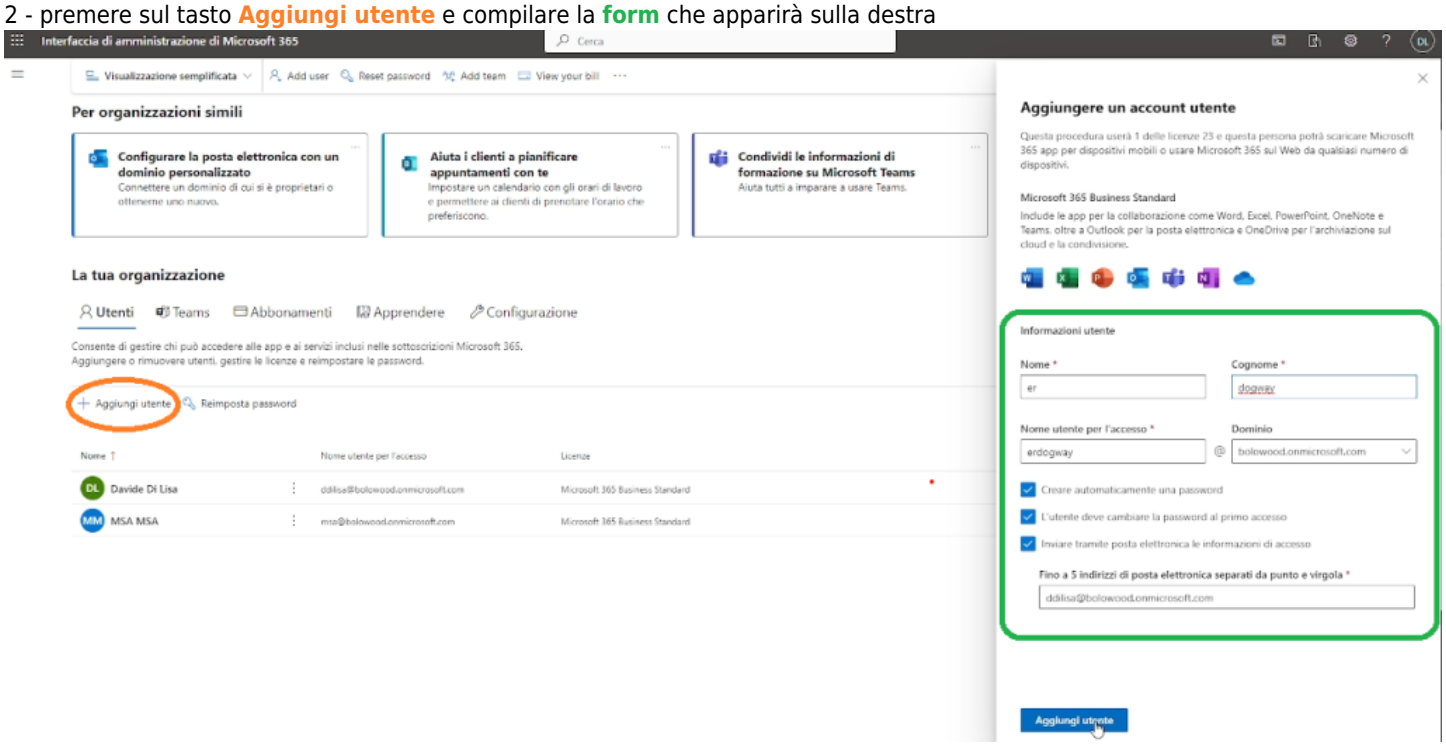
Creazione ed abilitazione nuova casella microsoft tramite Oauth

La procedura presuppone di avere già un account con privilegi da amministratore su https://account.microsoft.com/, di aver già registrato un' app per il dominio e di conoscere il **secret** rilasciato in fase di registrazione per l'applicazione.
La procedura verrà eseguita su una macchina windows.

Effettuare test recupero token application
Per effettuare un test di connessione con l'applicazione, effettuare la seguente curl modificando tutti i parametri tra # con i loro valori corrispondenti.

```
curl --location 'https://login.microsoftonline.com/#TENANT_ID#/oauth2/v2.0/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'client_id=#CLIENT_ID#' \
--data-urlencode 'scope=https://outlook.office365.com/.default' \
--data-urlencode 'client_secret=#CLIENT_SECRET#' \
--data-urlencode 'grant_type=client_credentials'
```

Creazione nuovo account
1 - andare all'indirizzo https://account.microsoft.com/ ed effettuare la login con le credenziali dell'amministratore
2 - premere sul tasto **Aggiungi utente** e compilare la **form** che apparirà sulla destra



3 - modificare o recuperare la password dell'account appena creato

Verificare dati nuovo account
1 - andare all'indirizzo: https://azure.microsoft.com/it-it ed effettuare la login con la mail appena creata
2 - premere su “Gestisci Azure Active Directory” e copiare il **ID_TENANT** che sarà presente nella form al centro
3 - premere su “Registrazioni app” del menu di sinistra e copiare l' “ID applicazione” o **CLIENT_ID** presente a schermo

Abilitare il nuovo account alla ricezione di mail tramite app
1 - aprire PowerShell con privilegi da amministratore
2 - qualora non fossero già importati, importare: Connect-AzureAd e Connect-ExchangeOnline
3 - eseguire: *Connect-AzureAd -Tenant ID_TENANT*
4 - selezionare l'account **amministratore** del dominio nella form di login microsoft
5 - eseguire: *Connect-ExchangeOnline -Organization ID_TENANT*
6 - selezionare l'account **amministratore** del dominio nella form di login microsoft
7 - eseguire: *Get-AzureADServicePrincipal -SearchString NOME_APPLICAZIONE*
8 - salvare i dati dell'applicazione in una variabile: *$MyApp = Get-AzureADServicePrincipal -SearchString NOME_APPLICAZIONE*
9 - eseguire: *Add-MailboxPermission -Identity “INDIRIZZO_MAIL_NUOVO_ACCOUNT” -User $MyApp.ObjectId -AccessRights FullAccess*

link utili https://www.codewrecks.com/post/security/accessing-office-365-imap-with-oauth2

Comandi utili
Get-Mailbox 'emaildaverificare@email.it'
Get-MailboxPermission -Identity 'emaildaverificare@email.it'

Abilitare il nuovo account all'invio di mail tramite app
1 - andare all'indirizzo https://account.microsoft.com/ ed effettuare la login con le credenziali dell'amministratore
2 - andare su Utenti –> Utenti attivi del menu a sinistra
3 - selezionare l'utente per il quale si vuole abilitare l'invio dalla lista e premere su Posta –> Gestisci le applicazioni di posta elettronica
4 - selezionare SMTP authentication e salvare le modifiche
.....

È stata creata una mini-guida per chi dovesse avere difficoltà nell'aggiunta dei vari protocolli di rete per i servizi mail batch.
Lascio il

PDF

allegato in caso fosse necessario.