GROUP LOCK on ACS 5.x using an ASA or Concentrator

ASA configuration

Step 1: On the CLI configuration or either on the ASDM you will have your tunnel groups which correspond to the connection profile used by the specific users.

Each specific tunnel group will have a group policy assign. In order for the group-lock to work properly every tunnel-group will have to be configured with a different group-policy. The group policies are highlighted in red for your reference.

```
tunnel-group VPNusers type remote-access
tunnel-group VPNusers general-attributes
        address-pool VPNPOOL
        authentication-server-group RADIUS
        default-group-policy VPNpolicy
tunnel-group VPNusers ipsec-attributes
        pre-shared-key *****

tunnel-group IT type remote-access
tunnel-group IT general-attributes
        address-pool VPNPOOL
        authentication-server-group RADIUS
        default-group-policy IT
tunnel-group IT ipsec-attributes
        pre-shared-key *****
```

Every tunnel group will need to have a group policy configure. Group policies are configured below.

Step 2: Under the group policies configuration you will need to apply the group-lock value with the specific tunnel-group that should be getting assign. Here is a summary of the configuration

group-policy VPNpolicy internal

group-policy VPNpolicy attributes

vpn-simultaneous-logins 3

vpn-tunnel-protocol IPSec svc

group-lock value VPNusers

group-policy ITpolicy internal

group-policy ITpolicy attributes

vpn-simultaneous-logins 3

vpn-tunnel-protocol IPSec svc

group-lock value IT

Step 3: On your Radius server you will have to assign your users or group with the specific group policy value under the attribute 25 (class).

For example if you have the following users:

a) User1 → this user should connect only to connection profile IT

Then on this user on your Radius server you will need to assign on the attribute 25 the value of the group policy: OU=ITpolicy;

b) User2 →this user should connect only to connection profile VPNusers

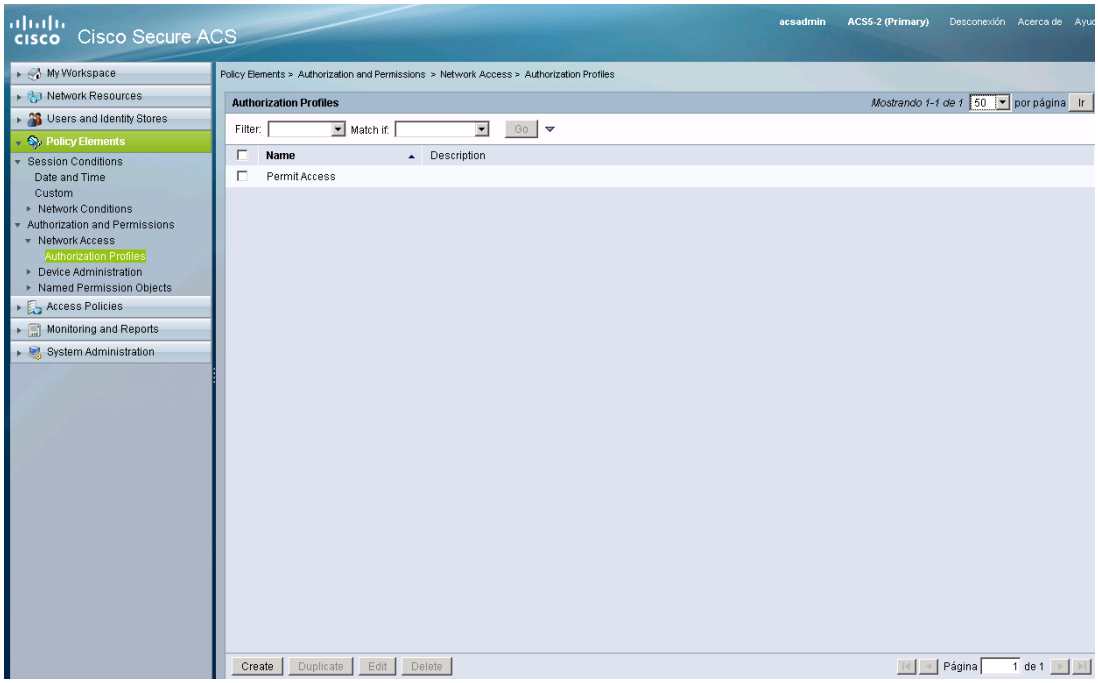
Then on these users on your Radius server you will need to assign on the attribute 25 the value of the group policy: OU=VPNpolicy;

As a summary each user on the Radius server need to point based on the attribute 25 to the specific group policy of the connection profile.

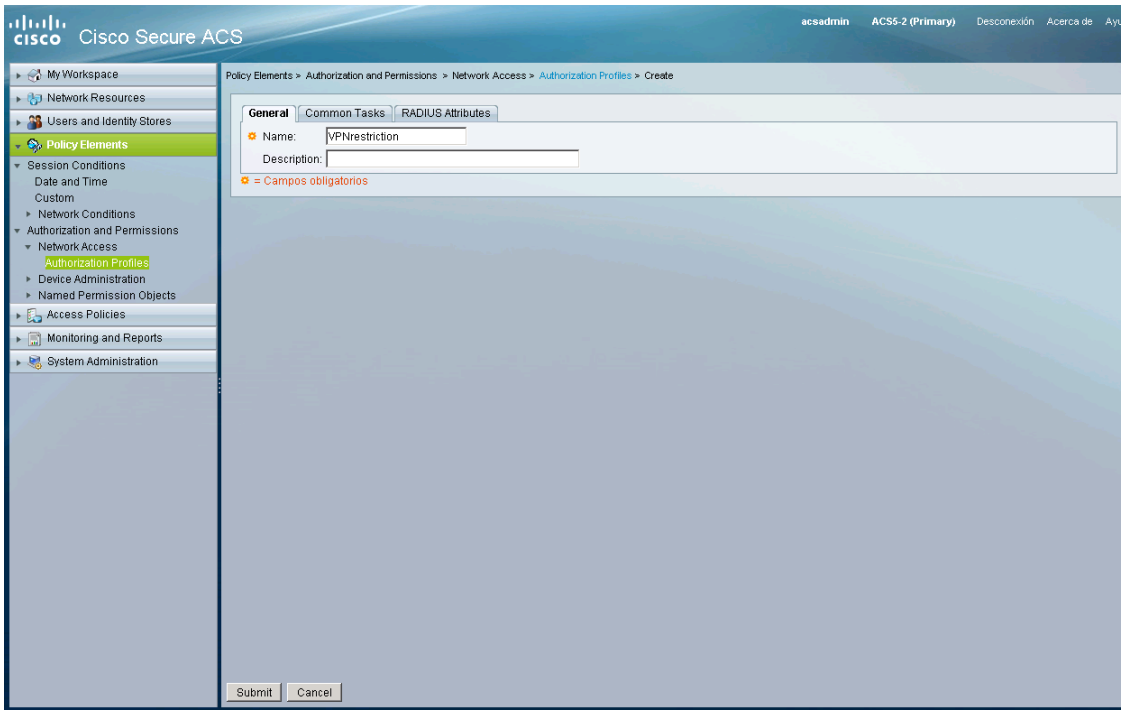
Each group policy assign need to contain the group-lock feature configure with the name of the connection profile (tunnel group) that the user is allow to used.

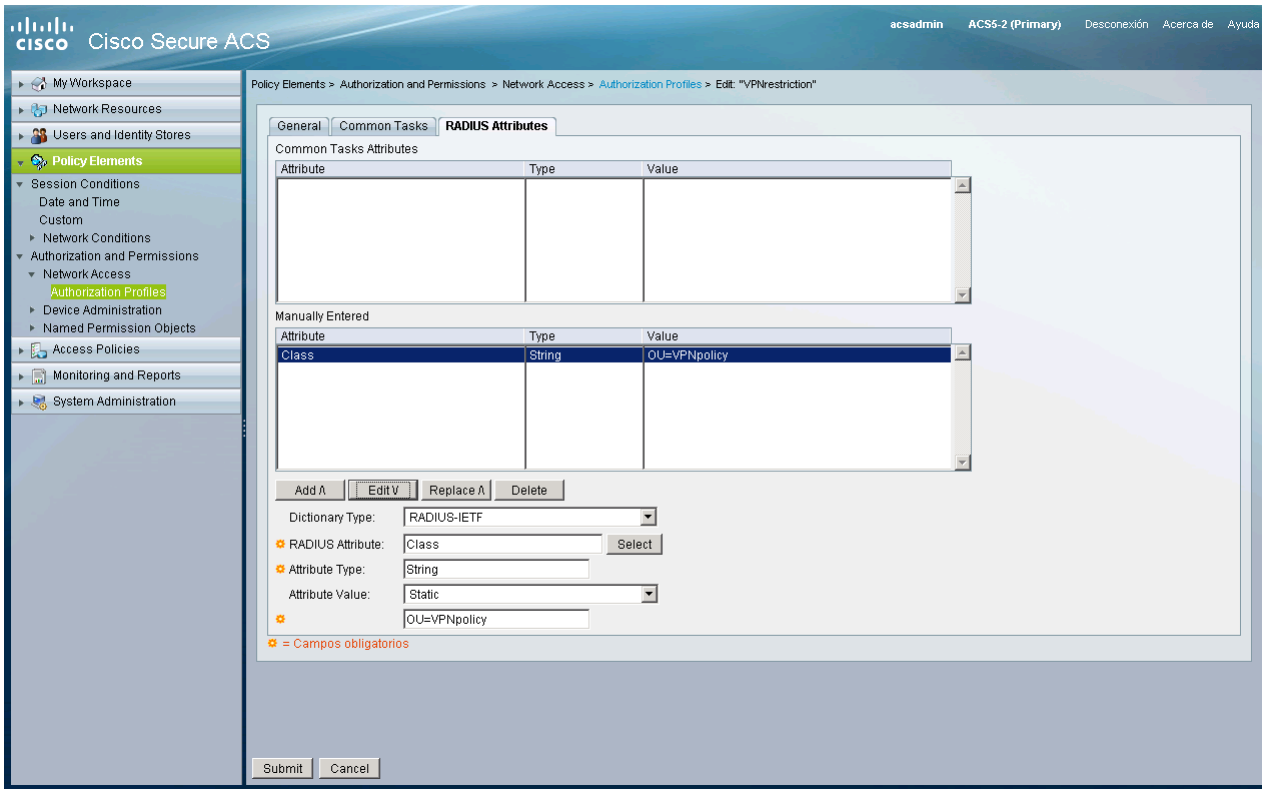
ACS 5.x configuration for group lock

Step 1: Configure the authorization profile on ACS 5.x under the Network access section.



Step 2: Click on Create and defined the Name of the profile and then go into the Radius attributes section to define the Class attribute

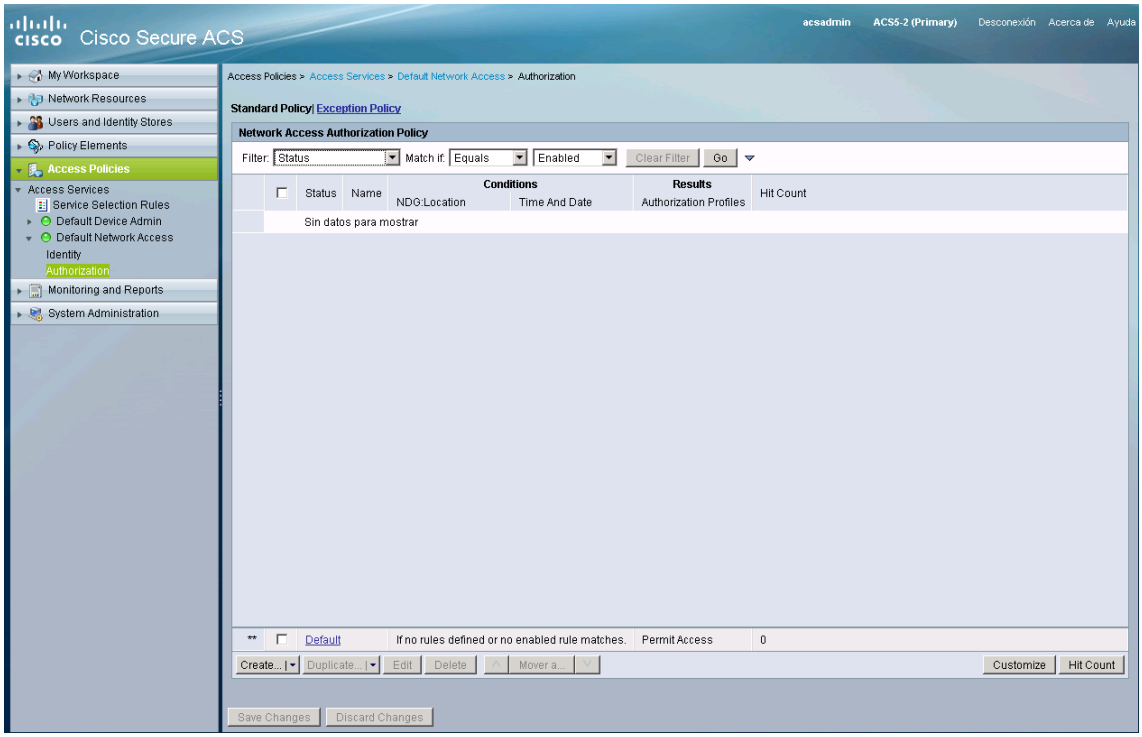




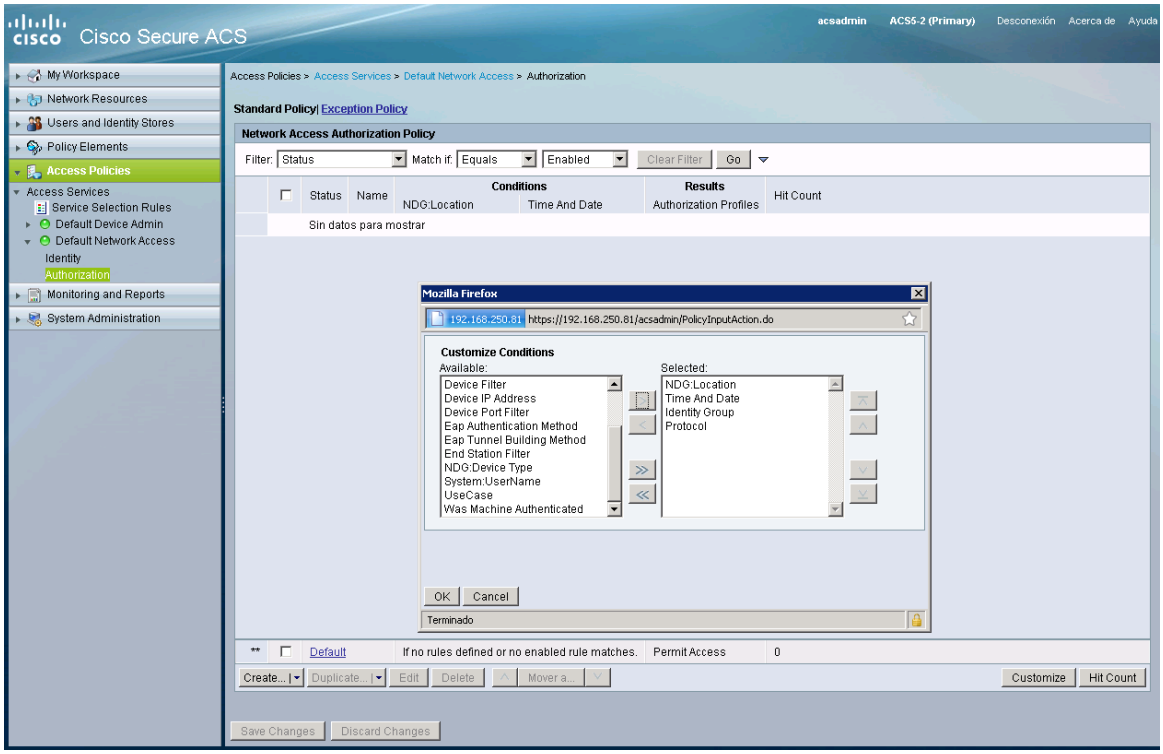
If an ASA is being used as VPN server for VPN client connectivity, then the **OU** value for the **attribute 25** needs to point to the specific **group-policy** that wants to be assign to the user or group on ACS.

If a concentrator is being used instead then the OU value needs to match with the **VPN group** configured and it is important to make sure that the names is matching exactly the same since it is case-sensitive.

Step 3: Then go into the **Access Policy /Default Network Access** or **specific access service** that was created for the VPN authentication and go into the **Authorization section**



Step 4: Customize the rules on the condition depending of your requirements in case that you want to apply the OU based on a group or based on any other criteria available. **On this example I will be using a local group from the ACS** but you can use this based on Device IP or even external servers like AD.



Step 5: Create the new condition and defined the criteria you required and provide as a result the specific authorization profile that was created on Step 2.