Contents

[On Call Support weekly responsibilities 1](#_Toc470082692)

[FTE weekly responsibilities 2](#_Toc470082693)

[Queues to monitor 2](#_Toc470082694)

[Tibco Support 3](#_Toc470082695)

[Continuous Integration Support - TODO 3](#_Toc470082696)

[3rd Party Contact for product support 3](#_Toc470082697)

[Appendix I – Production Application Certificate Expiration Notice 3](#_Toc470082698)

[Scenarios and Resolution 5](#_Toc470082699)

# On Call Support weekly responsibilities

Monitor ALL support request in Queues to monitor. All tickets must be assigned or on hold with an owner assigned. Tickets should not be left unassigned or open. Ticket history should be well documented. Provide short summary (1-2 sentence) of all contact (email, phone, IM and in person) vital to closing the ticket. Any documentation vital to closing the ticket should be included in the ticket as an attachment (log files, property files, email exchange). If a ticket is turned over to FTE or another member of on call support all the history should be contained in the ticket. Last activity on an open ticket should never exceed 24 hrs.

Note: When an artifact is created Symphony creates an artifact reply address. When replying to customer email always CC artifact reply address. The reply will be added as a comment to the Symphony artf. (Ex. To:Shashi Kumar Munugoti (OSV) shashi.munugoti.osv@fedex.com; CC: artf1302435@prh01246.prod.fedex.com).

1. Engage with current FTE on call and raise priority when the ticket fails to make progress in 3 days due to technical issues.
2. If a customer enters a ticket and fails to respond to email, IM, phone calls for 3 days email the customer to alert them the ticket will be closed if no response (update ticket). Wait 3 additional days and close the ticket if no response.
3. If a ticket has been turned over to FTE follow up to make sure ticket is being worked and closed.
4. Include in weekly on call report –status of tickets; include number of new tickets this week, number of current assigned tickets, age of ticket, number on hold tickets, and number of closed tickets this week. Include average age of all closed tickets. Send report to Framework-team-all email list.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Current Assigned** | **Current On Hold** | **Closed-Complete this week** | **New tickets this week** | **Average age of current Assigned tickets** | **Average age of Closed-Complete tickets this week** |
| **Number of current assigned tickets** | **Number of current on hold tickets** | **Number of tickets closed during support week** | **Number of new tickets opened during support week** | **date opened to current date/number of assigned tickets** | **date opened to date closed/number of tickets closed** |

To pull report go to Support Request Tracker page for EA-Framework.

* Average age of Closed-Complete tickets this week: Filters should all be set to Any. Click Export at the bottom of the table. Export Format: CSV, select Available Columns: Closed, Submitted On and Status. Open CVS file in Excel and select Closed column, then DATA from menu, click Filter then filter out everything but from required data (work week) and sort by newest to oldest. Remove anything closed before end of start of support week. Formula for each column Closed – Submitted On then take an average of the difference.
* Average age of current Assigned tickets: Filters should be set to Any and Status All Assigned. Click Export at the bottom of the table. Export Format: CSV, select Available Columns: Status and Submitted on. Open CVS file in Excel and add new column with current date. Create formula for each row current date – date opened then take the average off all the rows.

1. On hold tickets – For defects and customer request write a new story card and give to Sheril for prioritization. The Story card should include the Teamforge artifact#, defect# if applicable, product name (Ex. Framework), customer group requesting (Ex. Sales), requested work to be done and the business use. Also include the date of the request on back of story card.

Note: Symphony defect affecting support – Customers that do not include “E-mail Requestor Options: On Update” and include their email notification address at creation will not receive any email updates when comments are added to the ticket. This cannot be corrected after artifact is created. Be aware if support is only responding directly to the Symphony artifact the customer may not be getting a response.

# FTE weekly responsibilities

1. Assist with Open tickets that need to be addressed from weekly meeting (Schedule Monday 9:30am, Location 40-130 – Attendees Last FTE on call, New FTE on call, On call support lead). Tickets should be turned over to next on call unless additional help is needed.
2. Weekly Certificate Expiration Notice Email – Set up Tuesday Task in Outlook – See appendix.
3. Purple Hub – Check Daily - Set up Daily Task in Outlook. Development Framework Purple Hub Page

[http://collab.purplehub.fedex.com/Communities/Development Framework/SitePages/teamhome.aspx](http://collab.purplehub.fedex.com/Communities/Development%20Framework/SitePages/teamhome.aspx)

# Queues to monitor

Customers are able to enter tickets in public queue owned by the Development Frameworks Group. All of the following queues should be monitored and checked once a day. To monitor queue log into Teamforge (<http://itg.prod.fedex.com/sf/projects/symphonysupport/>) and project to monitor. Select Support Trackers from the Tracker section and select from the dropdown below the tracker table “Monitor.”

1. Support Trackers for “EA-Framework”

<http://itg.prod.fedex.com/sf/tracker/do/listArtifacts/projects.ea_framework/tracker.supportrequesttracker?openPriority=all>

* Anything in the following queues can and should be reassigned to EA-Framework.

1. Support Trackers for “Enterprise Security Center”

<http://itg.prod.fedex.com/sf/tracker/do/listArtifacts/projects.ea_enterprisesecuritycenter/tracker.supportrequesttracker?openPriority=all>

1. Support trackers for “Enterprise Workflow”

<http://itg.prod.fedex.com/sf/tracker/do/listArtifacts/projects.esd_enterpriseworkflow/tracker.supportrequesttracker?openPriority=all>

1. Support tracker for “Continuous-Integration\_Build” <http://itg.prod.fedex.com/sf/tracker/do/listArtifacts/projects.continuous_integration_build/tracker.supportrequesttracker>
2. Support tracker for “ESD-CommonServiceRuntime” <http://itg.prod.fedex.com/sf/tracker/do/listArtifacts/projects.esd_commonservicesruntime/tracker.supportrequesttracker>
3. Support tracker for “EAA-MobileAppArch” [http:itg.prod.fedex.com/sf/tracker/do/listArtifacts/projects.eaa\_mobileapparch/tracker.supportrequesttracker](http://itg.prod.fedex.com/sf/tracker/do/listArtifacts/projects.eaa_mobileapparch/tracker.supportrequesttracker)
4. Support tracker for “EAA-CloudAppArch” <http://itg.prod.fedex.com/sf/tracker/do/listArtifacts/projects.eaa_cloudapparch/tracker.supportrequesttracker>

# Tibco Support

1. Tibco Request for software – ticket to Tibco request page
   1. – keyword “tibco” or “tibcorequest” - <https://sso.secure.fedex.com/tibcorequest/home.jsf>
2. Any support for Tibco enter request in EA-Framework support tracker queue. Currently we are assisting with Token Generation and client/service authentication and authorization through ESC. Tibco knowledge is currently not a Development Framework skillset. Contact 3rd party for product support.

# Continuous Integration Support - TODO

1. Supported products
   1. Jenkins
   2. SonarQube
   3. Nexus
2. PDSM

# 3rd Party Contact for product support

List of users successfully using the Framework with 3rd party products

1. Ab Initio – Arvin Festejo (Sales), EDW (EDW-FCIS, EDW-ACQ) , David D. Reeves (Int'l Edit, Validate & Rating)
2. People Soft - Abheeshta Yerva (Contractor Initiatives – FXG)
3. BPM - TODO
4. C/C++ (Token Generation) – TODO
5. Tibco – TODO

# Appendix I – Production Application Certificate Expiration Notice

Every Tuesday by On Call FTE –

Go to keyword “Symphony,” log in, click Manage, click Profiles. In text box Application: type the EAI number reported from “App ID`s certificates due to expire within 30 days (PROD)” email to get EAI IT Architect and Profile IT Owner.

To: EAI IT Architect

CC: Framework-all, reported LDAP Cert owner, manager of IT Architect reported in EAI, and Profile IT Owner.

Note: in the event the IT architect from EAI is no longer with the company CC each Profile Lead and their manager.

Subject: Production Application Certificate Expiration Notice

Certificate Renewal Notification

You are identified in Symphony as the System IT architect for one of the following production applications:

App: ***XXX - Profile Long Name from Symphony Profile (Exp. Date) IT architect from EAI***

The application certificate for these applications will expire within the next 30 days.

Since this notification is for an automated renewal, no immediate action is required on your part if you are already using the development framework ver. 3.0 or higher.

Once approved and issued the new certificate will be loaded to CDS. The development framework can automatically install the certificate without any user intervention required if configured to do so. If you are not yet using 3.0 or higher, or if you do not have automatic certificate rotation enabled, then you will still be required to install the new certificate with your normal process(es). If automatic certificate rotation is enabled, we strongly recommend you manually confirm the rotation after it occurs by examining the timestamp on the certificate and client.properties file.

Please also note that you will still be notified when the new appid certificate is issued.

For information about certificate rotation configuration, please refer to the following documents.

• Framework migration guide (5.x to 5.2.0): <http://itg.prod.fedex.com/sf/go/doc1182542?nav=1>

* DFW 7.0.0 Migration guide: <http://itg.prod.fedex.com/sf/go/doc1193072?nav=1>

• Certificate rotation checklist: <http://itg.prod.fedex.com/sf/go/doc893951?nav=1>

If you no longer need this certificate and plan to allow it to expire, you need take no further action although you will continue to receive these notifications until it expires.

If you believe you have received this notification in error, or if you have any questions about your certs, please contact our team by replying to Framework-team Framework-team@corp.ds.fedex.com.

Thanks and Regards,

The Development Framework Team

# Scenarios and Resolution

**Scenario#1 (Refer** **artf1371782) - Error with the Configuration for Cert-Rotation**

L1 - auto cert rotation web service request fails w/ SSLKeyException: Hostname verification failed

User was trying to use the cert rotation functionality using web logic server12.1.2 but getting

I am trying to unit test auto cert rotation with our SQI Maintenance project (app id 7029) and I've made all the changes in the cert rotation best practices checklist. The app starts but the following error is found in the app log file "Error with the Configuration for Cert-Rotation"

2016-11-30 18:25:16,548 com.fedex.security.client.KeystoreRotation::getKeystoreFromCDS <KeystoreRotation.java:316> Caught exception e: java.lang.RuntimeException: javax.xml.ws.WebServiceException: **javax.net.ssl.SSLKeyException: Hostname verification failed: HostnameVerifier=weblogic.security.utils.SSLWLSHostnameVerifier, hostname=cds-level2.ute.fedex.com.**

**Resolution:** AST team suggested to use the -DUseSunHttpHandler=true JVM argument. User has no issues once he updated with this argument.

**Scenario#2 (Refer artf1374614) - CMDC : AutoCert Rotation : Not run in Production**

When we see logs for two different timers as below for the same application then refer the fix under Resolution section.

1. 2016-12-08 23:42:24,168 GMT-0600 pje07580 [Timer-4] INFO 910723 KeystoreRotation.getCDSCertExpirationDate New Cert Expiration Date from CDS ------- Sat Oct 14 10:02:00 CDT 2017  
   1.0 2016-12-08 23:42:24,169 GMT-0600 pje07580 [Timer-4] INFO 910723 KeystoreExpirationCheck.updateCacheFlag Setting APP910723\_cds\_cert\_query\_timestamp flag to: 12/8/2016 11:42:24.169  
   1.0 2016-12-08 23:42:24,169 GMT-0600 pje07580 [Timer-4] INFO 910723 KeystoreExpirationCheck.queryCDSForCert Found a CDS cert that is newer than the cached cert  
   1.0 2016-12-08 23:42:24,169 GMT-0600 pje07580 [Timer-4] INFO 910723 KeystoreExpirationCheck.queryCDSForCert cdsCertExpiredate: Sat Oct 14 10:02:00 CDT 2017 cacheExprDate: Tue Jan 17 16:23:00 CST 2017  
   1.0 2016-12-08 23:42:24,199 GMT-0600 pje07580 [Timer-4] INFO 910723 KeystoreRotation.getKeystoreFromCDS The Security API successfully retrieved the keystore from CDS  
   1.0 2016-12-08 23:42:24,615 GMT-0600 pje07580 [Timer-4] INFO 910723 KeystoreRotation.validateCDSCert The Security API successfully validated the new certificate and passphrase against LDAP  
   1.0 2016-12-08 23:42:24,617 GMT-0600 pje07580 [Timer-4] WARN 910723 KeystoreRotation.rotateCert Copied /opt/fedex/cmdc-app/appsec/cert/temp/APP910723.p12 to /opt/fedex/cmdc-app/appsec/cert/APP910723.p12  
   1.0 2016-12-08 23:42:24,622 GMT-0600 pje07580 [Timer-4] INFO 910723 KeystoreCipherProviderImpl.configure KeystoreCipherProviderImpl configured for use with client APP910723  
   1.0 2016-12-08 23:42:24,622 GMT-0600 pje07580 [**Timer-4**] INFO 910723 KeystoreCipherProviderImpl.configure KeystoreCipherProviderImpl already configured for client APP910723, ignoring  
   1.0 2016-12-08 23:42:24,623 GMT-0600 pje07580 [Timer-4] ALL 910723 KeystoreExpirationCheck.rotationHandler Inside rotated .Cert from CDS was retrieved & rotated into the file system.  
   1.0 2016-12-08 23:42:24,623 GMT-0600 pje07580 [**Timer-4]** ALL 910723 KeystoreExpirationCheck.deleteLockFile Inside delete lock file, lock file deleted .  
   1.0 2016-12-08 23:42:24,624 GMT-0600 pje07580 [Timer-4] INFO 910723 KeystoreExpirationCheck.logHandler Cert from CDS was retrieved & rotated into the file system.  
   1.0 2016-12-08 23:47:23,587 GMT-0600 pje07580 [**Timer-5**] INFO 910723 KeystoreExpirationCheck.getCertExprDt Keystore file name read from client.propertiesAPP910723.p12  
   1.0 2016-12-08 23:47:23,592 GMT-0600 pje07580 [**Timer-5**] ALL 910723 KeystoreExpirationCheck.rotationHandler Waited for lock file to be removed and new / old certificate dates are a match.  
   1.0 2016-12-08 23:47:23,698 GMT-0600 pje07580 [Timer-5] INFO 910723 KeystoreRotation.getKeystoreFromCDS The Security API successfully retrieved the keystore from CDS  
   1.0 2016-12-08 23:47:23,699 GMT-0600 pje07580 [Timer-5] INFO 910723 KeystoreRotation.getCDSCertExpirationDate New Cert Expiration Date from CDS ------- Sat Oct 14 10:02:00 CDT 2017  
   1.0 2016-12-08 23:47:23,699 GMT-0600 pje07580 [Timer-5] INFO 910723 KeystoreExpirationCheck.updateCacheFlag Setting APP910723\_cds\_cert\_query\_timestamp flag to: 12/8/2016 11:47:23.699  
   1.0 2016-12-08 23:47:23,699 GMT-0600 pje07580 [Timer-5] INFO 910723 KeystoreExpirationCheck.queryCDSForCert Found a CDS cert that is newer than the cached cert  
   1.0 2016-12-08 23:47:23,699 GMT-0600 pje07580 [Timer-5] INFO 910723 KeystoreExpirationCheck.queryCDSForCert cdsCertExpiredate: Sat Oct 14 10:02:00 CDT 2017 cacheExprDate: Tue Jan 17 16:23:00 CST 2017  
   1.0 2016-12-08 23:47:23,721 GMT-0600 pje07580 [Timer-5] INFO 910723 KeystoreRotation.getKeystoreFromCDS The Security API successfully retrieved the keystore from CDS  
   1.0 2016-12-08 23:47:23,780 GMT-0600 pje07580 [Timer-5] ERROR 910723 KeystoreRotation.decryptPassword Failed to decrypt the new passphrase. : Unrecoverable error in PBE decryption  
   1.0 2016-12-08 23:47:23,795 GMT-0600 pje07580 [Timer-5] WARN 910723 KeystoreRotation.validateCDSCert Validation of the keystore in CDS failed : com.fedex.security.client.CryptoException: Unrecoverable error in PBE decryption  
   1.0 2016-12-08 23:47:23,795 GMT-0600 pje07580 [Timer-5] ERROR 910723 KeystoreRotation.rotateCert Caught General Exception e: com.fedex.security.client.CryptoException: Unrecoverable error in PBE decryption  
   1.0 2016-12-08 23:47:23,796 GMT-0600 pje07580 [Timer-5] ALL 910723 KeystoreExpirationCheck.deleteLockFile Inside delete lock file, lock file deleted .  
   1.0 2016-12-08 23:47:23,796 GMT-0600 pje07580 [Timer-5] INFO 910723 KeystoreExpirationCheck.logHandler Current cert nearing expiration. Cert found in CDS but was invalid. Exception: The Security API could not automatically rotate the cert because it failed validation. com.fedex.security.client.CryptoException: Unrecoverable error in PBE decryption

**Resolution:**

The application was re-deployed to the server (WebLogic) and the previous rotation thread (5) was still executing. To keep this issue from happening on WebLogic, you can either always stop and start WebLogic when deploying your application, or update the application context file to destroy the threads when the application is undeployed. Please see section 5.4.2 of the users guide.  
<http://itg.prod.fedex.com/sf/go/doc325481?nav=1>

**Scenario#3 (Refer artf1357824) - AppId APP4502 is NOT authorized to queryByIndex authZ/rule**

When we see logs stating **“AppId is NOT authorized to queryByIndex authZ/rule; Service Id=943415\_cds,”** as below, then please refer fix in resolution section.

**“**2.0 2016-10-26 19:25:01,657 GMT+0000 vje56105 [Timer-20] 7.0.0 DEBUG 4502 WebServiceTemplate.handleFault Received Fault message for request [SaajSoapMessage {<http://www.fedex.com/xmlns/cds2>}indexQueryRequest]  
2.0 2016-10-26 19:25:01,657 GMT+0000 vje56105 [Timer-20] 7.0.0 ERROR 4502 CdsClient.logSoapException Unable to do an indexQuery.  SOAP errors: FailedAuthZ, Security Error: AppId APP4502 is NOT authorized to queryByIndex authZ/rule; Service Id=943415\_cds,**”**

**Resolution:**

We need to log in to ESC in respective environment and load 943415-CommonDataService application under ECUST-CommonDataSvc profile and go to roles tab. Then we need to add the mentioned application id in application accounts of **authZSiliconQueryClient** and **certzillaSiliconQueryClient roles.**

**Steps:**

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

**Scenario#4 (Refer artf1343665) - ESC Service Request**

User’s application was not having access to ESC Service. For such issues, please refer resolution section.

**Resolution:**

We need to log in to ESC in respective environment and load **4393-ESCService application under EA-EnterpriseSecurityCenter profile** and go to roles tab. Then we need to add the mentioned application id in application accounts **of authNClients role.**

**Steps:**

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

**Scenario#5 (Refer**[**artf1371310**](http://itg.prod.fedex.com/sf/go/artf1371310)**) – eShipmentGUI - Workflow Approval**

A client submits a workflow via the Create Service but when the user logs into GUI, the assigned workflow doesn’t appear in Manager’s approval queue in EWF. For such issues, please refer resolution section.

**Resolution:**

We need to log in to ESC in respective environment and load ***5688 – EntWFEngine* application under *ESD-EnterpriseWorkflow* profile** and go to roles tab. Then we need to add the application id which initiated the workflow in application accounts **of *GuiApplications* role.**

**Steps:**

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

**Scenario#6 (Refer** [**artf1381878**](http://itg.prod.fedex.com/sf/go/artf1381878)**) - Not able to add in the users in ESC System**

User wants to add fedEx id’s for one admin group in the DEV and TEST Environments of ESC.

But it says "Invalid FedEx Id"

**Resolution:**

We need to login in to the respective environments of ESC. We can check whether we are able to add these fedex id’s to any of the demo group and if the same error we are getting i.e. “Please enter a valid FedEx Id.” It means, those fedex id’s are not mapped or added to the corresponding level of LDAP.

So we can suggest to the user that, he/she needs to raise request to add those fedex ids by sending mail on LDAP: [ldap@request.fedex.com](mailto:ldap@request.fedex.com). Once theses fedex id’s mapped with corresponding level of LDAP user will able to add those fedex id’s to the group.

**Scenario#7 (Refer** [artf1372784](http://itg.prod.fedex.com/sf/go/artf1372784)**) - Request access to access ESC Dev, Test & Prod for ARMADA\_EDCW symphony profile**

User wants managing role access for the particular application. Here user wants managing role access to the ARMADA-EDCW (6934) app for all the environment of ESC.

For such scenario please refer resolution section.

**Resolution:**

For such scenario we need to check who is having the managing role for corresponding application. To check this we have to follow below steps:

Log in to the corresponding environment of ESC

1. click on the “Home” tab, typing in the Symphony profile “EA-EnterpriseSecurityCenter”
2. Select the “4112 – EnterpriseSecurityCenter” application. A Workflow tab will appear.
3. Click on “Workflow” Tab
4. Select “All workflows” from Workflow Type drop down list box
5. Click on “Run Report” button
6. Click on Export Data

Here we can download the excel sheet. Here we can check with app id. If the App ID is present in the sheet then we can check the status for that app in Status column. If it is already approved then we have to check corresponding Employee ID with that app. That Employee ID should be the part of managing role for the corresponding application. And If someone is already having managing role access to this application.

We can suggest to user to get in touch with the person who have managing role access for the corresponding application then that person will able to add more users/groups to the managing role by following below steps:

1. click on the “Home” tab, typing in the Symphony profile “EA-EnterpriseSecurityCenter”
2. Select the “4112 – EnterpriseSecurityCenter” application. A Role tab will appear.
3. Click on the Role tab and you will see a managing role for your application. Click on it.
4. Add users/groups to that role. The members in the managing role have access to the Enterprise Security-GUI and will be able to make changes to the authorization policy. (Note: It may take up to 5 minutes for the policy in the ESC to refresh the membership of the new role.).

In case the corresponding app id is not present in the downloaded excel sheet then we can ask user to follow below steps for getting managing role access to the required application.

1) Open ESC Home page

2) Enter new setup requests by clicking the "Sign Me up Link" on the Home Page of ESC

3) The welcome screen will displays with different esc level keywords. Click on OK

4) Select your application's Symphony profile in the Symphony profile picker and select your application id from the application id drop down. Click the submit button.

After this HFLOW will be initiated by the requestor and sent to the requestor's manager for approval.

Once manager approval is received, registration will be completed within 24 hours. The automated setup process will notify the requestor via email that the setup successfully completed and to verify access in the Enterprise Security Center.

**Scenario#8 (Refer** [**artf1373254**](http://itg.prod.fedex.com/sf/go/artf1373254)**) - Need connection details for ESC development environment**

User wants to integrate their application with ESC for reading the policies and authorization using css framework. So they need certificate and some client specific properties for css framework.

For such scenario please refer resolution section.

**Resolution:**

We can suggest user to get in touch with Certzilla team for certificate and passphrase in client.properties. Here is the mail address to contact: [certAuthAdmin@corp.ds.fedex.com](mailto:certAuthAdmin@corp.ds.fedex.com)

**Scenario#9 (Refer** [**artf1374767**](http://itg.prod.fedex.com/sf/go/artf1374767)**) – Remove ESC Groups No Longer Needed**

User wants to delete ESC groups that were created. At this time there is no support for deleting a group.  For such scenario please refer resolution section

**Resolution:**

If a group deletion is required, we can suggest user to contact LDAP by opening an RT request at: https://request.fedex.com

**Scenario#10 (Refer** [**artf1379084**](http://itg.prod.fedex.com/sf/go/artf1379084)**) - Permissions to create groups in ESC**

User wants to create groups in ESC. For such scenario please refer the resolution section

**Resolution:**

To create/modify the group user should be part of the managing role of corresponding application.  
To be a part of managing role of application, user have to follow the below steps:

1) Open ESC Home page in needed environment(Dev/Test/Prod)   
2) Enter new setup requests by clicking the "Sign Me up Link" on the Home Page of ESC   
3) The welcome screen will displays with different esc level keywords. Click on OK   
4) Select your application's Symphony profile in the Symphony profile picker and select your application id from the application id drop down. Click the submit button.   
Note:   
After this HFLOW will be initiated by the requestor and sent to the requestor's manager for approval.   
Once manager approval is received, registration will be completed within 24 hours. The automated setup process will notify the requestor via email that the setup successfully completed and to verify access in the Enterprise Security Center.  
Once you are in the managing role, you can add other users too in the managing role of your application.

Once user will get the managing role access for corresponding application, he/she will be able to create/modify the group by following below steps:

1. Open ESC Home page in needed environment(Dev/Test/Prod)
2. Click on the “Home” tab, typing in the Symphony profile the corresponding profile
3. Select the required application.
4. Click on “Select” button
5. Click on “Group” Tab Where user can find three option button Create New Group, View or Modify Existing, View Groups for a User.

As per the user’s requirement he/she can able to perform operation with Group tab.

**Scenario#11 (Refer** [**artf1381854**](http://itg.prod.fedex.com/sf/go/artf1381854)**) - Correct URL for accessing CDS groups.**

User noticed that their Sabre application is using 2 different URL’s for accessing the ESC groups in CDS. One module is using http://grs-sso.prod.fedex.com:2204/wsso/mygroups and the other one is using http://stg-mygroups.corp.fedex.com:2004/wsso/mygroups

They were not sure which one is the correct one to use. With help of DFW 7.0.0 user guide the information is specified in resolution section.

**Resolution:**

security.api.groups.grs.url:   
  
The URL for the GRS group service. Possible values include:  
  
Dev: http://dev-mygroups.corp.fedex.com:1904/wsso/mygroups  
Test: http://stg-mygroups.corp.fedex.com:2004/wsso/mygroups  
Prod: http://grs-sso.prod.fedex.com:2204/wsso/mygroups  
  
For ESC groups in production you can use:  
  
http://grs-sso.prod.fedex.com:2204/wsso/mygroups

**Scenario#12 (Refer** [artf1376436](http://itg.prod.fedex.com/sf/go/artf1376436)**) - Can multiple developers have ESC admin access for a given project?**

User wants to know is it possible for more than one user to have administrative rights to their project in Enterprise Security Center? Please refer Resolution section for this:

**Resolution:**

Yes it's possible for more than one user to have admin rights to their project in ESC.  
User having admin rights to their project in ESC can also add more user’s or groups to their project. He/she can do such by referring **Scenario#7** of this document

**Scenario#13 (Refer** [artf1377887](http://itg.prod.fedex.com/sf/go/artf1377887)**) - Need assistance with Eclipse settings for Maven**

User have installed Maven 3.3.9 and it runs successfully from the command line on his Windows 7 laptop. Problems arise when trying to create a Maven Project in Eclipse. During the creation process user consistently receiving the error shown below

.Could not resolve archetype org.apache.maven.archetypes:maven-archetype-quickstart:RELEASE from any of the configured repositories

**Resolution:**

The solution is to delete everything in the \.m2\repository directory and re index the repository.

**Scenario#14 (Refer** [**artf1376008**](http://itg.prod.fedex.com/sf/go/artf1376008)**) - Could you please restart SRS-GRS Jenkins**

If user are not able to build the jobs then we can restart the Jenkins server. Please refer below steps to restart the Jenkins server

**Resolution:**

Login in to the 10.255.249.52 VM Open C Drive -> WebLogic -> ALPS prod -> Alps client-> Batch file->

uid = \*\*enter valid UID\*\*

psw = \*\*enter valid password\*\*

provisioner = Tomcat

-> level L4

-> target jenkins

-> info -> all -> stop -> all ->

info -> all -> start -> all ->

info -> all

**Scenario#15 (Refer** [**artf1367258**](http://itg.prod.fedex.com/sf/go/artf1367258)**) – Can't start bootstrap**

When we see the logs for such scenario and getting the log error as:

411433 CSSBootstrap15.buildPolicy ...Configuring Client Functionality...

java.lang.IllegalArgumentException: FileLoader.alwaysLogFiles - fileName param is null

at com.fedex.security.common.FileLoader.alwaysLogFiles(FileLoader.java:265)

at com.fedex.security.client.KeystoreCipherProviderImpl.<init>(KeystoreCipherProviderImpl.java:104)

at com.fedex.security.client.KeystoreCipherProviderImpl.<init>(KeystoreCipherProviderImpl.java:39)

at com.fedex.security.client.KeystoreCipherProviderImpl$KeystoreCipherProviderImplHolder.getInstance(KeystoreCipherProviderImpl.java:173)

at com.fedex.security.client.KeystoreCipherProviderImpl.getInstance(KeystoreCipherProviderImpl.java:294)

at com.fedex.security.bootstrap.CSSBootstrap15.clientConfig(CSSBootstrap15.java:231)

at com.fedex.security.bootstrap.CSSBootstrap15.buildPolicy(CSSBootstrap15.java:164)

at com.fedex.dws.common.esc.EscAuthorizorFactory.getInstance(EscAuthorizorFactory.java:73)

at com.fedex.dws.common.esc.EscBO.isAuthorized(EscBO.java:71)

at com.fedex.dws.dawg.padgpsmgr.home.PadGpsMgrHomeAction.isAuthorizedForPadGpsMgr(PadGpsMgrHomeAction.java:144)

at com.fedex.dws.dawg.padgpsmgr.home.PadGpsMgrHomeAction.execute(PadGpsMgrHomeAction.java:64)

at org.apache.struts.action.RequestProcessor.processActionPerform(RequestProcessor.java:425)

at org.apache.struts.action.RequestProcessor.process(RequestProcessor.java:228)

at org.apache.struts.action.ActionServlet.process(ActionServlet.java:1913)

at org.apache.struts.action.ActionServlet.doGet(ActionServlet.java:449)

at javax.servlet.http.HttpServlet.service(HttpServlet.java:731)

at javax.servlet.http.HttpServlet.service(HttpServlet.java:844)

at weblogic.servlet.internal.StubSecurityHelper$ServletServiceAction.run(StubSecurityHelper.java:280)

at weblogic.servlet.internal.StubSecurityHelper$ServletServiceAction.run(StubSecurityHelper.java:254)

at weblogic.servlet.internal.StubSecurityHelper.invokeServlet(StubSecurityHelper.java:136)

at weblogic.servlet.internal.ServletStubImpl.execute(ServletStubImpl.java:346)

at weblogic.servlet.internal.TailFilter.doFilter(TailFilter.java:25)

at weblogic.servlet.internal.FilterChainImpl.doFilter(FilterChainImpl.java:79)

at com.fedex.dws.dawg.util.ReverseProxyPathAdjustmentFilter.doFilter(ReverseProxyPathAdjustmentFilter.java:136)

at weblogic.servlet.internal.FilterChainImpl.doFilter(FilterChainImpl.java:79)

at weblogic.servlet.internal.WebAppServletContext$ServletInvocationAction.wrapRun(WebAppServletContext.java:3436)

at weblogic.servlet.internal.WebAppServletContext$ServletInvocationAction.run(WebAppServletContext.java:3402)

at weblogic.security.acl.internal.AuthenticatedSubject.doAs(AuthenticatedSubject.java:321)

at weblogic.security.service.SecurityManager.runAs(SecurityManager.java:120)

at weblogic.servlet.provider.WlsSubjectHandle.run(WlsSubjectHandle.java:57)

at weblogic.servlet.internal.WebAppServletContext.doSecuredExecute(WebAppServletContext.java:2285)

at weblogic.servlet.internal.WebAppServletContext.securedExecute(WebAppServletContext.java:2201)

at weblogic.servlet.internal.WebAppServletContext.execute(WebAppServletContext.java:2179)

at weblogic.servlet.internal.ServletRequestImpl.run(ServletRequestImpl.java:1572)

at weblogic.servlet.provider.ContainerSupportProviderImpl$WlsRequestExecutor.run(ContainerSupportProviderImpl.java:255)

at weblogic.work.ExecuteThread.execute(ExecuteThread.java:311)

at weblogic.work.ExecuteThread.run(ExecuteThread.java:263)

2.0 2016-11-17 18:04:30,408 GMT+0000 COS-837763-L1 [[ACTIVE] ExecuteThread: '6' for queue: 'weblogic.kernel.Default (self-tuning)'] 7.0.0 FATAL 411433 CSSBootstrap15.buildPolicy !!!!!!!!!Error Starting Bootstrap!!!!!!!!!

This error generally occurs due to the issue in application-context.xml file. Need to check whether the files setup correctly or not

**Resolution:**

Have to setup following entries in application-context.xml:

CSSBootstrap15 bootstrap = new CSSBootstrap15();  
  
bootstrap.setClient(true);  
bootstrap.setService(true);  
bootstrap.setClientProperties(config.getString(ESCCommonConstants.ESC\_CLIENT\_PROPS));  
bootstrap.setSecurityProperties(config.getString(ESCCommonConstants.ESC\_SECURITY\_PROPS));  
  
bootstrap.buildPolicy();

**Scenario#16 (Refer** [**artf1380774**](http://itg.prod.fedex.com/sf/go/artf1380774)**) - Information on Dev Framework with permanent fix for the "400: Bad Request"**

With AST's help user included a temp workaround for the "400: Bad Request" exception

They had to include this jar from WL in the classpath when starting their managed server:

/opt/weblogic/wl12.1.3.0/oracle\_common/modules/com.sun.xml.messaging.saaj.saaj-impl\_1.3.jar

User wants in which development framework version the fix is available. For this please go through the resolution section.

**Resolution:**

The fix was available in development framework 7.0.1 version.  
  
Please get this from the URL:  
<http://nexus.test.cloud.fedex.com:8081/nexus/content/repositories/devframeworkrepo/devframework/PackageFramework/7.0.1/>

**Scenario#17 (Refer** [**artf1368949**](http://itg.prod.fedex.com/sf/go/artf1368949)**) - fwmetrics connection problem**

On L2 Source Tracking server, user facing issue with fwmetrics connection problem.

By looking to the logs:

Warning: org.apache.xerces.parsers.SAXParser: Feature 'http://javax.xml.XMLConstants/feature/secure-processing' is not recognized.

Warning: org.apache.xerces.parsers.SAXParser: Property 'http://javax.xml.XMLConstants/property/accessExternalDTD' is not recognized.

Warning: org.apache.xerces.parsers.SAXParser: Property 'http://www.oracle.com/xml/jaxp/properties/entityExpansionLimit' is not recognized.

WARNING: Could not connect from host [10.250.3.74] to the FedEx DevFramework Metrics Server at [http://fwmetricsstage.prod.cloud.fedex.com:9090/metricsservice/service.v1.wsdl]. Please check to ensure your firewall settings are correct.

ERROR StatusLogger No log4j2 configuration file found. Using default configuration: logging only errors to the console.

22:23:36.650 [[ACTIVE] ExecuteThread: '0' for queue: 'weblogic.kernel.Default (self-tuning)'] ALL com.fedex.framework.logging.FedExLoggerLog4j2Impl - Framework Version: 7.0.0

22:23:36.831 [[ACTIVE] ExecuteThread: '0' for queue: 'weblogic.kernel.Default (self-tuning)'] ALL com.fedex.security.client.PkcTokenGeneratorImpl.all - The Security API detected that this is not a Managed Environment and the autocertrotation.flag = false is set in security.properties therefore Automated Certificate Rotation will not execute.

22:23:36.900 [[ACTIVE] ExecuteThread: '0' for queue: 'weblogic.kernel.Default (self-tuning)'] ALL com.fedex.security.client.PkcTokenGeneratorImpl.all - Expiration Date of the APP105756 Application Certificate on the filesytem is (Tue May 09 13:54:00 GMT-00:00 2017)

Warning: org.apache.xerces.parsers.SAXParser: Feature 'http://javax.xml.XMLConstants/feature/secure-processing' is not recognized.

Warning: org.apache.xerces.parsers.SAXParser: Property 'http://javax.xml.XMLConstants/property/accessExternalDTD' is not recognized.

Warning: org.apache.xerces.parsers.SAXParser: Property 'http://www.oracle.com/xml/jaxp/properties/entityExpansionLimit' is not recognized.

22:23:37.471 [Timer-4] ERROR com.fedex.security.client.KeystoreExpirationCheck - client.properties cannot be resolved to an absolute file path because it does not reside on the file system

22:23:37.471 [Timer-4] ALL com.fedex.security.client.KeystoreExpirationCheck.all - The Security API detected that this is not a Managed Environment and the autocertrotation.flag = false is set in security.properties therefore Automated Certificate Rotation will not execute.

20161117 10:27:07:350 Initializing TrackServer EJB interface

20161117 10:27:07:352 Connecting to URL : t3://jtrackdev.idev.fedex.com:9901

20161117 10:27:07:352 Getting Initial Context for URL : t3://jtrackdev.idev.fedex.com:9901

20161117 10:27:07:393 Context lookup done for JNDI name : server.TrackServerHome

Please refer the resolution section for such issue.

**Resolution:**

We can ask user to set their firewall rule to talk to metrics service and update send.metrics=false  
in fp.properties file.

**Scenario#18 (Refer** [**artf1354785**](http://itg.prod.fedex.com/sf/go/artf1354785)**) - unable to download the new Dev Framework software.**

User wants to download Development Framework 7.0.0. So user can download the DFW 7.0.0 software from the link specified in resolution section.

**Resolution:**

You can download the Development Framework 7.0.0 from below link

URL for devframework 7.0.0 (POM):

<http://nexus.test.cloud.fedex.com:8081/nexus/content/repositories/devframeworkrepo/devframework/DeveloperFramework/7.0.0/>

devframework 7.0.0 (EAR/WAR file)

<http://nexus.test.cloud.fedex.com:8081/nexus/content/repositories/devframeworkrepo/devframework/PackageFramework/7.0.0/>

User can refer Development framework user guide. It will help him in installing Dev. framework in his machine.  
  
Link to user guide is:   
<http://itg.prod.fedex.com/sf/go/doc1186501?nav=1>

**Scenario#19 (Refer** [artf1333433](http://itg.prod.fedex.com/sf/go/artf1333433)**) - PROD ESC ldap, grs url entries**

User needs ldap, grs url entries for prod security.properties file. Please refer Resolution section

**Resolution:**

For ldap URL: ldap://directory.fedex.com:389/ou=people,o=fedex,c=us

For grs use  
# Groups Caching   
security.api.groups.refresh=3600   
security.api.groups.grs.url=http://grs-sso.prod.fedex.com:2204/wsso/mygroups   
security.api.groups.grs.readtimeout=20   
security.api.groups.grs.conntimeout=20

**Scenario#20 (Refer** [**artf1380774**](http://itg.prod.fedex.com/sf/go/artf1380774)**) 400 Bad Request**

Clients using devframework in 10.3.2 could make service calls to a target service without issue.  When the same client code and devframework was migrated to 12.1.X it resulted in the following type of error:

 com.sun.xml.ws.client.ClientTransportException: The server sent HTTP status code 400: Bad Request

**Resolution:  Force WLS to use a specific SAAJ implementation**

Pre-pend a reference to the MW\_HOME/oracle\_common/modules/com.sun.xml.messaging.saaj.saaj-impl\_1.3.jar to the server’s CLASSPATH, where MW\_HOME=/opt/weblogic/wl12.1.2.0 or /opt/weblogic/wl12.1.3.0

**Scenario#21 Hostname verification failed**

Web service clients using the “HTTPS” protocol along with devframework that were migrated to 12.1.X incorrectly experienced problems with SSL hostname verification that resulted in messages like the following being generated ‘even though’ the hostname in the certificate was correct:

WARN 5398 KeystoreRotation.getKeystoreFromCDS Caught exception e: java.lang.RuntimeException: javax.xml.ws.WebServiceException: javax.net.ssl.SSLKeyException: Hostname verification failed: HostnameVerifier=weblogic.security.utils.SSLWLSHostnameVerifier, hostname=cds-level3.ute.fedex.com.

**Resolution: Use Sun Http Handler instead of WebLogic Http Handler**

Set the following java system property in the WLS start script which forces the server to use the HttpHandler code built into the JVM instead of the weblogic specific handler code:

 -DuseSunHttpHandler=”true”

**Scenario#22 JAXB marshalling errors**

Web service clients using the devframework ran into java->XML marshalling errors similar to the following:

"[ACTIVE] ExecuteThread: '6' for queue: 'weblogic.kernel.Default (self-tuning)'" daemon prio=10 tid=0x00002b2e7113b000 nid=0x256f runnable [0x00002b2e75fa1000]

   java.lang.Thread.State: RUNNABLE

               at com.fedex.csr.common.util.ExceptionUtil.getRootCauseMessage(ExceptionUtil.java:16)

               at com.fedex.csr.common.oxm.JaxbMapper.marshal(JaxbMapper.java:48)

**Resolution: Override the WebLogic default JAXB Providers and use Glassfish RI Providers instead**

Prepend a reference to the WL\_HOME/modules/databinding.override\_1.1.0.0.jar to server’s CLASSPATH where WL\_HOME=/opt/weblogic/wl12.1.2.0/wlserver or /opt/weblogic/wl12.1.3.0/wlserver.  This forces WLS to use the Glassfish JAXB Provider and JAXB DataBinding Provider (which are included in the WLS distribution) instead of the default EclipseLink MOXy implementations.

[NOTE: Please check for the version on the server databinding.override\_1.1.0.0.jar or databinding.override\_1.2.0.0.jar]

**Scenario#23 (Refer** [artf1409463](http://itg.prod.fedex.com/sf/go/artf1409463) **) Devfw 5.2.0 and wily conflict**

Even though successfully loading properties files and proper configuration the application was not able to connect to CDS server. The application uses Wily for performance monitoring of web service transactions. If we simply turn off wily, the errors go away. No changes to our devframework files. We re-enable wily and this exact error comes back.

Please find the logs for the issue below:

2017-03-06T20:19:44.748||INFO|KeystoreRotation.canWrite The Security API is able to write to the client.properties file:/opt/fedex/traqs/current/lib/APP4820/traqs/client.properties  
2017-03-06T20:19:44.749||INFO|KeystoreRotation.canWrite The Security API is able to write to the keystore:/opt/fedex/traqs/current/lib/APP4820/traqs/APP4820.p12  
2017-03-06T20:19:44.750||INFO|KeystoreExpirationCheck.timeToQueryCDSForCert clientTokenCache doesn't contain APP4820\_cds\_cert\_query\_timestamp  
2017-03-06T20:19:44.751||DEBUG|KeystoreExpirationCheck.isLockFileExist Inside is lockfile exists. Exists: false, can write: false  
2017-03-06T20:19:44.751||DEBUG|FileLoader.getFileAsInputStream Loaded file: /opt/fedex/traqs/current/lib/APP4820/traqs/client.properties  
2017-03-06T20:19:44.752||DEBUG|FileLoader.getFileAsInputStream Loaded file: /opt/fedex/traqs/current/lib/APP4820/traqs/APP4820.p12  
2017-03-06T20:19:44.753||INFO|KeystoreExpirationCheck.getCertExprDt Keystore file name read from client.properties: APP4820.p12  
2017-03-06T20:19:44.769||DEBUG|KeystoreExpirationCheck.compareCacheExprWithDiskExprDt Inside compare CacheExprWithDiskExprDt .true  
2017-03-06T20:19:44.769||ALL|KeystoreExpirationCheck.rotationHandler lock file not exist and dates are match .  
2017-03-06T20:19:44.770||DEBUG|KeystoreExpirationCheck.createLockFile Inside create lock file, lock file created .true  
2017-03-06T20:19:44.779||WARN|KeystoreRotation.getKeystoreFromCDS Caught exception e: java.lang.RuntimeException: java.lang.ClassCastException: java.util.HashMap cannot be cast to com.sun.xml.ws.transport.Headers  
2017-03-06T20:19:44.780||WARN|KeystoreRotation.getCDSCertExpirationDate Failed to get the expiration date of the new cert from CDS. : java.lang.RuntimeException: java.lang.ClassCastException: java.util.HashMap cannot be cast to com.sun.xml.ws.transport.Headers  
2017-03-06T20:19:44.781||ALL|KeystoreExpirationCheck.deleteLockFile Inside delete lock file, lock file deleted .  
2017-03-06T20:19:44.781||ALL|KeystoreExpirationCheck.logHandler Current cert nearing expiration and the cert in CDS is invalid .  
2017-03-06T20:19:44.782||FATAL|PkcTokenGeneratorImpl.configure Configuration for certificate rotation is not set correctly. Please make sure the application is able to connect to the correct LDAP and CDS url inside security.properties. Check log messages for more details.  
2017-03-06T20:19:44.783||FATAL|PkcTokenGeneratorImpl.configure Exception encountered configuring generator for client APP4820  
2017-03-06T20:19:44.783||FATAL|CSSBootstrap15.<init> !!!!!!!!!Error Starting Bootstrap!!!!!!!!!  
java.lang.RuntimeException: Exception encountered configuring generator for client APP4820  
at com.fedex.security.client.PkcTokenGeneratorImpl.configure(PkcTokenGeneratorImpl.java:359)  
at com.fedex.security.client.PkcTokenGeneratorImpl.configure(PkcTokenGeneratorImpl.java:274)  
at com.fedex.security.bootstrap.CSSBootstrap15.clientConfig(CSSBootstrap15.java:323)  
at com.fedex.security.bootstrap.CSSBootstrap15.<init>(CSSBootstrap15.java:127)  
at sun.reflect.NativeConstructorAccessorImpl.newInstance0(Native Method)

The application though loading properties files correctly was not able to connect to CDS when wily is enabled and client=true

**Resolution:**Adding below two jars to classpath resolved the class not found error.

* WebServicesAgent.jar
* BoundaryOnlyTrace.jar

Also there is a setting in **IntroscopeAgent.profile** which has to be uncommented  
# JAXWS jar has changed some methods in 2.2.6 and later versions  
# Uncomment this property if JAXWS version is 2.2.6 or higher  
com.wily.introscope.agent.soa.JAXWSHeadersClassName=com.sun.xml.ws.transport.Headers

**Scenario#24 (Refer** [artf1407733](http://itg.prod.fedex.com/sf/go/artf1407733) **) New cert not being auto rotated for app 6686 in Production**

2017-02-22 18:00:00,069 | Timer-8 | INFO | com.fedex.security.client.KeystoreExpirationCheck |  Keystore Rotation Check being called : The state of the cert is :WARN

2017-02-22 18:00:00,070 | Timer-8 | INFO | com.fedex.security.client.KeystoreRotation | The Security API is able to write to the following directories:/var/fedex/trcimsg;  /var/fedex/trcimsg

2017-02-22 18:00:00,070 | Timer-8 | INFO | com.fedex.security.client.KeystoreRotation | The Security API is able to write to the client.properties file:/var/fedex/trcimsg/client.properties

2017-02-22 18:00:00,070 | Timer-8 | INFO | com.fedex.security.client.KeystoreRotation | The Security API is able to write to the keystore:/var/fedex/trcimsg/APP6686.p12

2017-02-22 18:00:00,070 | Timer-8 | INFO | com.fedex.security.client.KeystoreExpirationCheck |   No recent CDS query, allowing another.

2017-02-22 18:00:00,070 | Timer-8 | INFO | com.fedex.security.client.KeystoreExpirationCheck | Keystore file name read from client.propertiesAPP6686.p12

2017-02-22 18:00:00,075 | Timer-8 | ALL | com.fedex.security.client.KeystoreExpirationCheck.all |  lock file not exist and dates are match .

2017-02-22 18:00:00,115 | Timer-8 | INFO | com.fedex.security.client.KeystoreRotation | The Security API successfully retrieved the keystore from CDS

2017-02-22 18:00:00,115 | Timer-8 | INFO | com.fedex.security.client.KeystoreRotation |  New Cert Expiration Date from CDS ------- Mon Mar 20 16:40:00 GMT-00:00 2017

2017-02-22 18:00:00,115 | Timer-8 | INFO | com.fedex.security.client.KeystoreExpirationCheck | Setting APP6686\_cds\_cert\_query\_timestamp flag to: 2/22/2017 6:0:0.115

2017-02-22 18:00:00,115 | Timer-8 | INFO | com.fedex.security.client.KeystoreExpirationCheck |  Found CDS cert that has the same expiration date as the cached cert.

2017-02-22 18:00:00,115 | Timer-8 | INFO | com.fedex.security.client.KeystoreExpirationCheck |  cdsCertExpiredate: Mon Mar 20 16:40:00 GMT-00:00 2017 cacheExprDate: Mon Mar 20 16:40:00 GMT-00:00 2017

2017-02-22 18:00:00,115 | Timer-8 | ALL | com.fedex.security.client.KeystoreExpirationCheck.all | Inside delete lock file, lock file deleted .

2017-02-22 18:00:00,115 | Timer-8 | WARN | com.fedex.security.client.KeystoreExpirationCheck | Current cert nearing expiration and the cert in CDS is invalid .

2017-02-22 18:03:26,442 | Timer-0 | ALL | com.fedex.security.client.PkcTokenGeneratorImpl.all | Expiration Date of the cert on the filesytem is : Mon Mar 20 16:40:00 GMT-00:00 2017

**Resolution:** Changing the idm url to the correct version will resolve the issue. In this case it is idm.url=https://sso.secure.fedex.com/DelegationJWS/DelegationV2?wsdl.

**Scenario#25 (Refer** [artf1411687](http://itg.prod.fedex.com/sf/go/artf1411687) **) Jenkins CXS Build Error-Nexus Test Repo Issue**

Jenkins : Build jobs are failing in the environment due to Dev CXS Maven Repo connection

We are getting below errors in the Jenkins Job. As mentioned by Hydra team, they have faced similar errors before and after bouncing the below mentioned cxs-repository\_dev repo it started working. Please check if this is related to Nexus repo issue

http://fwkmaven.ute.fedex.com:8081/nexus/index.html#view-repositories;cxs-repository\_dev~browsestorage

Error From Jenkins

ERROR: Failed to parse POMs

java.io.IOException: Remote call on Channel to Maven [/opt/java/hotspot/7/current/bin/java, -Xmx2048m, -XX:MaxPermSize=512m, -cp, /opt/fedex/jenkins/maven3-agent.jar:/opt/fedex/FDXmaven/boot/plexus-classworlds-2.4.jar, org.jvnet.hudson.maven3.agent.Maven3Main, /opt/fedex/FDXmaven/, /opt/fedex/jenkins/slave.jar, /opt/fedex/jenkins/maven3-interceptor.jar, /opt/fedex/jenkins/maven3-interceptor-commons.jar, 40962] failed

at hudson.remoting.Channel.call(Channel.java:756)

at hudson.maven.AbstractMavenProcessFactory.newProcess(AbstractMavenProcessFactory.java:284)

at hudson.maven.ProcessCache.get(ProcessCache.java:236)

at hudson.maven.MavenModuleSetBuild$MavenModuleSetBuildExecution.doRun(MavenModuleSetBuild.java:764)

at hudson.model.AbstractBuild$AbstractBuildExecution.run(AbstractBuild.java:533)

**Resolution:** Bouncing the server fixed the issue.

**Scenario#26 (Refer** [artf1410533](http://itg.prod.fedex.com/sf/go/artf1410533)**) Created a group kats and now can't access it.**

I created a group kats yesterday and now I cannot access it.

**Resolution:** User was not in the managing role of the group. The group was managed by TRIP-VCom\_Admin and 17643- White, Stewart  
331206- Zellers, Danny  
49763- Pittman, Tony  
593079- Silbermann, Frank  
857909- Brice, Tim Brice

Were part of the managing role? So suggested user to ask them to add her to the managing role.

**Scenario#27 (Refer** [artf1403218](http://itg.prod.fedex.com/sf/go/artf1403218)**) Production configuration to connect to ESC servers**

ARMADA-EDCW profile will connect to production ESC /WSSO servers. Please let us know the

Production configuration to connect to ESC servers

Attached below are the properties that we have configured in our test system (Level2). Application MTP is planned for this weekend 19th Feb Belgium time and need this information urgently

security.properties

===========

cds.url=https://cds-level2.ute.fedex.com/CommonDataService/secure/cds2.wsdl

security.api.groups.grs.url=http://dev-mygroups.corp.fedex.com:1904/wsso/mygroups

ldap.url=ldap://dirdev.corp.fedex.com:389/ou=people,o=fedex,c=us

idm.url=https://test.secure.fedex.com/delegation/services/Delegation?wsdl

fp.properties

==========

framework.version=5.0.0

full.env.name=Level2

release.nbr=1.1

**Resolution:** We provided the production configurations to the user, which are as below:

security.properties  
===========  
cds.url=https://cds.prod.fedex.com/CommonDataService/secure/cds2.wsdl  
security.api.groups.grs.url=http://grs-sso.prod.fedex.com:2204/wsso/mygroups  
ldap.url=ldap://directory.fedex.com:389/ou=people,o=fedex,c=us  
idm.url=https://sso.secure.fedex.com/delegation/services/Delegation?wsdl  
  
fp.properties  
==========  
framework.version=5.0.0  
full.env.name=LP  
release.nbr=1.1

**Scenario#28 (Refer** [artf1401772](http://itg.prod.fedex.com/sf/go/artf1401772)) **Change managing role for CrispMXPAccessGroup**

Hi Team,

I can't update the managing roles for this group, I would delete the group and create it from scratch but I know that feature is not available. Can someone change the managing roles for this group to crisp\_admin please?

Regards

Saul

**Resolution:** This feature is not available in ESC as of now, so suggested user to delete the group by raising a request to [ldap@request.fedex.com](mailto:ldap@request.fedex.com), and then create a new group.

**Scenario#29 (Refer** [artf1405604](http://itg.prod.fedex.com/sf/go/artf1405604)) **CSR and Java 8**

I am using CSR 5.1.1 in my application and I am making an attempt to upgrade my java version to JAVA 8. Can I use Java 8 for CSR?

for CSR 7.1.0 are there any changes for SOAP version...SOAP 1.1 vs 1.2

**Resolution:** With Java 7, compatible SOAP version is 1.1 only, so there is no need to make any change in SOAP version.

**Scenario#30 (Refer** [artf1405535](http://itg.prod.fedex.com/sf/go/artf1405535) **) DevFramework Migration to 7.0.0 - log4j Priority class not found error**

ERROR StatusLogger No log4j2 configuration file found. Using default configuration: logging only errors to the console.

10:21:48.396 [main] ALL com.fedex.framework.logging.FedExLoggerLog4j2Impl - Framework Version: 7.0.0

Exception in thread "main" java.lang.NoClassDefFoundError: org/apache/log4j/Priority

at com.fedex.framework.logging.ALPSLoggerImpl.<init>(ALPSLoggerImpl.java:15)

at com.fedex.framework.logging.ALPSLogger.getLogger(ALPSLogger.java:15)

at com.fedex.framework.logging.ALPSLogger.getLogger(ALPSLogger.java:25)

at com.fedex.alps.comm.CommandTransport.<clinit>(CommandTransport.java:17)

at com.fedex.alps.client.AlpsClient.sendRequest(AlpsClient.java:239)

at com.fedex.alps.client.shell.AlpsShellClient.executeRequest(AlpsShellClient.java:64)

at com.fedex.alps.client.shell.AlpsShellClient.buildAndSendRequest(AlpsShellClient.java:262)

at com.fedex.alps.client.shell.AlpsShellClient.startClient(AlpsShellClient.java:419)

at com.fedex.alps.client.shell.AlpsShellClient.main(AlpsShellClient.java:345)

Caused by: java.lang.ClassNotFoundException: org.apache.log4j.Priority

at java.net.URLClassLoader$1.run(URLClassLoader.java:366)

at java.net.URLClassLoader$1.run(URLClassLoader.java:355)

at java.security.AccessController.doPrivileged(Native Method)

at java.net.URLClassLoader.findClass(URLClassLoader.java:354)

at java.lang.ClassLoader.loadClass(ClassLoader.java:425)

at sun.misc.Launcher$AppClassLoader.loadClass(Launcher.java:308)

at java.lang.ClassLoader.loadClass(ClassLoader.java:358)

... 9 more

**Resolution:** Used the FedExLoggerLog4j2Impl class instead of FedExLoggerLog4jImpl class in the application code.

Using correct implementation of FedExLoggerInterface resolved the issue.

**Scenario#31(Refer** [artf1475217](http://itg.prod.fedex.com/sf/go/artf1475217)**) App EAI cannot login as “isAllowed returns false”**

**error**

1. 2017-07-28 14:13:07,718 GMT+0000 c0003715 [[ACTIVE] ExecuteThread: '0' for queue: 'weblogic.kernel.Default (self-tuning)'] 7.1.1 INFO 7470 AuthorizorEnterpriseImpl.isAllowed 2017072802241307|authz|825633|CTSMaintenance|Access|false|

**Resolution:** Resource name is case sensitive and it is not the same in DEV and TEST. It is working after making the change.

**Scenario#32(Refer** [artf1494023](http://itg.prod.fedex.com/sf/go/artf1494023)**)how to retire app certs**

**error**

Exception below  
  
ID=943415\_cds  
1.0 2017-09-05 09:10:32,918 GMT+0000 pje75381 [Timer-18] WARN 7540 KeystoreRotation.getKeystoreFromCDS Caught exception e: java.lang.RuntimeException: com.sun.xml.ws.fault.ServerSOAPFaultException: Client received SOAP Fault from server: UnrecoverableClientError Please see the server log to find more detail regarding exact cause of the failure.  
1.0 2017-09-05 09:10:32,918 GMT+0000 pje75381 [Timer-18] WARN 7540 KeystoreRotation.getCDSCertExpirationDate Failed to get the expiration date of the new cert from CDS. : java.lang.RuntimeException: com.sun.xml.ws.fault.ServerSOAPFaultException: Client received SOAP Fault from server: UnrecoverableClientError Please see the server log to find more detail regarding exact cause of the failure.  
1.0 2017-09-05 09:10:32,918 GMT+0000 pje75381 [Timer-18] ALL 7540 KeystoreExpirationCheck.deleteLockFile Inside delete lock file, lock file deleted .  
1.0 2017-09-05 09:10:32,918 GMT+0000 pje75381 [Timer-18] INFO 7540 KeystoreExpirationCheck.timeToLogFatal Recent CRITICAL log write query, preventing another.  
1.0 2017-09-05 09:20:33,012 GMT+0000 pje75381 [Timer-15] INFO 7540 KeystoreExpirationCheck.timeToLogFatal Recent CRITICAL log write query, preventing another.  
1.0 2017-09-05 10:10:33,020 GMT+0000 pje75381 [Timer-15] ALL 7540 PkcTokenGeneratorImpl.cacheToken Expiration Date of the cert on the filesytem is : Wed Sep 06 14:00:00 GMT+00:00 2017  
1.0 2017-09-05 10:10:33,027 GMT+0000 pje75381 [Timer-15] INFO 7540 KeystoreExpirationCheck.timeToLogFatal Recent CRITICAL log write query, preventing another.  
1.0 2017-09-05 11:00:33,012 GMT+0000 pje75381 [Timer-15] INFO 7540 KeystoreExpirationCheck.timeToLogFatal Recent CRITICAL log write query, preventing another.  
1.0 2017-09-05 11:50:33,019 GMT+0000 pje75381 [Timer-15] ALL 7540 PkcTokenGeneratorImpl.cacheToken Expiration Date of the cert on the filesytem is : Wed Sep 06 14:00:00 GMT+00:00 2017  
1.0 2017-09-05 11:50:33,023 GMT+0000 pje75381 [Timer-15] INFO 7540 KeystoreExpirationCheck.timeToLogFatal Recent CRITICAL log write query, preventing another.  
1.0 2017-09-05 12:40:33,013 GMT+0000 pje75381 [Timer-15] INFO 7540 KeystoreExpirationCheck.timeToLogFatal Recent CRITICAL log write query, preventing another.  
1.0 2017-09-05 13:30:33,021 GMT+0000 pje75381 [Timer-15] ALL 7540 PkcTokenGeneratorImpl.cacheToken Expiration Date of the cert on the filesytem is : Wed Sep 06 14:00:00 GMT+00:00 2017  
1.0 2017-09-05 13:30:33,025 GMT+0000 pje75381 [Timer-15] INFO 7540 KeystoreExpirationCheck.timeToLogFatal Recent CRITICAL log write query, preventing another.  
1.0 2017-09-05 14:20:33,013 GMT+0000 pje75381 [Timer-15] INFO 7540 KeystoreExpirationCheck.timeToLogFatal No recent CRITICAL log write query, allowing another.  
1.0 2017-09-05 14:20:33,014 GMT+0000 pje75381 [Timer-15] FATAL 7540 KeystoreExpirationCheck.handleFatalLogs The state of the cert is FATAL, no rotation has happend.  
1.0 2017-09-05 14:20:33,015 GMT+0000 pje75381 [Timer-15] INFO 7540 KeystoreExpirationCheck.updateCacheFlag Setting APP7540\_fatal\_logged\_timestamp flag to: 9/5/2017 2:20:33.15  
1.0 2017-09-05 15:10:33,019 GMT+0000 pje75381 [Timer-15] ALL 7540 PkcTokenGeneratorImpl.cacheToken Expiration Date of the cert on the filesytem is : Wed Sep 06 14:00:00 GMT+00:00 2017  
1.0 2017-09-05 15:10:33,024 GMT+0000 pje75381 [Timer-15] INFO 7540 KeystoreExpirationCheck.timeToLogFatal Recent CRITICAL log write query, preventing another.

Also the applications do not make a secured call to any backend

**Resolution:** Firstly log into symphony profile and mark the application as retired

**Scenario#33(Refer** [artf1494621](http://itg.prod.fedex.com/sf/go/artf1494621)**) as there is no proper configuration for auto cert rotation not getting error logs and just printing the expiration date**

**Resolution:** Migration from dev framework 6.x.x to 7.1.1 resolved the issue

**Scenario#34(Refer** [artf1499784](http://itg.prod.fedex.com/sf/go/artf1499784)**)** **Trying to implement getToken: token provided by client APP33445 was not generated for this service**

**error**

<code>FailedAuthN</code><desc>Security Error: Authentication Failure: The token provided by client APP33445 was not generated for this service</desc>

**Resolution:** after adding service id-(202830\_EdmEnterpriseService) in PkcTokenGeneratorImpl.getInstance().getToken("202830\_EdmEnterpriseService", "33445"); instead of(APP33445) then resolved

**Scenario#35(Refer** [artf1490773](http://itg.prod.fedex.com/sf/go/artf1490773)**) cannot modify a group I created**

**Error**

You can not work with this group: Sorry, you are not authorized to view/modify this group.

**Resolution:** after refreshing the policies issue got resolved

**Scenario#36(Refer** [artf1494978](http://itg.prod.fedex.com/sf/go/artf1494978)**)** **eGRS Corrupt Cache - ESC Test Level**

**Error** I have permissions and I am listed as a member of several groups when I check the groups individually. But when I attempt to View all the Groups for which I am a member, it lists null.

**Resolution:** GRS team will fix the issue.

**Scenario#37(Refer** [artf1468495](http://itg.prod.fedex.com/sf/go/artf1468495)**)** **Test level Enterprise Workflow not sending workflow notices via email with testing mode info**

**Error** user is not receiving enterprise workflow mails

**Resolution:** restarting the service resolved issue

**Scenario#38(Refer** [artf1479647](http://itg.prod.fedex.com/sf/go/artf1479647)**)** **Where can I find the newest PMD for eclipse ruleset?**

**Resolution:** Please follow the section   
6. PMD Rulesets 13  
from the document listed below :: <http://itg.prod.fedex.com/sf/go/doc1242185?nav=1>