* 1. Copernicus supports tight integration and automatic user creation so once AD is configured and Groups are imported if user login in with AD credential user will be automatically created  in system and assign group policy.
  2. Access policy ( surfing quota , access time , Network Traffic etc ) are applicable on group/user property
  3. Web filter and Application filter policy are applicable on User Policy rules , so admin need to create user based security policy rule for all groups/users sharing same web filter and application filter.
  4. When user will be part of multiple group below is example  how group policy is applied.
     1. Access Policy ( User/Group Specific Policy) : When Multiple Group are configured for user in AD , user access policy will get primary group policy . Admin can check user group member to check the same
     2. Web and Application policy : All the member group will be will match against Security Policy

|  |  |  |  |
| --- | --- | --- | --- |
| Username | Primary Group | Secondary Group 1 | Secondary Group 2 |
| John | QA | R&D | General access |
| Alice | HR | Management | General access |
| Bob | Training | General access |  |

* + 1. In the above example user John, Alice and Bob will get their access policy of their respective primary group ( QA,HR & Training )
    2. But in Security policy if rule is configured in below order

|  |  |  |
| --- | --- | --- |
| Identity | Web Filter | Application Filter |
| Management | Allow All | Allow all |
| R&D | R&Dweb filter | General Corporate Policy |
| Any | General Corporate Policy | General Corporate Policy |

User John will get access of R&Dweb filter policy as it got access of R&D group also where in Alice will get Allow All as it is part of Management group also.