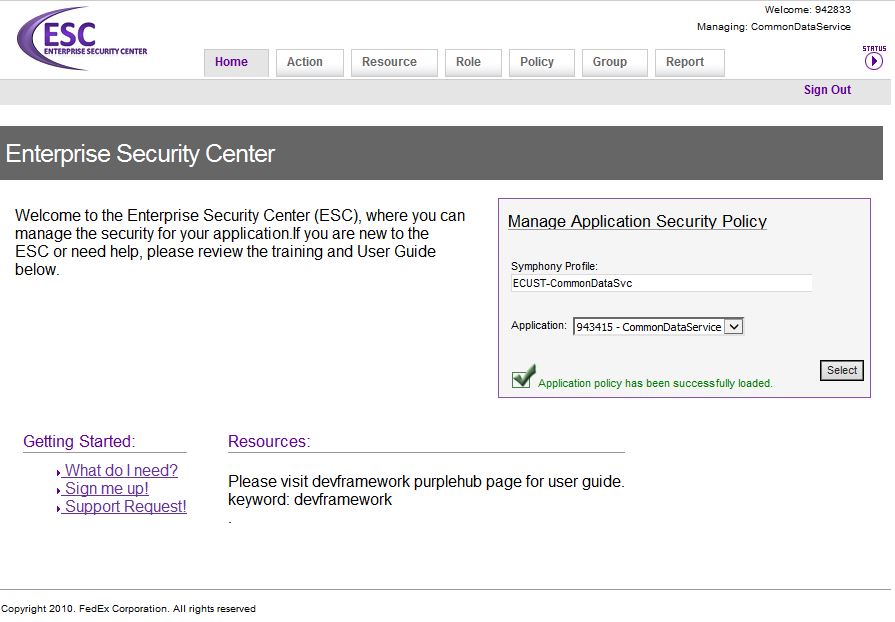
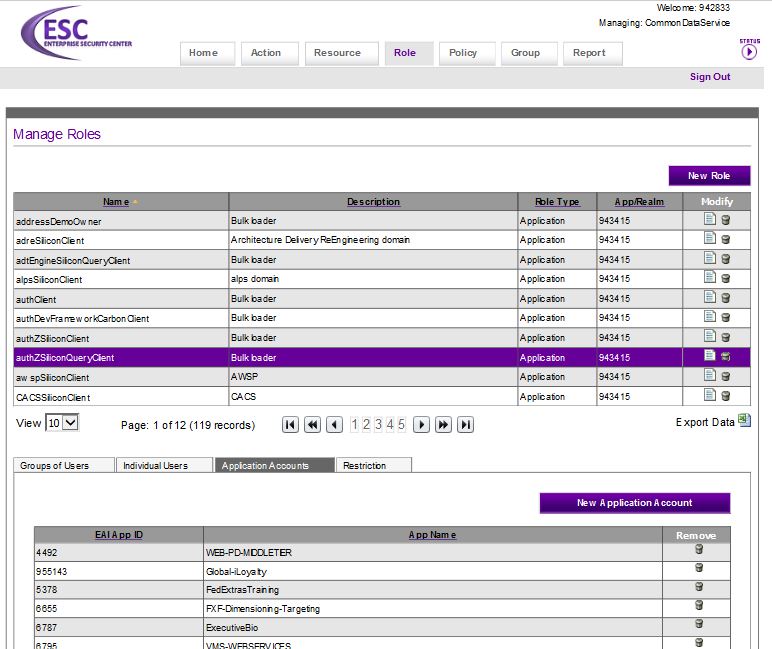
**Issue related to Cert Rotation expiring and CDS related:**

**Step1:** Login to dev esc with your USER ID and Password "Symphony Profile ID : ECUST-CommonDataSvc profile and APP ID: CommonDataService"



**Step 2:** Check the AppID is present both in authZSiliconQueryClient and certzillaSiliconQueryClient

* Go to **Role** tab
* Select the role **authZSiliconQueryClient**
* In the **Application Accounts** tab check whether the AppID is present or not.
* In the same way check for the role **certzillaSiliconQueryClient**
* If the AppID is not present, then click on **New Application Account** and add the AppID.



**Step 3:** Provide the access to all environments (Dev/Test/Prod).

**“We can suggest them to check with the server (Weblogic or Tomcat) and the CDS connection. CDS recently upgraded to SHA-2, so the connection lost between your server and the CDS. So please check it and try to establish the connection and this will solve your below issue.”**

**Step 4:** Check with the customer to try now, and if they still facing the error.  
  
**Step 5:** Customer need to check, the new cert is present in CDS or going to expire?  
  
**Step 6:** If the certificate is nearing expiration then the WORKFLOW would have been triggered 45 days in prior.

**Step 7:** Customer need to request his manager to approve the workflow for your application.

**Step 8:** Then the infosec team will approve the request and it will go to CERTZILLA team (CDS team) and they will issue the new certificate.

**Step 9:** Update the client.properties, Fp.properties and Security.property files with their APP ID and proper CDS URLs.

* **Application certificate file**
  + Must be external to the application WAR file. (refer to the [Platform Design guidelines](http://itg.prod.fedex.com/sf/go/doc88818?nav=1) on where to place this file).
  + The service user must have read & write permission to the file.
  + The service user must have read & write permission to the directory.
  + Unique applications cannot share this file (though each can have its own copy).
* **The client.properties file** 
  + Must be external to the application WAR file. (Refer to the [Platform Design guidelines](http://itg.prod.fedex.com/sf/go/doc88818?nav=1) on where to place this file).
  + The service user must have read & write permission to the file.
  + The service user must have read & write permission to the directory.
  + Unique applications cannot share this file (though each can have its own copy).
  + In **client.keystore.file** property path of cert should be mentioned properly.
* **The security. Properties file**
* Refer to the [Platform Design guidelines](http://itg.prod.fedex.com/sf/go/doc88818?nav=1) on where to place this file.
* ***autocertrotation.flag*** must be set to **true**.
  + OPTIONAL: the ***security.api.cert.rotation.time*** property is set with a *<HH:MM:SS>* format. If not set, the default is 06:00 GMT (01:00 central time).
  + The **ldap.url** property should be set to an appropriate value for the level (L2, L3, PROD, etc).
  + The **ldap.app.id.attr.name** property should be set to ‘uid’ Any other value will fail.
  + The **ldap.cert.attr.name** property should be set to ‘userCertificate’ Any other value will fail.
  + The **ldap.revoke.attr.name** property should be set to ‘FxAppSoxStatus’ Any other value will fail.
  + For non-Spring applications, the **cds.url** property should be set to an appropriate value for the level (L2, L3, PROD, etc).
* In case, if they are using <http://idmtest02.infosec.fedex.com:4388/DelegationJWS/DelegationV2?WSDL> in their security file, then that to be replaced with <https://test.secure.fedex.com/delegation/services/Delegation?wsdl>
* **For Reference Purpose:**
* **Attention:** IdM has released an updated service URL
* **Action Required:** Change to the Development Framework ‘*security*.*properties’* file
* IdM has released an updated service URL to be compliant with SHA-2 application requirements.  Any customer using the IdM delegation feature in conjunction with the isAllowed call will need to update the IdM URL.  The old IdM service will be retired and any service still using the retired service URL after the retirement date will lose delegation functionality.  **As a result, we are asking that all impacted applications update their ‘*security.properties*’ file by November 26, 2017.**
* Developers should review the application ‘*security.properties’* file for ‘*idm.url*’ property.  If present, update to latest corresponding URL outlined below.  Any changes to the ‘*security.properties’* file requires a bounce of the application after the property is updated.
* For Security API: If the ‘*idm.url*’ property is present in the ‘*security.properties*’ file, then an IdM check will be performed when the isAllowed method is called. This is used with custom authorizers.

* **Reference:**
* **L4**
  + Change <https://idmtest.web.fedex.com/delegation/services/Delegation?wsdl>

To <https://test.secure.fedex.com/delegation/services/Delegation?wsdl>

* + Change <https://idmtest.web.fedex.com/DelegationJWS/DelegationV2?wsdl>

To <https://test.secure.fedex.com/DelegationJWS/DelegationV2?wsdl>

* **PROD**
  + Change <https://identity.web.fedex.com/delegation/services/Delegation?wsdl>

To <https://sso.secure.fedex.com/delegation/services/Delegation?wsdl>

* + Change <https://identity.web.fedex.com/DelegationJWS/DelegationV2?wsdl>   
    To <https://sso.secure.fedex.com/DelegationJWS/DelegationV2?wsdl>
* **Fp.properties File:**

We have to check following parameters in fp.properties file as mentioned below.

*Example:*

* app.id=APP217
* log.dir.name=/var/fedex/wpor-web/logs/
* app.name=WPOR
* framework.version=5.1.1
* **JVM options:**
  + If set, the **-Dframework.managed** option must be set to **true**.
* **The application context file:**
* A **CSSBootstrap15** bean must be defined.
* User the **CSSBootstrap15** class provided by the Security API – do not create a custom implementation.
* The **CSSBootstrap15** bean must be configured with a destroy-method set to **cancelTimerTasks**.
* The ***isClient*** flag must be set to **true**.
* Import the two required framework context files.
* <import resource="classpath:FrameworkApplicationContext.xml"/>
* <import resource="classpath:DevFrameworkSecurityContext.xml"/>
* Note this file is internal to the WAR file.
* **Network:**
  + If the application is separated from either LDAP or CDS by a firewall, a firewall rule should be requested from network engineering.