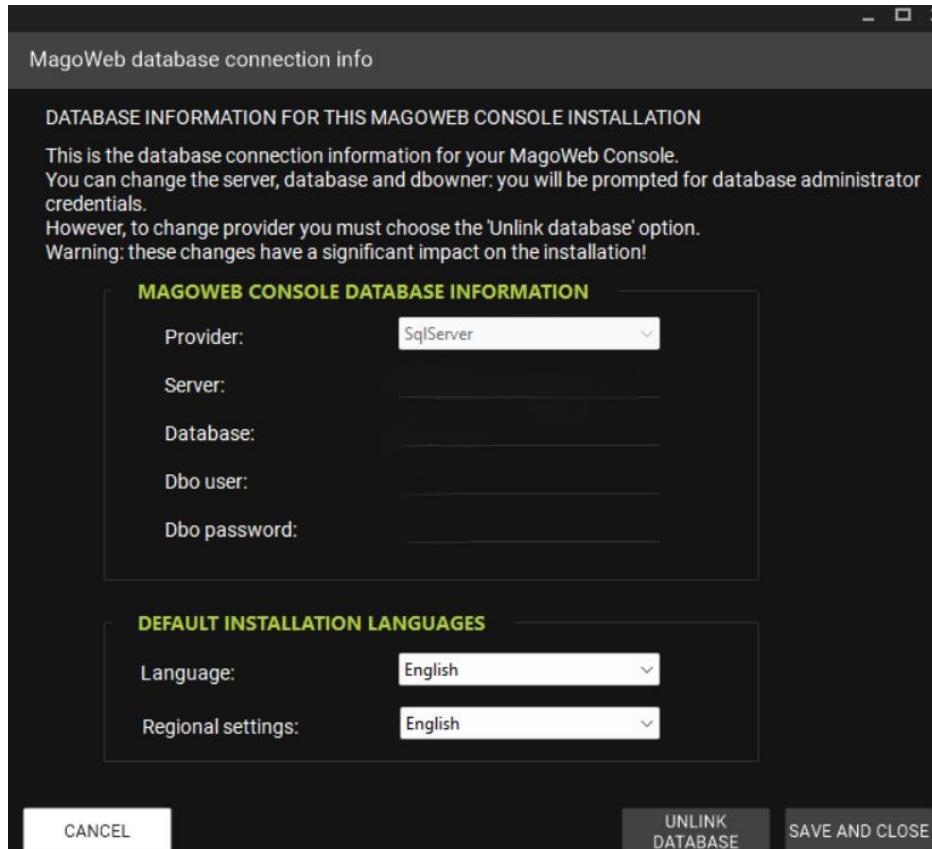
Nella sezione Provisioning, cliccando su Manage System DB, il MagoWeb Installer ti indirizzerà a una schermata che mostra tutte le informazioni relative alla connessione al database di sistema per MagoWeb





In questa schermata, troverai i seguenti dati:

- **Server:** Indica l'indirizzo del server che ospita il database.
- **Database:** Nome del database di sistema a cui l'applicazione si connette.
- **Dbo user:** Identifica il proprietario del database (dbowner).



Sarà possibile modificare le credenziali di connessione al database, per eseguire questa operazione ti verrà richiesto di inserire le credenziali dell'amministratore del database. Queste credenziali sono necessarie per autorizzare la modifica delle impostazioni e garantire l'accesso corretto al database.

Nel caso in cui sia necessario cambiare il provider di connessione, dovrà scegliere l'opzione Scollega DB. Questa operazione scollega il database attuale e ti permetterà di configurare una nuova connessione con un altro provider.

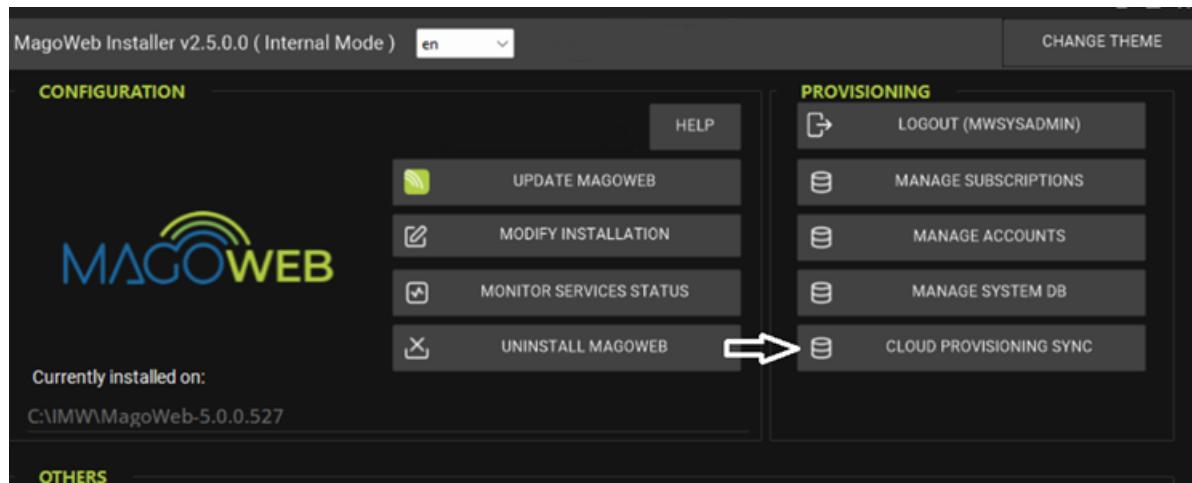
Sincronizzazione dati dal Cloud Provisioning

In caso di utilizzo di un'istanza di MagoWeb di versioni precedente alla 5.0, si rende necessario sincronizzare tutti i dati ad essa correllati ed attualmente memorizzati negli archivi del Provisioning in Cloud.

Nota: si ricorda che la sincronizzazione dati dal Provisioning Cloud viene eseguita automaticamente in coda al Wizard di configurazione del database di sistema.



La sincronizzazione dei dati può essere ripetuta tramite l'opzione Cloud Provisioning SYNC.



Quest'operazione è utile quando si desidera aggiornare i dati in locale con quelli presenti nel sistema di Provisioning in Cloud.

Se durante il processo di sincronizzazione si verificano conflitti con i dati esistenti, l'azione di Sync ne evita la sovrascrittura per non perdere informazioni importanti.

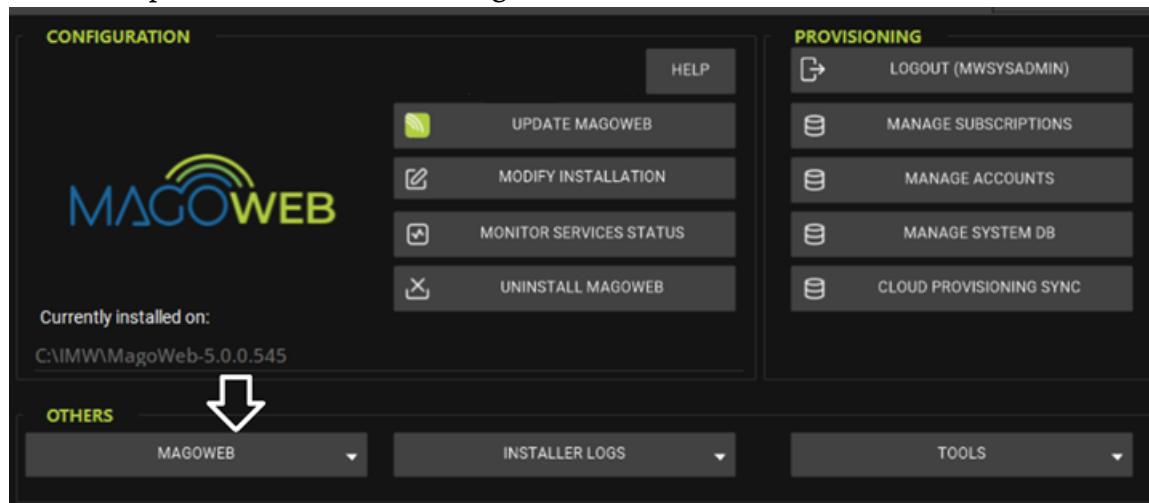
Gli accounts sono sincronizzati previa eliminazione di alcuni dati ritenuti sensibili, quali e-mail, full name e password.

Tramite la funzionalità “Reset password for all accounts” il Sys-Admin pre-impostare una password temporanea per tutti in un solo passaggio, affinché gli accounts stessi possano accedere al programma agevolmente.

Accesso a MagoWeb e configurazione del Two-Factor Authentication

Accesso a MagoWeb

Dalla console posizionandosi su Others-MagoWeb verrà aperto un menu a tendina. Cliccando Open Client si aprirà il browser della MagoWeb Autenticazione:





Autenticazione:

Una volta aperto il browser MagoWeb, verrà richiesto di inserire il nome utente e la password:



Dopo aver inserito le credenziali, il sistema chiederà di selezionare la sottoscrizione a cui si desidera accedere:

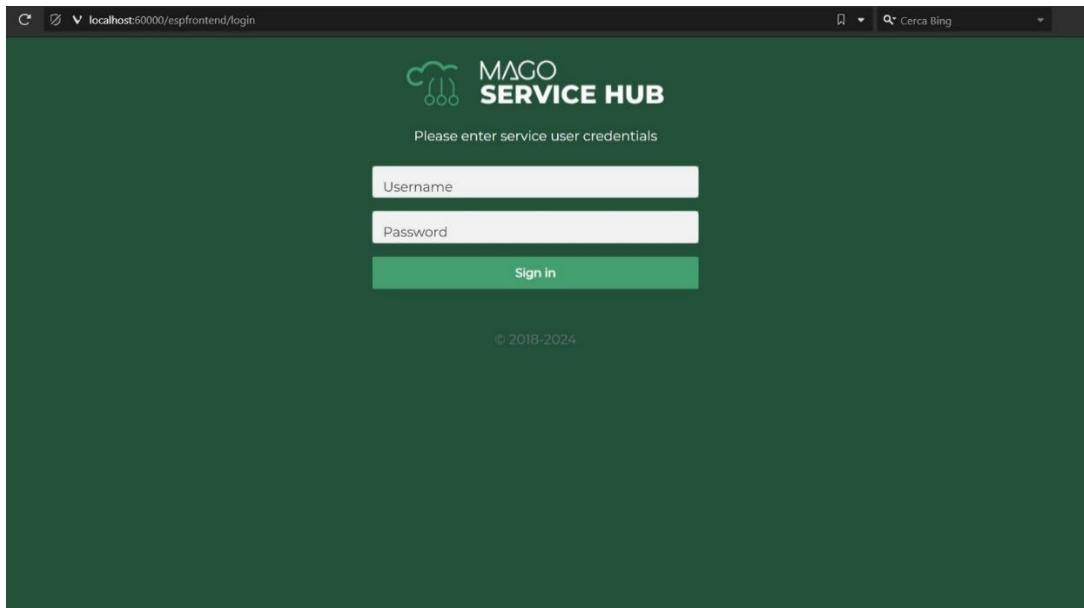


Dopo aver selezionato la sottoscrizione, clicca su Accedi per entrare nel sistema.



Accesso a MSH

L'opzione “Apri frontend di MSH” apre il frontend di MSH sul browser di default



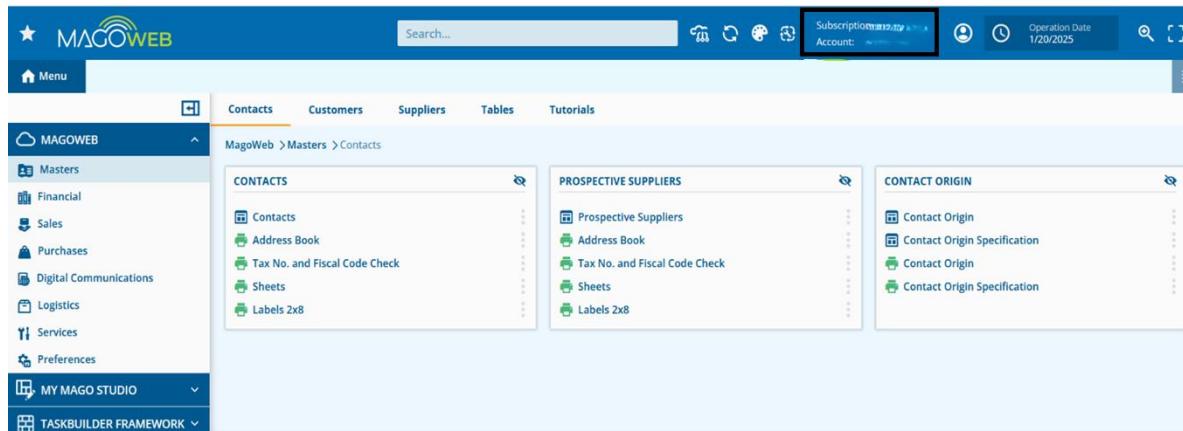
Nota: l'accesso al Frontend di MSH avviene con le stesse credenziali che si utilizzano per accedere allo Store di Mago, a differenza di Mago4 non è presente un'utenza di servizio per MSH.



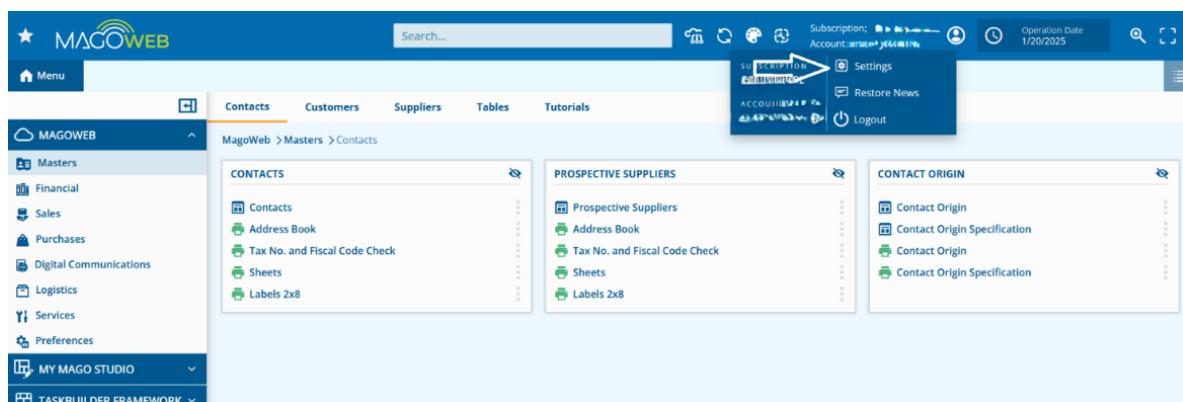
Gestione delle impostazioni dell'account

Visualizzazione e modifica delle impostazioni:

Eseguito l'accesso in MagoWeb, verranno riportati i dettagli relativi alla tua sottoscrizione e utente.

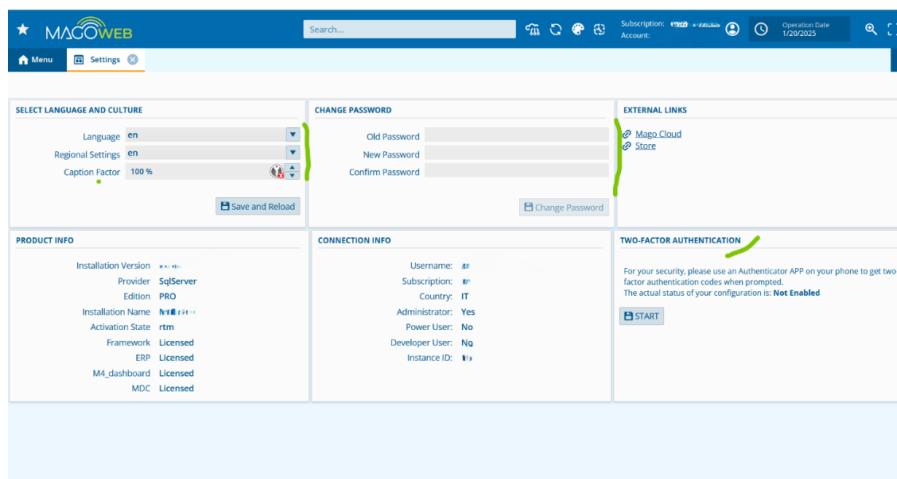


Per accedere alle impostazioni del tuo account, clicca su Informazioni Account e poi su Settings.



In questa sezione potrai:

- Cambiare la lingua del sistema.
- Modificare la password dell'account.
- Abilitare la Two-Factor Authentication (2FA).



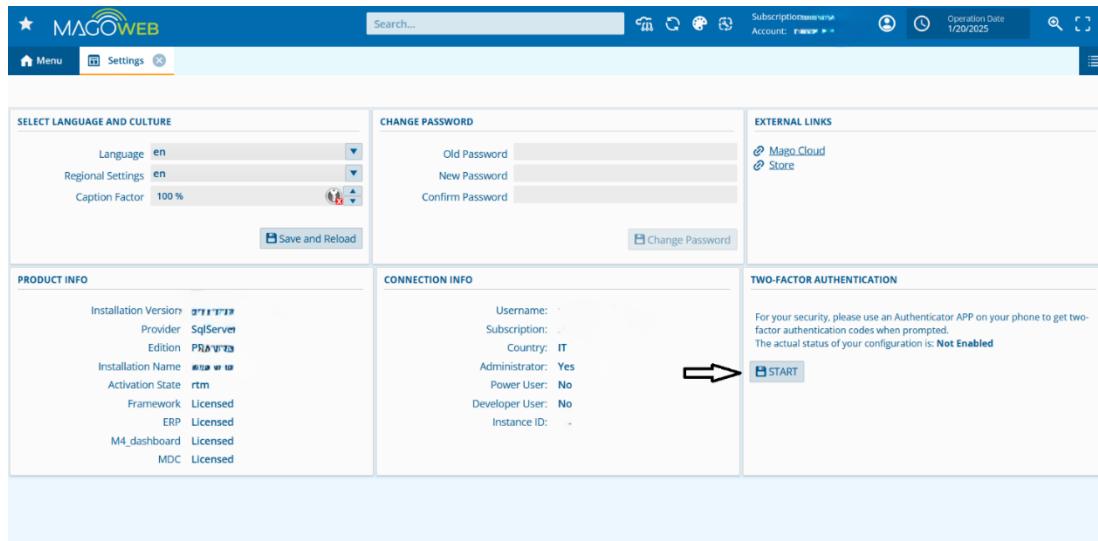


Abilitazione della Two-Factor Authentication (2FA)

Nota: in MagoWeb l'unico tipo di autenticazione ammesso per il 2FA è via TOTP, quindi tramite l'utilizzo di un'app di autenticazione.

Iniziare il processo di abilitazione:

Nella schermata delle impostazioni dell'account, clicca su Start per iniziare la configurazione della 2FA.



SELECT LANGUAGE AND CULTURE

Language: en
Regional Settings: en
Caption Factor: 100 %

CHANGE PASSWORD

Old Password
New Password
Confirm Password

EXTERNAL LINKS

MagoCloud
Store

PRODUCT INFO

Installation Version: 2024.1.1
Provider:SqlServer
Edition: PRO
Installation Name: MagoWeb
Activation State: rtm
Framework: Licensed
ERP: Licensed
M4_dashboard: Licensed
MDC: Licensed

CONNECTION INFO

Username: af
Subscription: af
Country: IT
Administrator: Yes
Power User: No
Developer User: No
Instance ID: af

TWO-FACTOR AUTHENTICATION

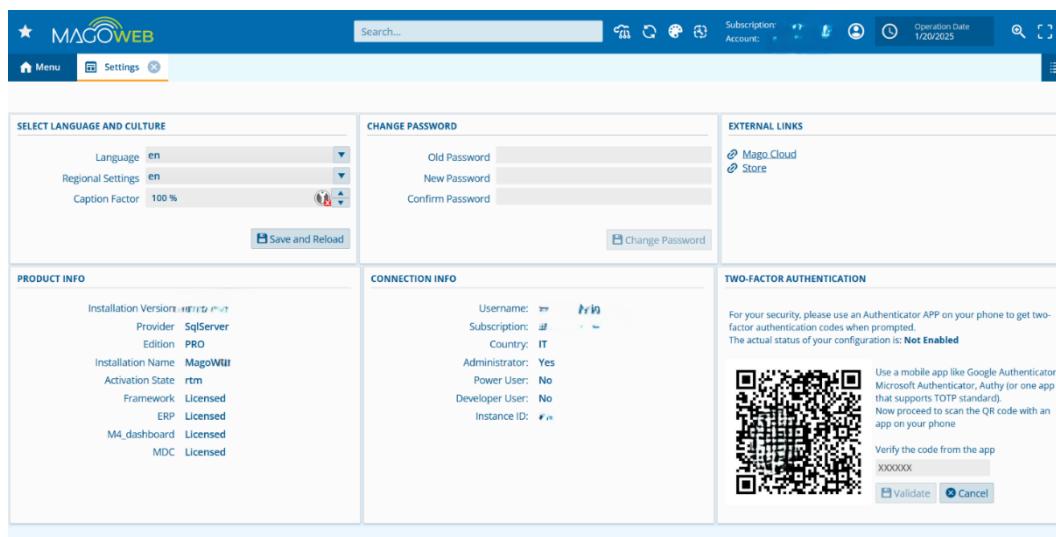
For your security, please use an Authenticator APP on your phone to get two-factor authentication codes when prompted.
The actual status of your configuration is: **Not Enabled**

START

Scansione del QR code:

Una volta avviato il processo, verrà mostrato un QR code sullo schermo.

Usa un'app di autenticazione (come Google Authenticator, Microsoft Authenticator, Authy o altre app compatibili con il sistema TOTP) per scansionare il QR code.



SELECT LANGUAGE AND CULTURE

Language: en
Regional Settings: en
Caption Factor: 100 %

CHANGE PASSWORD

Old Password
New Password
Confirm Password

EXTERNAL LINKS

MagoCloud
Store

PRODUCT INFO

Installation Version: 2024.1.1
Provider:SqlServer
Edition: PRO
Installation Name: MagoWeb
Activation State: rtm
Framework: Licensed
ERP: Licensed
M4_dashboard: Licensed
MDC: Licensed

CONNECTION INFO

Username: af
Subscription: af
Country: IT
Administrator: Yes
Power User: No
Developer User: No
Instance ID: af

TWO-FACTOR AUTHENTICATION

For your security, please use an Authenticator APP on your phone to get two-factor authentication codes when prompted.
The actual status of your configuration is: **Not Enabled**

Use a mobile app like Google Authenticator, Microsoft Authenticator, Authy (or one app that supports TOTP standard).
Now proceed to scan the QR code with an app on your phone

Verify the code from the app
XXXXXX

Validate **Cancel**

Verifica del codice OTP:

Dopo aver scansionato il QR code, l'app mobile genererà un codice temporaneo (OTP - One Time Password).



Inserisci il codice visualizzato nell'app e clicca su Valida per completare l'attivazione della Two-Factor Authentication.

Accesso futuro con Two-Factor Authentication attiva

Dopo aver abilitato la 2FA, la prossima volta che accederai a MagoWeb, oltre a inserire il nome utente e la password, dovrà inserire anche il codice OTP generato dall'app di autenticazione.



Questo codice temporaneo cambierà ogni 30 secondi e verrà generato automaticamente dall'app che hai configurato, garantendo un'ulteriore protezione al tuo account.

Disabilitazione della Two-Factor Authentication

Disattivazione della 2FA:

Se in seguito desideri disabilitare la Two-Factor Authentication, il Sys-Admin (amministratore del sistema) avrà la possibilità di disattivarla per te, se necessario.



Manage Accounts

CREATE NEW... RESET PASSWORD FOR ALL ACCOUNTS

RESET PASSWORD RESET TWO FACTOR AUTHENTICATION (with arrow pointing to the right)

ACCOUNT INFORMATION

Full name: <input type="text" value="Michele Zucchiatti"/>	Expiration date: <input type="text" value="21/02/2025"/>
Email: <input type="text" value="michele.zucchiatti@zucchetti.com"/>	Password expiration date: <input type="text" value="14/07/2025"/>
Language: <input type="text" value="English"/>	Login count failed: <input type="text" value="-1"/>
Regional settings: <input type="text" value="English"/>	<input type="checkbox"/> Disabled <input type="checkbox"/> Locked <input type="checkbox"/> Must change password
Notes: <input type="text" value="Verifica 1"/>	Roles: <input type="checkbox"/> ESP-ADMIN
Two FA Authentication (TOTP): <input checked="checked" type="checkbox" value="Enabled"/>	

ASSOCIATED TO THE FOLLOWING SUBSCRIPTIONS

	Subscription key	Description
Delete	SL2021-J2022	

DELETE SAVE CANCEL

Questo passaggio deve essere effettuato dal Sys-Admin che ha i privilegi necessari per modificare le impostazioni di sicurezza dell'account.

Appendice A

Dettagli su creazione applicazione Microsoft per Oauth

1. Registrazione

In fase di registrazione dell'applicazione, vi verrà chiesto di esplorare un 'Redirect URI' / 'URI di reindirizzamento autorizzato' (vedere Figura 1).

Specificare l'indirizzo: <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).

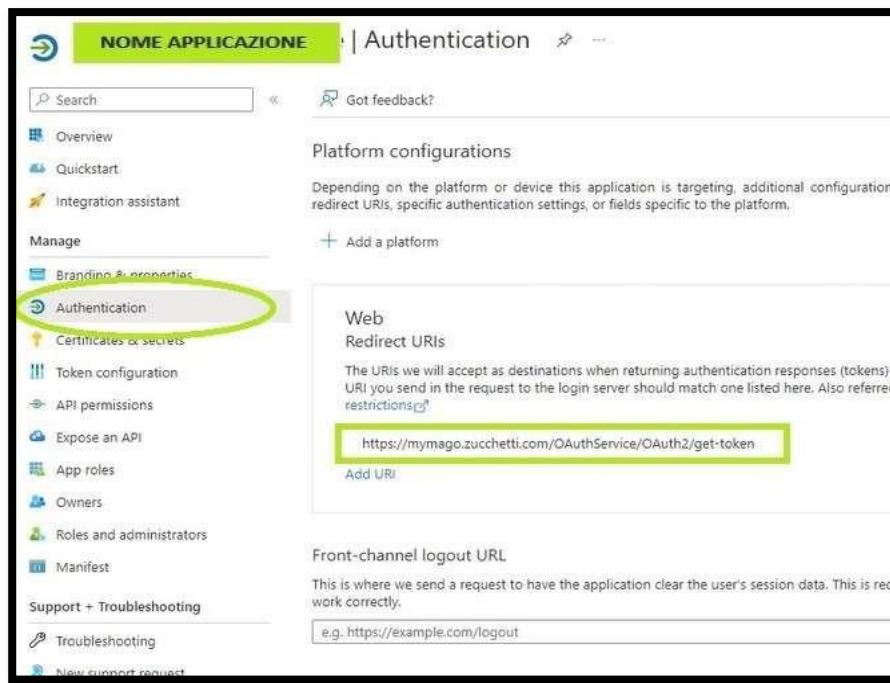
Supported account types
Who can use this application or access this API?
 Accounts in this organizational directory only (Zucchetti - Tenant Lab only - Single tenant)
 Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
 Accounts in any organizational directory (Any 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.

Figura 1



Nel caso in cui non si sia settato in creazione, è possibile esplicitare lo stesso valore nella sezione 'Authentication'/'Autenticazione', aggiungendo un nuovo URI (pulsante Add URI, vedi Figura 2)



The screenshot shows the Azure portal interface for managing an application. The left sidebar lists various application settings: Branding & properties, Authentication (circled in green), Certificates & secrets, Token configuration, API permissions, Expose an API, App roles, Owners, Roles and administrators, Manifest, Support + Troubleshooting, Troubleshooting, and New support request. The main content area is titled 'Authentication' and shows 'Platform configurations' with a note about redirect URIs. The 'Web' tab is selected, and the 'Redirect URIs' section contains the URL <https://mymago.zucchetti.com/AuthService/OAuth2/get-token>, which is highlighted with a green box. Below this, the 'Front-channel logout URL' section is shown with the placeholder 'e.g. https://example.com/logout'.

Figura 2



2. Parametri da salvare

I parametri richiesti nel MagoWebInstaller sono i seguenti:

- Client ID: potreste trovarlo chiamato ID Cliente, Application ID oppure ID Applicazione (vedere Figura 3).
- Tenant ID: potreste trovarlo chiamato Directory ID. (vedere Figura 3).

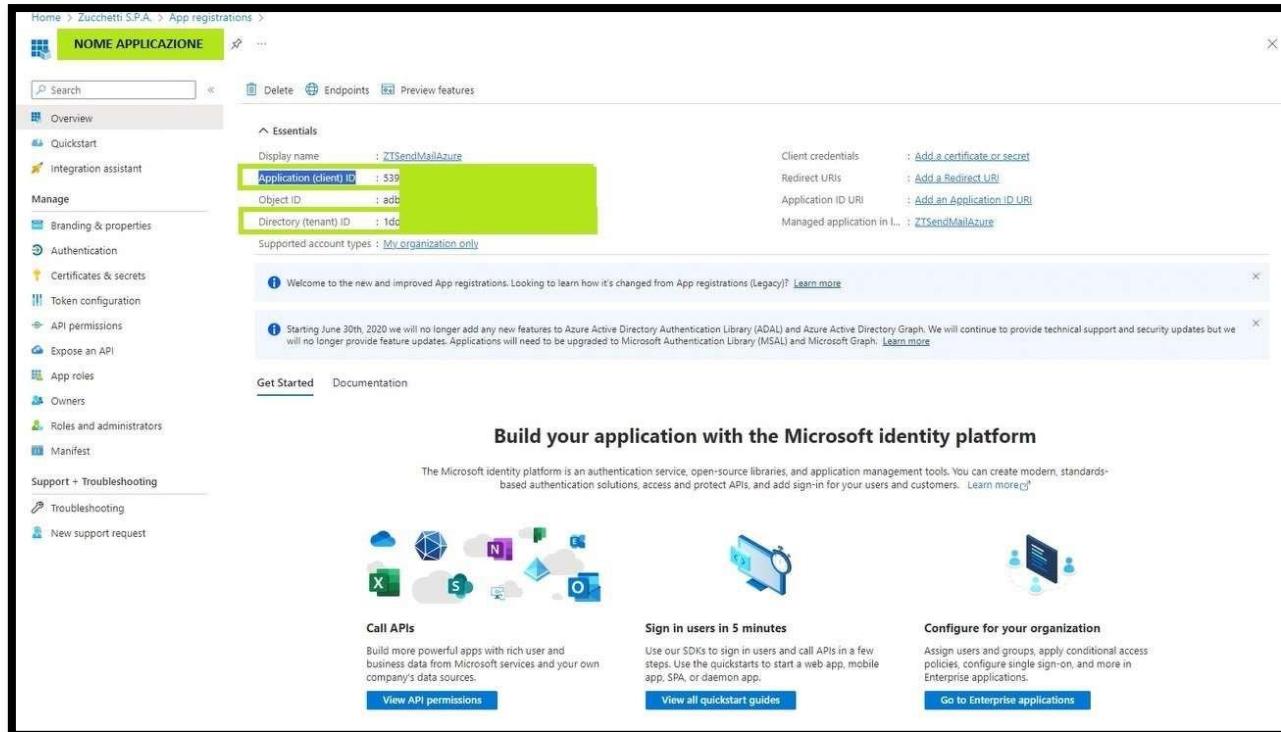


Figura 3

- Client Secret: corrisponde al 'Value'/'Valore' inquadrato in verde.
- Nella sezione 'Certificati e segreti', creare un nuovo segreto cliccando sul tasto cerchiato in verde in Figura 4. Si aprirà una barra laterale in cui esplicitare la durata del segreto. La scelta è libera, essendo consapevoli che ad ogni scadenza, un nuovo segreto andrà rigenerato e cambiato nei parametri del MagoWebInstaller.

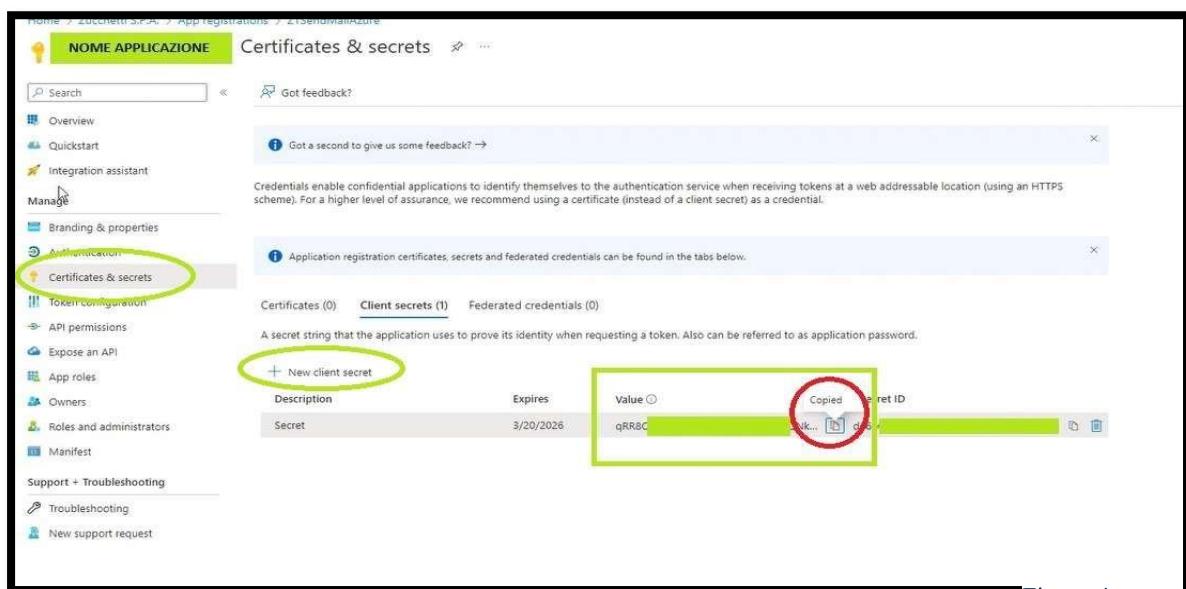
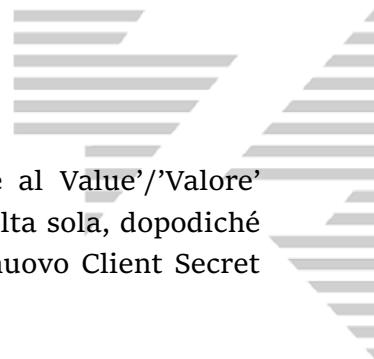


Figura 4

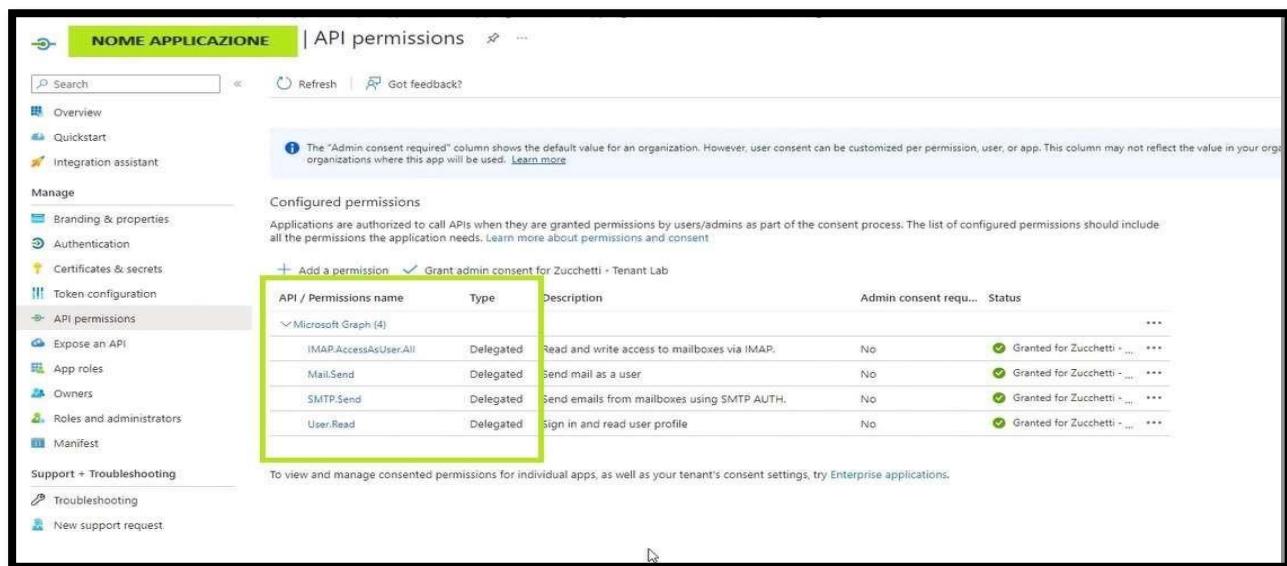


Il Client Secret da inserire nei parametri del MagoWebInstaller corrisponde al Value'/'Valore' inquadrato in verde. Fare attenzione che questo valore lo si può copiare una volta sola, dopodiché diventerà illeggibile. L'unico modo per avere un client secret sarà creare un nuovo Client Secret interamente.

3. Permissions/Permessi

L'elenco completo dei permessi necessari è il seguente:

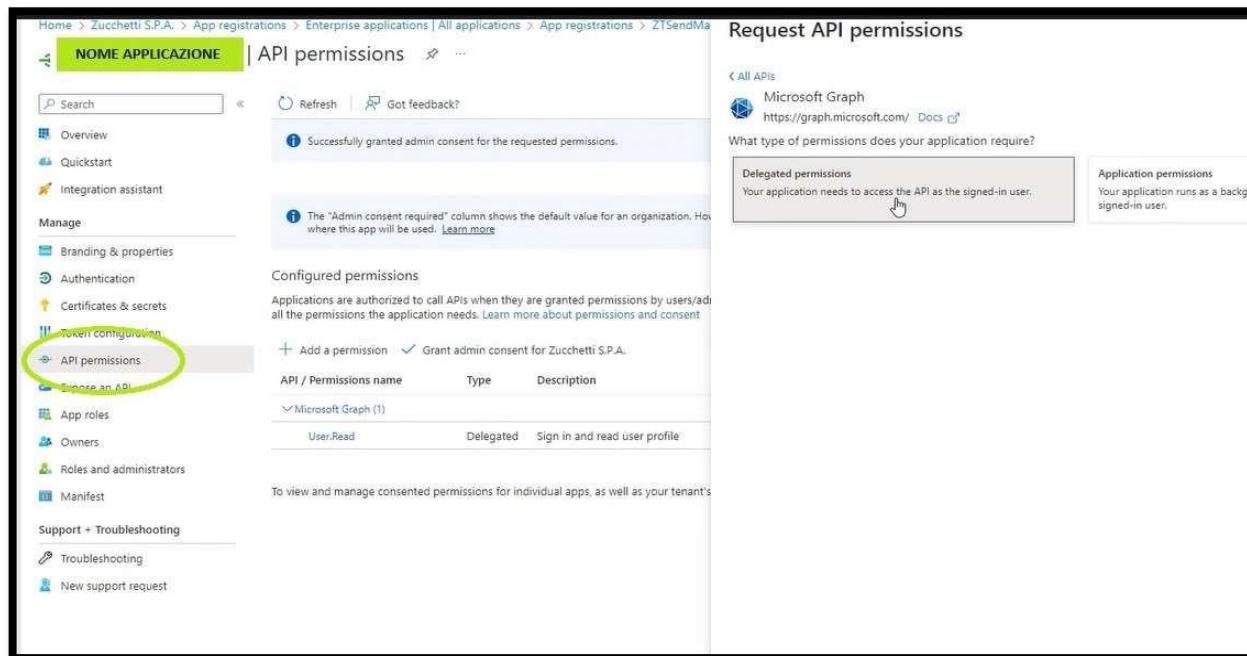
- IMAP.AccessAsUser.All
- Mail.Send
- SMTP.Send
- User.Read



API / Permissions name	Type	Description	Admin consent requ...	Status
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 - ... ***

Figura 5

Nella sezione 'API permissions' bisognerà aggiungere i permessi necessari all'invio e-mail. Cliccare sul pulsante 'add permission', scegliere 'Microsoft Graph' e 'Delegated permissions' (vedere Figura 6)



Request API permissions

Successfully granted admin consent for the requested permissions.

The "Admin consent required" column shows the default value for an organization. How where this app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admin 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

Delegated permissions

Application permissions

Your application runs as a background signed-in user.

Figura 6



Un esempio di ricerca è la Figura 7, in cui viene ricercato la permission 'mail.Send'.

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](#)

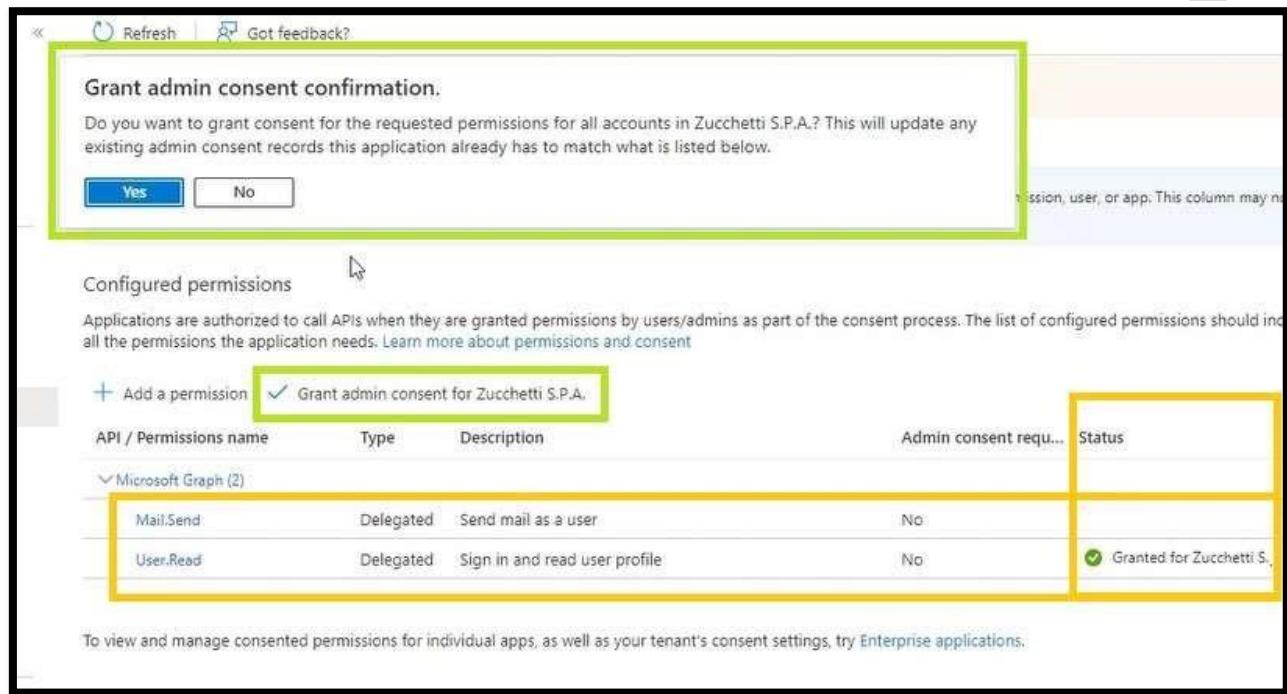
Permission	Admin consent required
ChannelMessage	No
ChatMessage	No
Mail (1)	
<input checked="" type="checkbox"/> Mail.Send ⓘ Send mail as a user	No
<input type="checkbox"/> Mail.Send.Shared ⓘ Send mail on behalf of others	No
SMTP	
<input type="checkbox"/> SMTP.Send ⓘ Send emails from mailboxes using SMTP AUTH.	No
TeamsActivity	
VirtualAppointmentNotification	

Add permissions **Discard**

Figura 7

Una volta aggiunto il permesso, sarà necessario conferirgli il 'consenso', ovvero cliccare sul tasto inquadrato 'Grant admin consent ...' e dare conferma (vedere figura 8).

Nei riquadri in giallo si potrà notare la differenza di stato tra un permesso concesso e uno non ancora.



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 include 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	<input checked="" type="checkbox"/> Granted for Zucchetti S.P.A.

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

Figura 8



Appendice B

Esposizione in rete di MagoWeb

Per la configurazione di rete al fine di esporre pubblicamente MagoWeb per raggiungerlo dall'esterno queste sono le configurazioni indicate in linea di massima.

1. Inserire IP/DNS pubblico del server alla voce hostname dell'installer di MagoWeb
2. Lato firewall abilitare delle regole in ingresso che accettino le chiamate verso il server dai client che effettuano la login a MagoWeb, avendo cura di aprire le porte comprese nell'intervallo 60000 - 60300, con una regola di questo tipo: ES:
 - Tipo: Tutte le regole TCP (o tutto il traffico)
 - Protocollo: tutti i protocolli
 - Intervallo Porte: 60000 - 60300
 - Origine: ip client/32
3. In uscita tutte le chiamate devono essere aperte con una regola di questo tipo:
 - Tipo: Tutte le regole TCP (o tutto il traffico)
 - Protocollo: tutti i protocolli
 - Intervallo Porte: Tutte
 - Destinazione: 0.0.0.0/0
4. Impostare una regola in ingresso per cui siano consentite anche le chiamate dall'IP pubblico/privato stesso della macchina server:
 - Tipo: Tutte le regole TCP (o tutto il traffico)
 - Protocollo: tutti i protocolli
 - Intervallo Porte: 60000 - 60300
 - Origine: ip server/32

Un'alternativa è quella di censire un DNS interno e uno esterno. Cioè, indicare nel file di host del server, l'indirizzo Ip privato e il nome dns registrato; nella gestione del server DNS esterno, censire il medesimo DNS e assegnargli l'ip pubblico dell'host.

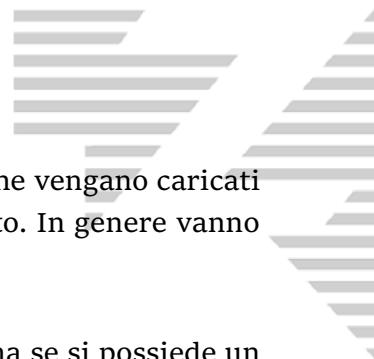
Nota: Queste sono indicazioni di massima, specifici parametri o configurazioni possono variare in base alla struttura della rete dove è presente MagoWeb.

Appendice C

Configurazione certificati

In generale è possibile utilizzare qualsiasi tipo di certificato che rientri nei formati supportati (*.pem, *.crt, *.der, *.cer, *.ca-bundle, *.p7b, *.p7c, *.p7s, *.der, *.pfx, *.p12, *.key).

E quelli non autofirmati generati e rilasciati da una CA valida.



Non esistono integrazioni "ufficiali" lato MagoWeb. All'installer interessa solo che vengano caricati i due file del certificato e che il medesimo sia correttamente installato e validato. In genere vanno bene sia i certificati a pagamento che quelli rilasciati da una Ca pubblica.

In genere i due parametri riferiti alla chiavi private e pubbliche sono separati, ma se si possiede un unico certificato che contiene entrambe le parti pubbliche e private, si può usare anche solo il primo (se il formato è tra quelli consentiti).

I due file indicati vanno caricati alla prima voce, però potrebbe darsi che, se il certificato contenga entrambe le parti (pubbliche e private), non separate, venga letta solo una delle due e quindi viene generato l'errore. Vi sono molte configurazioni possibili e suggeriamo di effettuare diversi test.

Per esempio, per quanto riguarda i certificati generati da Certbot/Let's Encrypt, quello che il cliente/rivenditore può fare, lato installer, è ovviamente quello di selezionare un path sul file system relativamente ai due certificati (ad esempio C:\Users\Administrator\Documents\certificate.cer e C:\Users\Administrator\Documents\certificate.key).

Conversione formato Certificati

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 from 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

Dove reperire i log

I log di Magoweb si trovano nel path impostato in fase di installazione (di default c:\logs), suddivisi in file per i diversi servizi di Magoweb.

I log dell'Installer sono nel percorso C:\Users\user\AppData\Roaming\MagoWebInstaller\Logs



Linee guida generali:

- Potrebbe essere necessario disattivare il firewall durante l'installazione di *Mago Web*.
- Verificare che le porte assegnate ai servizi non siano già impegnate o utilizzate.
- Verificare che UAC sia impostato al valore di Default (2), questo è necessario per la corretta esecuzione degli script di installazione, nel caso non sia stato settato correttamente, comparirà un avviso nell'installer

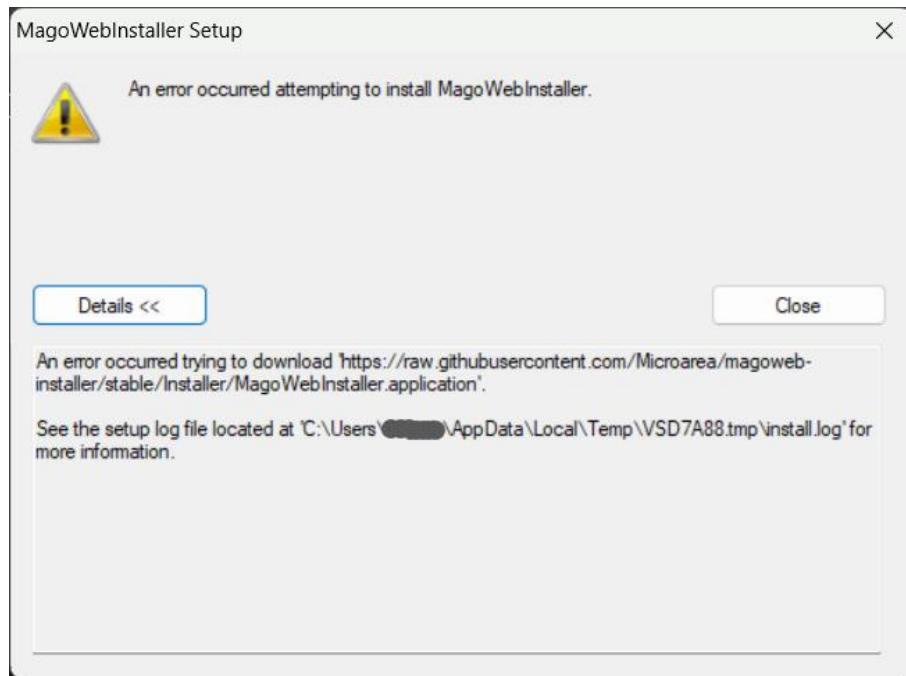
Importante: Dopo ogni modifica apportata sull'interfaccia dell'installer, premere INIZIA per salvare le modifiche.

Importante: All'uscita di una nuova build, scaricare dal sito mymago.zucchetti.com entrambi i pacchetti nuovi, installer e ztds. Per effettuare la procedura di upgrade utilizzare sempre l'installer allineato alla versione che si sta installando/aggiornando.

Importante: Prima di effettuare l'upgrade da una release consecutiva (Es da 1.2 a 1.3) assicurarsi che la voce Usa configurazione esistente non sia flaggato. Vedere anomalia 34747.

Importante: In fase di creazione di un nuovo database memorizzare e conservare le credenziali relative alla parte dbowner, queste saranno necessarie qualora dovessero venire effettuate operazioni di backup/restore sul database server, o migrazioni su provider database (per esempio da postgres a sql, o viceversa). Se vengono inserite credenziali diverse dal display possono comparire errori legati ai permessi.

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



Aprire l'editor del registro di sistema, posizionarsi sul percorso `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings` Verificare la chiave `DisableCachingOfSSLPages` se il valore è 1 impostarlo a 0 Lanciare nuovamente l'installer.

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

Verificare dallo stato dei servizi, dall'interfaccia dell'installatore di Magoweb, che il microservizio `traefik` sia arrivato correttamente e che la porta utilizzata non sia già in uso. Riavviare il servizio corrispondente e riprovare ad accedere. Se il problema persiste, modificare l'installazione e riavviare Start.

Verifica installazione dotnet

Affinché MagoWeb funzioni correttamente è necessario che dotnet e i suoi tool siano installati correttamente. Per verificare che sia così, è possibile fare quanto segue:

- aprire powershell e posizionarsi sulla cartella che contiene l'exe del MagoWeb installer (e quindi Psexec)
- eseguire: `.\psexec -s -i powershell`
- si aprirà una seconda finestra di powershell, qui eseguire: `dotnet ef`

Se la shell disegna l'immagine di un unicorno (<https://learn.microsoft.com/en-us/ef/core/cli/dotnet#verify-installation>), l'installazione è avvenuta con successo. In caso di errore, seguire il workaround indicato nell'anomalia 34337.

Promtail non si avvia



Eliminare il file positions.yaml presente in
C:\ProgramData\scoop\apps\promtail\current\positions.yaml
Riavviare il servizio di Promtail

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

Questo errore si verifica quando durante l'inizializzazione della propria istanza MagoWeb, all'interno dell'interfaccia, alla voce modifica installazione, è stato immesso un codice di istanza (instance key) o un codice sicurezza errato (security value). Reinserrire il security value corretto da modifica installazione e fare clic su INIZIA.

Problema caricamento frontend per versioni anteriori alla 1.4

Può verificarsi su versioni antecedenti alla 1.4 che si verifichi un problema di caricamento del frontend, con il seguente errore: net::ERR_CONTENT_LENGTH_MISMATCH 200 (OK). Anche facendo il refresh della pagina può continuare a ripresentarsi. Il problema è stato corretto dalla versione 1.4 in poi e si risolve aggiornando a questa versione di MagoWeb. Qualora il partner non potesse effettuare l'upgrade a breve, ma solo su programmazione con il cliente, nell'attesa dell'upgrade risolutivo, esiste un workaround temporaneo con delle istruzioni specifiche che risolvono il problema. Contattare il supporto per approfondimenti.