

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:

Microsoft Azure | Cerca risorse, servizi e documentazione (G+)

Benvenuti in Azure.
Non si ha una sottoscrizione? Vedere le opzioni seguenti.

- Inizia con una versione di valutazione gratuita**
Offre un credito gratuito di \$ 200 per l'acquisto di prodotti e servizi di Azure, oltre a 12 mesi di servizi gratuiti tra quelli più diffusi.
[Avvia](#)
- Gestisci Microsoft Entra ID**
È possibile gestire l'accesso, impostare criteri intelligenti e migliorare la sicurezza con Microsoft Entra ID.
[Vista](#) [Altre informazioni](#)
- Accedi ai vantaggi per gli studenti**
Dopo aver verificato il livello accademico, sarà possibile ottenere software gratuito, credito Azure o l'accesso ad Azure Dev Tools for Teaching.
[Esplora](#) [Altre informazioni](#)

Servizi di Azure

- [Crea una risorsa](#)
- Applicazioni aziendali** (highlighted with a red box)
- [Tutte le risorse](#)
- [Microsoft Entra ID](#)
- [Sicurezza di Microsoft Ent...](#)
- [Proprietà del tenant](#)
- [Gruppi di risorse](#)
- [Gestione dei costi e...](#)
- [App per le funzioni](#)
- [Altri servizi](#)

Risorse

- [Recenti](#)
- [Preferiti](#)

Registra un'applicazione

* Nome

Nome visualizzato rivolto all'utente per questa applicazione. È possibile modificarlo in seguito.

vtenext-ss0-oidc

Tipi di account supportati

Utenti che possono usare questa applicazione o accedere all'API

- Account solo in questa directory dell'organizzazione (Solo crmillage - Tenant singolo)
- Account in qualsiasi directory dell'organizzazione (qualsiasi tenant di Microsoft Entra ID - Multi-tenant)
- Account in qualsiasi directory dell'organizzazione (qualsiasi tenant di Microsoft Entra ID - Multi-tenant) e account Microsoft personali (ad esempio, Skype, Xbox)
- Solo account Microsoft personali

[Aiutami a scegliere...](#)

URI di reindirizzamento (facoltativo)

La risposta di autenticazione verrà restituita a questo URI dopo il completamento dell'autenticazione dell'utente. Può essere specificato facoltativamente adesso e può essere modificato in seguito, ma un valore è necessario per la maggior parte degli scenari di autenticazione.

Web https://labs2.vtecrm.net:8443/vte2878/hub/oidc/callback.php

Registrare qui un'app su cui si sta lavorando. Integrare le app della raccolta e altre app dall'esterno dell'organizzazione mediante l'aggiunta da [Applicazioni aziendali](#).

Se si continua, si accettano i criteri della piattaforma Microsoft

Registra

Cerca...

Abilitato

Logout remoto Se attivo, il logout dall'IdP forzerà un logout in Vtenext

Client ID

Client Secret

Tenant ID Indicare il Tenant ID della propria organizzazione se l'app non è multi-tenant, altrimenti lasciare vuoto

Flusso OAuth Implicito Il flusso da usare: Implicito per ricevere direttamente un id_token (raccomandato), Authorization Code per ottenere un access_token con cui ottenere informazioni sull'utente

Scope openid profile email Gli scope da utilizzare, separati da spazi; di solito "openid profile email"

Variabile da usare Campo degli Utenti

Match User email Email Utilizza questi parametri restituiti da OpenID Connect per trovare l'utente corrispondente in Vtenext; di solito basta l'email, se univoca tra gli utenti

Aggiungi campo

Informazioni **Callback URL:** https://labs2.vtecrm.net:8443/vte2878/hub/oidc/callback.php **Logout URL:** https://labs2.vtecrm.net:8443/vte2878/hub/oidc/logout.php?id=5 URL per la configurazione dell'integrazione all'interno del Provider. L'url di logout supporta sia Back-Channel che Front-Channel Logout

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

Microsoft Azure

Cerca risorse, servizi e documentazione (G+)

Copilot

vtenext@crmillage.c
CRMVILLAGE (CRMVILLAGE)

Home page > Applicazioni aziendali | Tutte le applicazioni > vtenext-ss-o-oidc

vtenext-ss-o-oidc | Accesso basato su OIDC

Applicazione aziendale

- Panoramica
- Piano di distribuzione
- Diagnostica e risoluzione dei problemi
- Gestione
 - Proprietà
 - Proprietari
 - Ruoli e amministratori
 - Utenti e gruppi**
 - Single Sign-On
 - Provisioning
 - Proxy dell'applicazione
 - Self-service
 - Attributi di sicurezza personalizzati
- Sicurezza
 - Accesso condizionale
 - Autorizzazioni
 - Crittografia di token
- Attività

Le applicazioni OIDC richiedono chiavi di firma personalizzate per personalizzare le attestazioni. Controllare le considerazioni sulla sicurezza prima di personalizzare le attestazioni per l'applicazione. [Altre informazioni](#)

Questa applicazione usa OpenID Connect e OAuth. Questo protocollo semplifica la configurazione dell'applicazione, include SDK facili da usare e consente all'applicazione di usare MS Graph. [Altre informazioni](#)

Poiché questa applicazione usa OpenID Connect e OAuth, la maggior parte della configurazione di Single Sign-On è già completa. [Altre informazioni sugli oggetti applicazione e sugli oggetti entità servizio in Microsoft Entra](#)

- Configurare le proprietà dell'applicazione [Vai all'applicazione](#)
 Passare a vtenext-ss-o-oidc nell'esperienza Registros app per modificare proprietà quali URL di risposta, identificatori, attestazioni opzionali e altre ancora. L'account deve avere le autorizzazioni necessarie (Amministratore globale, Amministratore applicazione cloud, Amministratore applicazione o Proprietario dell'oggetto applicazione). [Altre informazioni sui ruoli di amministratore in Microsoft Entra](#)
- Attributi e attestazioni [Modifica](#)
 Per questa applicazione non sono configurate attestazioni basate su JWT. Fare clic su Modifica per avviare la configurazione delle attestazioni.

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

Microsoft Azure

Cerca risorse, servizi e documentazione (G+)

Copilot

vtenext@crmillage.c
CRMVILLAGE (CRMVILLAGE)

Home page > Applicazioni aziendali | Tutte le applicazioni > vtenext-ss-o-oidc

vtenext-ss-o-oidc | Certificati e segreti

Cerca

Sono disponibili commenti?

- Panoramica
- Avvio rapido
- Assistente all'integrazione
- Diagnostica e risolvi i problemi
- Gestione
 - Personalizzazione e proprietà
 - Certificati e segreti**
 - Configurazione dei token
 - Autorizzazioni API
 - Esporre un'API
 - Ruoli dell'app
 - Proprietari
 - Ruoli e amministratori
 - Manifesto
- Supporto e risoluzione dei problemi

Le credenziali consentono alle applicazioni riservate di identificarsi rispetto al servizio di autenticazione durante la ricezione di token in una posizione indirizzabile sul web (mediante uno schema HTTPS). Per una maggiore sicurezza, è consigliabile usare un certificato, invece di un segreto client, come credenziale.

I certificati di registrazione delle applicazioni, i segreti e le credenziali federate sono disponibili nelle schede seguenti.

Certificati (0) **Segreti client (0)** Credenziali federate (0)

Stringa segreta usata dall'applicazione per dimostrare la rispettiva identità durante la richiesta di un token. Può essere definita anche password dell'applicazione.

+ Nuovo segreto client

Descrizione	Scadenza	Valore	ID segreto
Non sono stati creati segreti client per questa applicazione.			

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

Microsoft Azure | Cerca risorse, servizi e documentazione (G+)

Home page > Applicazioni aziendali | Tutte le applicazioni > vtenext-ss-oidc

vtenext-ss-oidc | Certificati e segreti

Cerca

Sono disponibili commenti?

Le credenziali consentono alle applicazioni riservate di identificarsi rispetto al servizio di autenticazione durante la ricezione di token in una posizione indirizzabile sul web (mediante uno schema HTTPS). Per una maggiore sicurezza, è consigliabile usare un certificato, invece di un segreto client, come credenziale.

I certificati di registrazione delle applicazioni, i segreti e le credenziali federate sono disponibili nelle schede seguenti.

Certificati (0) **Segreti client (0)** Credenziali federate (0)

Stringa segreta usata dall'applicazione per dimostrare la rispettiva identità durante la richiesta di un token. Può essere definita anche password dell'applicazione.

+ Nuovo segreto client

Descrizione	Scadenza	Valore
Non sono stati creati segreti client per questa applicazione.		

Aggiungi Annulla

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

Microsoft Azure | Cerca risorse, servizi e documentazione (G+)

Home page > Applicazioni aziendali | Tutte le applicazioni > vtenext-ss-oidc

vtenext-ss-oidc | Certificati e segreti

Cerca

Sono disponibili commenti?

Puoi dedicare qualche secondo all'invio di feedback? →

Le credenziali consentono alle applicazioni riservate di identificarsi rispetto al servizio di autenticazione durante la ricezione di token in una posizione indirizzabile sul web (mediante uno schema HTTPS). Per una maggiore sicurezza, è consigliabile usare un certificato, invece di un segreto client, come credenziale.

I certificati di registrazione delle applicazioni, i segreti e le credenziali federate sono disponibili nelle schede seguenti.

Certificati (0) **Segreti client (1)** Credenziali federate (0)

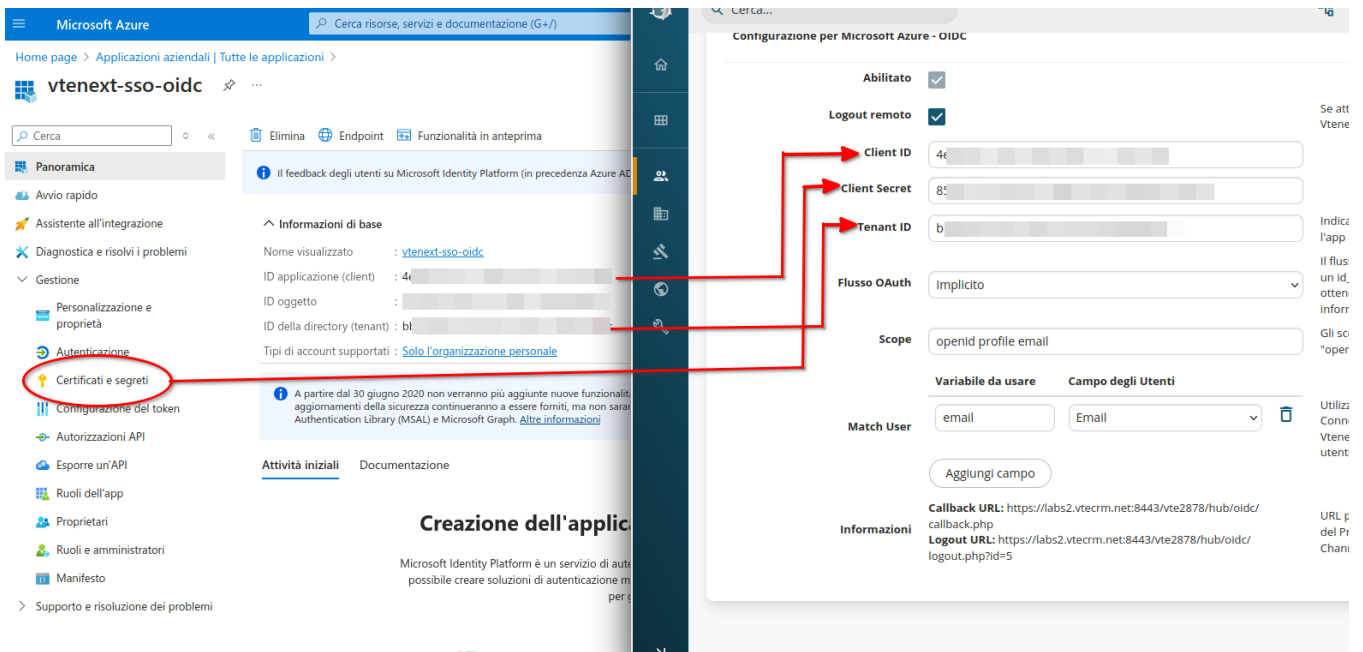
Stringa segreta usata dall'applicazione per dimostrare la rispettiva identità durante la richiesta di un token. Può essere definita anche password dell'applicazione.

+ Nuovo segreto client

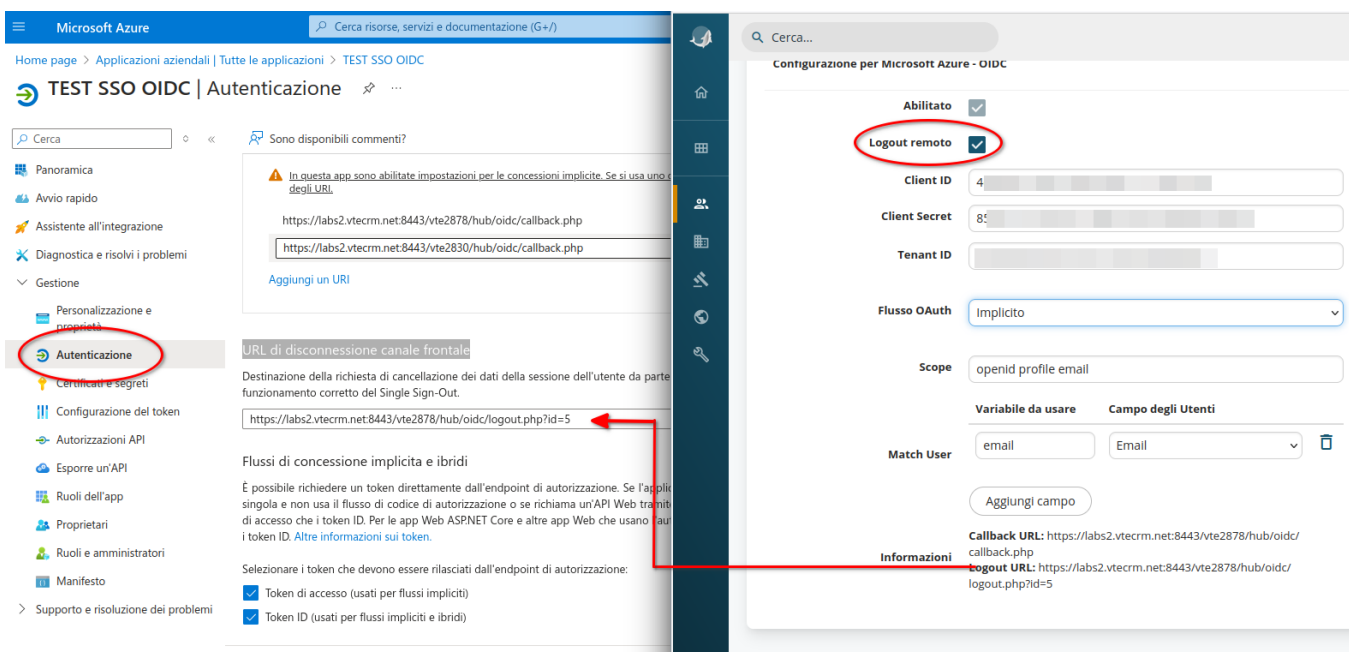
Descrizione	Scadenza	Valore
vtenext sso	15/1/2027	85N... d74actb8-a47d-4ca3-9a69-12c58d4c9553

Copia negli appunti

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



- (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:



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

Microsoft Azure | Cerca risorse, servizi e documentazione (G+)

Home page > vtenext-ss0

vtenext-ss0 | Utenti e gruppi

Applicazione aziendale

+ Aggiungi utente/gruppo | Modifica assegnazione | Rimuovi assegnazione | Aggiorna credenziali | Aggiorna | Gestisci visualizzazione

L'applicazione verrà visualizzata per gli utenti assegnati in App personali. Per disabilitare questa funzionalità, impostare "Visibile agli utenti?" su No nelle proprietà.

Assegnare qui utenti e gruppi ai ruoli dell'app per l'applicazione. Per creare nuovi ruoli dell'app per questa applicazione, usare la [registrazione dell'applicazione](#)

Primi 200 visualizzati, cerca tutti gli utenti e ...

Nome visualizzato	Tipo di oggetto
Non sono state trovate assegnazioni di applicazioni	

- Panoramica
- Piano di distribuzione
- Diagnostica e risoluzione dei problemi
- Gestione
 - Proprietà
 - Proprietari
 - Ruoli e amministratori
 - Utenti e gruppi**
 - Single Sign-On
 - Provisioning
 - Proxy dell'applicazione
 - Self-service
 - Attributi di sicurezza personalizzati
- Sicurezza
- Attività
- Risoluzione dei problemi e supporto

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

Utente SSO AZURE TEST

TEST SSO AZURE - testsso

testsso@crmillage.onmicrosoft.com

Ruolo e Login Utente

Nome Utente	testsso
Amministratore	off
Autenticazione a 2 fattori	Disattivata
Stato	Active
Valuta	Euro : €
Vista Lead di Default	

Usa Single Sign-On Salva - Annulla

Microsoft Azure - OIDC

- No
- LDAP
- OpenID Connect
- SAML
- Microsoft Azure - OIDC**
- Microsoft Azure - SAML
- Google - OIDC

Cognome

SSO AZURE

Ruolo

Revision #1

Created 2025-01-15 13:40:26 UTC by Daniele

Updated 2025-01-15 14:53:27 UTC by Daniele