Azure - Single sign-on

Guide su come creare app in Azure da usare per il Single Sign-on in vtenext

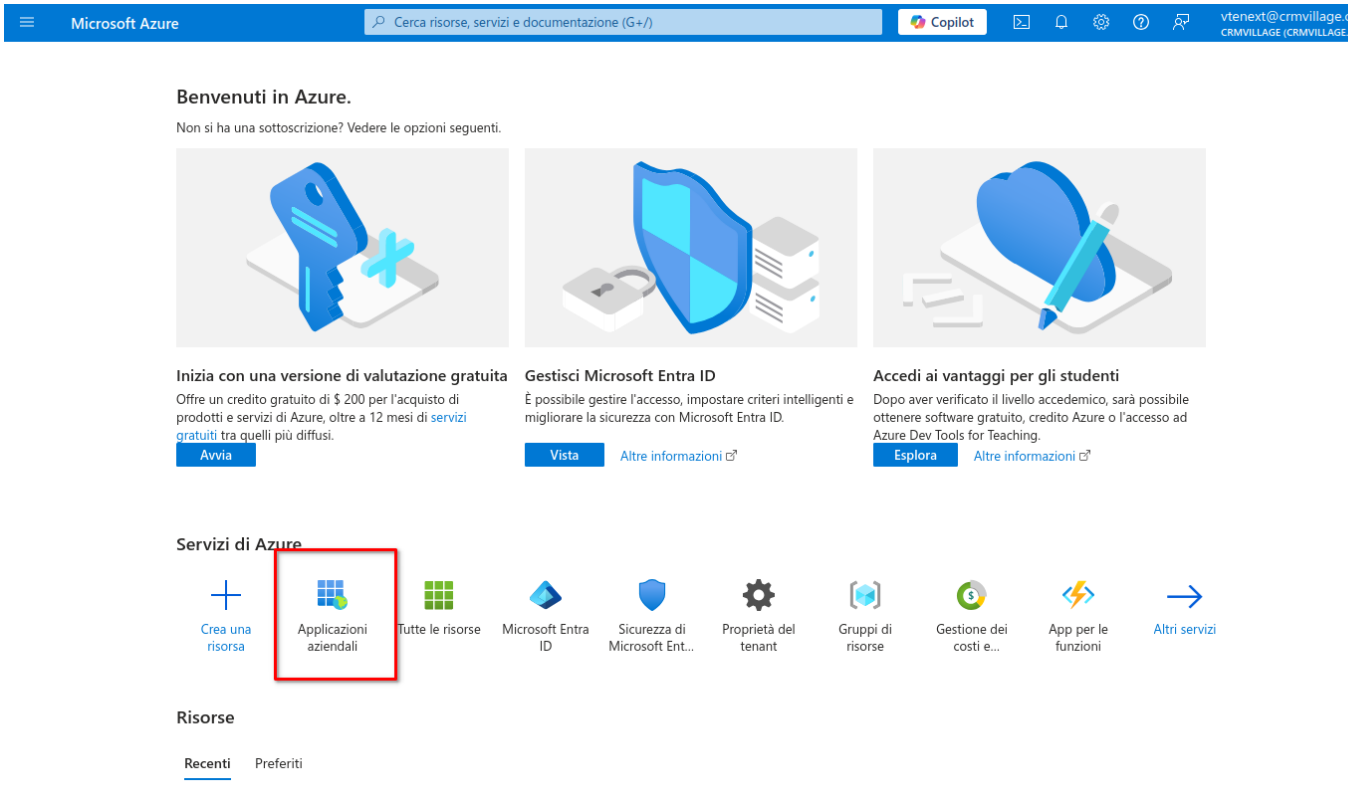
- OIDC (OpenID Connect)
- SAML

OIDC (OpenID Connect)

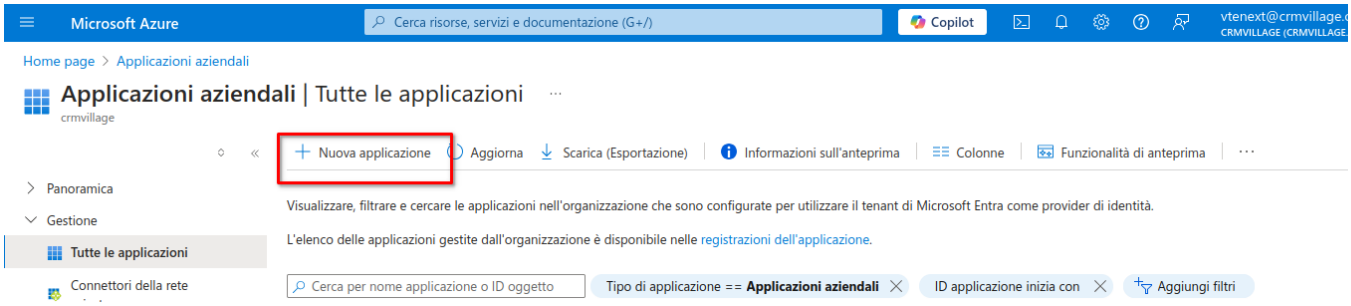
Questa guida mostra come creare un'app in Microsoft Azure, da usare in vtenext per il Single Sign-on, utilizzando il protocollo OpenID Connect.

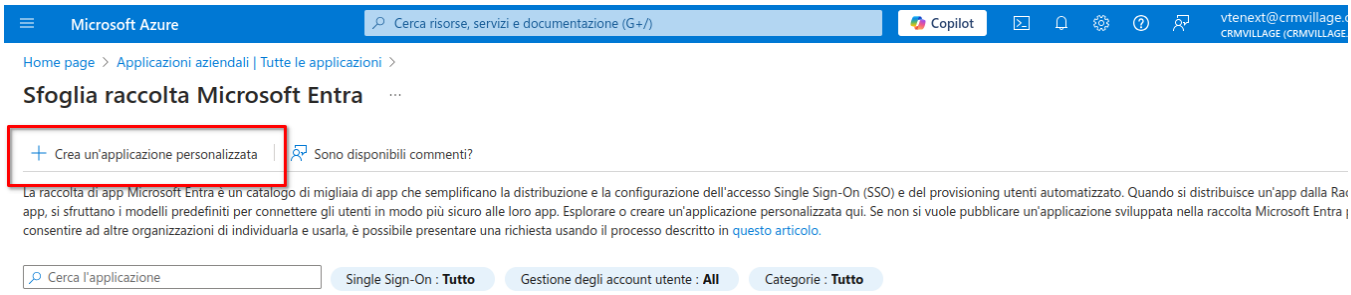
1. Effettuare il login su Azure con una utenza amministrativa: https://portal.azure.com/

2. Cliccare su Applicazioni aziendali:

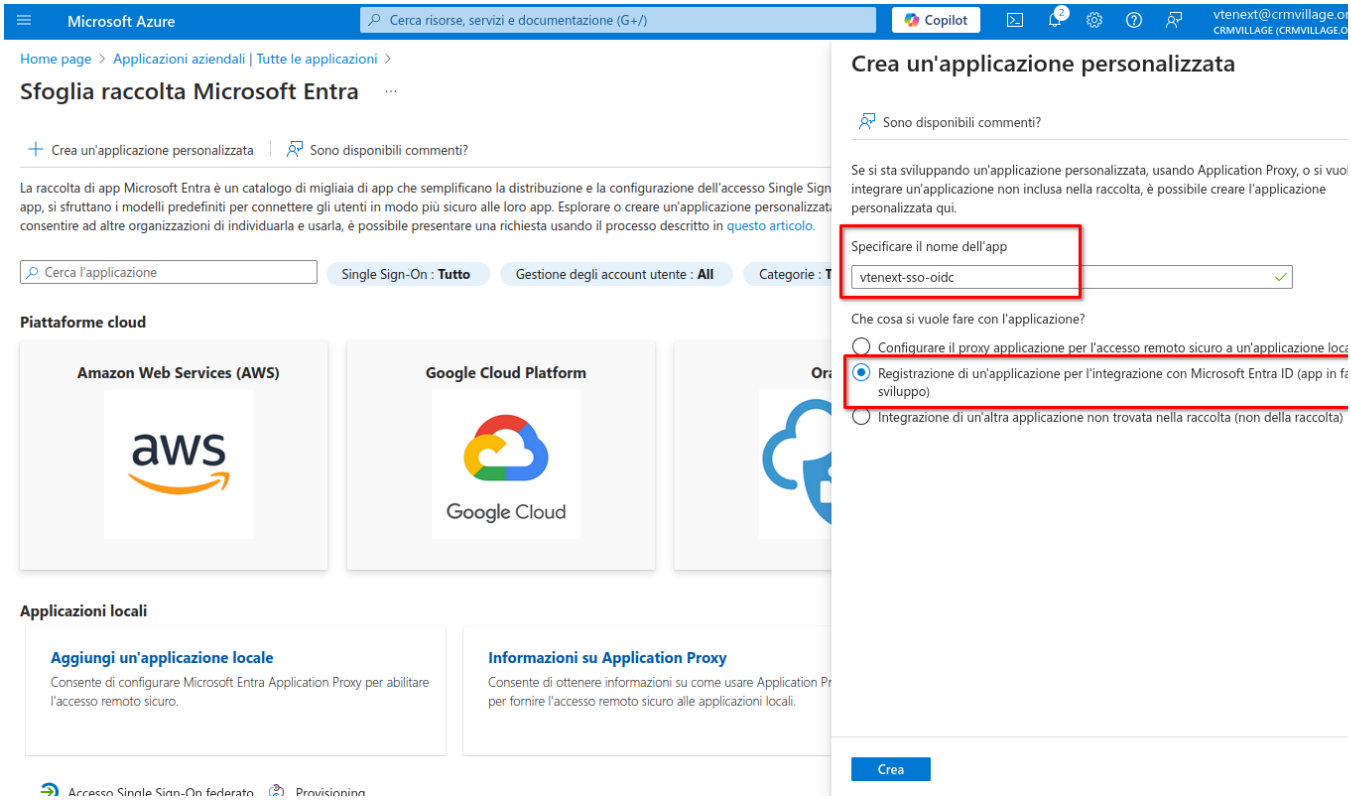


3. Cliccare poi su Nuova applicazione e Crea un'applicazione personalizzata:

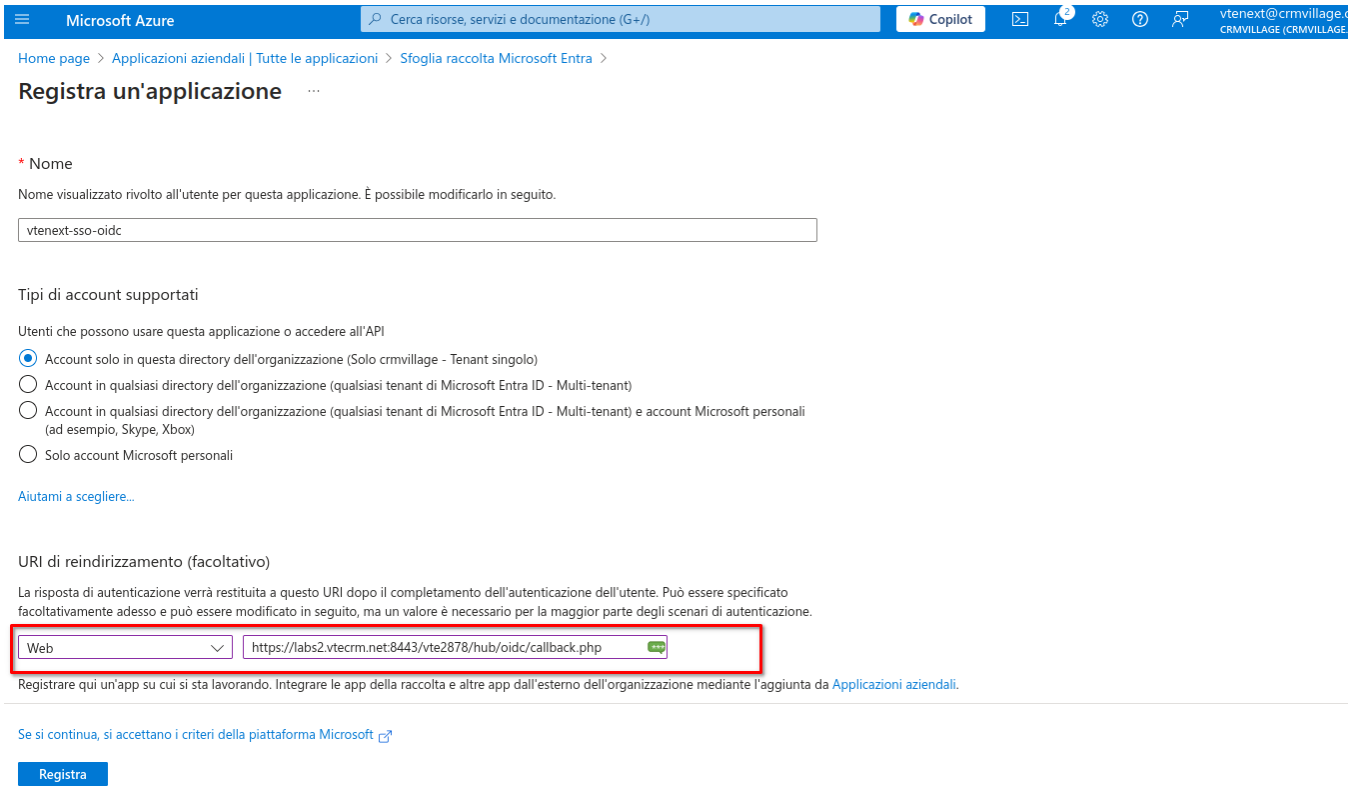


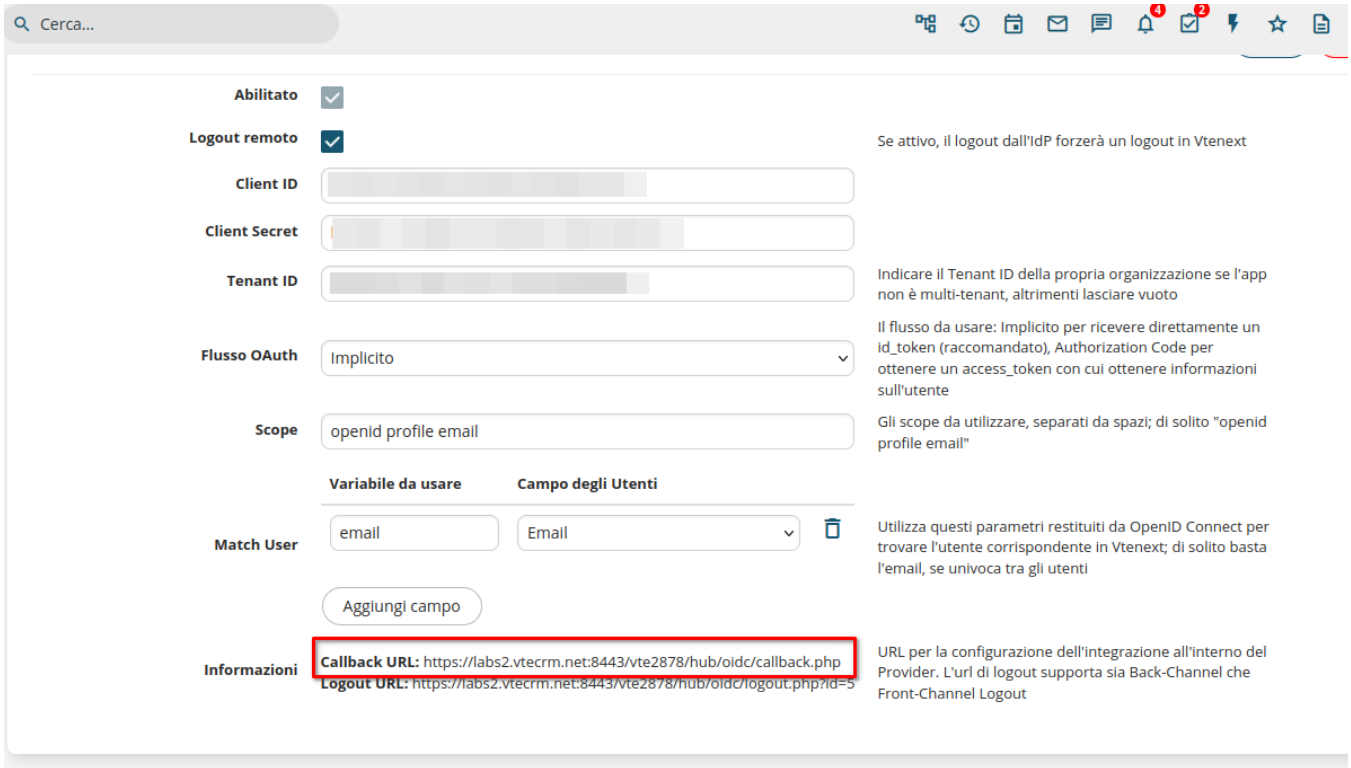


4. Dare un nome all'applicazione, ad esempio "vtenext-sso-oidc", selezionando l'opzione di integrazione con Microsoft Entra ID:

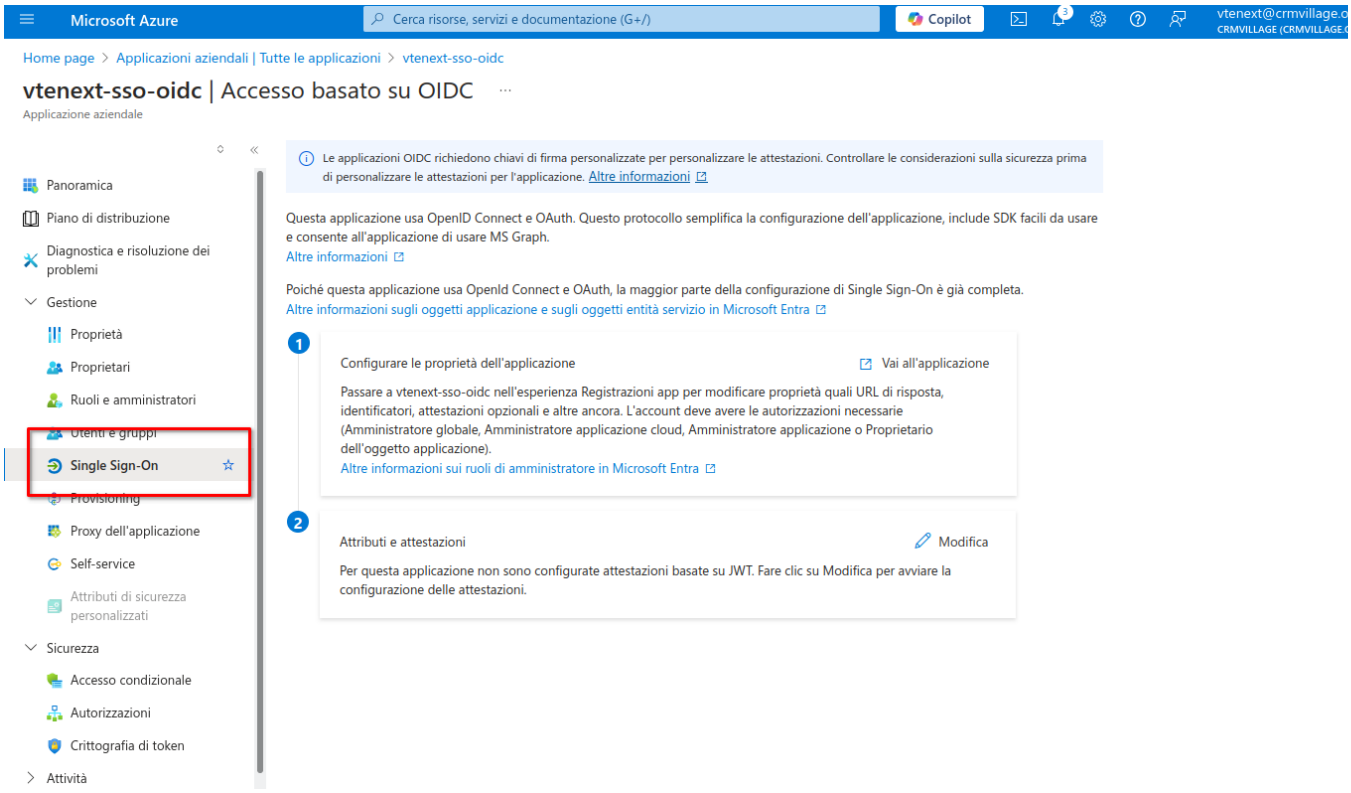


5. Nella schermata successiva impostare Tenant singolo come tipo di account e come URI di reindirizzamento scegliere Web e incollare l'url indicato da Vte nella pagina di configurazione sso:

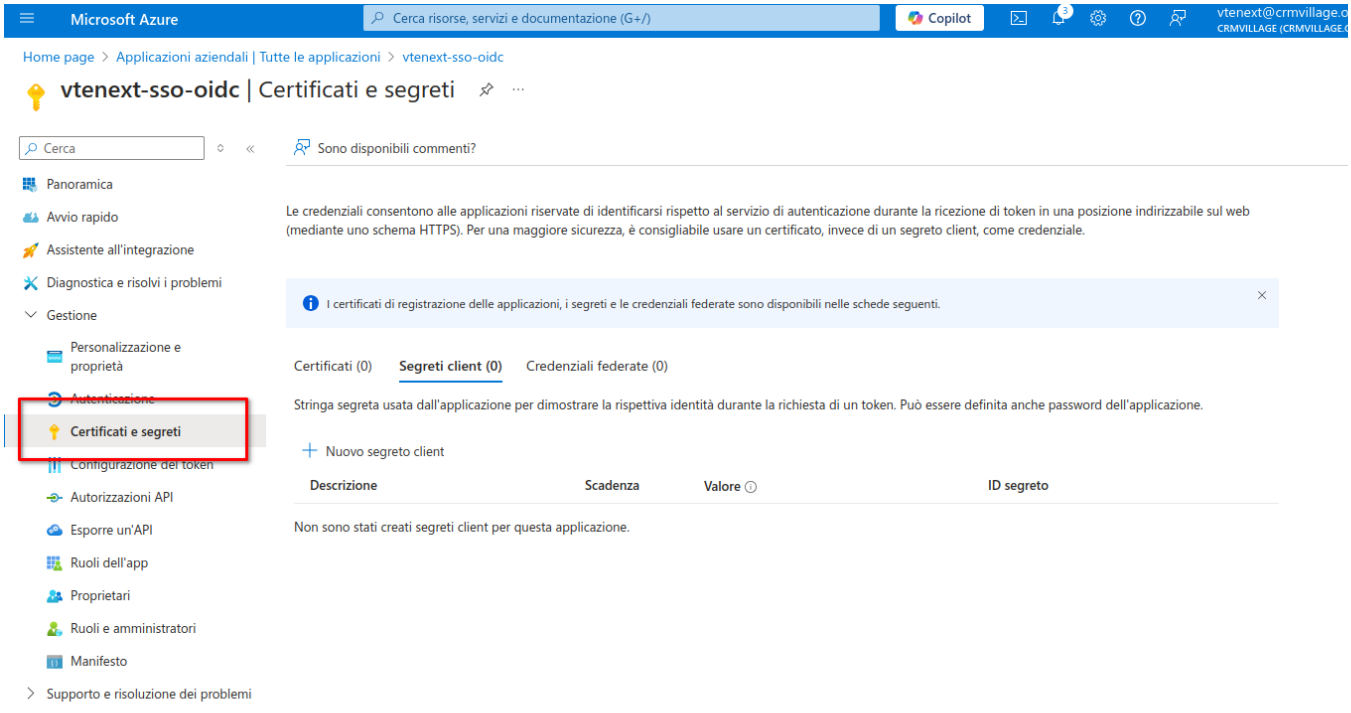




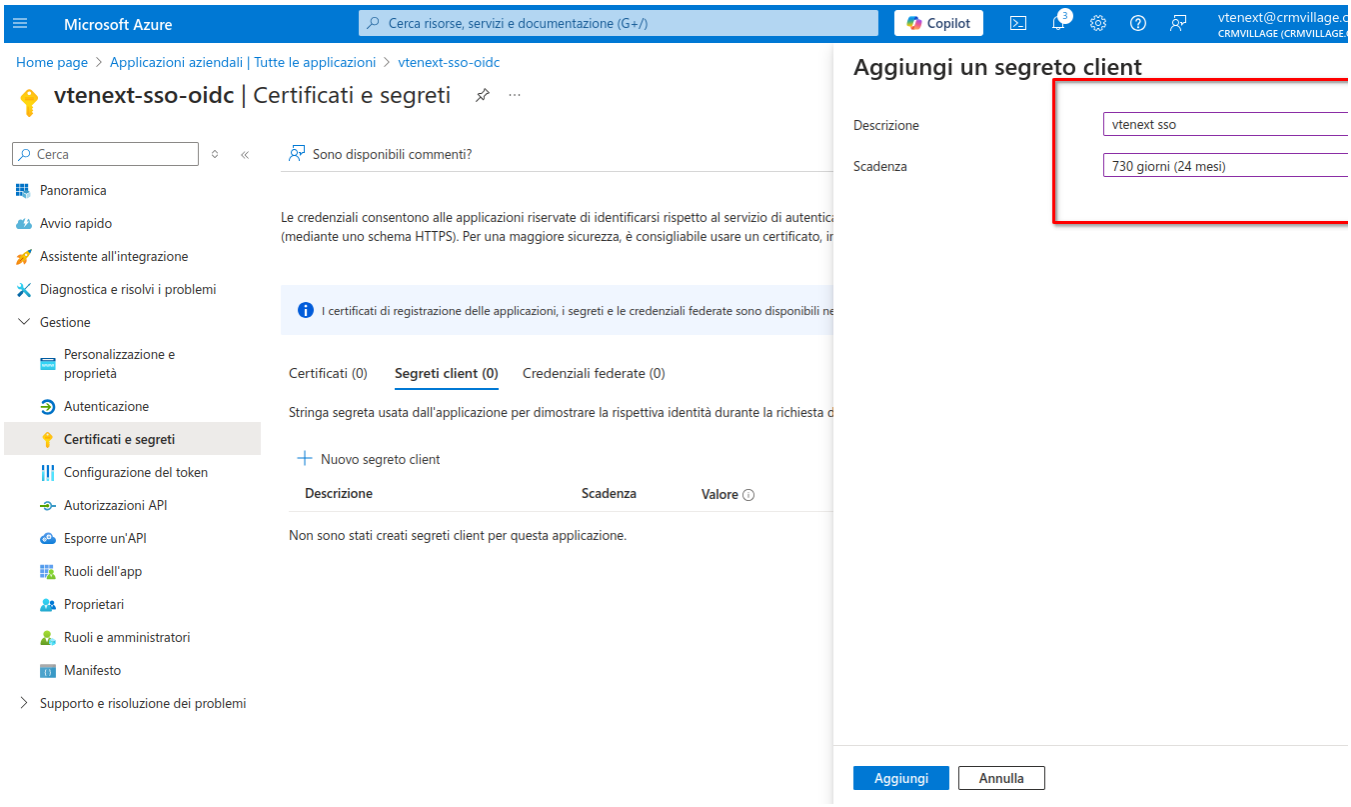
6. Successivamente, navigare a Applicazioni aziendali -> Tutte le applicazioni, selezionare quella appena creata e cliccare su Single Sign-On:



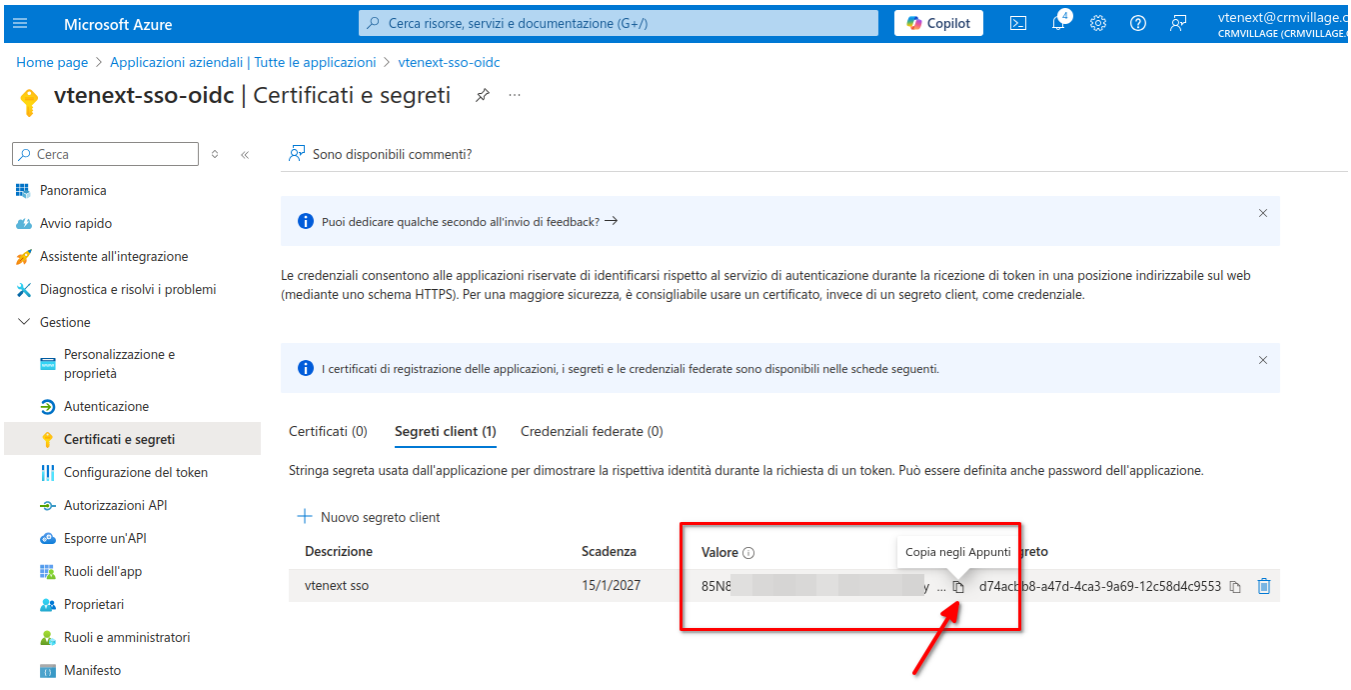
7. Cliccare su "Vai all'applicazione" e poi su "Certificati e segreti":



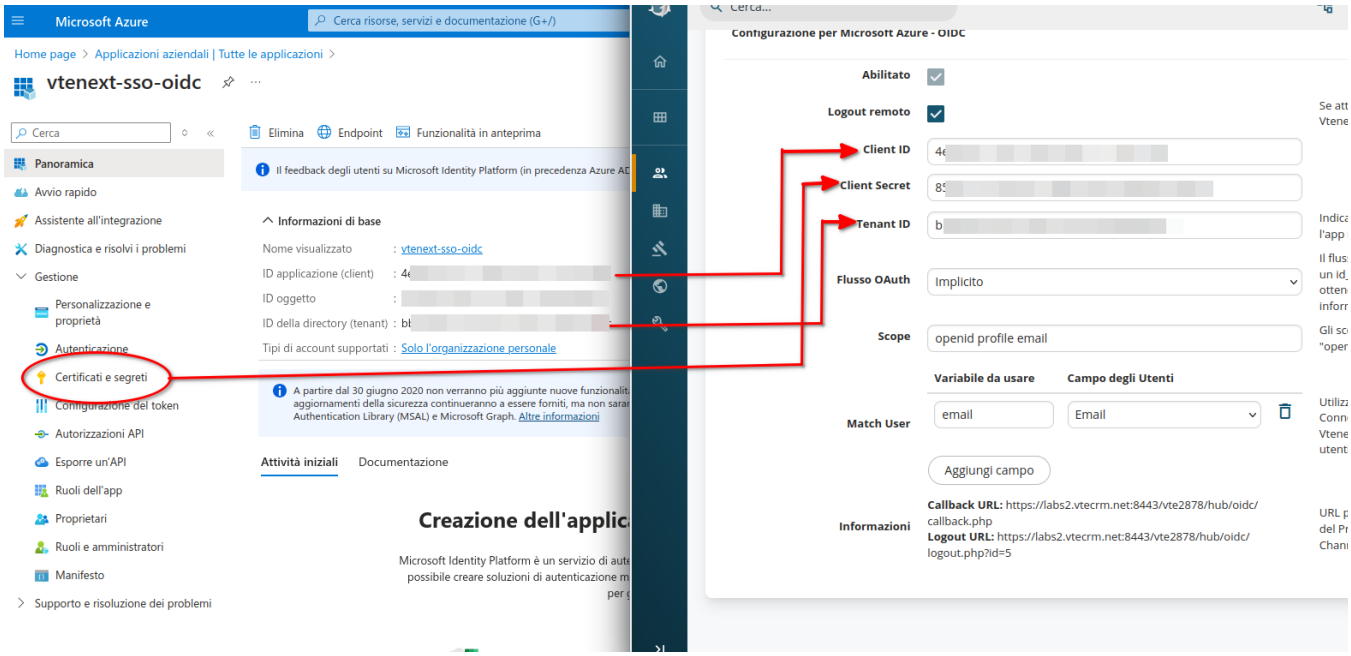
8. Cliccare "Nuovo segreto client" e nella finestra che appare impostare un nome e una scadenza:



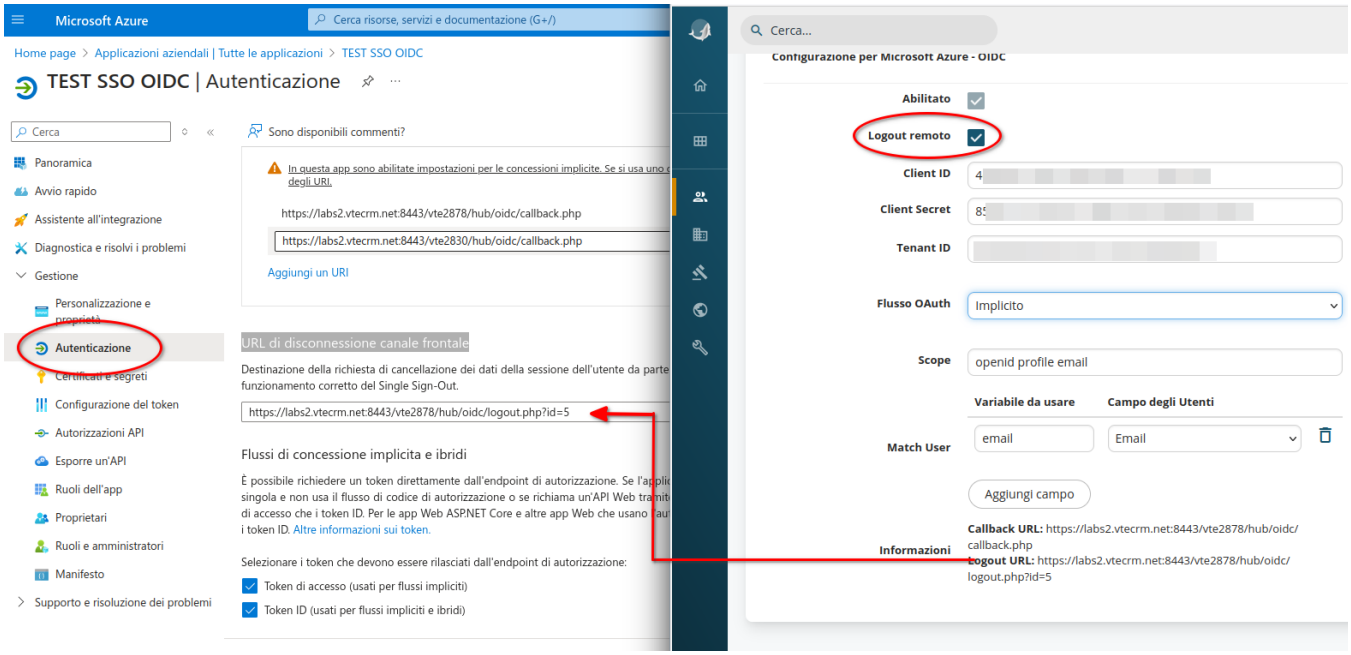
9. Copiare il campo "Valore" della chiave segreta e tenerlo da parte



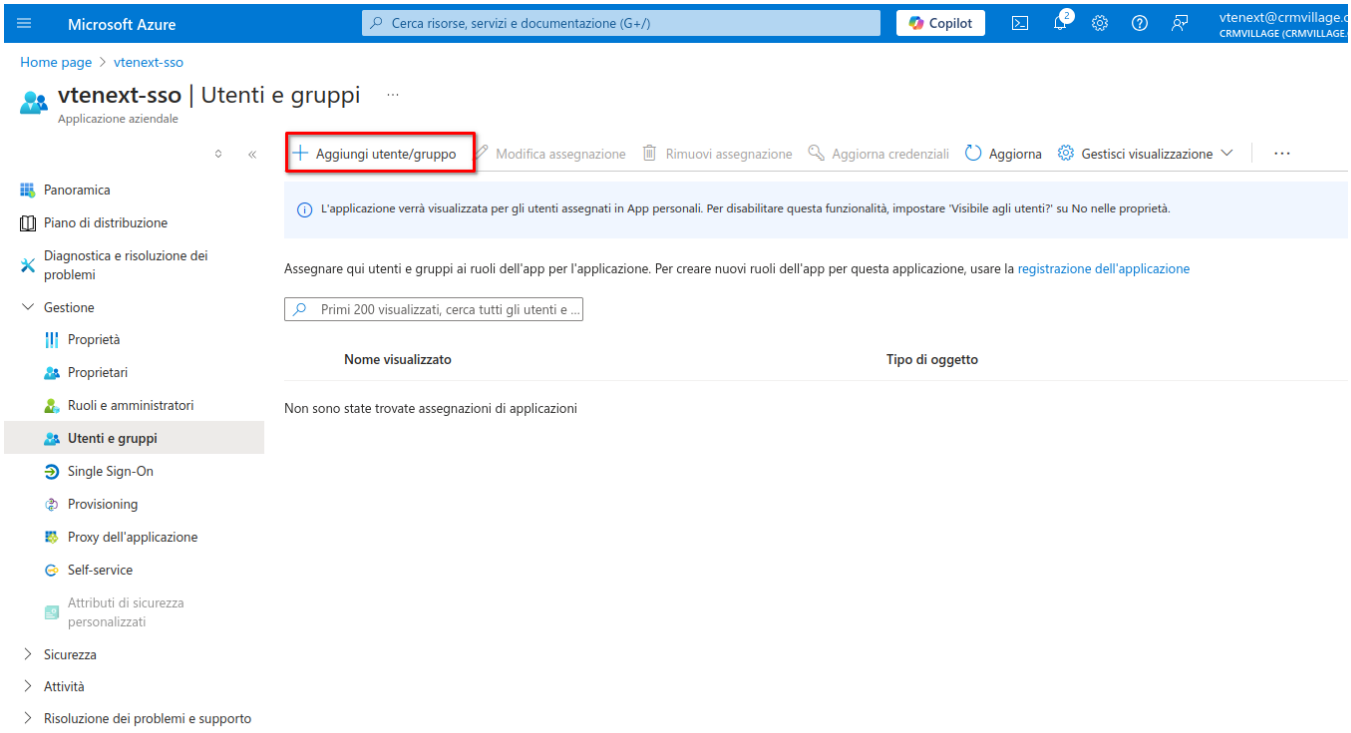
10. Cliccare ora su Panoramica e prendere nota dei campi "ID Applicazione" e "ID tenant" e incollare tutto nella pagina di configurazione in vte:



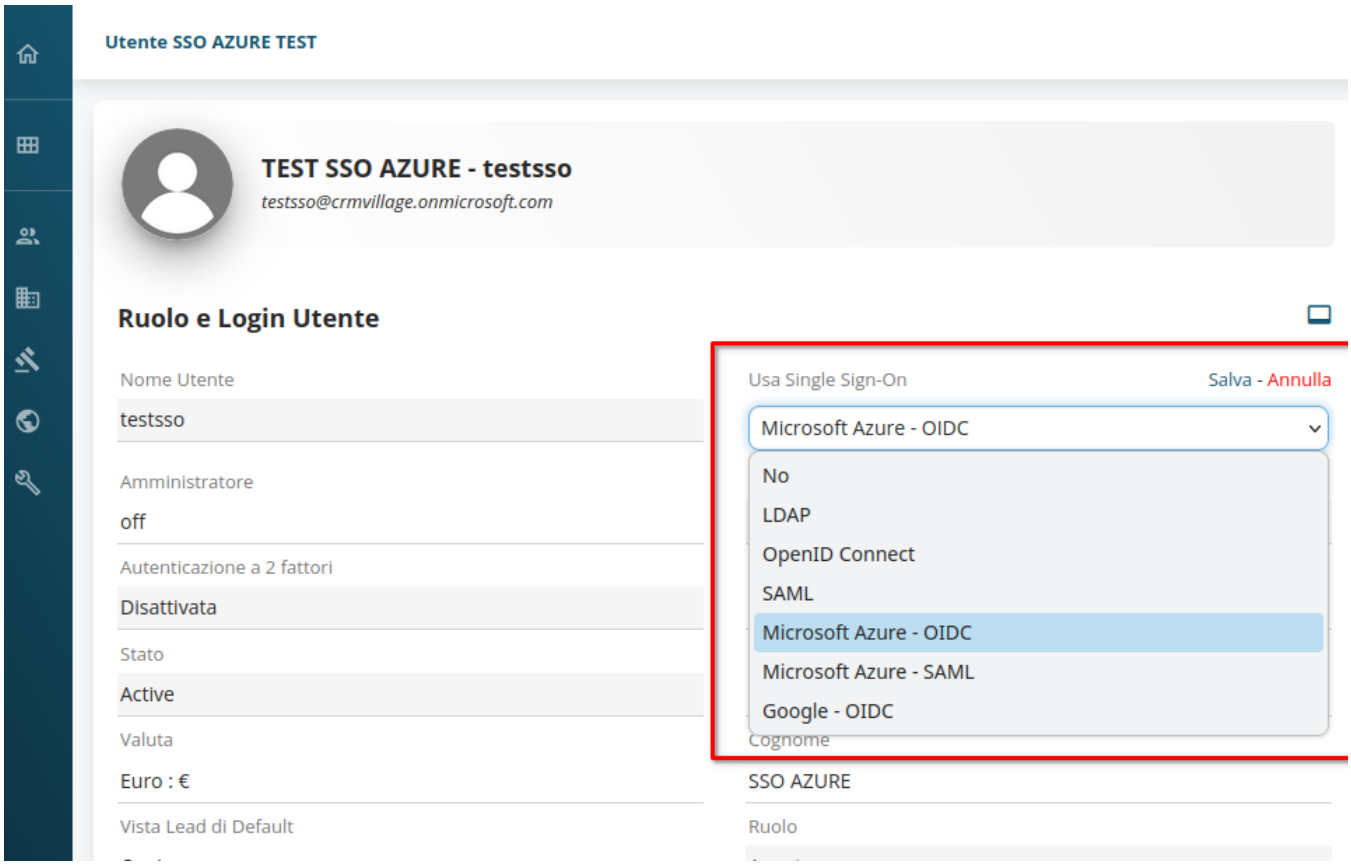
11. (Opzionale) Se si desidera sfruttare anche il logout dall'Idp (Front-Channel Logout), andare su Autenticazione e nel campo "URL di disconnessione canale frontale" impostare l'url fornito da vte e abilitare il logout remoto:



12. Fatto ciò, andare in Utenti e gruppi nel menu a sinistra e aggiungere gli utenti o gruppi che possono usare l'applicazione:



13. A questo punto è possibile configurare gli utenti in vte in modo che utilizzino il SSO con Azure (OIDC):

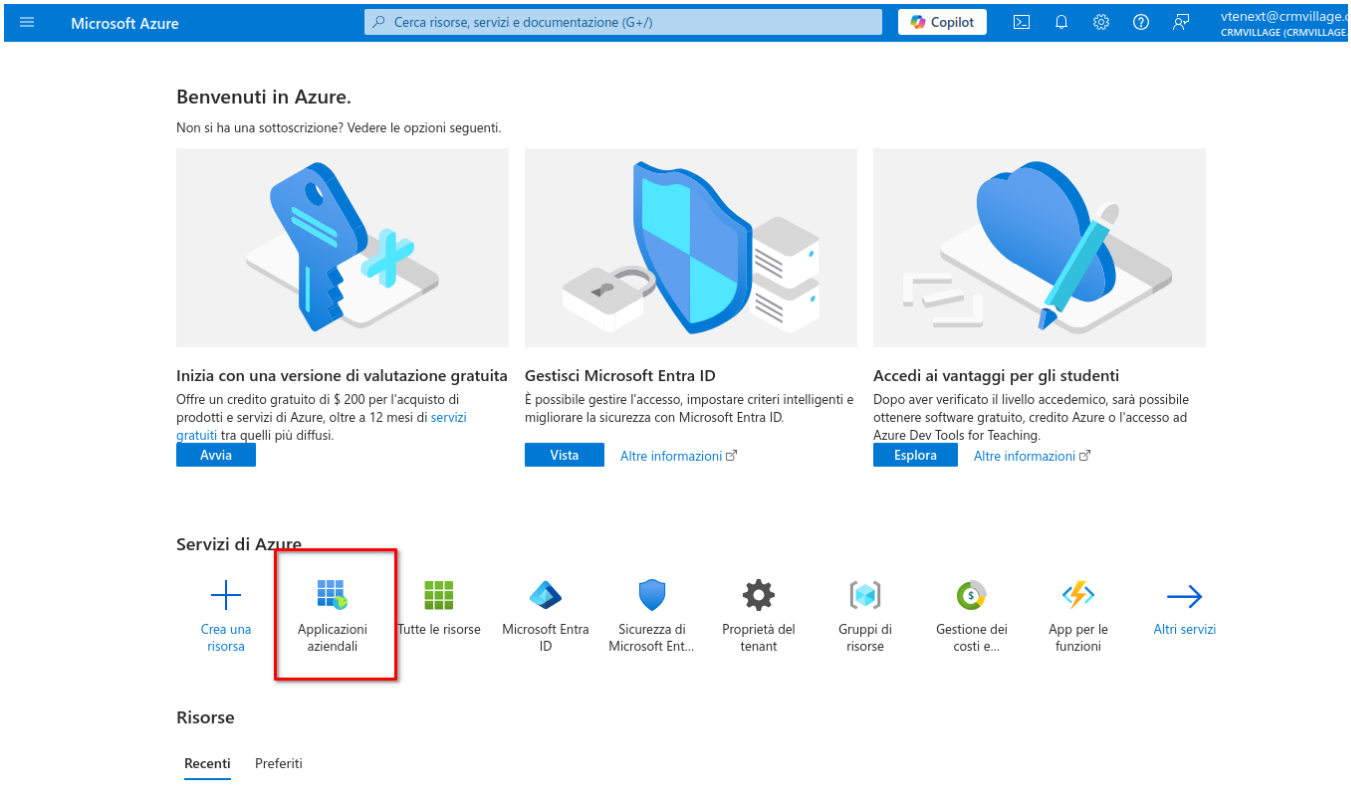


SAML

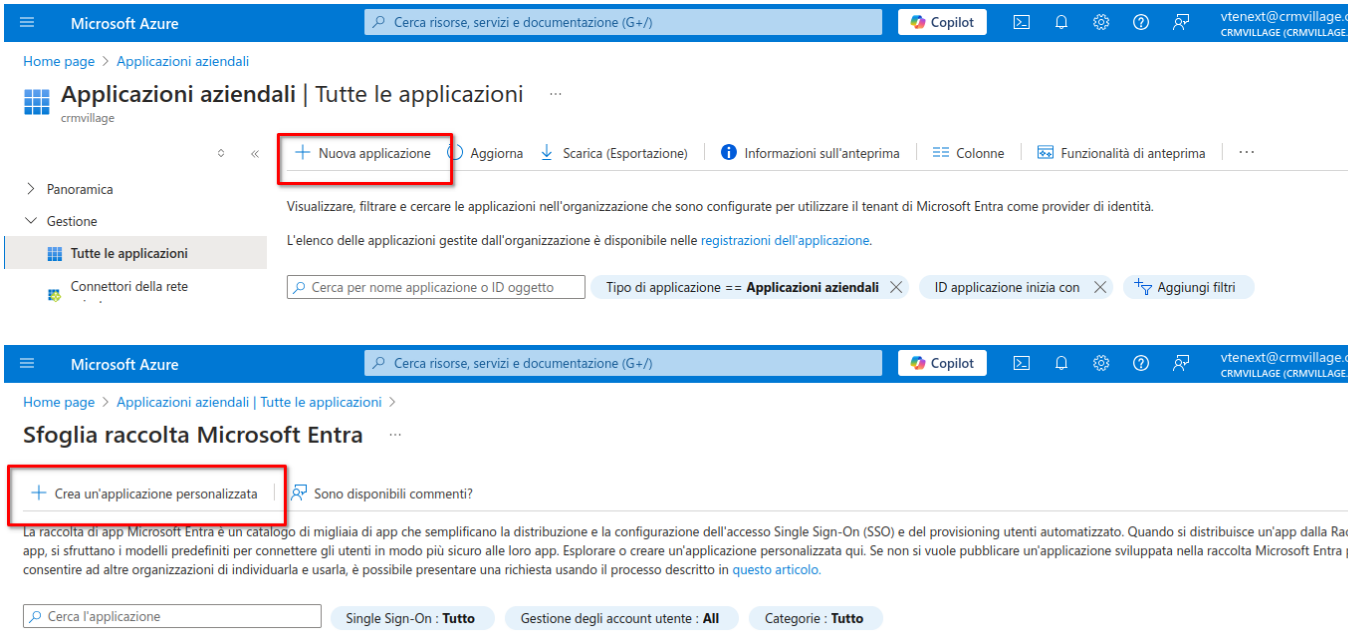
Questa guida mostra come creare un'app in Microsoft Azure, da usare in vtenext per il Single Sign-on, utilizzando il protocollo SAML.

1. Effettuare il login su Azure con una utenza amministrativa: https://portal.azure.com/

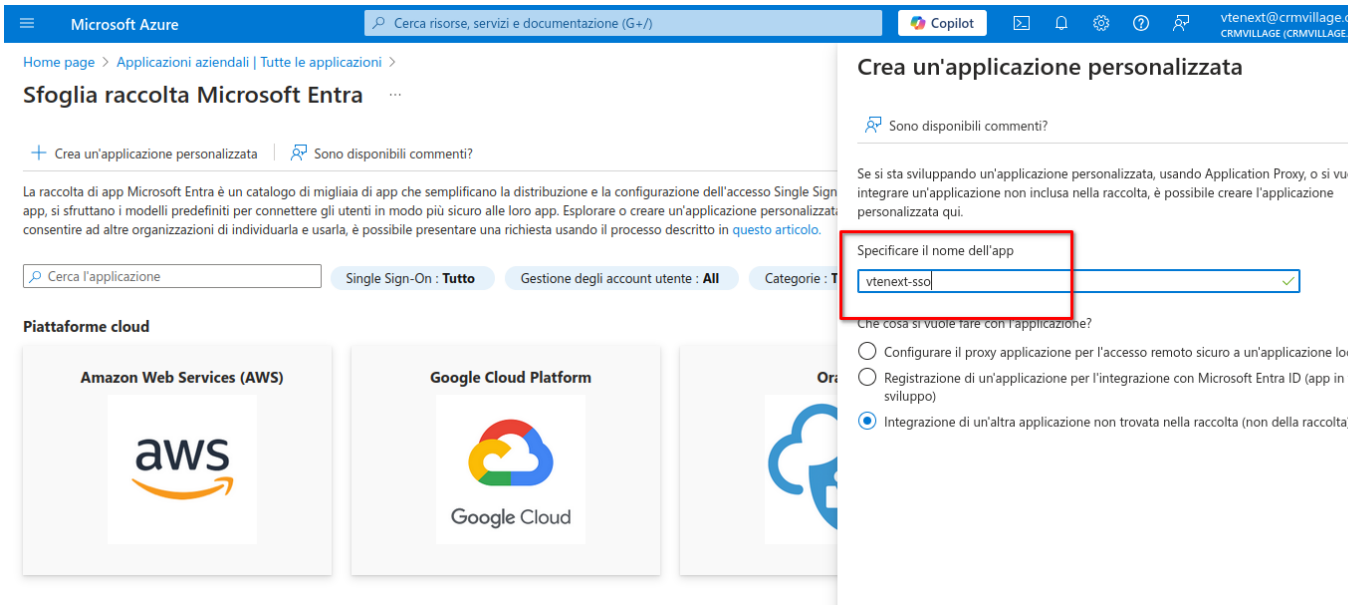
2. Cliccare su Applicazioni aziendali:



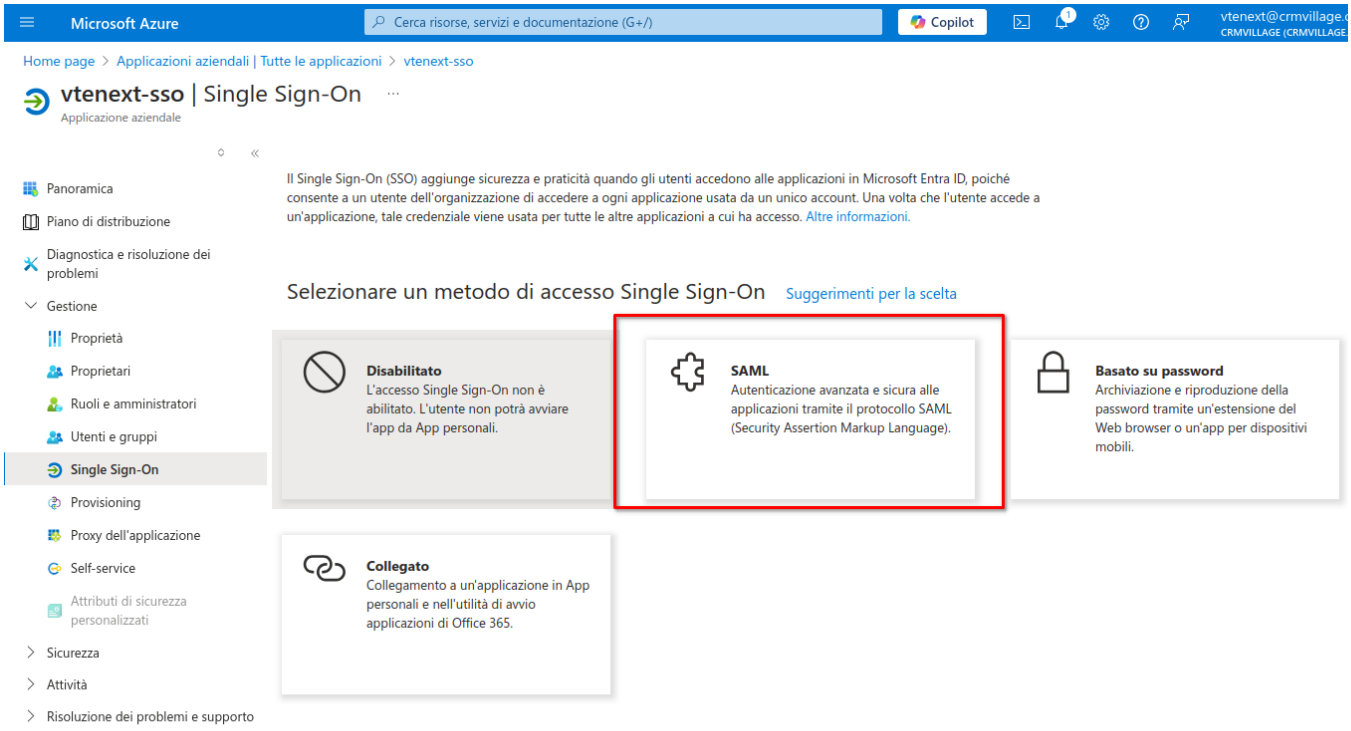
3. Cliccare poi su Nuova applicazione e Crea un'applicazione personalizzata:



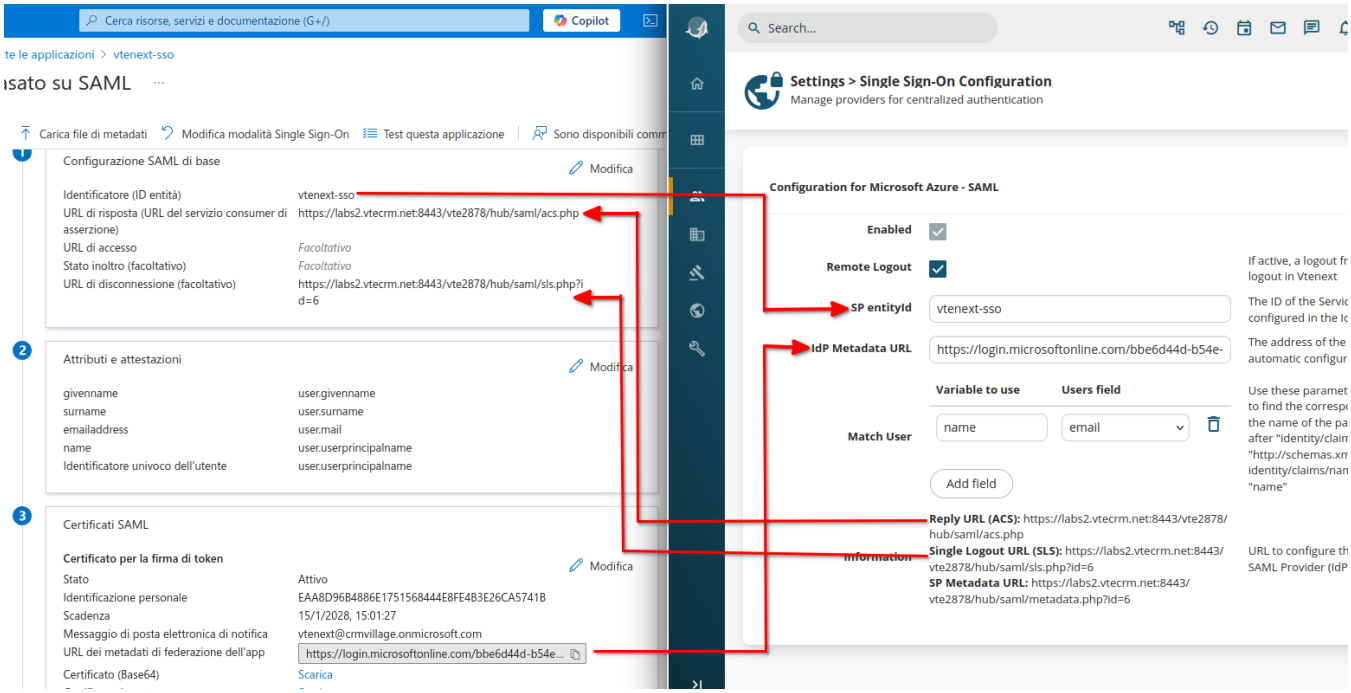
4. Dare un nome all'applicazione, ad esempio "vtenext-sso":



5. Una volta creata, dal menu di sinistra scegliere "Single Sign-On" e poi "SAML":

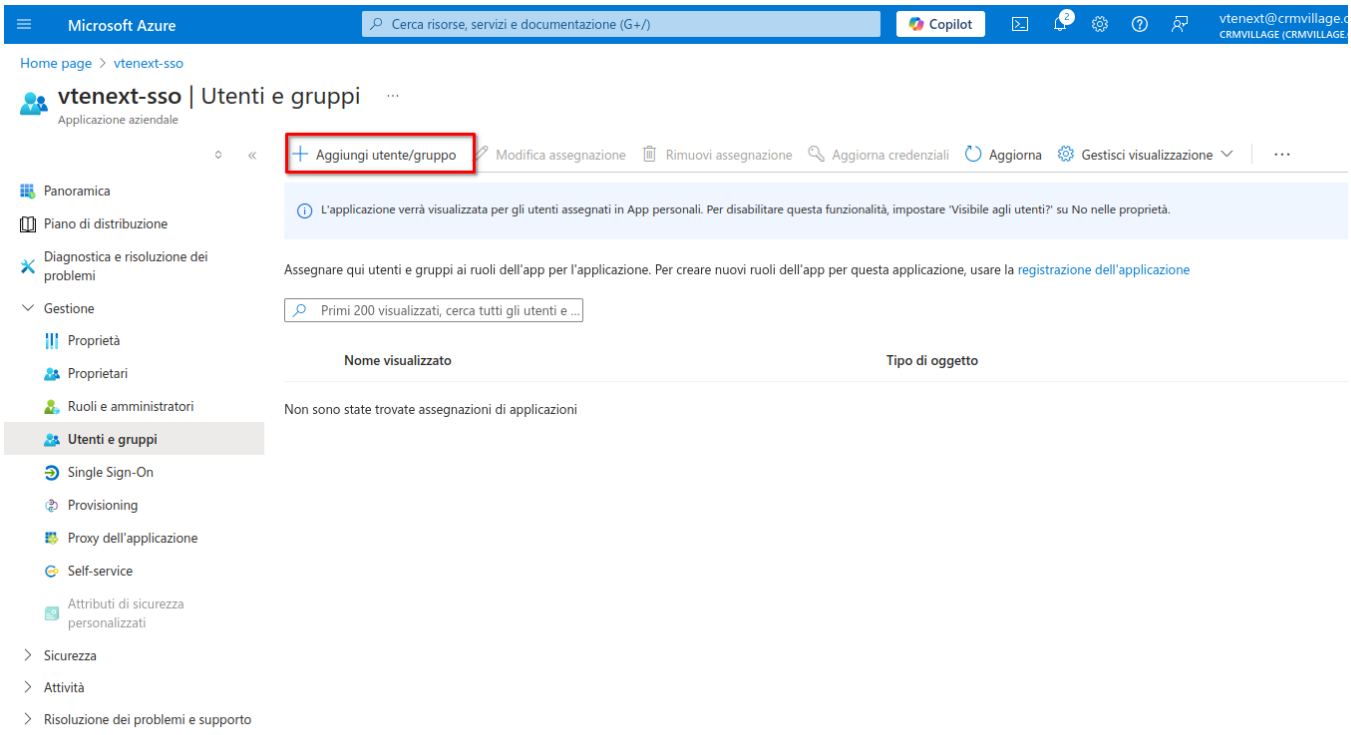


6. Configurare i campi come mostrato, usando le informazioni fornite da vtenext:



Perciò, impostare in Vte i campi "SP entityId" e "IdP Metadata URL" presi da Azure, mentre in Azure impostare "URL di risposta" e "URL di disconnessione" con i valori indicati in Vte.

7. Fatto ciò, andare in Utenti e gruppi nel menu a sinistra e aggiungere gli utenti o gruppi che possono usare l'applicazione:



8. A questo punto è possibile configurare gli utenti in vte in modo che utilizzino il SSO con Azure (SAML):