

# 15.10 Applicazioni esterne

Questa funzione di vtenext, che si trova in **Impostazioni > Applicazioni esterne**, permette di configurare il crm come un Server per OAuth2 e quindi far collegare altre applicazioni direttamente a vtenext.

Cerca...

159

79

5

151

Impostazioni > Applicazioni esterne

Gestione di applicazioni esterne che comunicano con vtenext tramite protocollo di autorizzazione OAuth 2.0

Configurazioni globali

Abilita accesso tramite OAuth2

✓

Permetti agli utenti di vedere e modificare la chiave segreta delle app a loro associate

✓

Abilita connessioni con utenti amministratori

✗

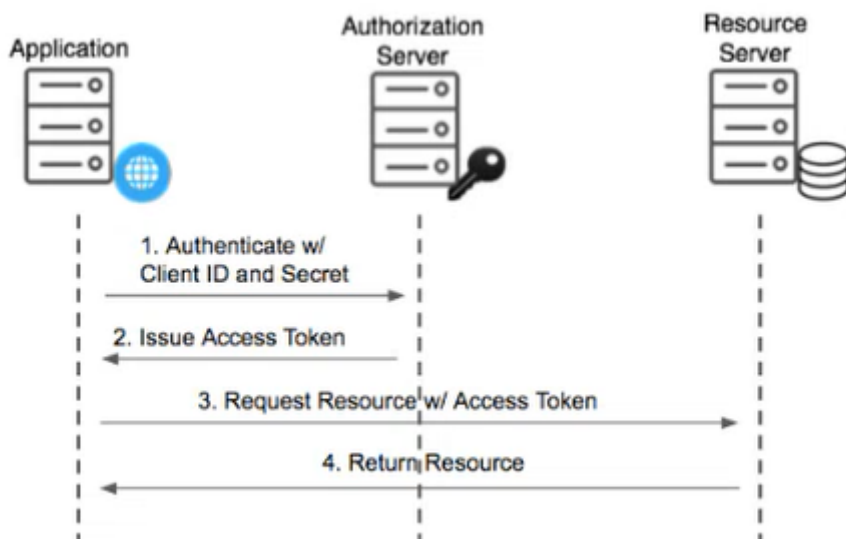
Applicazioni registrate

Aggiungi

Icona	Nome	Tipo di client	Client ID	Utenti autorizzati	Stato dei token	Abilitato	Strumenti
-------	------	----------------	-----------	--------------------	-----------------	-----------	-----------

*Schermata di configurazione per le Applicazioni esterne*

Quindi come funziona esattamente? L'OAuth2 mette a disposizione dei flussi di autorizzazione che permettono alle applicazioni esterne, di accedere al crm tramite dei token ed inviare delle richieste in modo che il crm eroghi i dati richiesti e li invii all'applicazione richiedente. Vediamo una immagine esplicativa:



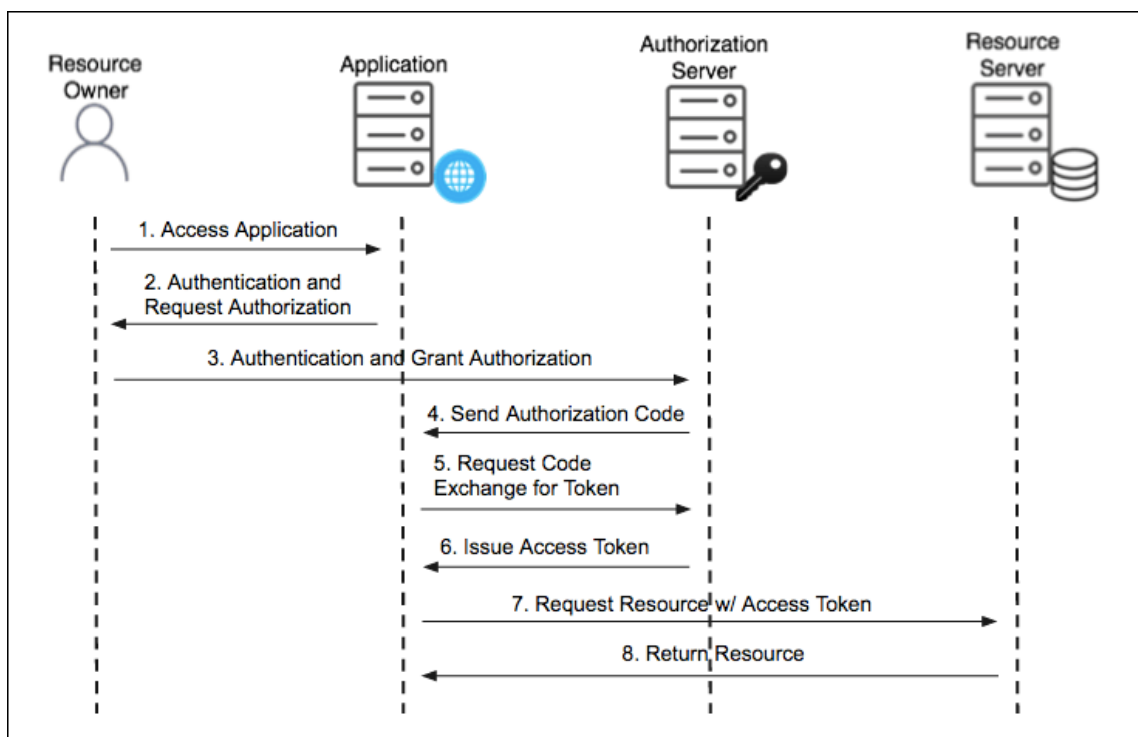
Questo flusso raffigurato, è denominato **Client Credentials**. Ci sono tre parti coinvolte:

1. Applicazione (per esempio un Gestionale)
2. Il Server di Autorizzazione (spesso equiparabile al punto 3)
3. Il Server che contiene di Dati (nel nostro caso vtenext)

In pratica, l'Applicazione (che potrebbe essere un Gestionale che deve leggere le Fatture su vtenext), chiede al Server di Autorizzazione una chiave di accesso (Client ID e Secret Key) per poter accedere al Server che contiene i Dati. Quindi nel nostro esempio, vtenext, genera la coppia di chiavi (Client ID e Secret Key) e le passa all'applicazione la quale le usa per richiedere l'accesso al Server di Autorizzazione (che è sempre vtenext), il quale fornirà all'Applicazione stessa un Token, che permetterà di leggere direttamente le Fatture sul crm.

Il vantaggio è che l'access Token ha una durata limitata, è revocabile lato server e quindi è possibile consentire l'accesso alle app in maniera controllata e, soprattutto, non vengono divulgate o condivise password di sistema. Naturalmente allo scadere del Token, sarà necessario crearne uno di nuovo ripetendo la procedura sopra menzionata.

Il secondo tipo di flusso, è denominato **OAuth2 Authorization Code**. Questo flusso coinvolge un elemento in più, che identificheremo come Utente.



Nell'esempio, diremo che l'Applicazione che si vuole connettere a vtenext questa volta, è Facebook che necessita di leggere i Lead presenti in vtenext. Facebook però è collegato ad un Utente, che è il richiedente di questi dati, quindi è l'utente che in realtà sta chiedendo a Facebook di connettersi a vtenext per leggere i Lead. L'Utente in questo caso ha anche un account in vtenext, quindi l'obiettivo, è che l'utente dia il permesso a Facebook di leggere i Lead su vtenext, quindi sarà fatta un'autenticazione da parte dell'utente su vte, il quale risponderà a Facebook con un OAuth2 Authorization Code. Facebook userà quell'Auth Code per richiedere all'Authorization Server l'Access Token temporaneo e leggere finalmente i dati nel Server.

Quindi Facebook ha avuto accesso ai Lead di vtenext, non ha in pancia le credenziali dell'utente, e dopo circa un'ora scadranno e quindi l'accesso ai dati sensibili resteranno al sicuro.

## Configurazione Service Account

**Settings > External applications**  
Manage external applications that integrate with vtenext with authorization protocol OAuth 2.0

**General configurations**

Enable OAuth2 access	✓
Allow users to view and change the secret key of apps associated to them	✓
Allow connections with admin users	✗

**Registered applications**

Icon	Name	Client type	Client ID	Authorized users	Token status	Enabled	Tools
	facebook background	Service account	vte_99e3e791051bc773aa54	aldo	No active tokens	✓	✎ ⚙ 🗑
	gestionale fico	Service account	vte_5a0391ecbe3d04058d56	aldo	2 expired tokens	✓	✎ ⚙ 🗑
	La mia bella app	Web or mobile app	vte_a75fdb752584846f2566	Only selected	2 expired tokens	✓	✎ ⚙ 🗑

*Cliccare sul pulsante AGGIUNGI sulla destra*

**Impostazioni > Applicazioni esterne**  
Gestione di applicazioni esterne che comunicano con vtenext tramite protocollo di autorizzazione OAuth 2.0

Creazione applicazione

Dati di accesso

**Tipo di client** --Prego Selezionare--  
Web or mobile application  
Service account

Informazioni di configurazione

Endpoints  
Auth endpoint: <http://trial01.vtecrm.net/31883/oauth2/v2.0/auth.php>  
Token endpoint: <http://trial01.vtecrm.net/31883/oauth2/v2.0/token.php>  
Revoke endpoint: <http://trial01.vtecrm.net/31883/oauth2/v2.0/revoke.php>

Flusso OAuth 2.0

Si accede ad una schermata con un Wizard che ci aiuta a determinare il flusso che vogliamo configurare. Come prima cosa impostare il Tipo di Client e si potrà scegliere tra:

- **Web or Mobile application** se abbiamo bisogno di un accesso tramite login con utente
- **Service account** se l'accesso avviene in background tra due server

Volendo dunque configurare un flusso **Client Credentials**, come **Tipo di Chiave = Service Account** e come **Tipo di Segreto = Chiave segreta**. Compariranno dunque altri campi da configurare che vediamo di seguito:

Impostazioni > Applicazioni esterne  
Gestione di applicazioni esterne che comunicano con vtenext tramite protocollo di autorizzazione OAuth 2.0

Creazione applicazione

Dati di accesso

**Tipo di client**: Service account  
Se l'applicazione esterna richiede accesso interattivo da parte dell'utente, scegliere Web or mobile application altrimenti se l'accesso avviene in background usare Service account

**Tipo di segreto**: Chiave segreta  
Con Chiave segreta verrà usato il flusso OAuth 2.0 Client Credentials con client id e chiave segreta, mentre con JWT firmato va generato un JWT firmato con la chiave segreta.

**Nome**: Il mio gestionale bello zuccheti  
Nome per l'applicazione che accede a vtenext, ad esempio: "Gestionale"

**Client ID**: vte\_13301a8  
ID da usare nell'applicazione per accedere a vtenext

**Chiave segreta**: 1067270695e011f38de4c2f  
Chiave da usare nell'applicazione, in caso di accesso non interattivo

**Scope**: rest.all.read (Accesso in sola lettura via webservice REST)  
Scope da usare nell'applicazione per accedere a vtenext

**Utente**: cwm1nuyhdxrewnmdsr@kvhrs.com (Ciccio Pasticcio)  
Utente legato a queste credenziali

Informazioni di configurazione

**Endpoints**:  
Auth endpoint: <http://trial01.vtecrm.net/3188>  
Token endpoint: <http://trial01.vtecrm.net/318>  
Revoke endpoint: <http://trial01.vtecrm.net/31>

A questo punto si dovrà dare un **Nome** a questa configurazione, che tipicamente identifica anche quello che fa (nell'esempio fa connettere ad un gestionale). Vengono già messe in evidenza il **Client ID e la Chiave Segreta** autogenerate. Infine si deve determinare lo **Scope**, ovvero come i dati verranno fruiti dal sistema (sola lettura, sola scrittura, oppure in lettura/scrittura) e l'**Utente** al quale questa configurazione dovrà fare riferimento (se lo Scope è in sola lettura o lettura/scrittura per esempio, sarà possibile gestire solamente i dati di quell'utente con le limitazioni che la sua profilazione prevede. E' chiaro che se si desidera pieno controllo senza limitazioni, dovrà essere selezionato un utente Admin).

Fornendo dunque gli Endpoints, il Client ID e la Chiave Segreta all'ipotetico tecnico del gestionale al quale ci si vuole connettere, sarà possibile finalizzare il collegamento.

Tornando alla configurazione iniziale, dopo aver scelto **Tipo di Chiave = Service Account** e come **Tipo di Segreto = JWT firmato**, ci sono più o meno le stesse informazioni da configurare e come unica differenza, troviamo che la **Chiave Segreta** verrà generata solamente dopo il salvataggio della configurazione.

Cerca...

Creazione applicazione

Dati di accesso

Tipo di client: Service account

Tipo di segreto: JWT firmato

Nome: Il mio gestionale bello zucchetti

Client ID: vte\_13301a833b5f4f087471

Scope: rest.all.read (Accesso in sola lettura via webservice REST)

Utente: cwmInuyhdrewnmdsr@kvhrs.com (Ciccio Pasticcio)

Informazioni di configurazione

Endpoints: Auth endpoint: http://trial01.vtecrm.net/31883/oauth2/v2.0/auth.php  
Token endpoint: http://trial01.vtecrm.net/31883/oauth2/v2.0/token.php  
Revoke endpoint: http://trial01.vtecrm.net/31883/oauth2/v2.0/revoke.php

Flusso OAuth 2.0: Client Credentials with JWT assertion

Salva Annulla

VTEEXT 24.08.1

© 2008-2024 vtenext.com | Licenza

## Configurazione Web or Mobile Application

Cerca...

Settings > External applications

Manage external applications that integrate with vtenext with authorization protocol OAuth 2.0

General configurations

Enable OAuth2 access: ✓

Allow users to view and change the secret key of apps associated to them: ✓

Allow connections with admin users: ✗

Registered applications

Icon	Name	Client type	Client ID	Authorized users	Token status	Enabled	Tools
	facebook background	Service account	vte_99e3e791051bc773aa54	aldo	No active tokens	✓	
	gestionale fico	Service account	vte_5a0391ecbe3d04058d56	aldo	2 expired tokens	✓	
	La mia bella app	Web or mobile app	vte_a75fdb752584846f2566	Only selected	2 expired tokens	✓	

Add

Cliccare sul pulsante AGGIUNGI sulla destra

Cerca...

Impostazioni > Applicazioni esterne

Gestione di applicazioni esterne che comunicano con vtenext tramite protocollo di autorizzazione OAuth 2.0

Creazione applicazione

Dati di accesso

Tipo di client: --Prego Selezionare--

Informazioni di configurazione

Endpoints: Auth endpoint: http://trial01.vtecrm.net/31883/oauth2/v2.0/auth.php  
Token endpoint: http://trial01.vtecrm.net/31883/oauth2/v2.0/token.php  
Revoke endpoint: http://trial01.vtecrm.net/31883/oauth2/v2.0/revoke.php

Flusso OAuth 2.0

Salva Annulla

Si accede dunque nuovamente al Wizard e selezioneremo **Web or mobile application**. Comparirà la schermata seguente:

Impostazioni > Applicazioni esterne  
Gestione di applicazioni esterne che comunicano con vtenext tramite protocollo di autorizzazione OAuth 2.0

Creazione applicazione

Dati di accesso

Tipo di client: Web or mobile application

Tipo di applicazione: Web application (Selezionato)  
--Prego Selezionare--  
Web application  
Native or Single Page App

Client ID: Web application

Chiave segreta: 1067270695e011f38de4c2fde0710af2e125b3e2f50165e715d61bda5387

Se l'applicazione esterna richiede accesso interattivo da parte dell'utente, scegliere Web or mobile application altrimenti se l'accesso avviene in background usare Service account

Se l'applicazione è una Single Page App o per dispositivi mobili, senza una componente server, andrà usato il flusso del codice di autorizzazione con PKCE, altrimenti basta il normale flusso del codice di autorizzazione.

ID da usare nell'applicazione per accedere a vtenext

Chiave da usare nell'applicazione, in caso di accesso non interattivo

In **Tipo di applicazione**, è possibile scegliere **Web application** se si tratta di un App che funziona tramite browser, oppure **Native or Single Page App** se invece si tratta di un'applicazione nativa come un'app presente su un dispositivo mobile.

Scegliendo **Web application**, verrà generata come per la configurazione vista in precedenza, un **Client ID** ed una **Chiave Segreta** e sarà possibile determinare il tipo di accesso, **Scope**, in sola lettura, sola scrittura o lettura/scrittura.

Client ID: vte\_13301a833b5f4f087471

Chiave segreta: 1067270695e011f38de4c2fde0710af2e125b3e2f50165e715d61bda5387

Scope: rest.all.read (Accesso in sola lettura via webservice REST)

Accesso offline: ☒

ID da usare nell'applicazione per accedere a vtenext

Chiave da usare nell'applicazione, in caso di accesso non interattivo

Scope da usare nell'applicazione per accedere a vtenext

Se attivo, l'applicazione potrà accedere a vtenext in autonomia dopo la prima autorizzazione

E' possibile decidere le attivare l'**Accesso offline**, ovvero invece di far scadere il Token come si diceva in precedenza (il Token ha una durata limitata e va rinnovato), in questo modo è possibile dare accesso a tempo indeterminato all'app verso vtenext. Quindi cosa succede? Il server chiede il "refresh token" e quindi l'app può richiedere nuovamente il token che sarà il medesimo e rimarrà valido fino a che non viene deciso di togliere la spunta da Offline.

Accesso offline: ☒

URL di ritorno: https://www.starfleet.com



Utenti autorizzati: Tutti gli utenti

Se attivo, l'applicazione potrà accedere a vtenext in autonomia dopo la prima autorizzazione

Indirizzi ammessi per reindirizzare l'utente all'applicazione, uno per riga

Utenti che possono utilizzare questa applicazione

Quindi poi si configurerà l'**URL di ritorno**, che permetterà di reindirizzare l'utente, dopo il Login al Server (ovvero vtenext), direttamente all'app in cui deve accedere (es. Facebook o altro). E' anche possibile decidere quali sono gli **Utenti autorizzati** ad utilizzare questa configurazione. Possono essere Tutti gli utenti, oppure quelli che si vogliono selezionare dalla lista Gruppi o Utenti.



Schermata di autorizzazione

Nome

Nome per l'applicazione che accede a vtenext, ad esempio: "Gestionale"

Descrizione


Icona

Scegli file

Nessun file selezionato

Icona mostrata nella schermata di autorizzazione. Se più grande di 64x64, verrà ridimensionata

E' possibile configurare la Schermata di autorizzazione, ovvero quando l'utente viene indirizzato alla richiesta di autorizzazione (es. l'applicazione Facebook richiede di accedere ai dati di vtenext, vuoi autorizzare?), comparirà una schermata che è possibile personalizzare con un **Nome**, una **Descrizione** ed un'Icona.



L'applicazione **appella** vuole accedere a VTENEXT.  
Consentire l'accesso?

Descrizione app

mobile appella

L'autorizzazione consente all'app:

◦ Accesso completo via webservice REST

L'app può visualizzare e modificare tutti i dati accessibili all'utenza associata, solamente tramite API REST.

No

Sì

☐ Autorizza in modo permanente

Tornando all'inizio di questo tipo di settaggio, in **Tipo di applicazione** è possibile selezionare anche **Native or Single Page App**, la cui configurazione è molto simile a quella appena illustrata.

Dalla schermata iniziale, **Impostazioni > Applicazioni esterne**, è possibile vedere la lista delle **Applicazioni registrate** ed è possibile decidere se revocarne qualcuna. Ad esempio, non è più richiesto che Facebook possa accedere a vtenext, nonostante l'autorizzazione sia già stata configurata e concessa, è possibile disabilitarla cliccando sulla spunta verde sulla destra della lista.

Impostazioni > Applicazioni esterne

Gestione di applicazioni esterne che comunicano con vtenext tramite protocollo di autorizzazione OAuth 2.0

**Configurazioni globali**

Abilita accesso tramite OAuth2	✓
Permetti agli utenti di vedere e modificare la chiave segreta delle app a loro associate	✓
Abilita connessioni con utenti amministratori	✗

**Applicazioni registrate**

Icona	Nome	Tipo di client	Client ID	Utenti autorizzati	Stato dei token	Abilitato	Strumenti
	facebook background	Service account	vte_99e3e791051bc773aa54	aldo	Nessun token attivo	✗	✎ ⛔ 🗑
	gestionale fico	Service account	vte_5a0391ecbe3d04058d56	aldo	2 token scaduti	✎	✎ ⛔ 🗑
	La mia bella app	Web or mobile app	vte_a75fdb752584846f2566	Solo selezionati	2 token scaduti	✓	✎ ⛔ 🗑

In questa lista è anche possibile vedere se ci sono **Token scaduti** oppure di **non attivi**. Nel caso di Token scaduti l'utente è tenuto a rifare il login al sistema. Nella stessa lista, sulla destra, troviamo gli **Strumenti**:

- ✎ serve per modificare la configurazione
- ⛔ per revocare tutti i Token
- 🗑 per eliminare la configurazione eseguita

Utente Administrator

Modifica Richiedi assistenza remota ⓘ

Opportunità	✓	✓
Ordini di Acquisto	✗	✗
Ordini di Vendita	✗	✗
Planificazioni	✓	✓
Preventivi	✗	✗
Processi	✗	✗
Prodotti	✗	✗
Prodotti configurabili	✗	✗
Report Visite	✗	✗
Scadenze	✓	✓
Scansioni Mobile	✗	✗
Servizi	✗	✗
Servizi a Contratto	✗	✗
Target	✗	✗
Topic Klondike	✗	✗

**INFORMAZIONI**

- Ruolo e Login Utente
- Più Informazioni
- Indirizzo utente
- Fotografia Utente
- Configurazione Calendario
- Configurazione Asterisk
- Configurazione Book me
- Configurazione servizi web REST
- Componenti di Home Page
- I Miei Gruppi
- Storia Login
- Impostazioni Notifiche Moduli
- Applicazioni collegate**

**Applicazioni collegate**

Icona	Nome	Tipo di client	Client ID	Stato dei token	Abilitato	Strumenti
		Web or mobile app	vte_22fd1e9	Nessun token attivo	✓	✎ ⛔

Nelle **Preferenze Utente**, c'è una voce sulla destra, denominata **Applicazioni collegate**, che permette di visualizzare tutte le applicazioni che sono state create e relazionate allo specifico utente. Da quella stessa related, è possibile vedere il dettaglio della configurazione (ma non modificarla se non è un utente admin), ed è possibile anche disabilitarla o revocarne i token.

Revision #35

Created 14 November 2024 16:06:22 by Admin

Updated 18 November 2024 16:49:46 by Admin