Installation Guide

Explore and Checkout for Off-Platform Usage (DC WC + DC SDK)

**Table Of Contents**

**Installing the Org DX DataPack 4**

**Installing the Vlocity DC VIP MultiPack file containing VIP for the checkout process 4**

**Installing the DC WC Reference Application 4**

**Retrieving the SDK and WC from the npm registry 4**

**Setting up a Digital Commerce Server SDK Reference Implementation 5**

**How to use Server SDK in DC WC 15**

#### **Whitelisting URL in Secure Server App 19**

**Setting up Cross-Origin Resource Sharing (CORS) in Salesforce 19**

**Create CSP Trusted Sites to Access Third-Party APIs 20**

Access to the Vlocity Process Library requires acceptance of the disclosure below:

**RESTRICTED CONTENT: AUTHORIZED USE ONLY**

***The content on the following pages is intended to be viewed only by Vlocity employees, contractors who have been authorized by Vlocity or customers who have been authorized by Vlocity. The content should be considered the sensitive confidential information of Vlocity and is protected under the nondisclosure agreement entered into between your party and Vlocity. Accordingly, further distribution is prohibited without prior written consent from Vlocity.***

***I Accept Vlocity’s Terms and Conditions*** [***https://vlocity.com/terms***](https://vlocity.com/terms)

**Installing the** **Org DX DataPack**

To run the sample application, you use the Vlocity DX desktop application to migrate the Vlocity DataPack from the Vlocity Process Library to your org.

1. Install the latest DX tool from [https://docs.vlocity.com/en/Vlocity-DX-Desktop-Application.htm](https://docs.vlocity.com/en/Vlocity-DX-Desktop-Application.html)
2. Download the DX org data pack and unzip it.
3. Open the DX tool and select your unzipped DX org DataPack folder as the repository.
4. Select your unzipped DX org DataPack folder as the Source.
5. Select your Salesforce org as the Target.
6. Click on a new project and specify a name (such as ImportDCOrgData).
7. Select **VlocityTypes** as **all** and **Salesforce Types** as **all**.
8. Click **Fetch DataPacks** and then click **Save**.
9. Click **Migrate With Dependencies**.

**Installing the Vlocity DC VIP MultiPack file containing VIP for the checkout process.**

1. Go to **Vlocity Integration Procedure Designer**.
2. Click **Import** and choose the VIP multipack, then click **Next**.
3. Click **Deploy**.

**Installing the DC WC Reference Application**

1. Download the file UI\_Partner.zip and unzip the contents.
2. Copy the authorization token from the Vlocity Project Team and paste it into the .npmrc file.
3. Run **npm install** and then run **npm start** in the root directory
4. Run the app by using a navigating to [http://localhost:8081](http://localhost:8081/)

**Retrieving the SDK and WC from the npm registry**

1. Add **digitalcommerce-sdk** and **digitalcommerce-components-src** dependency in your package.json file.

"@vlocity-cme-sdk/translation-sdk": "^109.0.1",

"@vlocity-cme-sdk/digitalcommerce-sdk": "^109.0.1",

"@vlocity-cme-wc/digitalcommerce-components-src": "^109.0.0"  
 "@vlocity-cme-sdk/account-sdk": "^109.0.1",

2. Add .npmrc file. The .npmrc file is required to authenticate with the Vlocity private npm registry. For public access please use the default access token.

email=your\_email\_id

always-auth=true

\_auth= “PROVIDE VALID AUTH TOKEN”

registry=<https://repo.vlocity.com/repository/npm-public/>

3. For the authorization token please contact Vlocity Support Team.

**1.** To fetch the modules required, run **npm install.** The Digital Commerce WC’s artefacts will be found in the node\_modules folder.

**Setting up of Digital Commerce Server SDK Reference Implementation**

Server SDK Reference Implementation app is a node application that could be deployed to any of the hosting servers for eg. Heroku, AWS, etc

### **Step 1: Download Server SDK Reference App** Download Server SDK Reference App from the VPL.

### **Step 2: SF Org Setup**

In Server SDK we are using OAuth 2.0 JSON Web Token (JWT) bearer flow to authenticate a server. Therefore, we re require to -

* Generate a public/private key pair
* Create a Connected App

#### **Generating public/private key pair**

Generate a public/private keypair using openssl and fill in the required info when you generate the certificate.

openssl req -newkey rsa:2048 -nodes -keyout private\_key.pem -x509 -days 365 -out certificate.pem

openssl x509 -outform der -in certificate.pem -out public\_key.der

openssl x509 -in certificate.pem -pubkey > public\_key.pem  
See Doc: <https://github.com/lekkimworld/salesforce-jwt-generator>

#### **Create connected APP & upload CER file (ie certificate) to SFDC**

In Salesforce create a Connected App through the App Manager in Setup and upload the public key (public\_key.cer from the above steps) to the app. Be sure to select the offline\_access scope as well as other required scopes. Save the Connected App and make a note of the **consumer key (issuer\_id).**See Doc: <https://help.salesforce.com/articleView?id=connected_app_create.htm&type=5>

### **Step 3: Auth Config**

Server SDK app has an authentication layer which is responsible for validating a user identity against an authentication server like Firebase, Cognito etc. A reference implementation using Firebase as an authentication strategy has been used in the app by default. However, you could easily swap firebase for any other third party authentication system by creating a custom authentication strategy.

* Create a folder inside *vop\_server\_sdk/secure-server-reference-app/authentication/strategies* directory and inside it create a file and Implement IAuthenticationStrategy interface. The implementing class should define the properties with the corresponding method of the third party authentication system. For example, the implementation of signIn method should have the signIn logic of your third party authentication system that you want to use.
* Once you have created your custom authentication strategy, open *AuthenticationStrategy.ts* file and import your customise strategy and initialise it inside the constructor.

### **Step 4: Setting up** config.json **file**

find config.json file in vop\_server\_sdk/secure-server-reference-app/config.json  


* Enter the **consumer key (issuer\_id)** which you noted down in step 2.
* **org Id -** Enter the **username** of the salesforce user.
* **org namespace** - enter the SF org namespace.

### 

### 

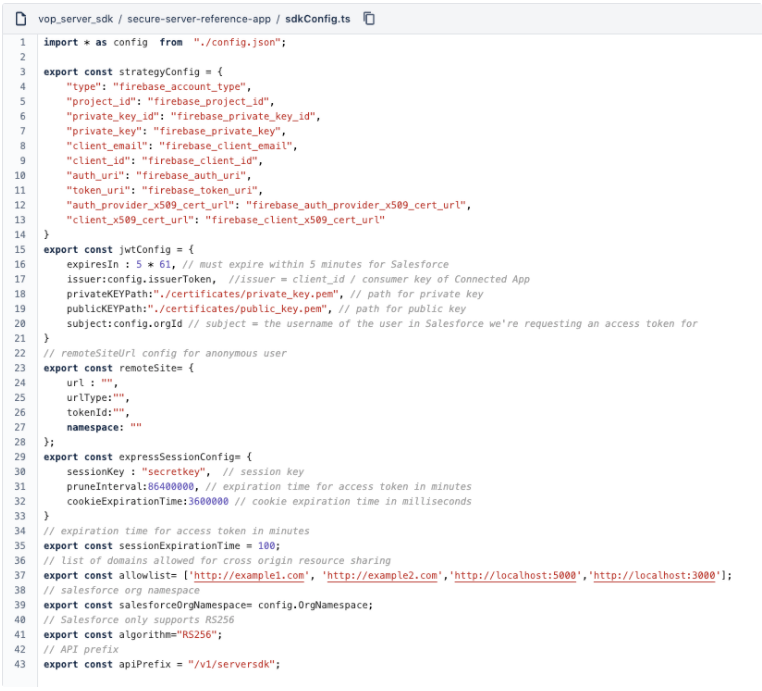
### 

### 

### 

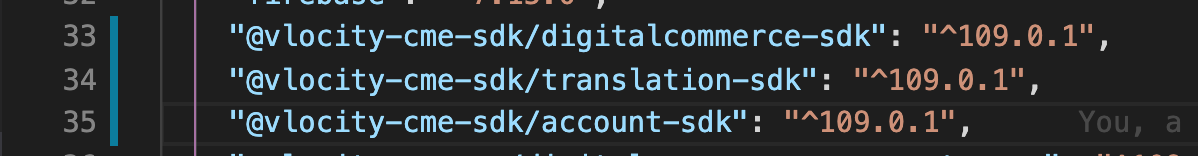
### 

### **Step 5: Setting up** sdkConfig.ts **file**

find sdkConfig.ts file in vop\_server\_sdk/secure-server-reference-app/sdkConfig.ts  


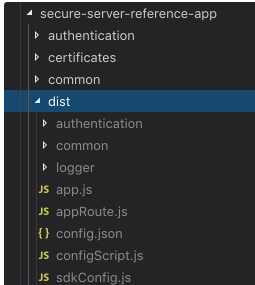
* **strategyConfig**: If you're using default firebase as authentication server then just set a strategyConfig object.
* **jwtConfig:** Paste private\_key.pem & public\_key.pem files generated from step2 in vop\_server\_sdk/secure-server-reference-app/certificates folder for JWT sign
* **remoteSite:** for anonymous users, url will be anonymous URL of org & namespace will be org namespace.
* **allowlist:** when you're requesting from cors domain then you need to whitelist that domain here.

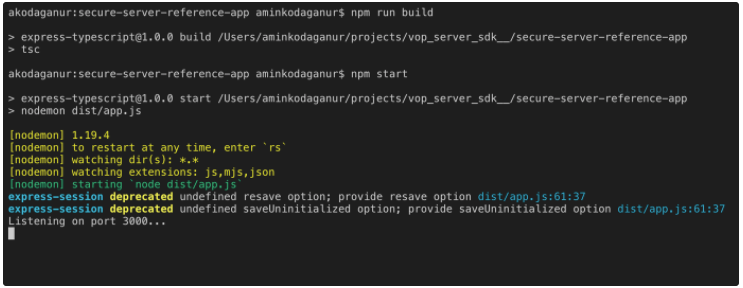
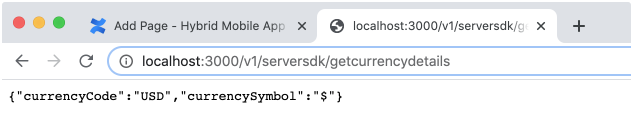
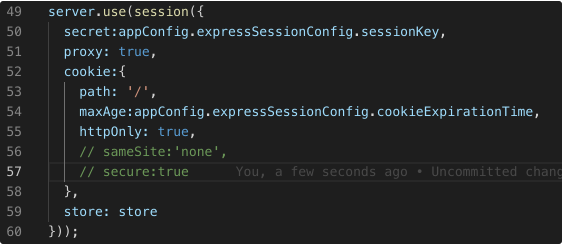
### **Step 6: Setting up** package.json



* In vop\_server\_sdk/secure-server-reference-app/package.json file under dependencies object please update SDKs with 109 version  
  **Note:** please make sure you add a .npmrc file. The .npmrc file is required to authenticate with the Vlocity private npm registry. For public access please use the default access token.

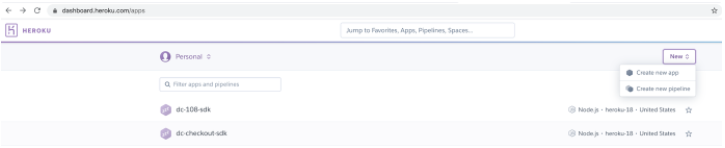
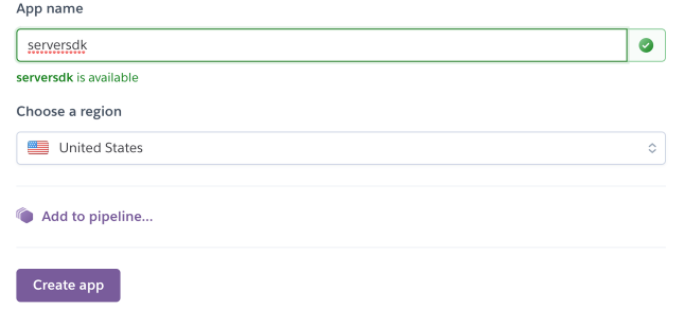
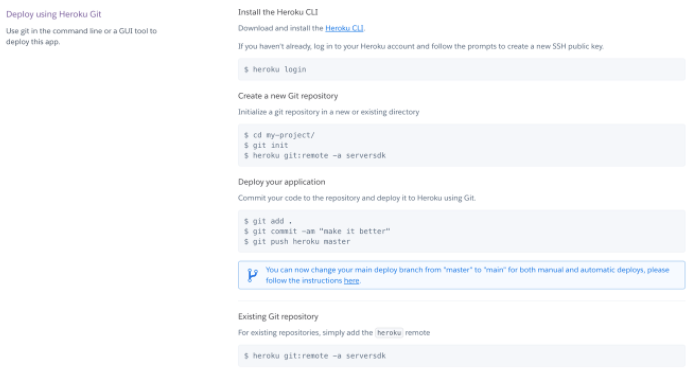
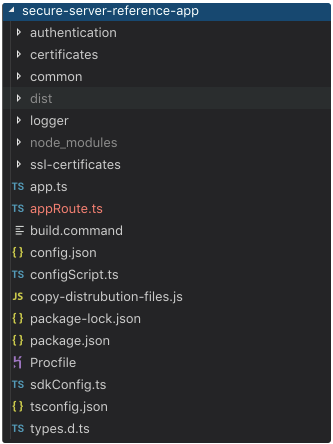
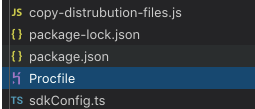
### **Step 7: Running in local machine (Optional)**

* Open root directory(vop\_server\_sdk/secure-server-reference-app) in the terminal.
* run $ npm install will install all dependency.
* run command below commands  
    
   $ npm run build - will take few seconds to compile & build typescript files  
  Once this is successful it will generate /dist folder in the root directory.  
    
  Now the $ npm start will run the server.  
  Your terminal logs should look like below

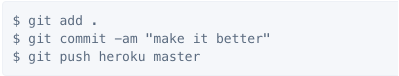
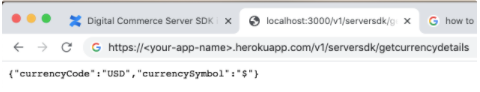
  
  
By default server will start listening to port no 3000 so now base API URL will be  
http://localhost:3000/v1/serversdk  
  
 Just to test if the api is working fine you can hit http://localhost:3000/v1/serversdk/getcurrencydetails in the browser it will fetch default currency details.  
  
**Note:** make sure you comment below lines in vop\_server\_sdk/secure-server-reference-app/app.ts these settings required only when you host in third party server like heroku  


### **Step 8: Deploying in heroku**

You can deploy/host this ServerSDK application in any node supported server. one of famous server is heroku below are steps to deploy/host in same

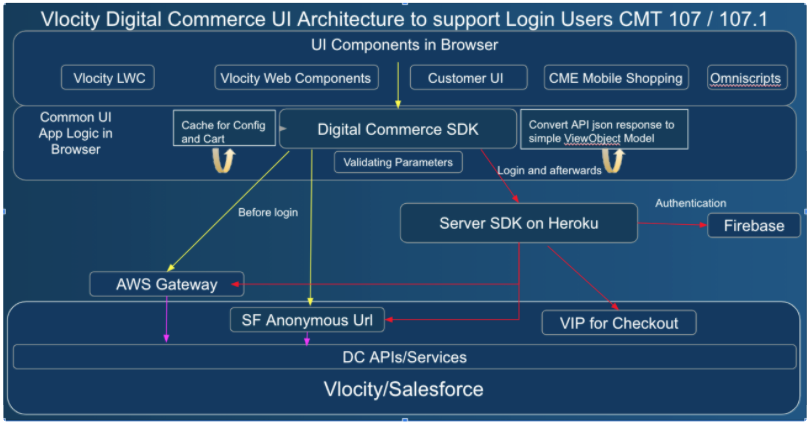
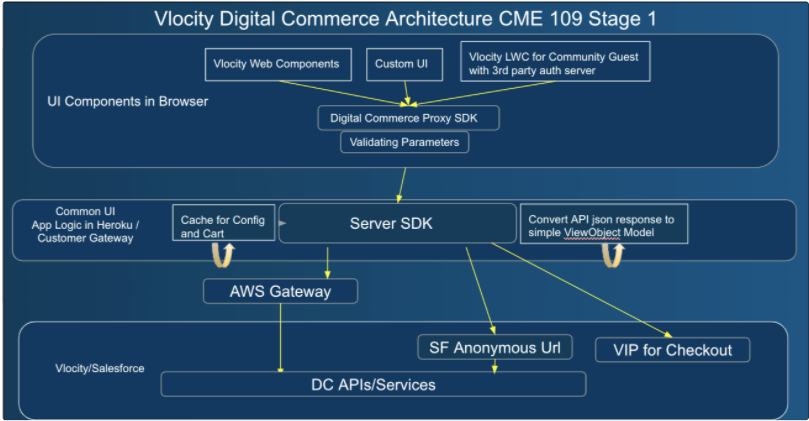
* Login to your Heroku account  
  <https://id.heroku.com/login>
* Click New button & select Create a new App from Dashboard  
  
* Enter app name & click create app button  
  
* Navigate to deploy tab  
  
* Follow Deploy using heroku git doc  
  
* After following the above step you should have a folder where you have cloned/setup with git heroku origin.  
  now we need to copy our serverSDK into heroku cloned/setup folder  
  Copy entire files under vop\_server\_sdk/secure-server-reference-app  
    
  Note: no need to copy dist & node\_modules folder
* create a new file with Procfile in root of heroku cloned/setup folder. It should look like below  
  

Paste below contain into Procfile file  
web: npm run start-prod-server  
this will run our serverSDK in heroku after code push.

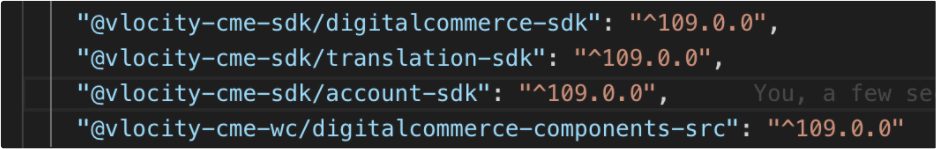
* Now open heroku cloned/setup folder in terminal, commit & push the files to heroku.  
  
* Once you push code Heroku will automatically detect as NodeJS app it will create build & start serving. Your log should look like below once you push  
    
    
  Notice it will log base API URL at end in above case it’s https://server-sdk-109-pref.herokuapp.com/
* Once you pushed & deployed successfully your base URL will be  
   https://<your-app-name>.herokuapp.com/v1/serversdk  
  You can also find it in Heroku dashboard > Settings > Domains section  
  **Note:** /v1/serversdk is a default API prefix you can change it vop\_server\_sdk/secure-server-reference-app/sdkConfig.ts
* To verify if heroku setup is working fine open browser and hit below your  
   https://<your-app-name>.herokuapp.com/v1/serversdk/getcurrencydetails it will fetch default currency details  
  

## **How to use in DC WC & LWC:**

We can you use Server SDK in two ways

* **With Client side SDK:** This is same as v107 implementation where DC API will be called directly from client for guest user after signIn all DC API will be called from ServerSDK below is architecture of it  
  
* **With Proxy SDK:**In this case all DC API will be called from Server SDK. We can easily implement it by using Proxy SDK library which is very light weight and shares the same signatures as other SDK so that there will be no change required in UI code to support this. Below is architecture of it  
  

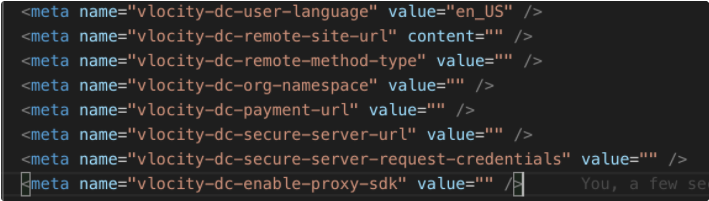
**DC WC Setup:**

**Step 1:**Add SDK & digitalcommerce-components-src in your package.json file.  


**Step 2:**

Add .npmrc file. The .npmrc file is required to authenticate with the Vlocity private npm registry. For public access please use the default access token. For the authorization token please contact Vlocity Project Team.  

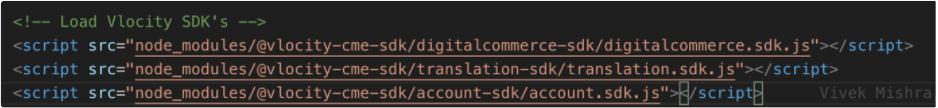

**Step 3:**

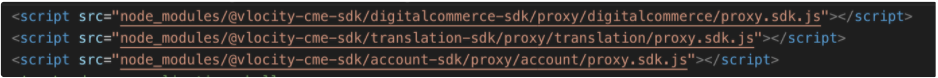
In your index.html add and define below meta tag  


* meta tag with name attribute (vlocity-dc-remote-site-url) contains content attribute which can be SalesForce instance URL for known users and AWS url for anonymous users.
* meta tag with name attribute (vlocity-dc-remote-method-type) has attribute value which specifies logon method which can either be "knownUser" for known users and "anonymousUser" for anonymous users.
* meta tag with name attribute (vlocity-dc-org-namespace) has value attributes which contains org namespace.
* meta tag with name attribute (vlocity-dc-payment-url) has value attributes which contains checkout payment URL.
* meta tag with name attribute (vlocity-dc-secure-server-url) has value attributes which contains the url where server SDK is hosted.
* meta tag with name attribute (vlocity-dc-secure-server-request-credentials) has value attributes which contains value indicating whether the user agent should send cookies to the secure server if it's hosted on another domain in the case of cross-origin requests. Possible values are:include,omit and same-origin(default value)
* meta tag with name attribute (vlocity-dc-enable-proxy-sdk) has value attributes which contains value “enable”. If it set to enable: Digital Commerce, Account, Translation Proxy SDK instance will be created

**Step 4:**

In your index.html import SDK using script tag

If using **Client side SDK  
**

Or if using **With Proxy SDK  
**

**Step 5:**

**From you JS file import SDK-util file &**

import { digitalCommerceSDKInstance } from "@vlocity-cme-wc/digitalcommerce-components-src/vlocity-dc-utils/vlocity-dc-sdk-utils";

**Get SDK instance**  
this.digitalCommerceSDK = digitalCommerceSDKInstance().digitalCommerce;

**Call SDK Methods**  
let input = this.digitalCommerceSDK.createGetOffersInput()  
this.digitalCommerceSDK.getOffers(input).then(response => {});

#### 

#### 

#### 

#### 

#### 

#### 

#### 

#### 

#### **Whitelisting URL in Secure Server App**

Secure server reference app uses cookies to persist user sessions. These cookies are not sent by default over CORS.Therefore, you need to whitelist the client URL from where you would be accessing the server. This could be configured in the property whiteList of **sdkConfig.ts** filepresent in the root directory.

**Fixing CORS issue on client side**

If the origin of your client application is different from that of the secure server you would get a CORS issue due to [Same-origin policy](https://developer.mozilla.org/en-US/docs/Web/Security/Same-origin_policy) and hence resource sharing between client and server will not take place. Therefore to fix the CORS issue you need to follow two steps -

1. Whitelist the client origin URL on the server SDK reference app.
2. Make sure to include credentials: 'include' in the request header options for REST calls.

In CME 109 to add credentials: 'include' property you can override the Digital commerce SDK checkout methods to create the REST API body and attach credentials: 'include' in the options of the request header. Then using datasource SDK we can invoke the REST API call to the server.

**Setting up CORS in salesforce**

Cross-Origin Resource Sharing (CORS) enables web browsers to request resources from origins other than their own (cross-origin). For example, using CORS, JavaScript code at https://www.example.com could request a resource from https://www.salesforce.com. To access supported Salesforce APIs, Apex REST resources, and Lightning Out from JavaScript code in a web browser, add the origin serving the code to a Salesforce CORS whitelist.

1. From Setup, enter CORS in the Quick Find box, then select CORS.
2. Select New.
3. Enter an origin URL pattern.  
   The origin URL pattern must include the HTTPS protocol (unless you’re using your localhost) and a domain name and can include a port. The wildcard character (\*) is supported and must be in front of a second-level domain name. For example, https://\*.example.com adds all subdomains of example.com to the whitelist.  
   The origin URL pattern can be an IP address. However, an IP address and a domain that resolve to the same address are not the same origin, and you must add them to the CORS whitelist as separate entries.  
   The origin URL pattern might not match the URL that appears in the address bar in your browser. Make sure that you’re whitelisting the origin in the request header.

Note - For the salesforce document on CORS follow this [link](https://help.salesforce.com/articleView?id=extend_code_cors.htm&type=5).

# **Create CSP Trusted Sites to Access Third-Party APIs**

The Lightning Component framework uses Content Security Policy ([CSP](http://www.w3.org/TR/CSP/)) to impose restrictions on content. The main objective is to help prevent cross-site scripting ([XSS](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))) and other code injection attacks. To use third-party APIs that make requests to an external (non-Salesforce) server or to use a WebSocket connection, add a CSP Trusted Site.

1. From Setup, enter CSP in the Quick Find box, then select CSP Trusted Sites.
2. Select New Trusted Sites.
3. Enter Trusted Site Name
4. Enter Trusted Site URL

You can use the wildcard character \* (asterisk) to reduce repetition. The URL must include a domain name, and can include a port. For example, https://example.com:8080. For a third-party API, the URL must begin with https://.

1. Enter Trusted Site Description

Note - For the salesforce document on creating CSP Trusted Sites follow this [link](https://help.salesforce.com/articleView?id=csp_trusted_sites.htm&type=5).

**Note**: Post Winter’21 , user need permission to access an Apex class containing an @AuraEnabled method to access in LWC’s.

**How to update profiles and permissions to access Apex with @AuraEnabled**

In setup, you can add Apex classes to a profile under “Enabled Apex Classes Access”. For a permission set, you’ll see it under Apps as “Apex Class Access”.