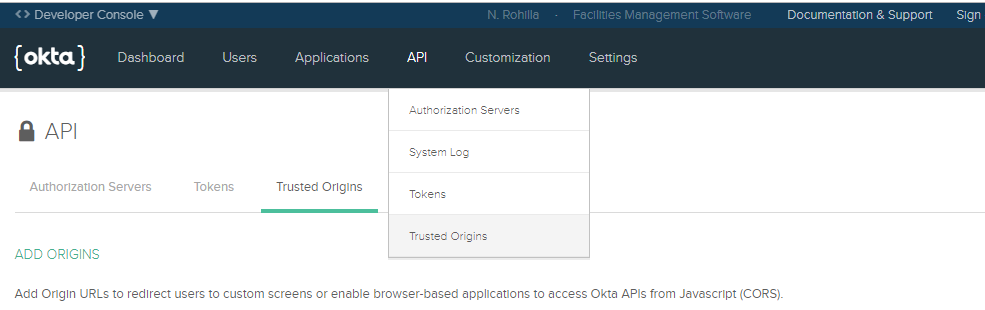
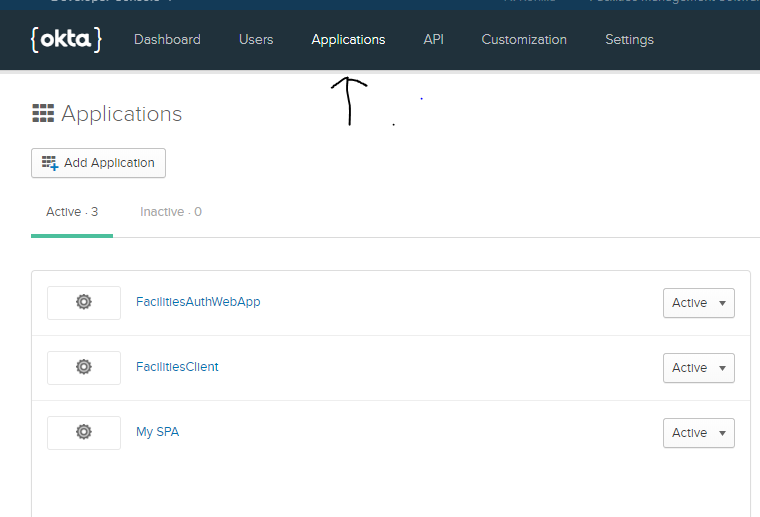
**Changes needed for new domains for the environment in Okta for the applications**

1. Please log in to the admin account of okta account
2. We need to first do the CORS settings in Okta. Please Go to > API> Trusted Origin

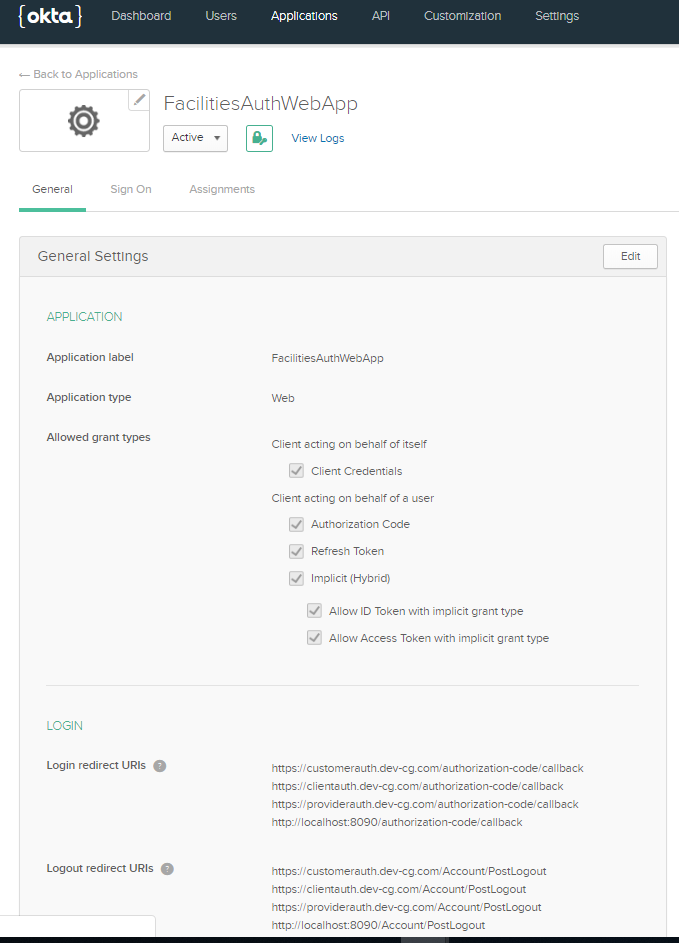


Here please put the domain URL of your application. This is needed to allow the applications to communicate with the Okta making the domain whitelisted in Okta. Else the requests will be blocked.

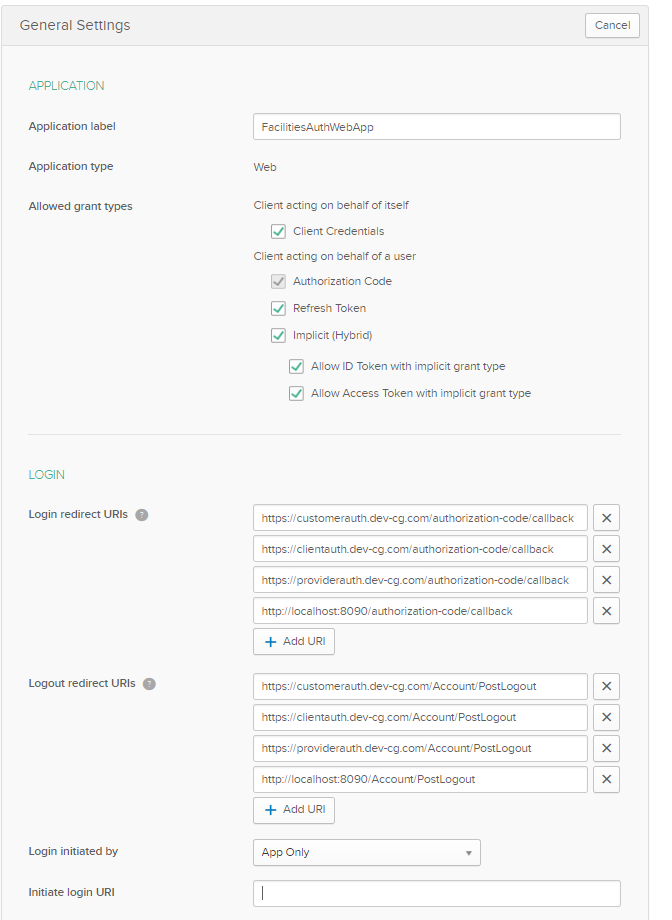
1. We now need to put the authorization settings for the application to allow Okta to redirect the user to the respective application after successful authentication. Please go to Applications Menu at the top



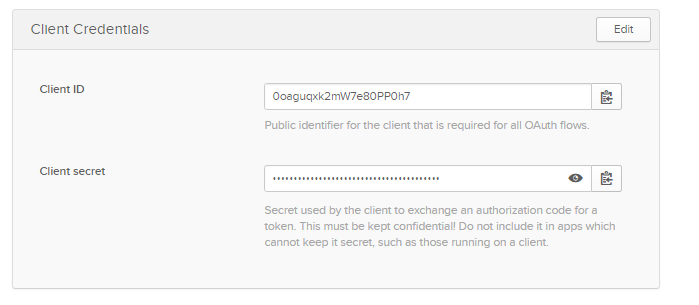
1. Please click on the Application. In our case for dev environment, it is “[FacilitiesAuthWebApp](https://dev-857564-admin.oktapreview.com/admin/app/oidc_client/instance/0oaguqxk2mW7e80PP0h7/" \o "OpenID Connect Client)”. After clicking it, the user will land on below page where the settings need to be configured:

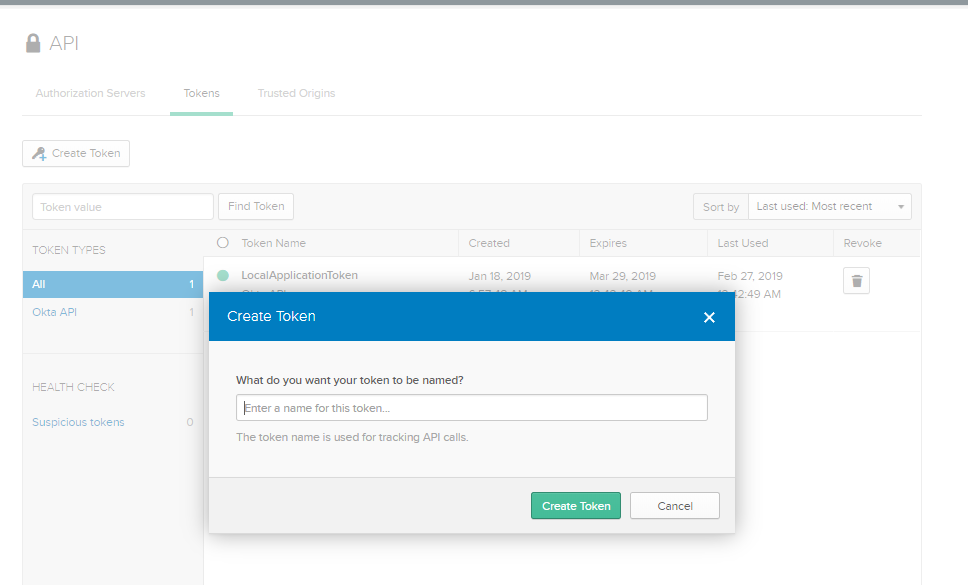


1. Please select “General” Tab. And click on “Edit” inside this panel. The input fields in sections “Login redirect URLs” and “Logout redirect URLs” will get editable as shown below:



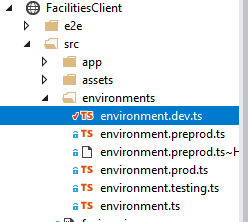
1. Enter the base URL of your authentication project from which the request of authentication is going to the Okta. In the Login Urls fields, please append the domain/Base URL with “authorization/callback”. In the “Logout redirect URls” section’s fields, please append the domain/Base URL with “Account/PostLogout”.
2. Please also Note down the application key and the secret. These will go in the Auth Project’s Web.Config key



1. Please delete the “**Initiate login URI**” field’s values.
2. Please check all the checkboxes in “**Allowed grant types“ section**. This will give us the refresh and the access token after authentication.
3. Please create token to allow the application to identify itself to the Okta. Go to Menu “API” and click submenu “Tokens”. Please click on Create token button in the middle panel “Tokens”. Using this you can generate the token which is to be used by the angular application to authorize its identity to the Okta when calling its API. Please note down the value of this token once generated. This is shown below:
4. 

**Changes needed for new domains for the environment in Angular Projects**

1. Please open each angular application (Client/Customer/Vendor/PM) and go to environments folder as shown below:



1. Please change following fields values for the new domains (Fields may vary per application. This is client application’s environment file’s example):

export const environment = {

production: false, **// This will have value true for Production**

development: true, **// This will have value true for Development**

testing: false, **// This will have value true for Pre-Production**

PMModuleUrl: "https://pm.dev-cg.com/?PM", **// PM Module URL with new domain**

baseAPIUrl: "https://apinterface.dev-cg.com/API/",// **Services URL with new domain**

baseCustomerApplicationURL: "https://customers.dev-cg.com/#/",// **Customer App URL with new domain**

baseApplicationURL: "https://clients.dev-cg.com/#/", // **Client URL with new domain**

baseOKTAUrl: "https://dev-857564.oktapreview.com/api/v1/", // **Okta URL** (*Please exclude admin word from this URL*)

baseOKTAToken: "00CcFZ6xz4f9FHzHabgx3iVjcyffjqOe8ivv5GM7ut", // **This is Okta Application Token Step** 10 of previous Okta section

BaseAuthUrl: <https://clientauth.dev-cg.com//> **URL of the auth project**

};

**\*\***Above setting is to be done **for all the projects** for the particular environment (**Dev/PreProd/Prod**)

For dev: Please modify the .dev.ts file with the needed values

For PreProd: Please modify the .peprod.ts file with the needed values

For Prod: Please modify the .prod.ts file with the needed values

**\*\*** Environment folder may reside in “src” folder as well as it may reside inside the “app” folder in the application.

**Changes needed for new domains for the environment in Auth Project**

1. Please open the Auth Project and go to the Web.Config file in the root directory. Please change below values in the <appSettings> section

This is the Base API URL

<add key="Api:BaseUrl" value="https://apinterface.dev-cg.com/API/" />

This is the Client Angular Application URL for the environment

<add key="AngularClientApp:RedirectURL" value="https://clients.dev-cg.com/#/" />

This is the Customer Angular Application URL for the environment

<add key="AngularCustomerApp:RedirectURL" value="https://customers.dev-cg.com/#/" />

This is the Vendor/Provider Angular Application URL for the environment

<add key="AngularVendorApp:RedirectURL" value="https://providers.dev-cg.com/#/" />

This is the Client ID for the environment from the Okta

<add key="okta:ClientId" value="0oaguqxk2mW7e80PP0h7"/>

This is the Client secret for the environment for the okta

<add key="okta:ClientSecret" value="INgKYFEJg-yRVSlnezdsIoWNZQSjhS7reCUyzGmz"/>

This is the okta URL for the environment from Okta.

<add key="okta:OktaDomain" value="https://dev-857564.oktapreview.com/"/>

This is the Auth Application URL for the environment for Client Application

<add key="AuthApplication:RedirectUri" value="https://clientauth.dev-cg.com/Home/About"/>

This is the Auth Application URL for the environment to where the okta redirects user to on successful Authentication from Okta.

<add key="okta:RedirectUri" value="https://clientauth.dev-cg.com/authorization-code/callback"/>

This is the Auth Application URL for the environment to where okta redirects user to on Logout

<add key="okta:PostLogoutRedirectUri" value="https://clientauth.dev-cg.com/Account/PostLogout"/>

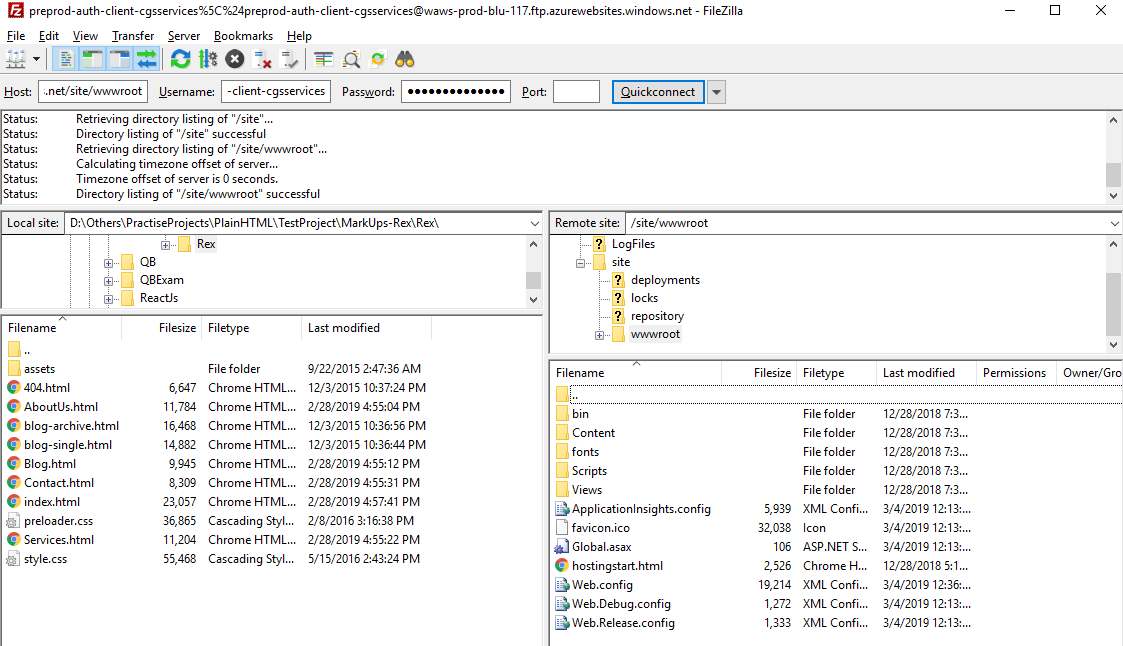
For Dev Environment, we only need to check in the Web.Config file. It should replicate the values to dev environment.

For Preprod and Prod environments, we need to connect to the publish location of Auth Project files using FileZilla. Use these values to connect to Published Files Location using FileZilla:

**publishUrl**=<ftp://waws-prod-blu-117.ftp.azurewebsites.windows.net/site/wwwroot> (Host in FileZilla)

**userName**="preprod-auth-client-cgsservices\$preprod-auth-client-cgsservices" (UserName in FileZilla)

**userPWD**="ynryb3JAn65pcfq5lxcbcCHMjnatYpQuTs6npnmYvyu7aoxxR1MRiZMxTvu7" (Password in FileZilla)



After connecting to the location where our files are uploaded on the right panel, Please download the Web.Config and update its values for the environment. Upload the file to this location upon changing with the right values.

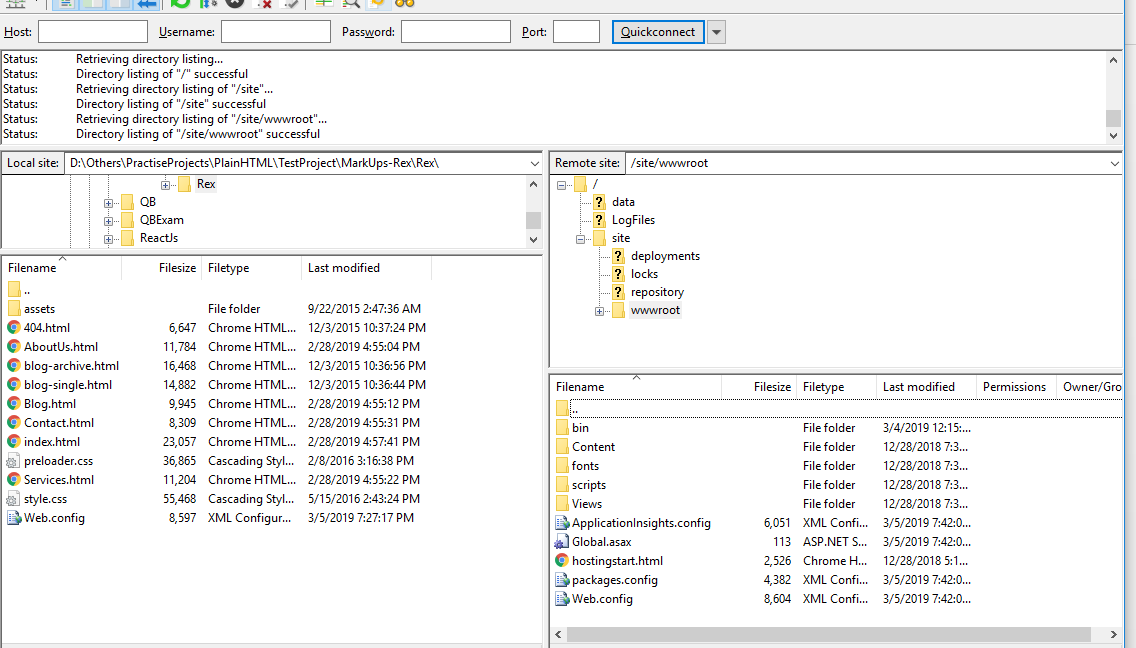
**Changes needed for new domains for the environment in Services Project**

Please connect to the published files location on azure for the services. This will follow the same steps as described above for the Auth project. Please connect to location using filezilla with the credentials. For example below are the credentials to connect to the preprod services location:

**publishUrl**= ftp://waws-prod-blu-087.ftp.azurewebsites.windows.net/site/wwwroot (Host in FileZilla)

**userName**=" prod-api-cgsservices\$prod-api-cgsservices" (UserName in FileZilla)

**userPWD**=" i4BaylwqS1i6jsm9ZBZRr4Xvn250N0JyfCGTJwlgJcK4tE6YrQQjuJDsAJ5d" (Password in FileZilla)



Please download the Web.Config on the right panel and open the downloaded file for editing purposes.

Please change the following keys in it for the Okta configurations:

<add key="okta:OktaDomain" value="https://dev-634905.okta.com/" /> // This is the URL of your Okta account

<add key="okta:ClientId" value="0oabq3f1uzFjeoNol356" /> // This is the ClientID of the application

After the modifications have been made for the above changes, please overwrite the file back to the right panel just to updated it on the server