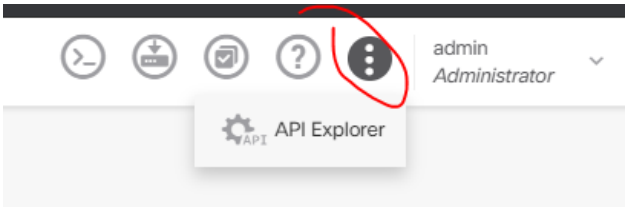
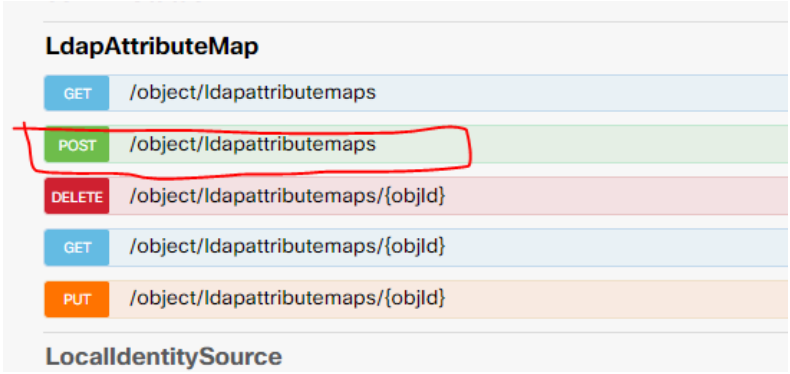
LDAP attribute mapping FDM Rest API

1. Gather required AD group membership values and group policy names.
2. Create a NoAccess group-policy on the FDM that specifies 1 simultaneous login in the “Session Settings” of the group policy and assign it to the connection profile.
3. Go to the Rest API on the FDM by clicking the three dots on the top left of the screen.



And clicking on API Explorer

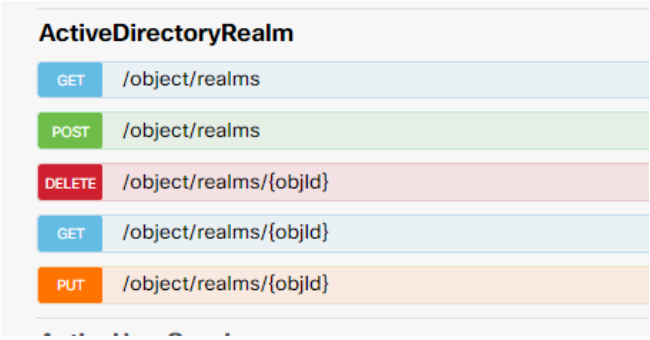
4. Create the attribute mapping by going to the LdapAttributeMap section and click on POST



5. Use the following format to map the group policy names and AD memberOf values.

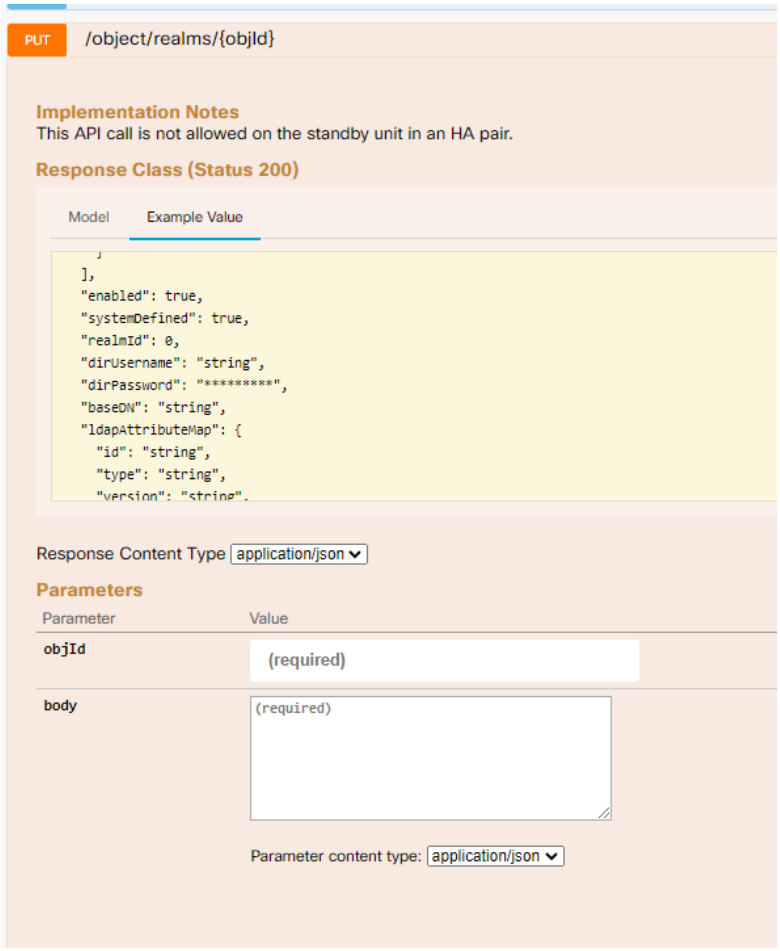
```
"name": "Map2",
"ldapAttributeMaps": [
  {
    "ldapName": "memberOf",
    "ciscoName": "GROUP_POLICY",
    "valueMappings": [
      {
        "ldapValue": "\"AnyConnect Admins,CN=Users,DC=test,DC=com\"",
        "ciscoValue": "NOACCESS",
        "type": "ldaptociscovaluemapping"
      },
      {
        "ldapValue": "CN=Admin,CN=Users,DC=test,DC=com",
        "ciscoValue": "NOACCESS2",
        "type": "ldaptociscovaluemapping"
      }
    ],
    "type": "ldapattributemapping"
  }
```

6. Next use the POST command to add the attribute map configuration to the device.
7. Next get the current AD realm configuration from the GET command in the ActiveDirectoryRealm section:



8. Add the following information from the attribute map configuration to the attribute map section of the AD realm.
    a. Version
    b. Name
    c. ID
    d. “type”: “ldapattributemap”

9. Use the PUT command to add the attribute map config to the AD realm using the objectID of the particular AD realm you are adding the mapping to.



10. After this Deploy the changes and test using a username from each required AD group, including one that should not be able to log in.
11. Log into the CLI and use the command: “show vpn-sessiondb anyconnect filter name <username>” to test. This will show the connection profile used to connect and the group-policy assigned when the user logs in.
12. When everything is working correctly, modify the NoAccess group policy to all 0 simultaneous logins, this will prevent unauthorized users from being able to connect.
13. At this point no one but those in groups specified in the LDAP attribute mapping should be able to connect with AnyConnect and all you need is one connection profile that specifies the NoAccess policy as the default group policy.