

<https://www.youtube.com/watch?v=WdAhD6p1nKM>

<https://www.youtube.com/watch?v=I6iMwTgKdek>

<https://developer.salesforce.com/docs/atlas.en-us.sfdx_dev.meta/sfdx_dev/sfdx_dev_auth_connected_app.htm>

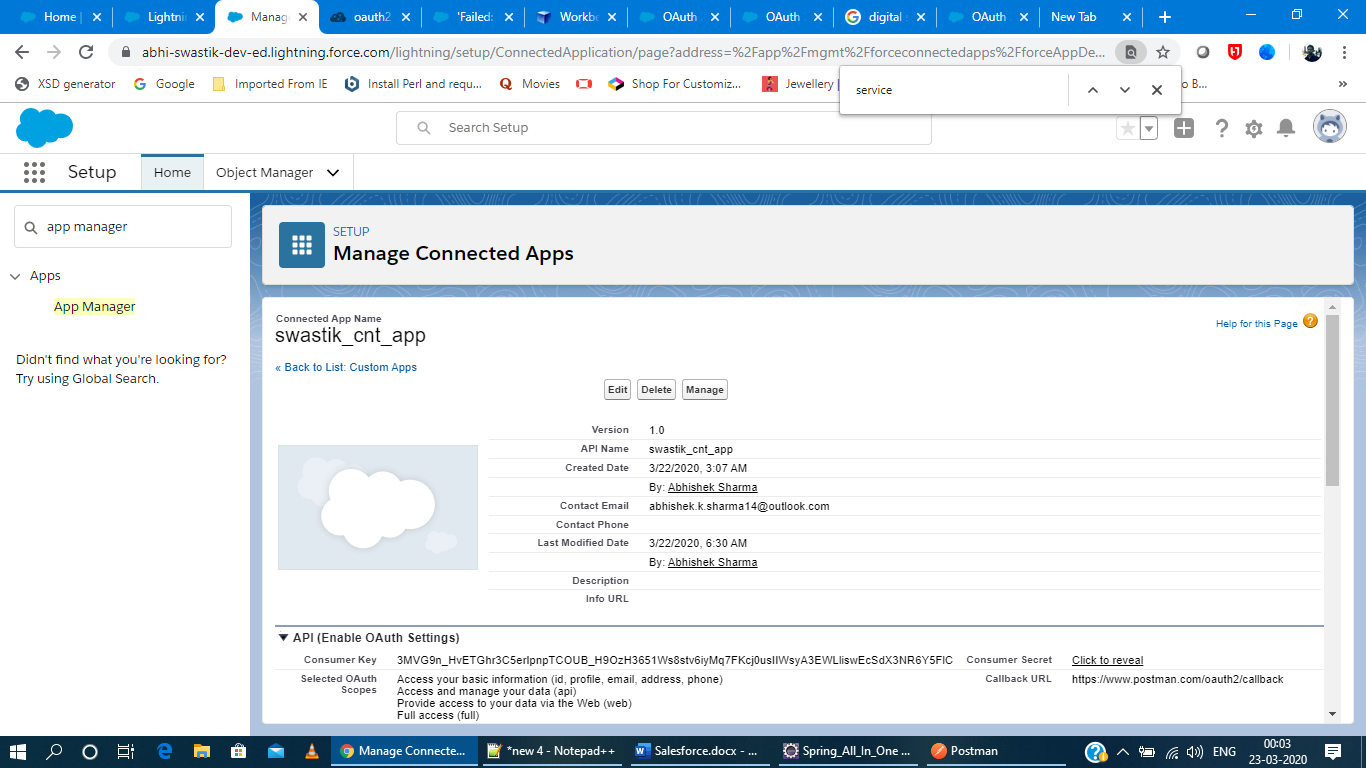
<https://developer.salesforce.com/docs/atlas.en-us.sfdx_dev.meta/sfdx_dev/sfdx_dev_auth_key_and_cert.htm>

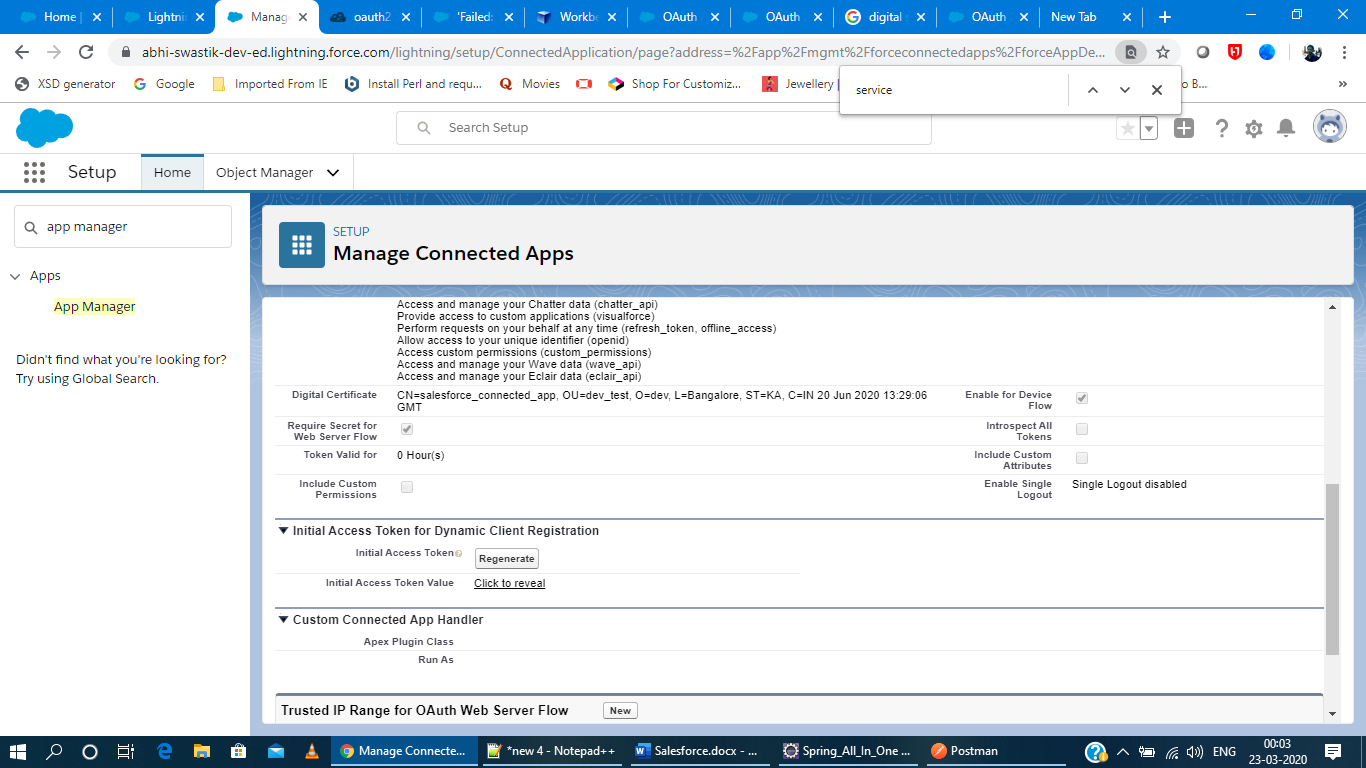
Command to generate store files:

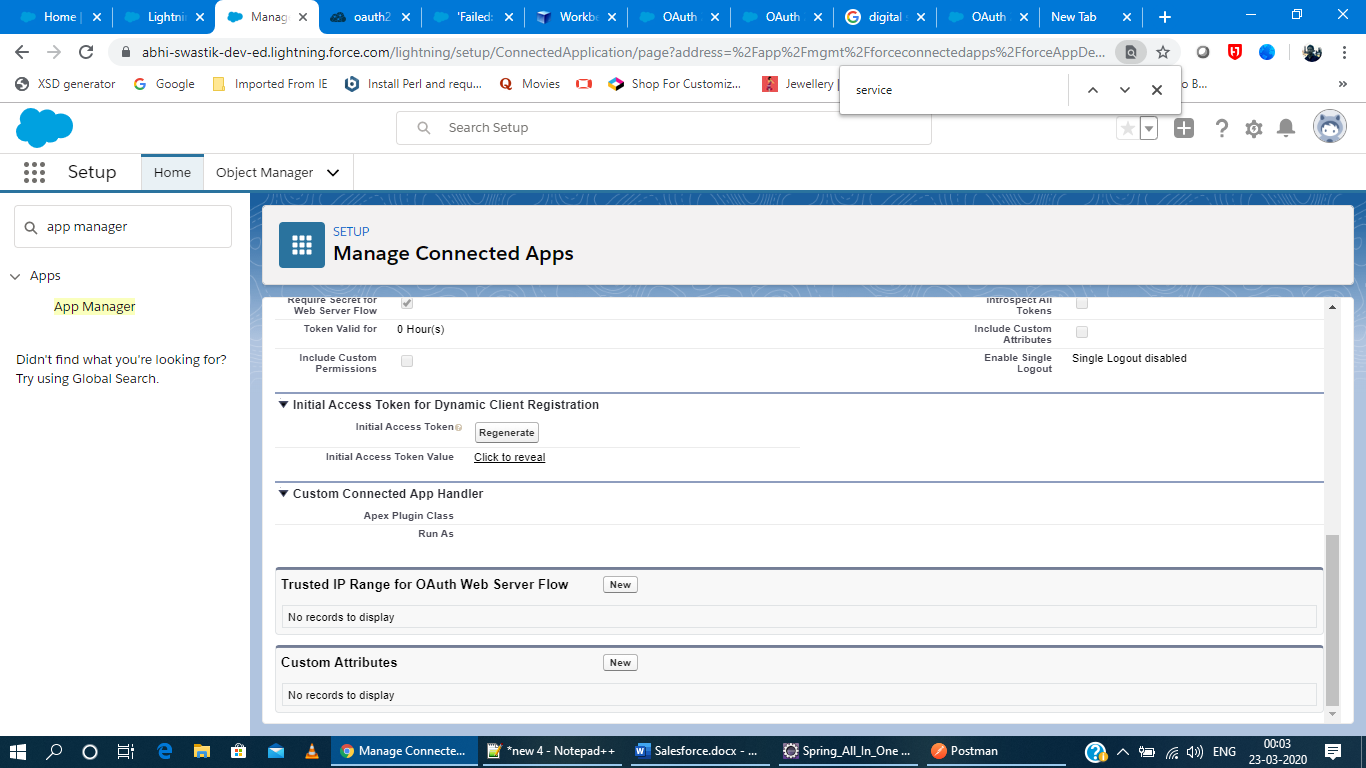
keytool -genkey -alias swastik\_cnt\_app -keyalg RSA -sigalg SHA256withRSA -keystore server.keystore -storepass Json!Xml -keypass Madrid!Bull -dname "CN=salesforce\_connected\_app, OU=dev\_test, O=dev, L=Bangalore, ST=KA, C=IN"

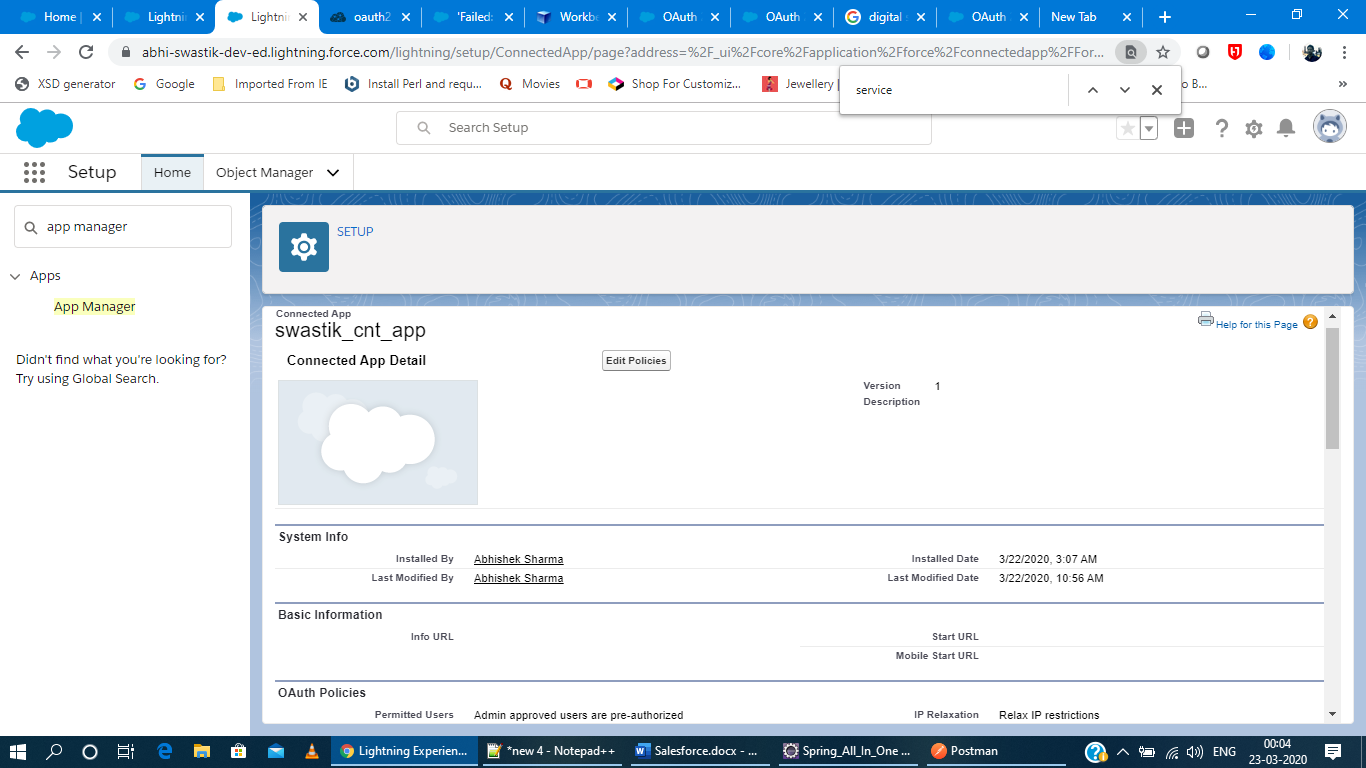
keytool -export -alias swastik\_cnt\_app -keystore server.keystore -storepass Json!Xml -file server.cer

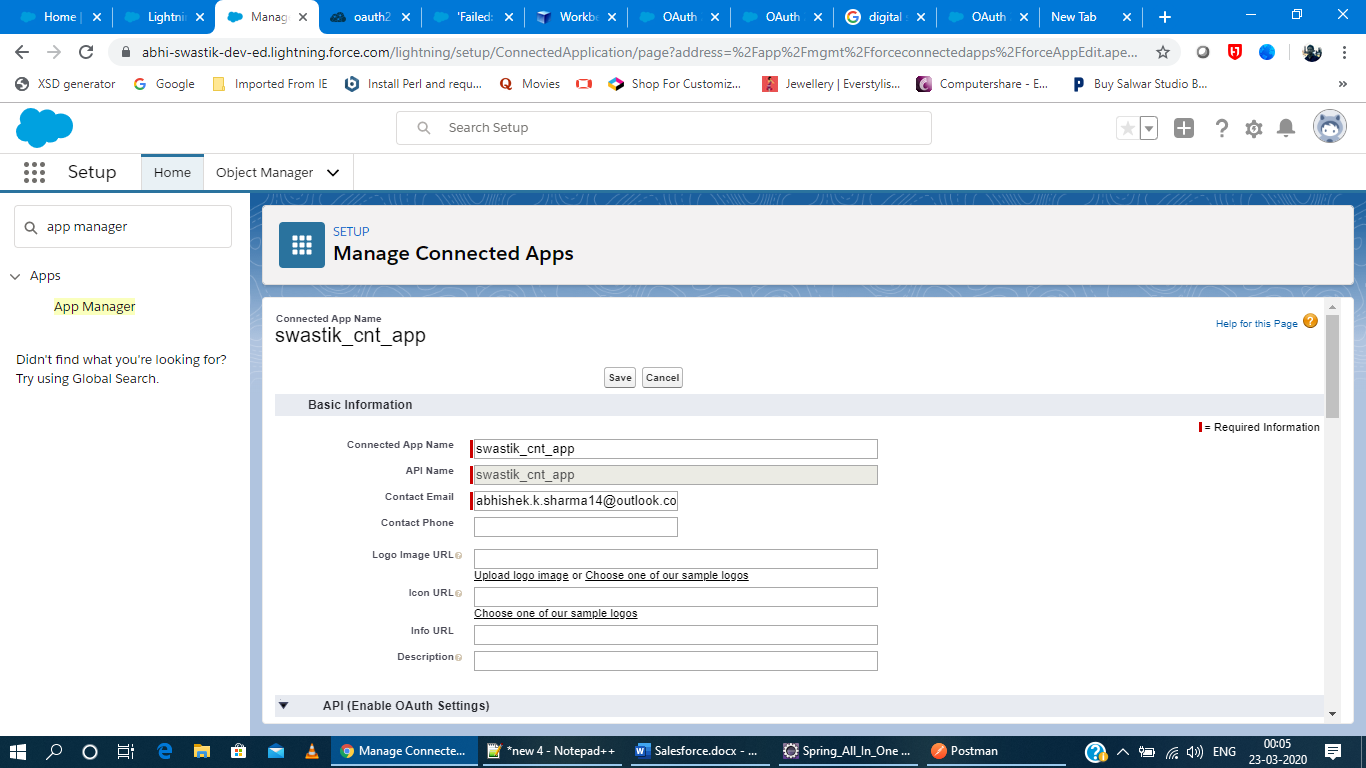
keytool -import -v -keystore client.truststore -storepass Json!Xml -file server.

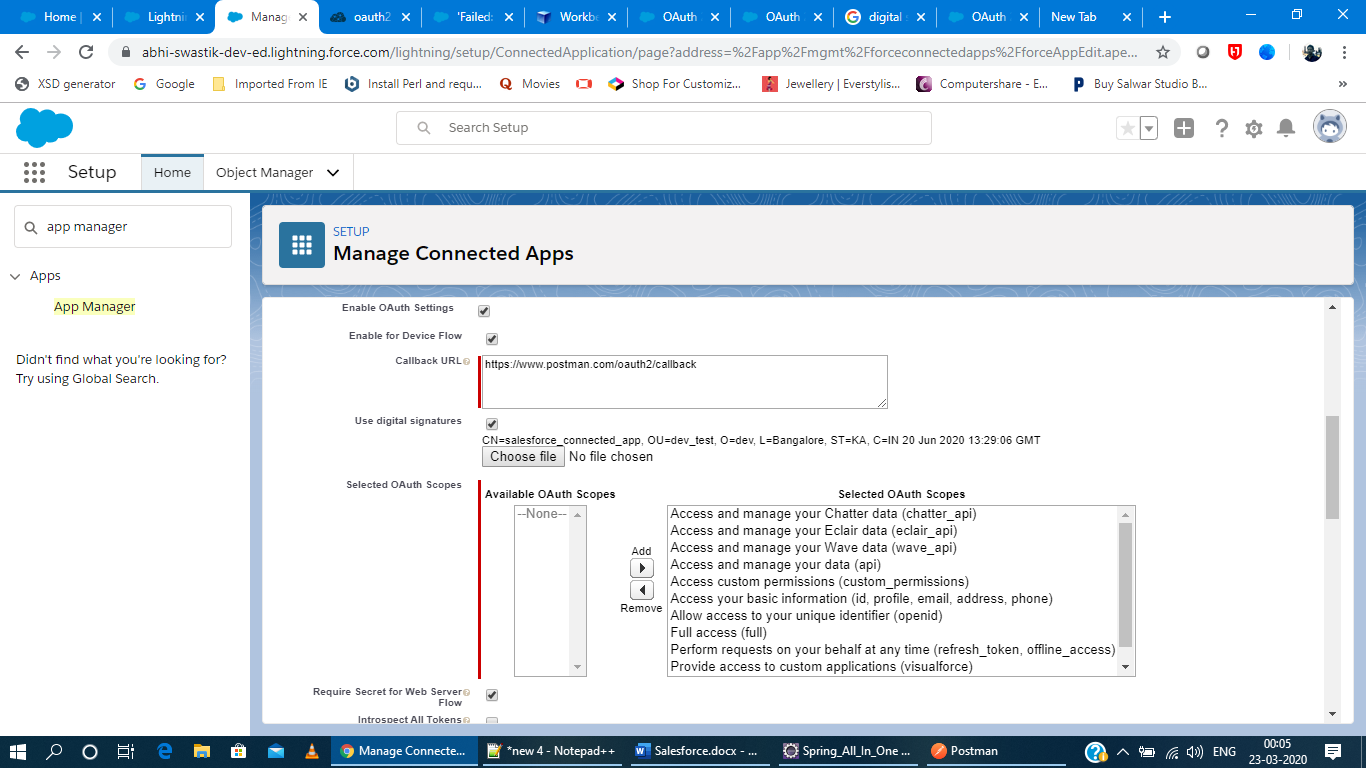


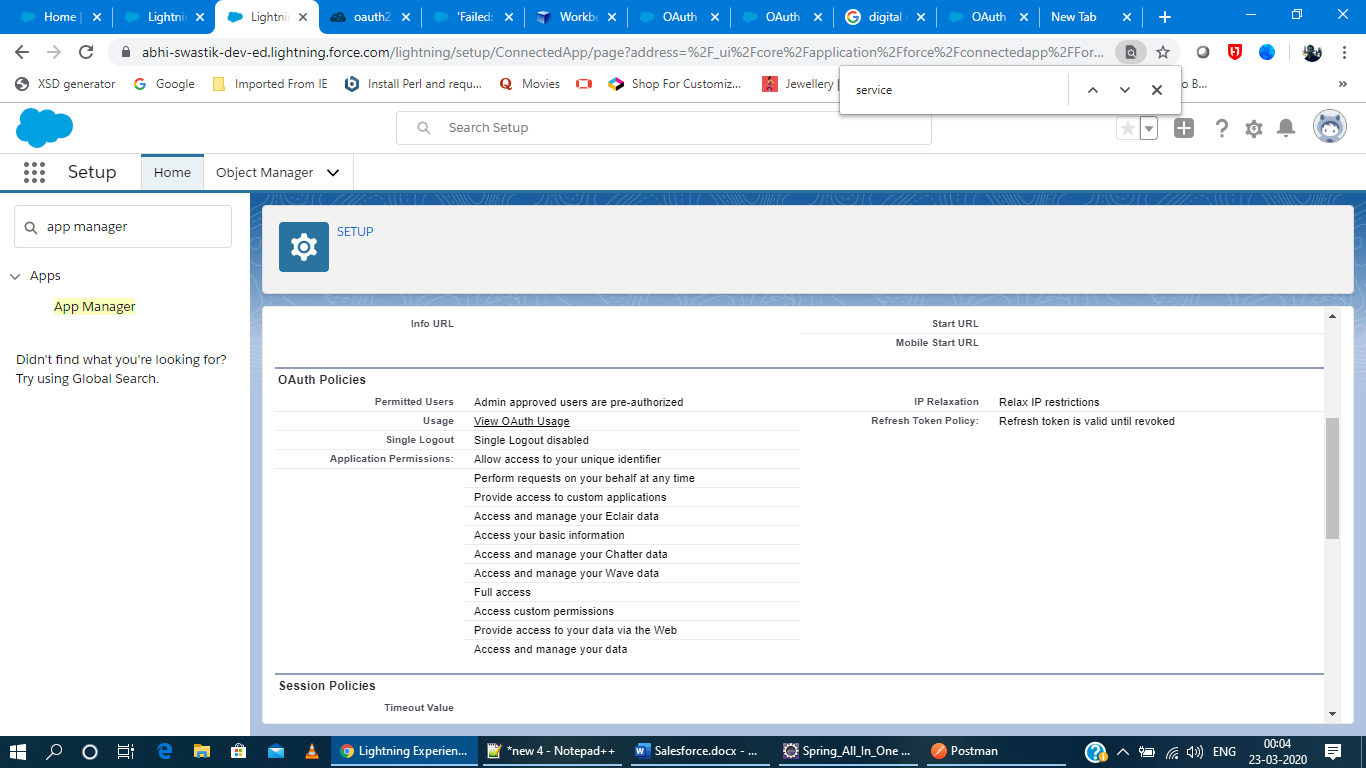


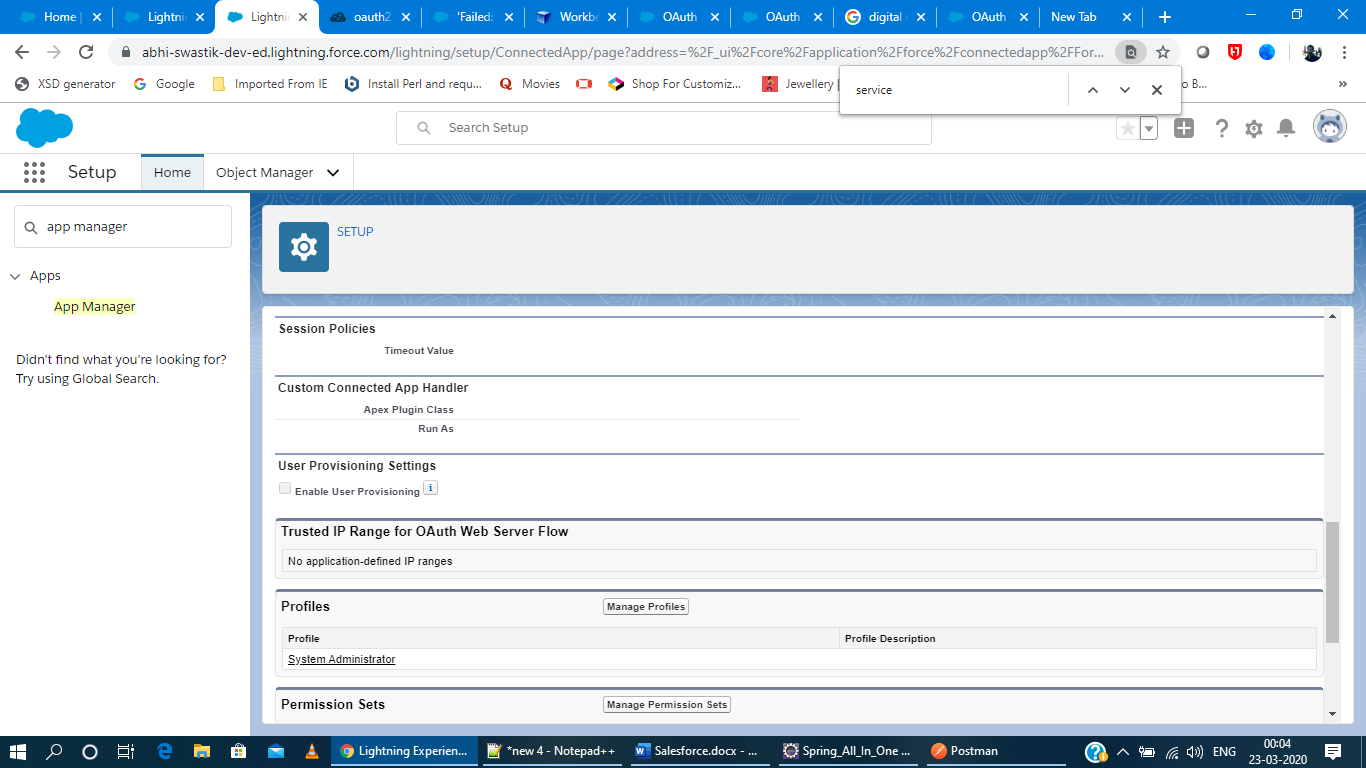


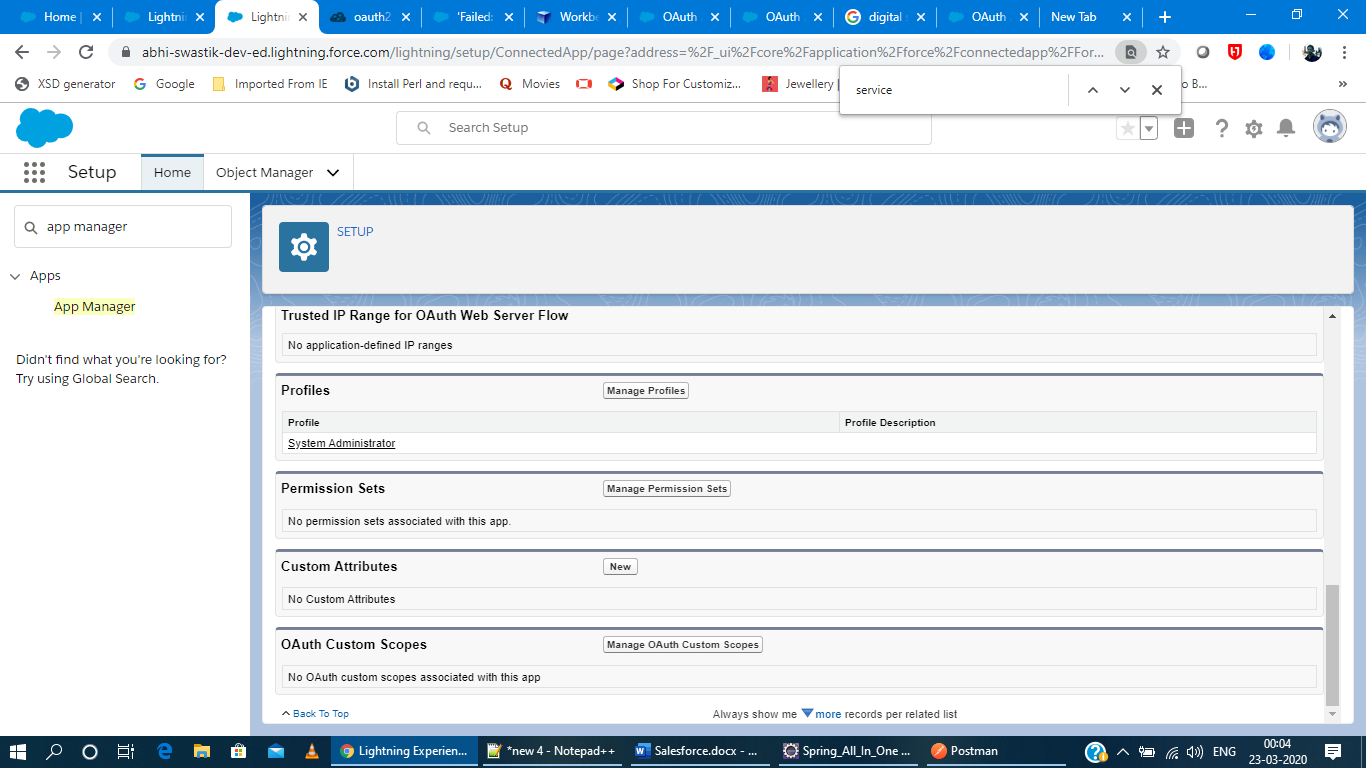








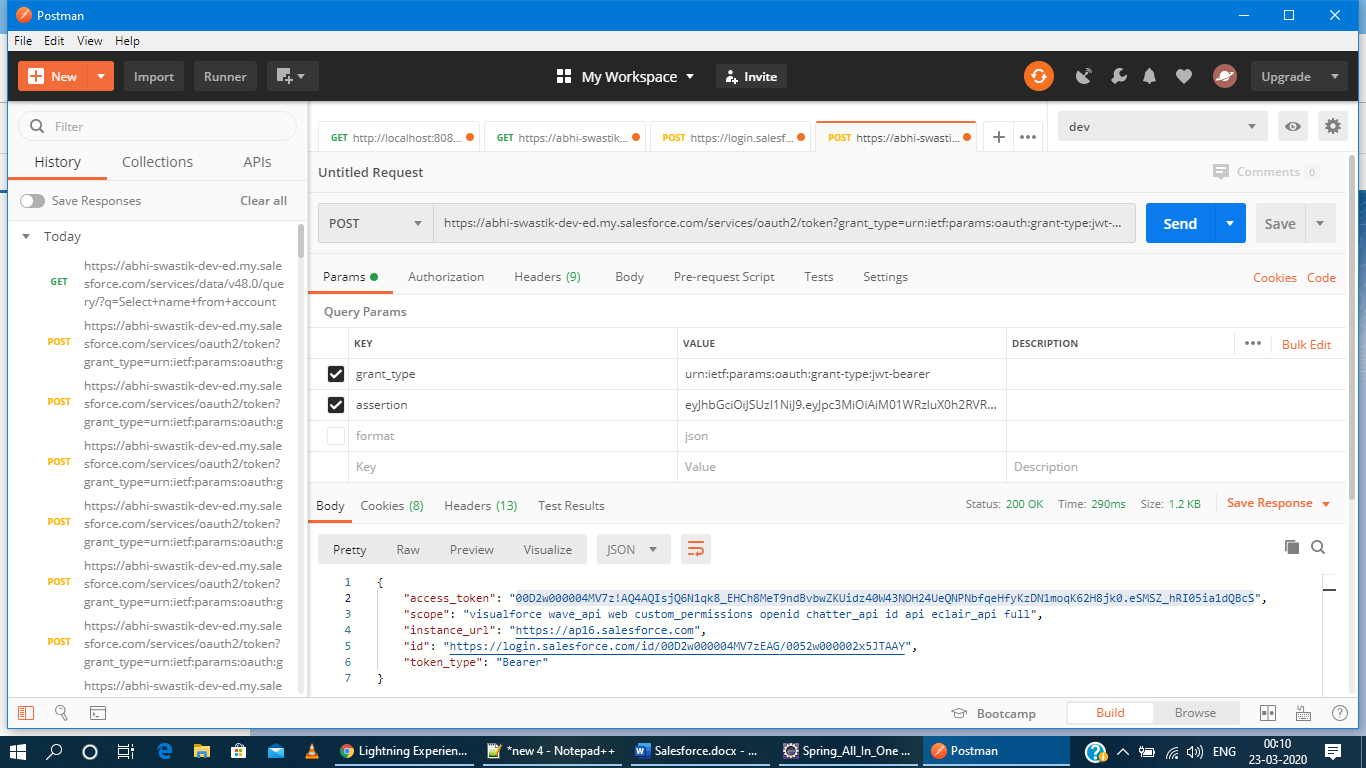


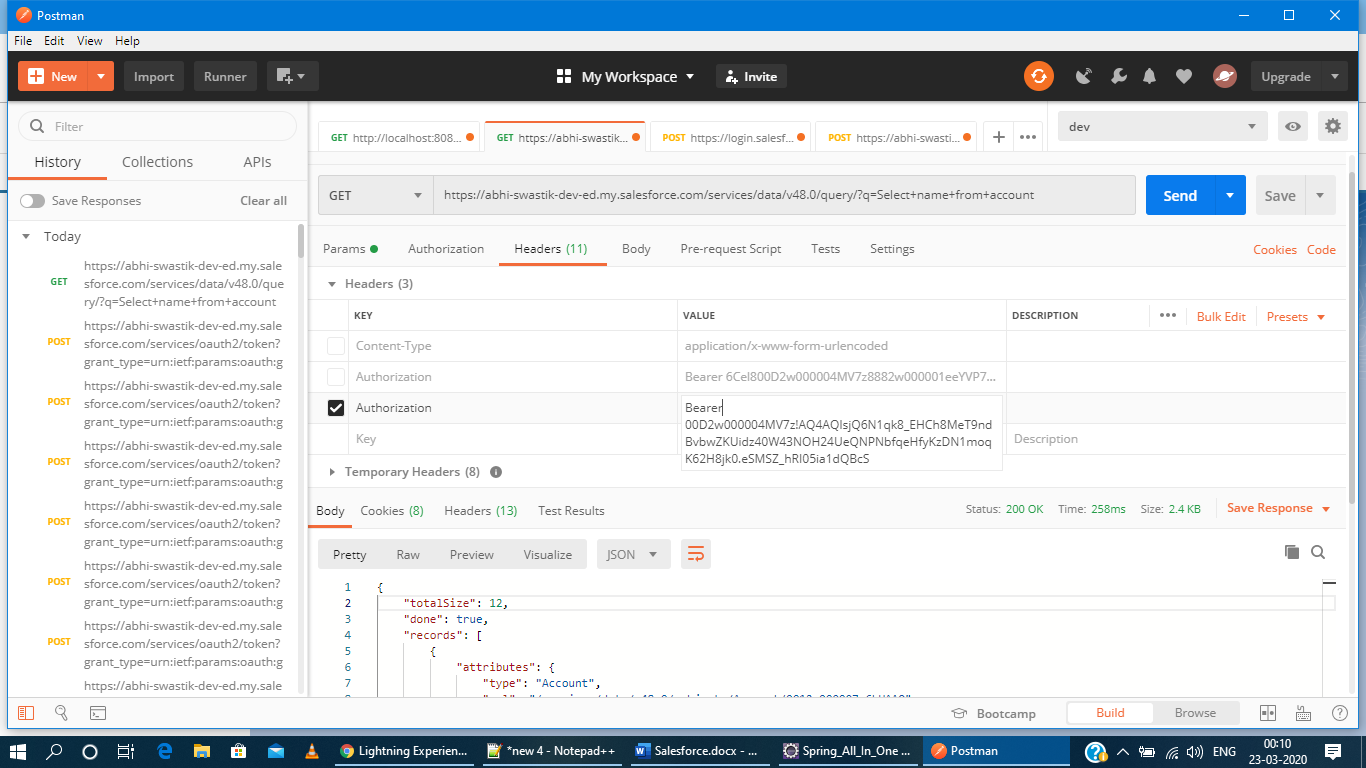


Creating/Editing the Connected app by selecting the digital signatures option and attach the certificate file.

Updating the policies by selecting OAuth policies > Permitted Users > Admin Approved users are pre-authorized.

Updating the connected app policies with the Profile Set, select the profile set as per the profile of user that can connect to it.





import org.apache.commons.codec.binary.Base64;

import java.io.\*;

import java.security.\*;

import java.text.MessageFormat;

public class Pca {

public static void main(String[] args) {

String header = "{\"alg\":\"RS256\"}";

String claimTemplate = "'{'\"iss\": \"{0}\", \"sub\": \"{1}\", \"aud\": \"{2}\", \"exp\": \"{3}\"'}'";

try {

StringBuffer token = new StringBuffer();

//Encode the JWT Header and add it to our string to sign

token.append(Base64.encodeBase64URLSafeString(header.getBytes("UTF-8")));

//Separate with a period

token.append(".");

//Create the JWT Claims Object

String[] claimArray = new String[4];

claimArray[0] = "3MVG9n\_HvETGhr3C5erIpnpTCOUB\_H9OzH3651Ws8stv6iyMq7FKcj0usIIWsyA3EWLliswEcSdX3NR6Y5FlC";

claimArray[1] = "abhi\_dev@personal.com";

claimArray[2] = "https://login.salesforce.com";

claimArray[3] = Long.toString( ( System.currentTimeMillis()/1000 ) + 30000);

// claimArray[4]=<JTI>

MessageFormat claims;

claims = new MessageFormat(claimTemplate);

String payload = claims.format(claimArray);

//Add the encoded claims object

token.append(Base64.encodeBase64URLSafeString(payload.getBytes("UTF-8")));

//Load the private key from a keystore

KeyStore keystore = KeyStore.getInstance("JKS");

keystore.load(new FileInputStream("C:\\Users\\Abhishek\\Downloads\\server\_certificates\\server.keystore"), "Json!Xml".toCharArray());

PrivateKey privateKey = (PrivateKey) keystore.getKey("swastik\_cnt\_app", "Madrid!Bull".toCharArray());

//Sign the JWT Header + "." + JWT Claims Object

Signature signature = Signature.getInstance("SHA256withRSA");

signature.initSign(privateKey);

signature.update(token.toString().getBytes("UTF-8"));

String signedPayload = Base64.encodeBase64URLSafeString(signature.sign());

//Separate with a period

token.append(".");

//Add the encoded signature

token.append(signedPayload);

System.out.println(token.toString());

} catch (Exception e) {

e.printStackTrace();

}

}

}