# Requirements:-

## On Gateway

Version Supported: 9.4 or above or Custom Javascript Assertion required

## Gateway Cluster Properties

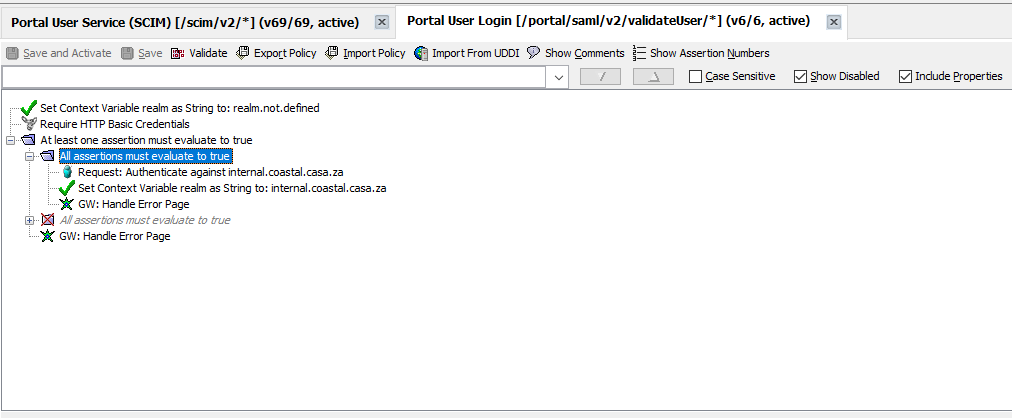
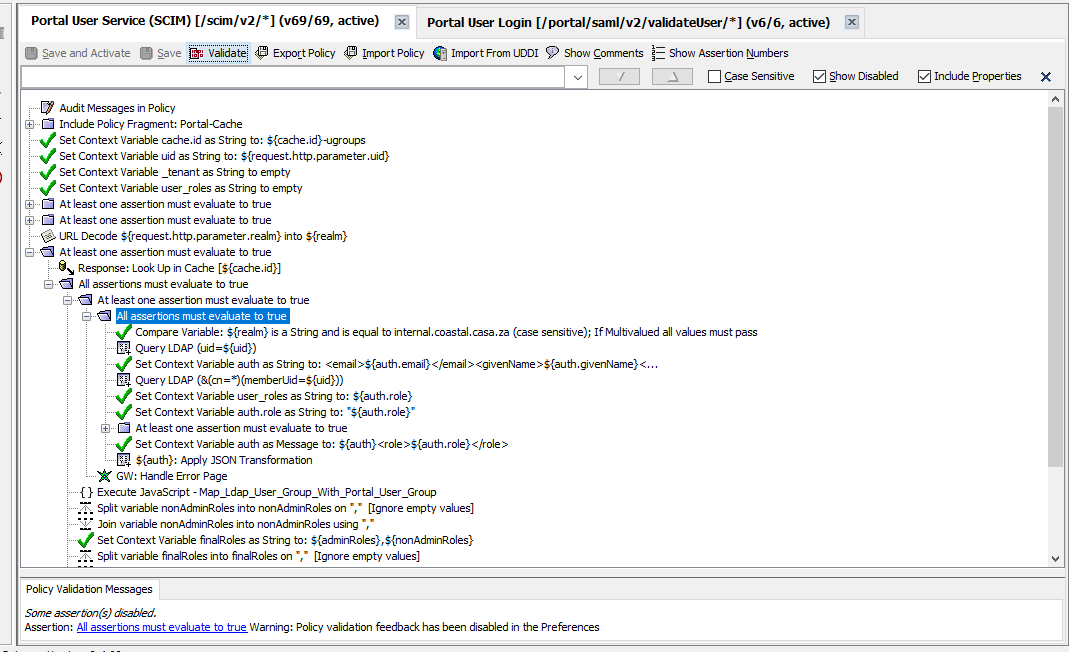
* cluster.hostname: Gateway Cluster hostname
* saml.domaincheck :- domain name (e.g. for api gateway as api.coastal.casa.za and portal as portal.coastal.casa.za) domain check parameter will be .coastal.casa.za
* saml.portal.tenant :- PORTAL tenant name e.g. portal
* saml.portal.tenantName:- PORTAL tenant user friendly name

### Option 1:-

#### GMU Import Scripts:- portal\_sso\_integration.zip

### Option 2:-

#### Create Policy and Folder Manually

* **Note**: The Guid are only if you are using restman to create folder structure
* Create Folders
  + Portal Single Sign On (Root) [guid: 9e2bda6f90670a0a14c18f2a51cf2af7]
    - Encapsulation [guid: 9e2bda6f90670a0a14c18f2a51cf2b3a]
    - Policy [guid: 9e2bda6f90670a0a14c18f2a51cf293f]
    - Service [guid: 9e2bda6f90670a0a14c18f2a51cf2b7b]
* Import Encapsulation
  + handle\_error\_encaps (Location portal\_sso\_integration\_manual\encapsulation\handle\_error\_encaps.xml)
  + search\_in\_array\_encaps (Location portal\_sso\_integration\_manual\encapsulation\ search\_in\_array\_encaps.xml)
* Create and Import Policy
  + Portal-Cache [guid: 9e2bda6f90670a0a14c18f2a51cf2912]
  + Import Policy: (Location portal\_sso\_integration\_manual\policy\portal-cache.xml)
* Create and Import Services
  + Service Folder: (Location portal\_sso\_integration\_manual\service\\*.xml)
  + Services
    - Name: Portal Single Sign On
      * GUID: 9e2bda6f90670a0a14c18f2a51cf28b9
      * Path: /portal/saml/v2/\*
      * Method: GET|POST
      * XML: portal\_sso.xml
    - Name: Portal User Login
      * GUID: 9e2bda6f90670a0a14c18f2a51cf305b
      * Path: /portal/saml/v2/validateUser/\*
      * Method:POST
      * XML: validateUser.xml
    - Name: Portal User Service (SCIM)
      * GUID: 9e2bda6f90670a0a14c18f2a51cf2bdf
      * Path: /scim/v2/\*
      * Method:GET
      * XML:scim.xml
* Create and Import LDAP Setting for validation and query
  + Update LDAP parameter in
    - Portal User Login Page
    - Portal User Service (SCIM) 

## LDAP Service

### Create Groups and Add user to the groups

#### General Group

* Api Owner 🡪 maps to Api Owner on Portal SSO Config
* Portal Administrator 🡪 maps to Portal Administrator on Portal SSO Config

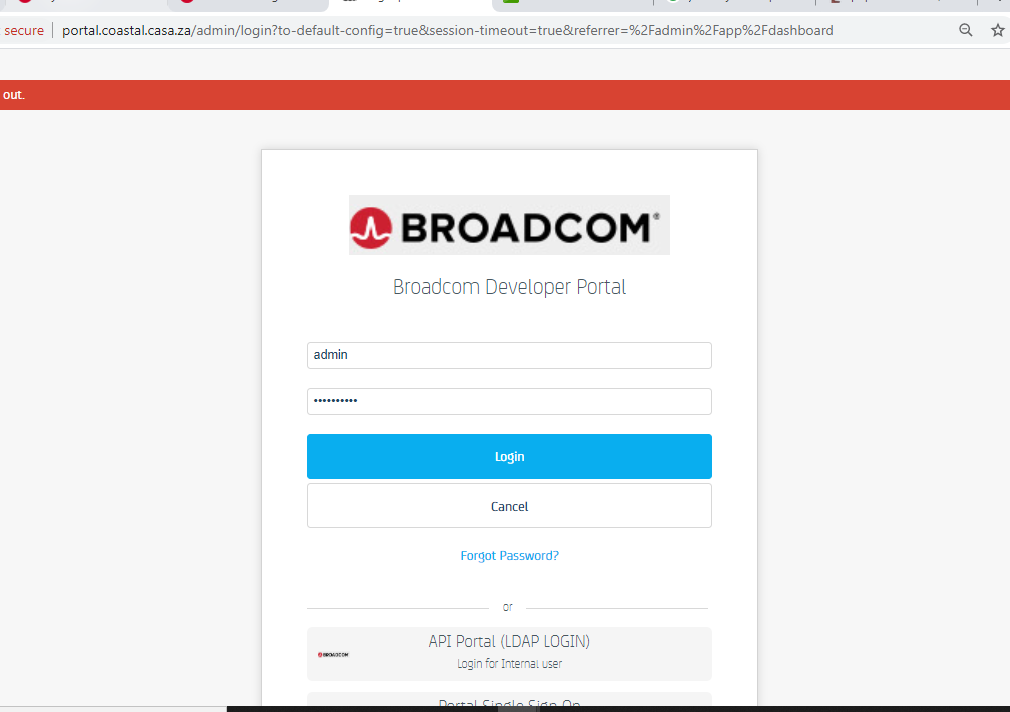
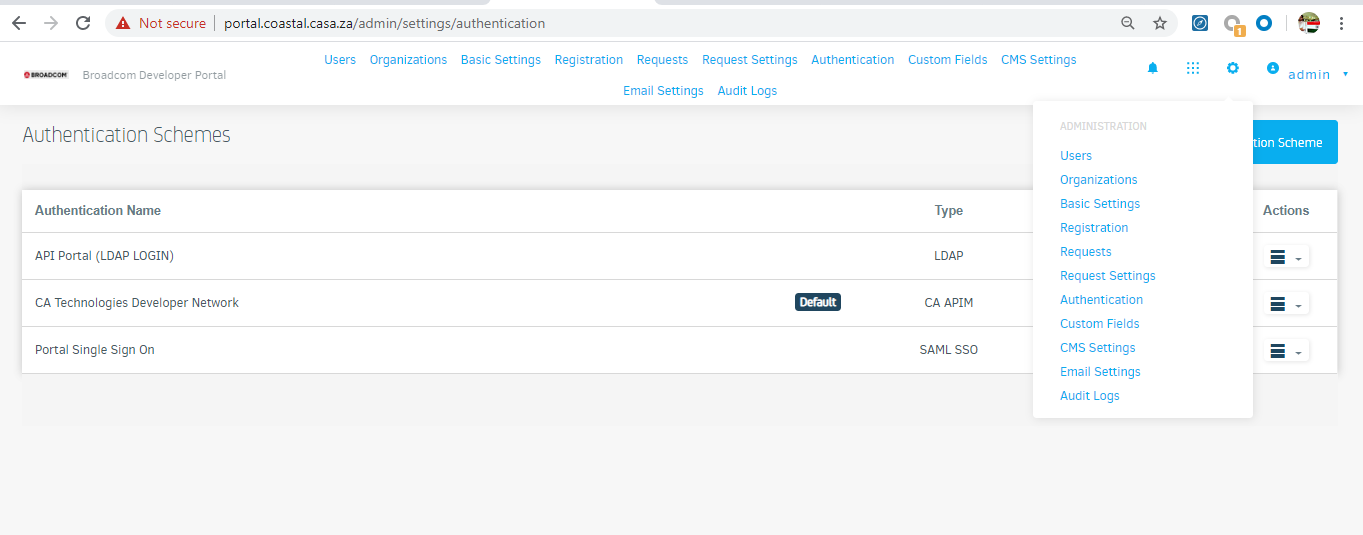
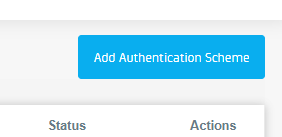
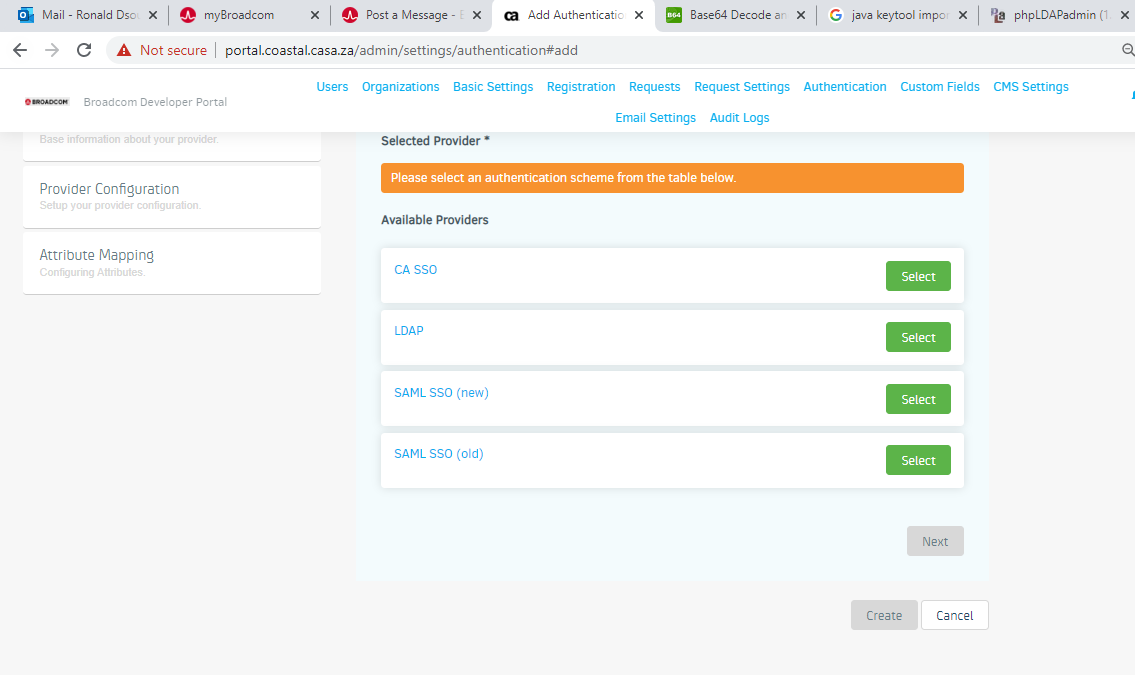
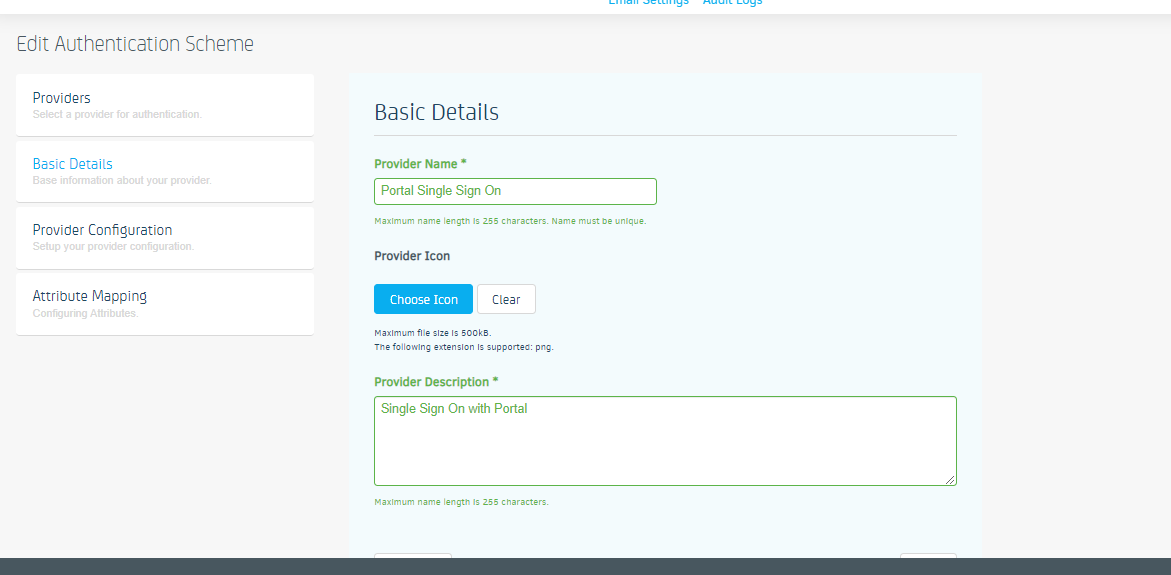
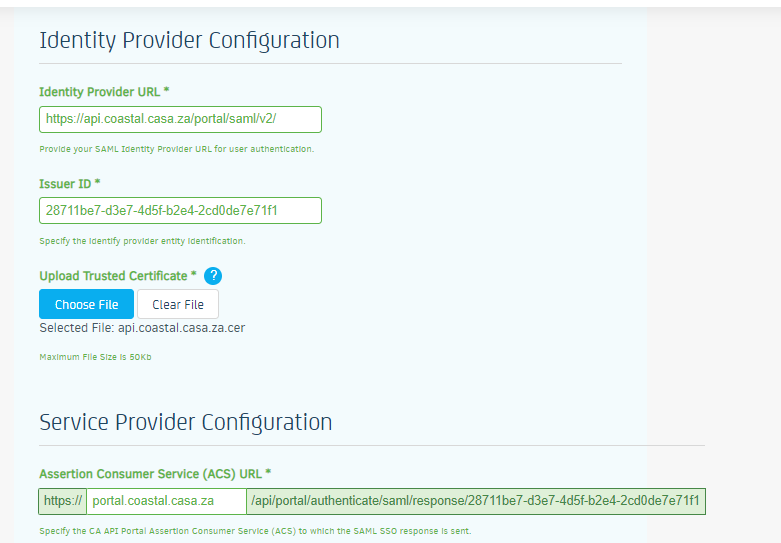
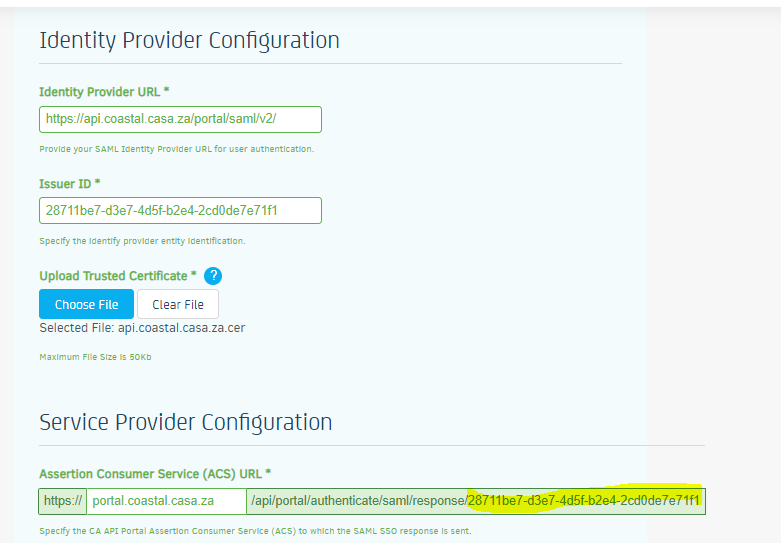
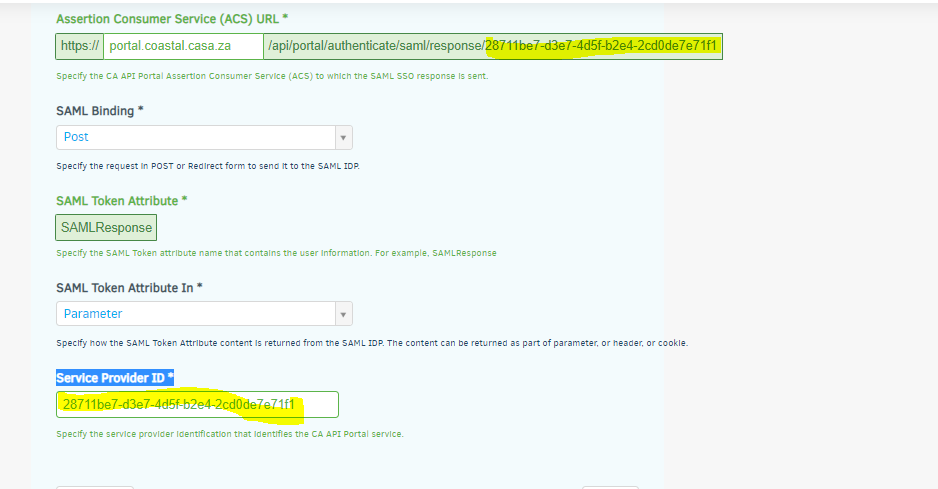
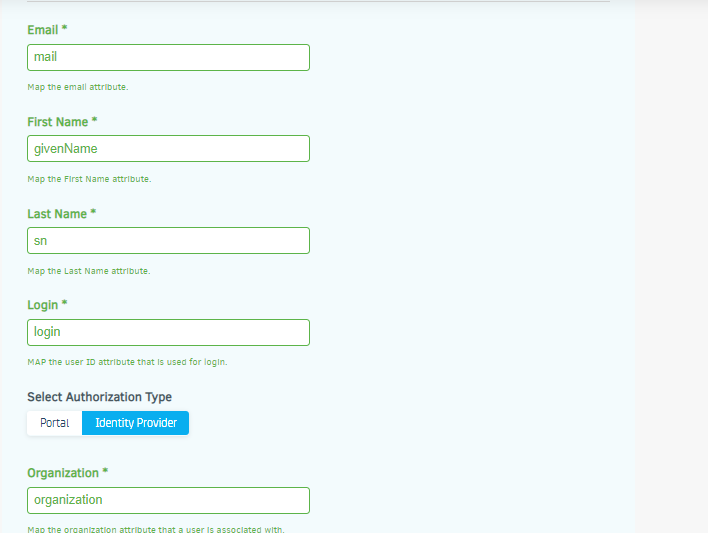
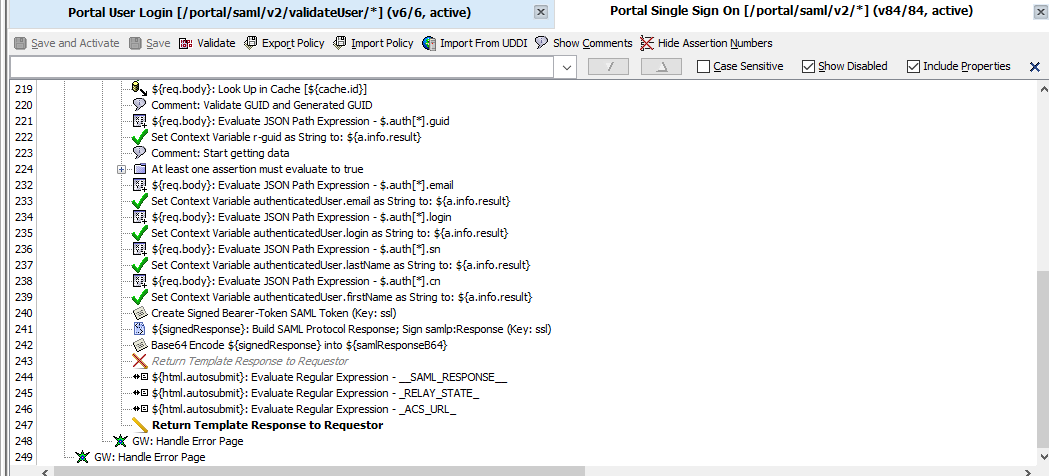
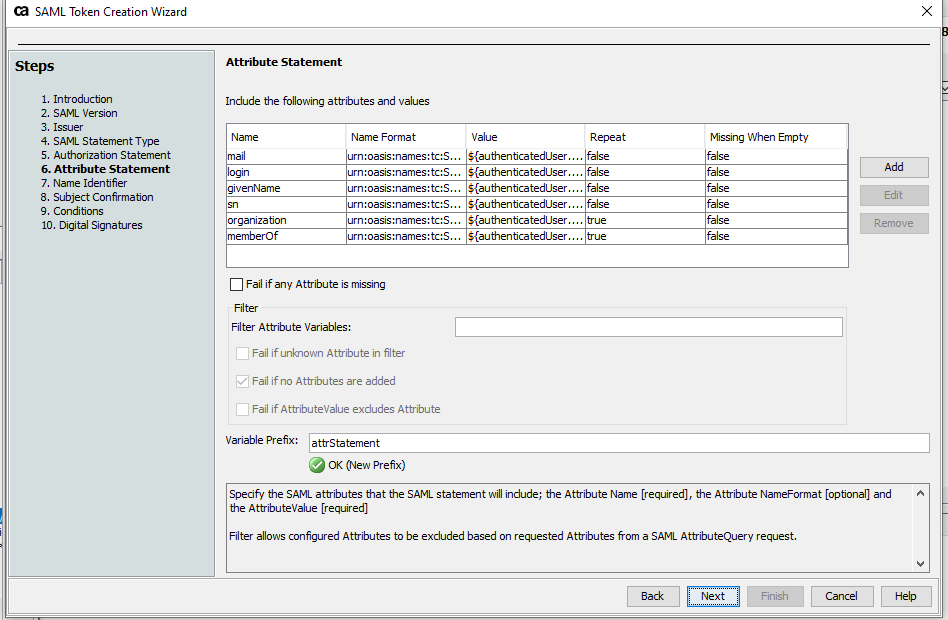
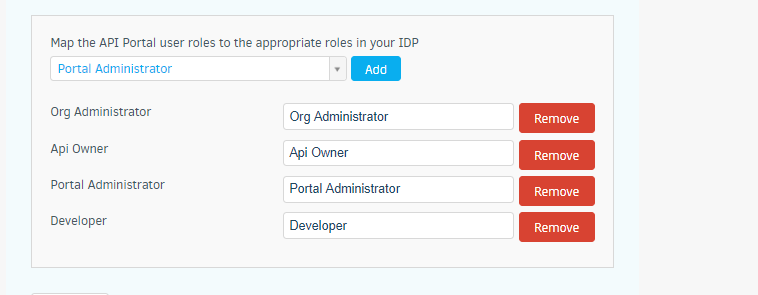
#### For each Organization create 2 groups

* E.g. If you have an organization on Portal as **Broadcom Internal**
* Create the following groups
  + **Developer#Broadcom Internal** 🡪 maps to *Developer* role on Portal to **Broadcom Internal** Organization
  + **Org Administrator#Broadcom Internal** 🡪 maps to *Org Administrator* role on Portal to **Broadcom Internal** Organization

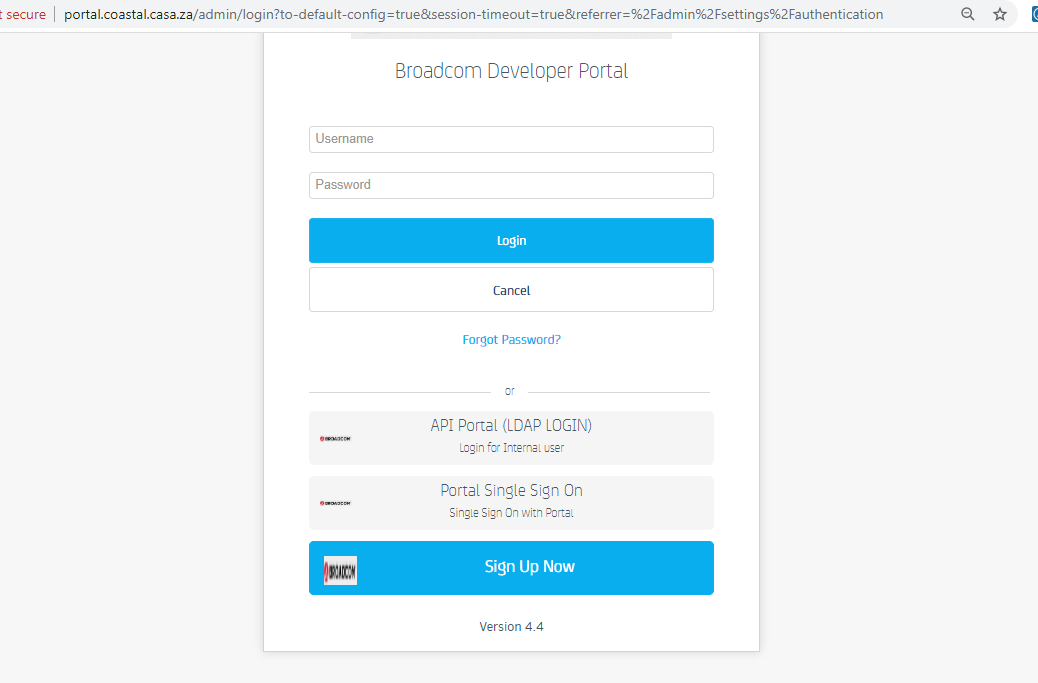
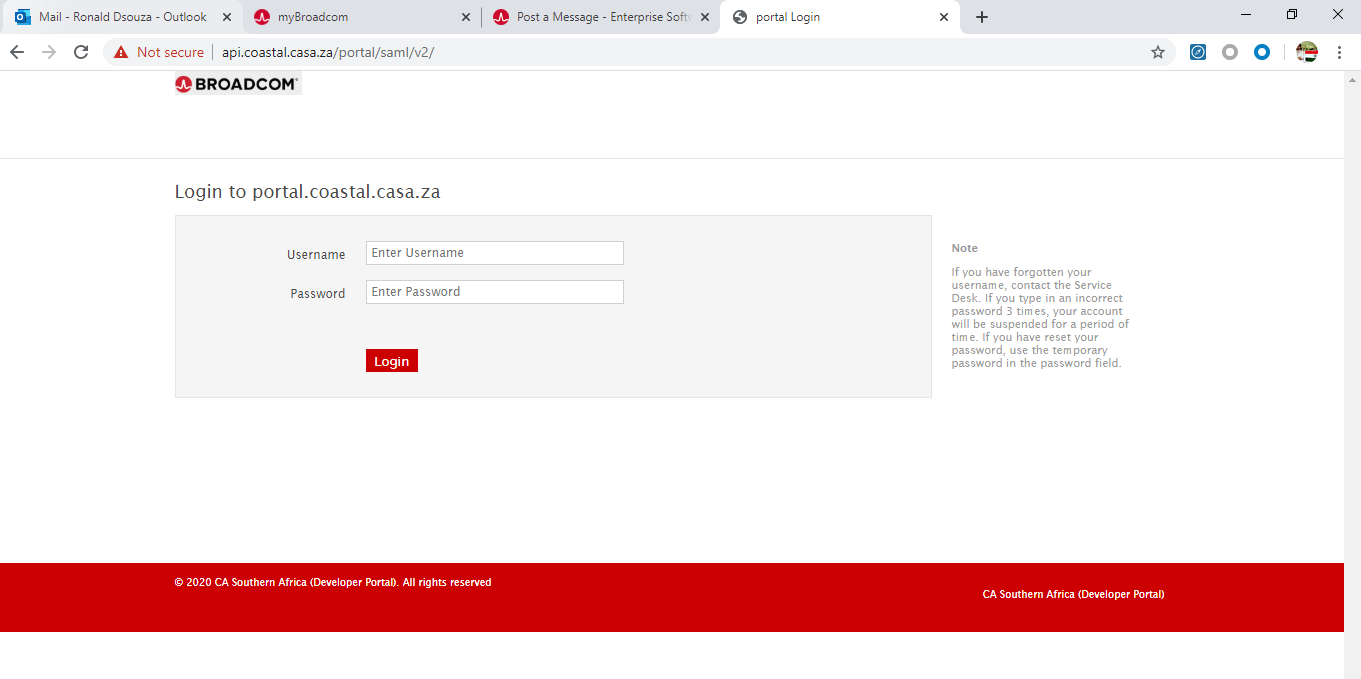
NOTE: The following role mapping and organization is case sensitive must map correctly in the Portal Authentication scheme else the user will not login as SAML

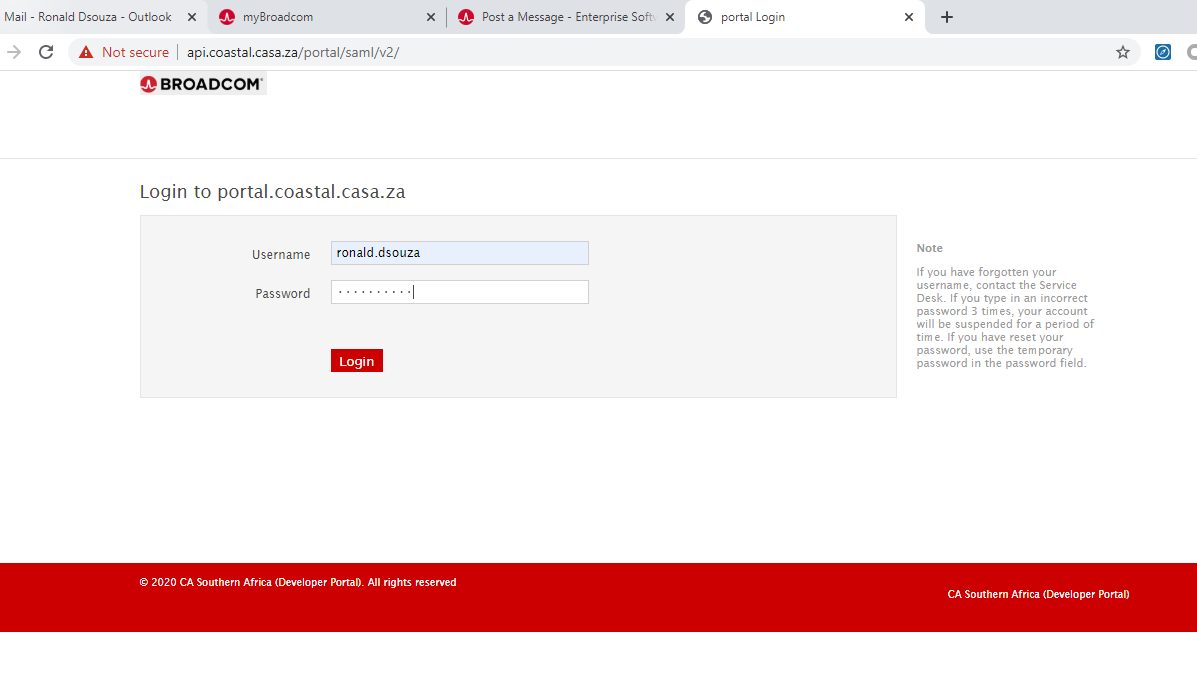
## On Portal

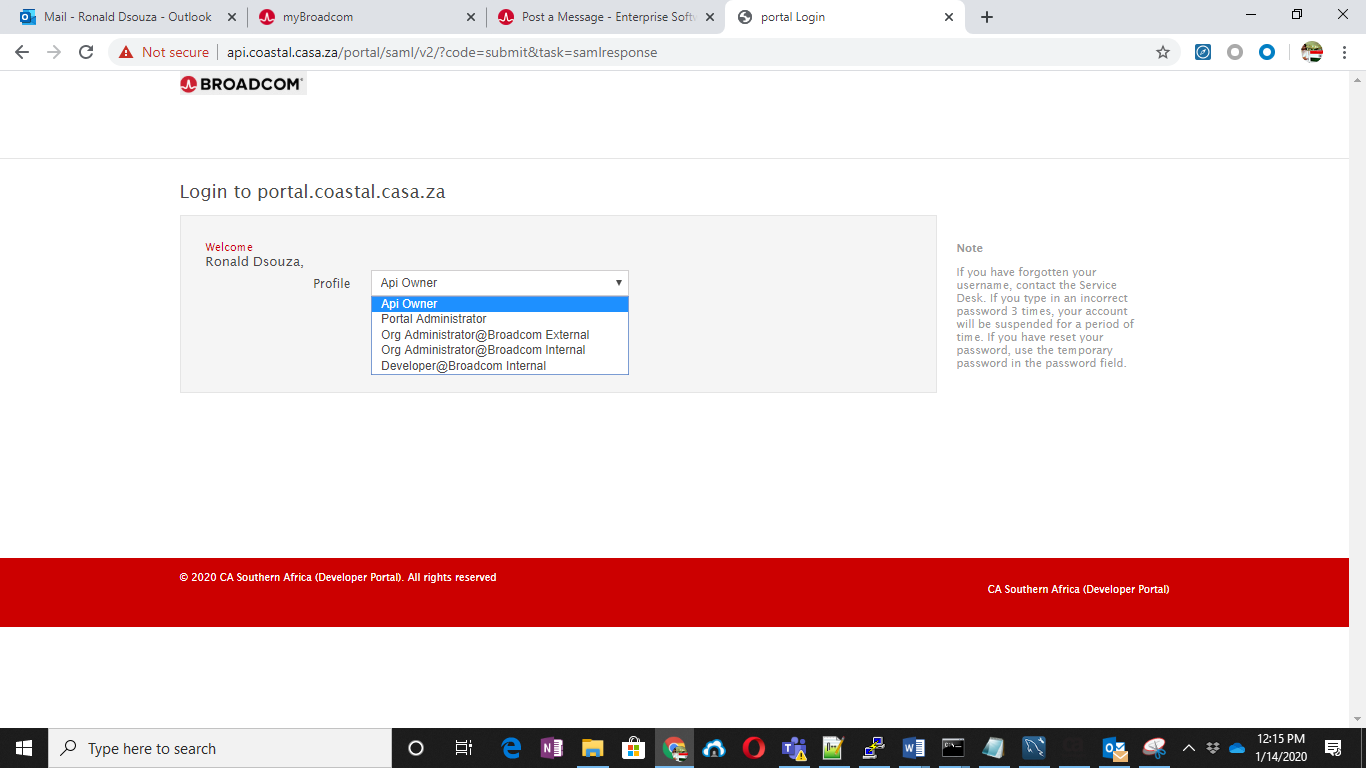
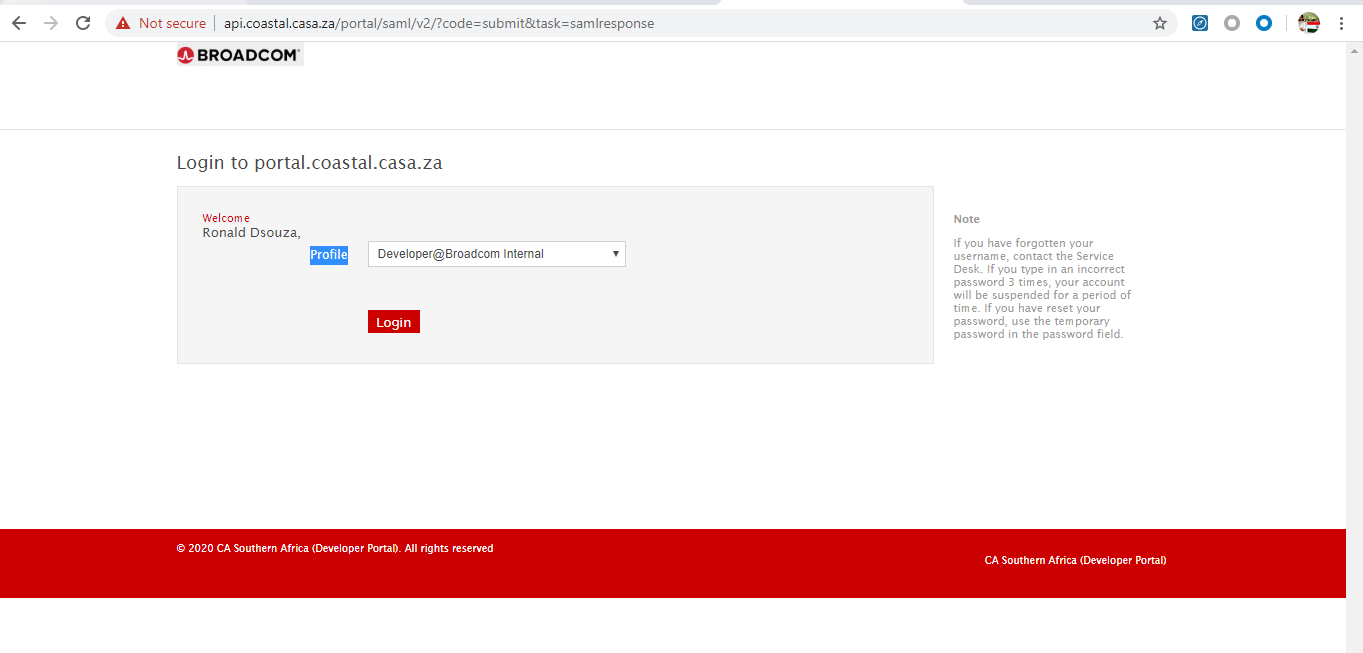
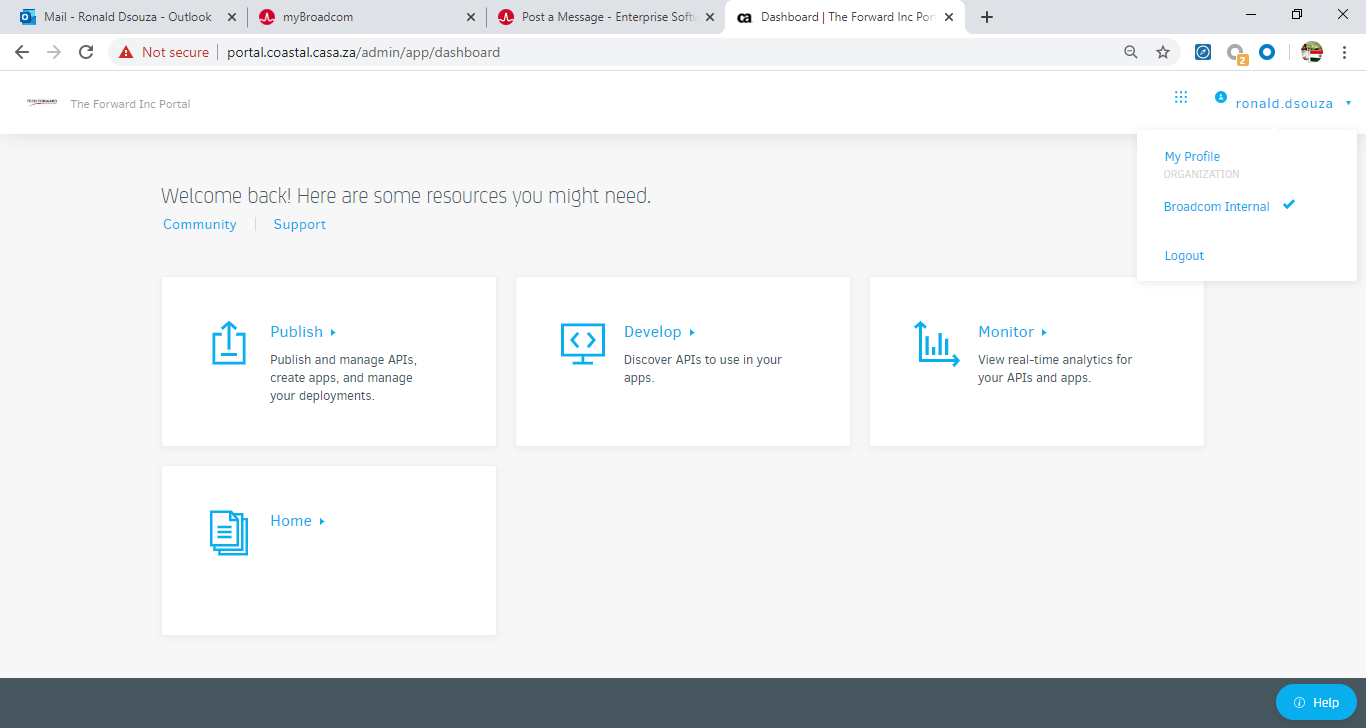
### Configure Auth Scheme

* Login as Portal Administrator 
* Navigate to Setting 🡪Administration🡪Authentication 
* Click on Add Authentication Scheme   
  
* Select SSO SAML (new) as the provider 
* Provide Basic Details as required 
* Provide Identity details
  + Identity Provider URL:
    - API Gateway URL for Portal Single Sign On Service
  + Issuer ID
    - Copy the Secton from ACS Url that hold the guid 
  + Upload Trusted Certificate
    - Copy Certificate from CA API Gateway URL
  + ACS url
    - No Change
  + Saml Bindings
    - Keep default POST
  + Saml Attribute token in
    - Keep default Parameter
  + Service Provider ID \*
    - Same as Issuer ID (guid) 
* Click Next
* Provide Attribute Mappings
  + Email 🡪 mail
  + First Name 🡪givenName
  + Last Name 🡪sn
  + Login 🡪login
  + Organization 🡪organization
  + Role 🡪 memberOf
  + **NOTE:** The attribute are from SAML Response if you want to change these value refer 242 of Portal Single Sign On Service (Create Signed Bearer Token SAML) and update the name value pair as required 
* Update the setting for Portal Role – SAML ROLE mapping as below 
  + **Note:** This value can be updated in SCIM policy under Javascript assertion on Gateway
* Save the settings

# Test Setup:-

* On Portal login page Select 🡪 Auth Scheme for Portal Login e.g. Portal Signle Sign On
* You will be redirected to API Gateway page for SAML login 
* Enter your username and password



* Click on Login
* Based on your groups assignment on ldap you will get a drop down with ROLE#Organization Mapping 
  + Here I have access as Org Administrator role for Broadcom External and Broadcom Internal and Developer role for Broadcom Internal
  + In real world you will belong to different organization with different roles all will be listed down here
  + Select the profile   
    
  + Click Login
  + Based on your profile selection you are logged in as 
  + Broadcom Internal as Developer