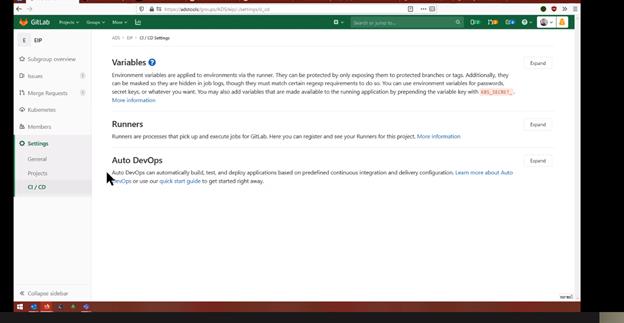
**EIP Post-Production Support Manual**

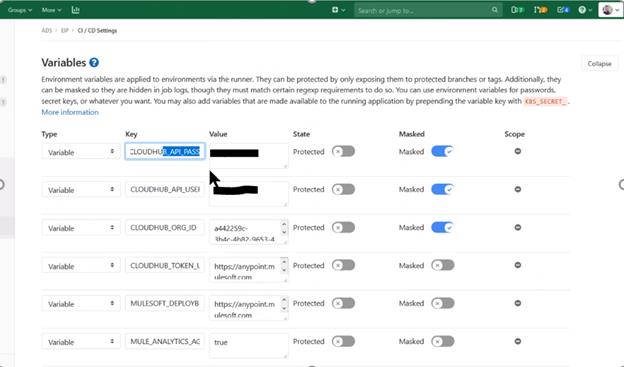
**Last Update: 12/15/2020**

1. **Mandatory field missing error for Accuity interface**
   1. Support user receives an error notification
   2. Support person(EAD) logs into Anypoint platform
   3. Select accuity experience API and click on logs towards your left panel
   4. Review the logs and identify the error message saying ‘missing field’ in the response
   5. Copy the latest correlation Id from the payload
   6. Select accuity process and system API to confirm the latest correlation Id
   7. Click on Anypoint MQ and open the latest error message based on correlation Id **or** login to Azure MuleSoft integration Db and open the error payload based on correlation Id
   8. Copy the encrypted payload and decrypt the payload using the decrypt API and decryption key. Now, you will be able to view the request payload and based on SSN update the missing field in target systems (Maeve/IBS) accordingly
   9. When the accuity requests the details for the same SSN next time, the call with be successful without any issues
2. **500 Server Error / Timeout in Response**
   1. Support user receives an error notification
   2. Support person(EAD) logs into Anypoint platform
   3. Please note 500 server error means one of the systems involved in the interface is not available
   4. Click on the IBS system API application and verify if the IBS system API is down
   5. Click on the Maeve system API application and verify if the Maeve system API is down
   6. Reach out to the respective system SMEs to confirm when the system will be back available
3. **Internal Dataweave / Application Error**
   1. Support user receives an error notification
   2. Support person(EAD) logs into Anypoint platform
   3. Select accuity experience API and click on logs towards your left panel
   4. Review the logs and identify the error message saying ‘internal application’ in the response
   5. Copy the latest correlation Id from the payload
   6. Select accuity process and system API to confirm the latest correlation Id
   7. Support person will download the application logs from Cloudhub
4. **Account Type Mapping Error - if there is no account type mapping in lookup Db then we are sending ‘Other’ in response**
   1. Support user receives an error notification
   2. Support person(EAD) logs into Anypoint platform
   3. Select accuity experience API and click on logs towards your left panel
   4. Review the logs and identify the error message saying ‘mapping not available’ in the response
5. **Mulesoft / FIS (Code connect) APIs Unavailable or Down**
   1. Brittany from Accuity confirmed that in case of unexpected downtime with our APIs, we can send an email to Accuity requesting to stop
   2. Confirm the timeline that Runtime Manager is downtime
   3. Login to Accuity user interface and send the responses manually based on the request email
   4. Check with Brittany if they can still send the requests in an email
6. **Stingray Credential Validation Error**
   1. Support user receives an error notification
   2. Support person(EAD) logs into Anypoint platform
   3. Select IBS system API and click on the logs towards your left panel
   4. Review the logs and identify the error message saying ‘incorrect credentials’ in the response
   5. Click on the settings and review the username and password details and update the details if needed
   6. Upon your update to the credentials, application will get restarted
   7. If there is no update needed to the credentials, make sure appName and accountName are accurate
7. **Account type mapping does not exist in the Azure Db lookup table**
   1. We are maintaining the mapping for Account Type Codes between Accuity and WSFS in the WSFSToAccuityLookup Table (Azure)
   2. Currently, Devon is receiving a notification to add new product codes in IBS. While you were adding the product code in IBS, please make sure to update the WSFSToAccuityLookup table in Azure (non-prod & prod environments) similarly

1. **Platform account created for deploying the applications to Cloudhub from gitlab. Username: mulesoft-deployment**
   1. Mulesoft-deployment user credentials are only used to deploy the mulesoft applications from gitlab to dev/sit/uat/prod environments
   2. Any notifications related to this user like reset password / forgot password email will be sent to the following email address [DL\_MuleSoft\_Owner@wsfsfc.net](mailto:DL_MuleSoft_Owner@wsfsfc.net)
   3. Devon Smith is the primary owner and Chris Zupko is the secondary owner of this account
2. **Platform account created to pull the logs from Cloudhub to LogRhythm. Username: minfosa**
   1. minfosa credentials are only used to pull the logs from Cloudhub and synchronize them to LogRhythm
   2. Any notifications related to this user like reset password / forgot password email will be sent to the following email address informationsecurity@wsfsbank.com
   3. Jamal Pecou is the primary owner and Jon Allen is the secondary owner of this account
3. **How to update the Deployment user password in Gitlab**
   1. Log into Gitlab and select the EIP folder. Click on Settings to your left

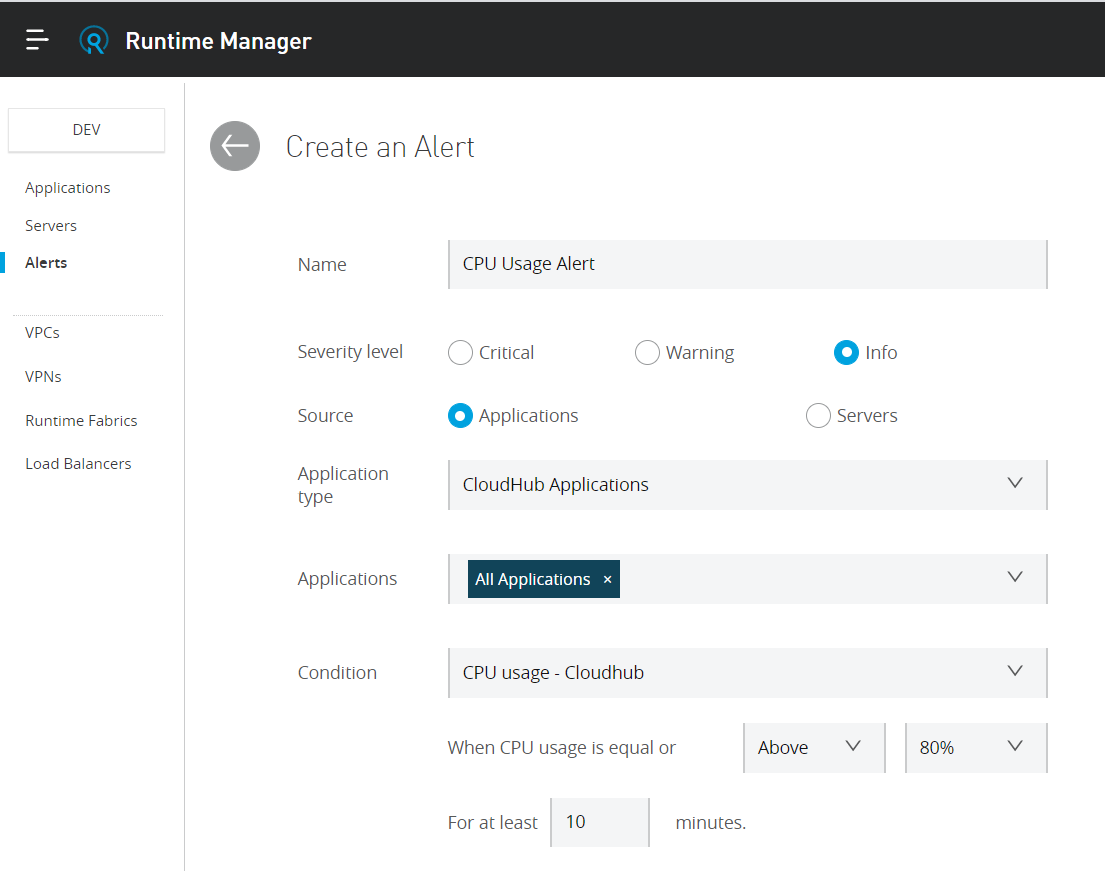
****

* 1. Click on Variables and update the CLOUDHUB\_API\_USERNAME & CLOUDHUB\_API\_PASSWORD fields

****

* 1. Following explains the meaning of each variable state
     1. **Masked** means it doesn’t show in the logs
     2. **Protected** means only certain branches have access to the variable
     3. Don’t want protected on the cloudhub variables since deploying from all branches
     4. There is a “reveal values” button at the bottom of the page. Values are starred out until that button is clicked.

1. **Adding WSFS systems CIDR to MuleSoft VPN**
   1. EAD team will review the existing CIDR notations configured in Anypoint VPN (non-prod/prod)
   2. If the required system IP range is included within the existing CIDR notation, then ignore the below steps
   3. If the required system IP range is not included in the existing CIDR notation, EAD team sends a request to InfoSec inorder to add the respective IP address / CIDR range
   4. InfoSec team logs into Anypoint platform
   5. Click on Runtime Manager and select VPN
   6. Click on wsfs-non-prod-vpn, update the IP address / CIDR range given by EAD team and then click on apply changes
   7. InfoSec (Brandon) will open necessary ports in non-production so that MuleSoft can access the required system
   8. EAD team to confirm that they are able to access the required system / application in non-production
   9. Upon successful confirmation of EAD team, InfoSec should add the same CIDR range in ‘wsfs-prod-vpn’ in Anypoint platform and make necessary port changes in WSFS data center
2. **How to recreate VPC**
   1. Stop the applications in Runtime Manager
   2. Remove the associated environments under VPC
   3. Restart the Applications in Run time Manager
   4. Delete Dedicated Load balancer associated with VPC
   5. Delete associated VPN
   6. Delete the VPC
   7. Now, follow the steps in platform runbook and create a VPC with updated CIDR range
3. **How to update certificates in DLB**
   1. Prerequisites:
      1. Brandon to generate a CSR and send the public and private keys to John, steps are listed in the following document
      2. John Bailey to get the CA signed certificate and will send the .PEM file to Brandon
      3. Brandon / Infosec team will follow the following steps to update the cert in Anypoint platform
   2. Sign into Anypoint Platform and select Runtime Manager
   3. Click on ‘Load Balancer’ to your left
   4. Select the DLB (non-prod / prod) where you want to update the certificate
   5. Click on 'Add Certificate'
   6. Update the Public key
   7. Update the private key
   8. Click on submit and apply changes
4. **How to add Client Certificate in DLB**
   1. Prerequisites:
      1. Make sure you have the client certificate(.pem file) sent by third party vendor
   2. Sign into Anypoint Platform and select Runtime Manager.
   3. Click on ‘Load Balancer’ to your left
   4. Select the DLB (non-prod / prod) where you want to update the certificate
   5. Click on 'Add Certificate'
   6. Update the client certificate under Client Certificate (Optional) section by clicking on Choose file
   7. Click on submit and apply changes
5. **How to add multiple client certificates to DLB?**
   1. In DLB, you can only add one client certificate. In order to add multiple certs, you have to append the multiple certificates (.pem files) in a single file and attach it to DLB
      1. Open the .pem file and copy the certificate from BEGIN CERTIFICATE to END CERTIFICATE to one file
      2. Open the next client certificate (.pem file) and copy the certificate from BEGIN CERTIFICATE to END CERTIFICATE to the same file
   2. Now, attach that file in DLB
6. **Policy Violation Error**
   1. Logrhythm will receive the logs from Cloudhub
   2. InfoSec team will create notifications inside logrhythm when policy violation happens
   3. Infosec team will reach out to EAD team incase of continuous policy violations
   4. EAD team will log into cloudhub and monitor the applications where the policy is getting violated
      1. For the Client Id Enforcement policy it does not show you against which clientId it is validating, for a reason of not exposing the clientId. If you are receiving continuous client\_id policy violation error, reach out to EAD team to make sure if any of the developer using wrong client\_id credentials to access the API
      2. For the IP Whitelist policy, you will receive the source IP which is violating the API in the log message. Infosec team can look at the IP and take respective measures
   5. If you need any additional details, create a support ticket with MuleSoft ( reach out to Devon Smith if you need assistance)
7. **How to create CPU Usage Alert**
   1. Create a custom alert in Runtime Manager for the application that you want to receive an alert
      1. Sign into Anypoint Platform and select Runtime Manager
      2. Click on Alerts to your left and click New (+ icon)
      3. Update the details accordingly along with Recipient who should get an email alert and click on Submit



1. **CPU Usage Exceeded Alert**
   1. EAD team will receive an alert from MuleSoft platform that the CPU usage is exceeded
   2. EAD team to download the system log of the application which exceeded the limit
   3. Troubleshoot the application