

# TechCello How-To Guide

## Authorization Server Setup



Contents

- 1 Introduction to Authorization Server..... 3
  - 1.1 Deployment of an Authorization Server ..... 3
  - 1.2 Clients..... 3
    - Multi-Tenant Access*..... 3
    - Single-Tenant Access*..... 4
  - 1.3 Applications targeting Authorization server ..... 5
  - 1.4 Tenant Provisioning Process ..... 5
  - 1.5 Tenant Management ..... 6
  - 1.6 User Management ..... 8
    - User Registration process ..... 9
    - User Consent Management ..... 9
  - 1.7 Setting up a Tenant ..... 11
    - Using Social Logins ..... 11
    - Using Cello Open Id Connect..... 12
    - Using Active Directory..... 12
    - Cello as Open Identity Provider for clients ..... 13
    - Endpoints ..... 13
    - Authorization Server Configuration ..... 14
- 2 Contact Information..... 14

## 1 Introduction to Authorization Server

The authorization server is a web Api enabled application that takes care of identifying the client that tries to access the resource on behalf of the tenant and its users by prompting the user to login using the appropriate configuration. Each user's authentication provider is governed by the tenant identity provider configuration.

Tech Cello supports the three modes of authorization

- Cello Open-Id connect
- Social Logins: Google, Facebook, Twitter
- Active Directory via LDAP

### 1.1 Deployment of an Authorization Server

The deployment modes which are supported by the authorization server are

- I) Multi-Tenancy Mode
  - a. A separate server to host the authorization server (OR)
  - b. Web Application along with the Authorization Server
- II) On-Premise Setup [Single-Tenancy Mode]
  - a. The Authorization server resides on the same server in the client, where the LDAP access is available. Example: The server in the tenant premises which can access the Active directory.
- III) Authorization server [On-Premise / Multi-Tenant] should be available for access under SSL over HTTP.

Authorization server requires Microsoft .Net version 4.5 or higher is required for the deployment and should have access to CelloSaaS tables for reading the metadata and storing the setting information.

### 1.2 Clients

Applications that allow users to be authenticated by various options have to register themselves as a client. The different types of are: Web Client, Webbrowser enabled client and Native application.

These client applications have one of the two modes of operation

#### *Multi-Tenant Access*

The client will access the application via a shared URL. This functionality is supported in the following one of the following means

1. Tenant has a registered client with enabled multi-tenant access.
2. The ISV Admin has a Multi-tenant access enabled client

Single-Tenant Access

Each client under a tenant has a unique URI that is used as a means to identify itself.

Every client has a redirect-url to get back the authentication information from the Authorization Server and has settings to control

- a. Type of token [Supported : JWT]
- b. Lifetime of Access Tokens etc.

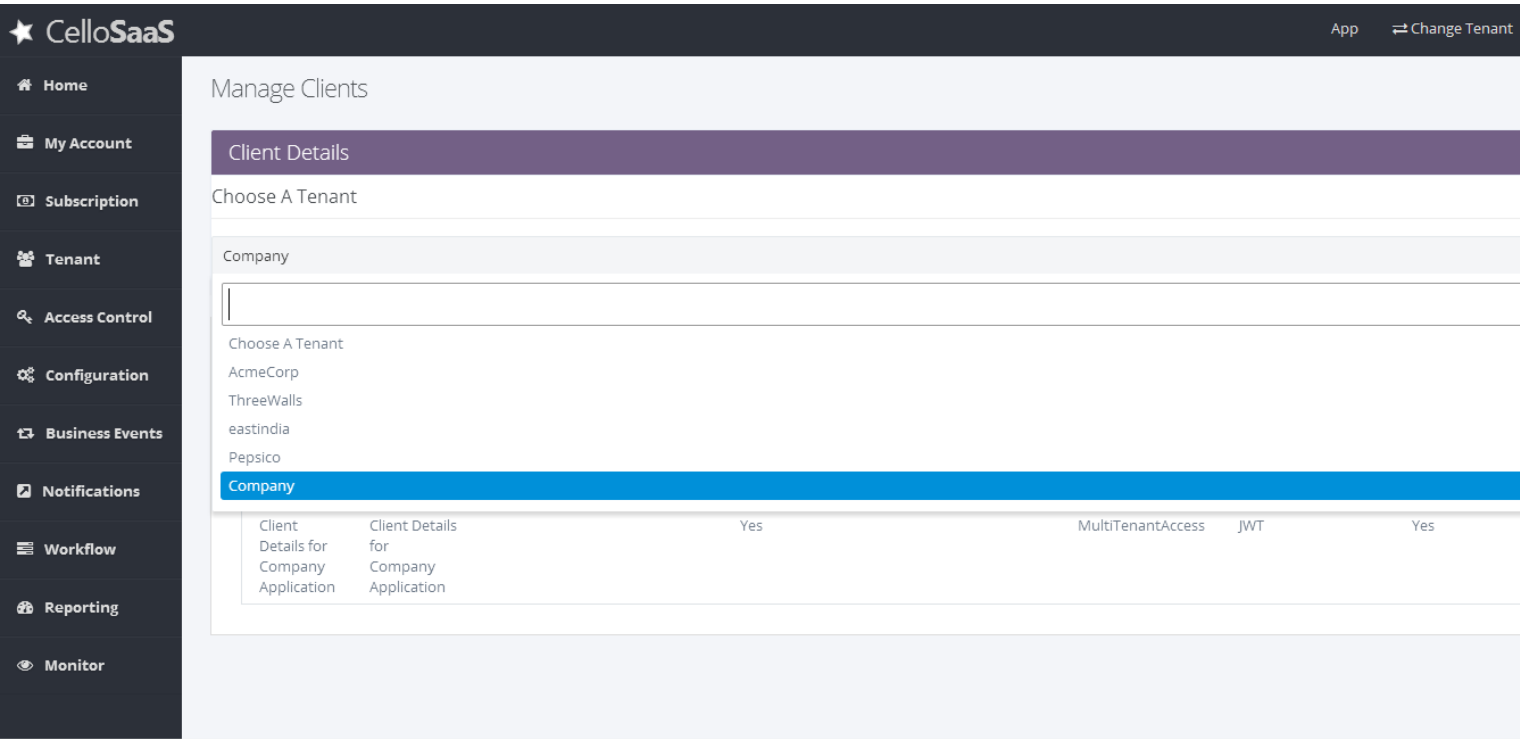


Fig: Manage Clients at ISV level

Whenever a tenant is provisioned with a URI, a client is automatically created and then mapped to the tenant based on the configured default values. This client defaults to the "InternalWeb" application type. However, a tenant can have other types of clients such as "MultiTenantAccess" so that any application within the tenant can consume the client. This client management process applies to the self-registration process also.

**Note:** The ISV Admin alone has access to the client management wherein he can pick a tenant and then manage the tenant's clients, like adding a new one, updating the existing ones etc.

Client Details for "Admin Client App"

Name	Admin Client App	Description	Admin Client App..
Secret	*****	Client Type	Web
Uri	https://company.cello.com:443/	LogoUri	
RequireConsent	<input checked="" type="checkbox"/>	AllowRememberConsent	<input checked="" type="checkbox"/>
Flows	Code	RedirectUri	http://localhost:51632/Account/AuthorizationCallBack
SigningKeyType	Default	ApplicationTypes	InternalWeb
IdentityTokenLifetime	60	AccessTokenLifetime	360
RefreshTokenLifetime	60	AuthorizationCodeLifetime	60
ScopeRestrictions		AccessTokenType	JWT
Is Publicly Accessible	<input checked="" type="checkbox"/>		

Save Cancel

**Fig: Client Particulars**

## 1.3 Applications targeting Authorization server

Any application that requires using the authorization server will have to perform the following three steps

1. Client Identification,
2. Resolving the client redirection URI
3. Scopes [means for filtering application access to resources]

Requesting the Authorization server can be done either by using Cello Middlewares or Microsoft .Net WebClient / HttpClient. The authorization server will return the user profile information in a JSON format which will be used by the client application to log the user into the application.

## 1.4 Tenant Provisioning Process

Tenants can be provisioned through one of the following ways.

- Self-Registration  
A Tenant can self-register himself undergoing an approval process. In the process of registration, the tenant also has options to set the identity and authentication profiles.
- Enterprise Tenants  
Any tenant that will be provisioned into the application by the ISV admin will also be required to choose the identity and authentication profile.

**Fig: Tenant self-registration page with the identity provider and authentication type options.**

## 1.5 Tenant Management

All tenants are required to sign-up with a specific identity and authentication provider and these cannot be changed in later point of time. The users of the tenant will have to comply with the same identity provider with an option to choose the authentication type for the corresponding identity provider has been opted, by the tenant. By default these are set to Cello Open ID

Authorization Providers

Identity Provider

CelloOpenId

CelloOpenId

LDAP

Social Logins

Authentication Types

Tax Rate

Description

Name	Description	Percentage	Order
------	-------------	------------	-------

+ Add

Fig: Options to choose an Identity Provider

Authorization Providers

Identity Provider

Social Logins

Authentication Types

Twitter

Facebook

Google

Tax Rate

Description

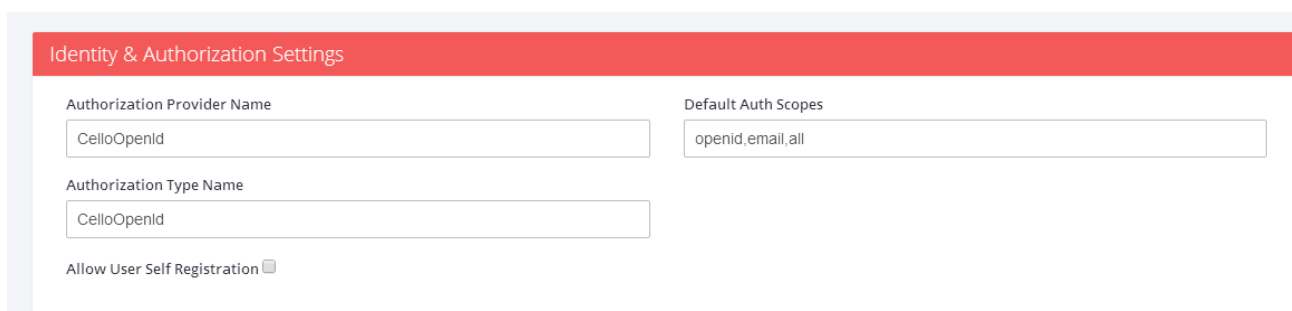
Name	Description	Percentage	Order
------	-------------	------------	-------

+ Add

Fig: Options to choose an Authentication Type [Identity Provider : Social Logins]

When a tenant is being provisioned with a specific URI, a separate client is provisioned along with it and is made accessible to that tenant with application type value set to “InternalWeb”. To opt for an On-Premise Identity and authentication, the tenant should provision the on-premise authorization server in a single-tenant mode and provide that URI during tenant creation.

Any tenant that wishes to open-up a user self-registration can do so through the account settings portal.



**Fig: Enabling Self registration process**

**Note:** This option to be exercised with caution as this will reflect in the billing. Any user that is registered does not reflect immediately in the billing, unless the approver approves the user.

## 1.6 User Management

Any user, be it an ISV admin or Tenant Admin or a member of the application has to be covered under an identity provider, In Techcello the default value is CelloOpenId.

The authentication types which support the process of user registration are

- Social Logins [Google, Facebook, Twitter]
- CelloOpenId Connect
- LDAP [On-Premise]

The user actions matrix below provides the action capabilities of each of the authentication type.

Function	Social Logins	CelloOpenId Connect	LDAP
First Time User	-	Yes	-
Force Password Reset	-	Yes	-
Password Change	-	Yes	-
Registration	Yes	Yes	Yes
Approval Cycle	Yes*	Yes*	Yes*
Expire Passwords	-	Yes	-

\* - only for registered users

Each user should have username that should match with that of the identity provider.

**Example:** User with mobile number login for Twitter should register / be created with the mobile number as the user name.



## User Registration process

The process of registration varies for each of the authentication methods. Self-registration is available only if the tenant has enabled it.

### *Cello Open-Id*

- The user gets the login page
- Clicks on the register link
- Prompted for the registration parameters
- Signs – up
- Gets notified about the registration status
- Approver gets the notification about the registration
- Approver approves the user
- User gets notified about his approval
- Users logins in and uses the application

### *LDAP*

- The user tries to login through the login page
- First time users will be redirected to the registration page
- If prompted the user has to update the registration parameters
- Signs – up
- Gets notified about the registration status
- Approver gets the notification about the registration
- Approver approves the user
- User gets notified about his approval
- Users logins in and uses the application

### *Social Logins*

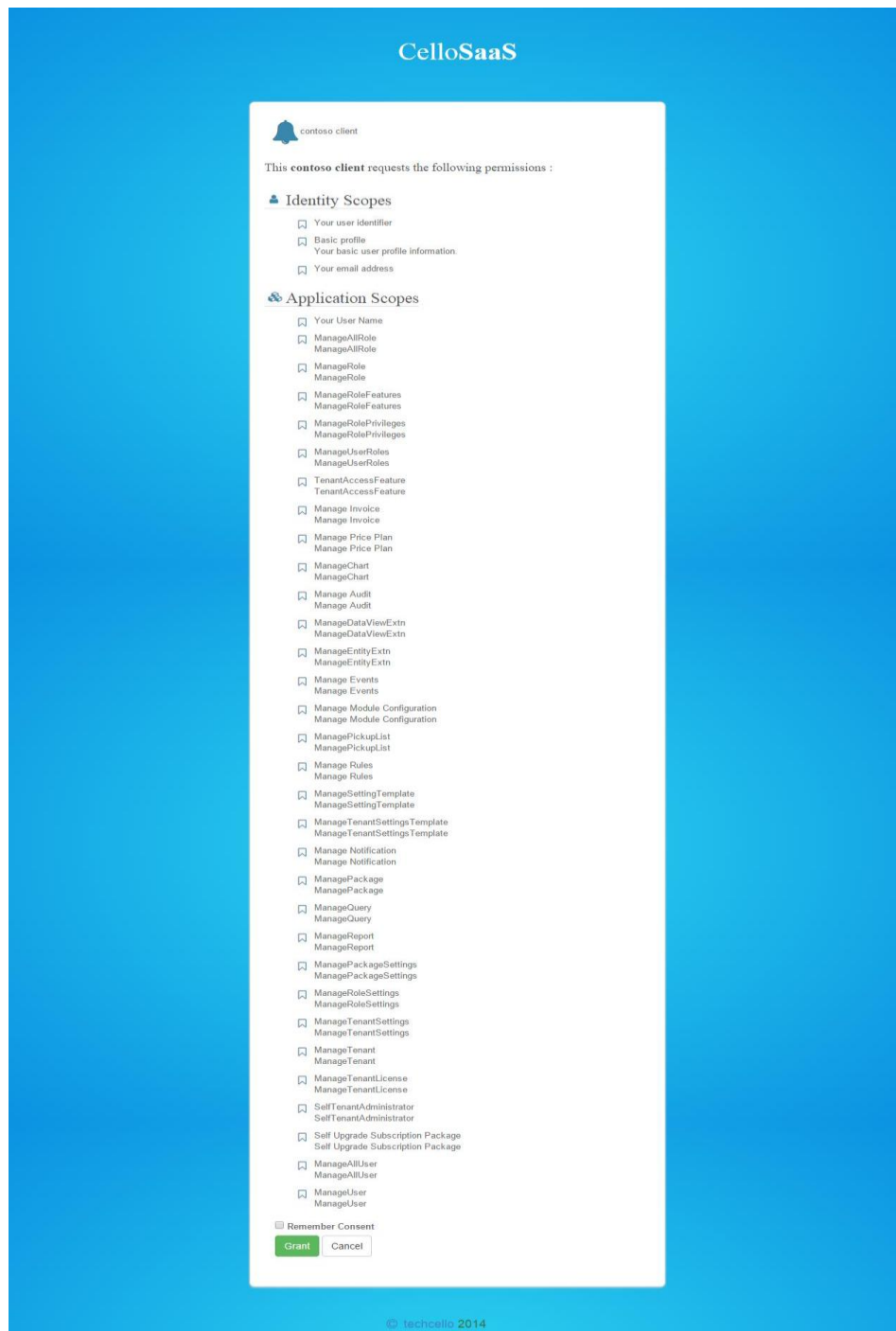
- User logs in to the application via any social login [Google / Facebook / Twitter]
- Upon successful authentication, user is returned back to the Authorization Server
- Upon registration, the user will be able to use the system after the user is approved by the approver

## User Consent Management

User Consent page, lists the features which the client requires the user to agree upon, so that the client can use those on-behalf of the user. This consent will be persisted or be shown to the user on each login based on the different criteria such as

- The client requires consent and does not remember consent
- The client requires and remembers consent

- The application type of “InternalWeb” will have the consent page only when authorization server is operating on a single tenant mode.



**Fig: Consent page**

**A user can revoke these permissions which they consented earlier.**

## 1.7 *Setting up a Tenant*

A tenant can be setup using different authentication providers using different steps depending on the authentication provider.

### Using Social Logins

For a tenant to use a social login authentication, they have to choose the option “Social Logins” from the list of identity providers that are shown either at the “Manage tenant” or the “Self-Registration” page.

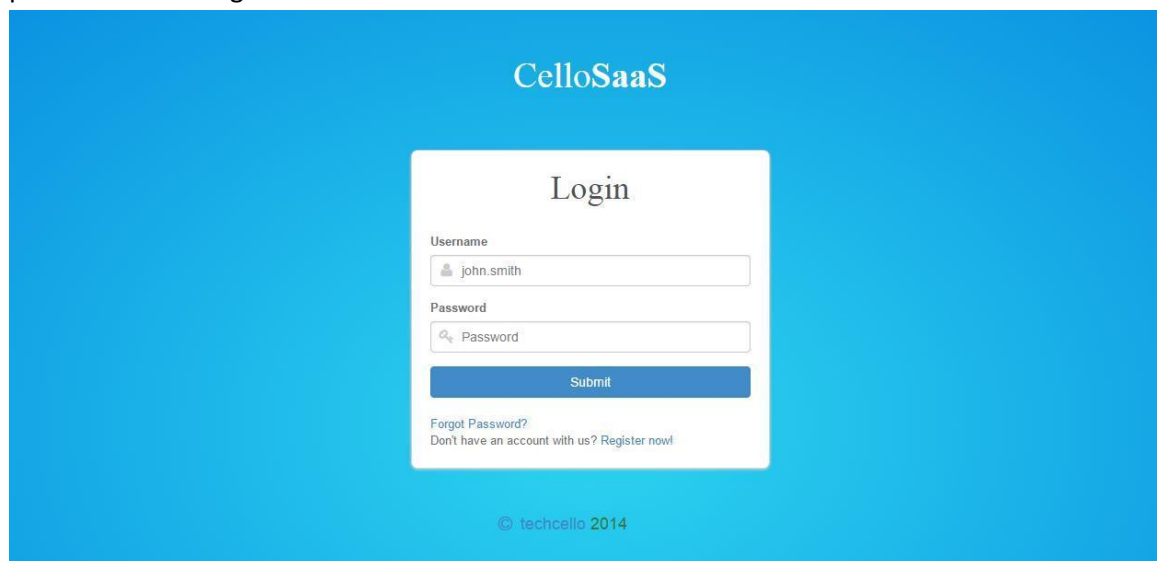
Once setup, the tenant admin and the users will be required to login to the application through the authentication type chosen.



**Fig: Opting social authentication at login**

## Using Cello Open Id Connect

By default the authorization method for Techcello will be Cello open ID connect. This is a username and password based login.



**Fig: Opting Cello/LDAP authentication at login**

The tenant can choose Cello Open Id Connect from either the “Manage tenant” or the “Self-Registration” page. Once setup, tenant admin and users are required to login to the application via Cello Open Id.

## Using Active Directory

This model is useful for tenants planning to use the Active directory via the On-Premise AD. The Authorization Server should be setup in the client On-Premise server which can gain access to the Active Directory. The configuration should be set to work in the Single-Tenancy Mode and the database should be up with the corresponding tenant, client and other settings. All the Active Directory users have to be imported to the On-Premise database. The authorization server URI should be set in the servers “authserverconfig.json” file.

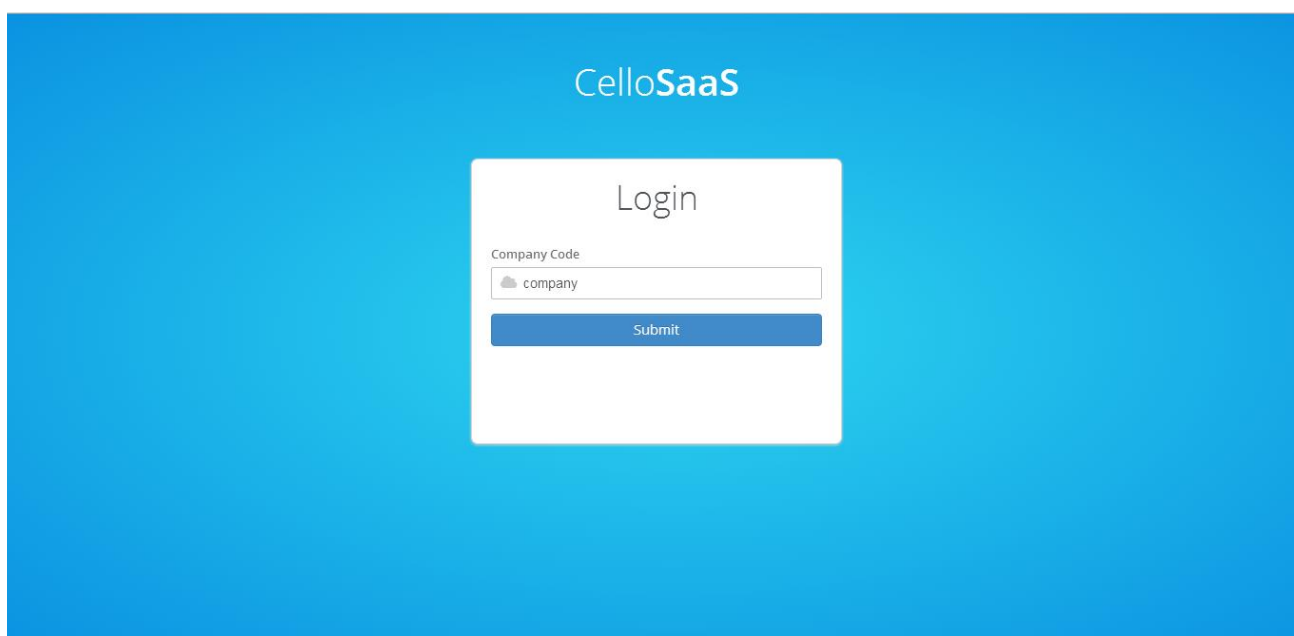
In this mode of operation, the following is the request flow

- User accesses the client application
- Redirection happens to the authorization server
- Authorization server identifies the tenant, client and based on the identity provider, identifies the On-Premise server URI
- The request is redirected to the On-Premise Authorization server
- Upon successful authentication, the user is redirected back to the authorization server
- The Authorization server provides the received token information back to the caller [client application]

## Cello as Open Identity Provider for clients

To open up Cello Identity for the client applications, the following steps are to be followed

- The client has to be registered with the corresponding client application type
- The tenant is required to use Cello Open-Id as the Identity provider
- Client access the authorize end point of the Authorization server
- Cello Open-Id authentication happens
- In case the client has been registered as a Multi-Tenant access type, the client will be shown with a custom page that will require a company code
- The company code identification happens to let the authorization server know the appropriate client settings for authentication to happen
- In case of the client registering with other than the Multi-Tenant Access mode, the client will be shown the corresponding identity page instead of the company code identification page



**Fig: Company code identification**

When the Authorization server is configured to work as a multi-tenant access mode, the client can be used by any application that will be required to identify the company code. If the authorization server is dedicated to a client, the company code identification is not shown and is inferred from the client profile.

In case of using the Authorization server other than the “InternalWeb” application type, the authorization shows the consent page if the client does not override the consent page display in the client profile.

## Endpoints

The following are the end points used within the Authorization Server

- Authorize End point [initial access]

- b. Token End point [Responsible for the generation of the access / identity tokens]
- c. User Info End point [Provides the user profile information]
- d. Cache End point [for flushing authorization server cache]
- e. Client End point [For managing clients & user consents from the client application]

### Authorization Server Configuration

The authorization is extensible with respect to the following

- a. Pluggable Services
- b. Configuration aspects
- c. View Pages customizations
- d. Validators
- e. Claim Maps

## 2 Contact Information

Any problem using this guide (or) using Techcello Framework. Please feel free to contact us, we will be happy to assist you in getting started with Techcello.

**Email:** [support@techcello.com](mailto:support@techcello.com)

**Phone:** +1(609)503-7163

**Skype:** techcello