Configure Cisco Firepower and Cisco ISE for AnyConnect VPN Authentication and Dynamic Group Policy Mapping

Device Versions in this document:

1. Cisco ISE – Version 2.4 Patch 11
2. Cisco FMC – Version 6.5.0.4
3. Cisco FTD – Version 6.5.0.4

In this article we will see how to configure Cisco Firepower using Firepower Management Centre (FMC) and Cisco ISE for AnyConnect VPN authentication and authorisation using dynamic Group Policy mapping from ISE. For example, you have different rules and ACL for Employees, Vendors, etc, you can create different Group Policy with all these rules and based on used connecting via AnyConnect, you can dynamically assign Group Policy from ISE. If vendor user connects, he will be allocated Vendor VPN Group Policy, hence restricting with Vendor ACL and other rules.

Cisco ISE is a AAA server supporting RADIUS (as default) and TACACS+ protocol for Authentication Authorization and Accounting. We can use ISE with Firepower to authenticate VPN clients and apply specific VPN group policy based on centralised directory like MS Active Directory (AD).

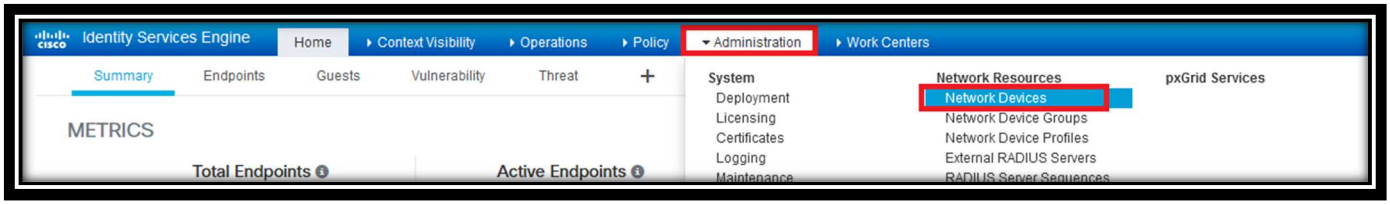
Steps Overview:

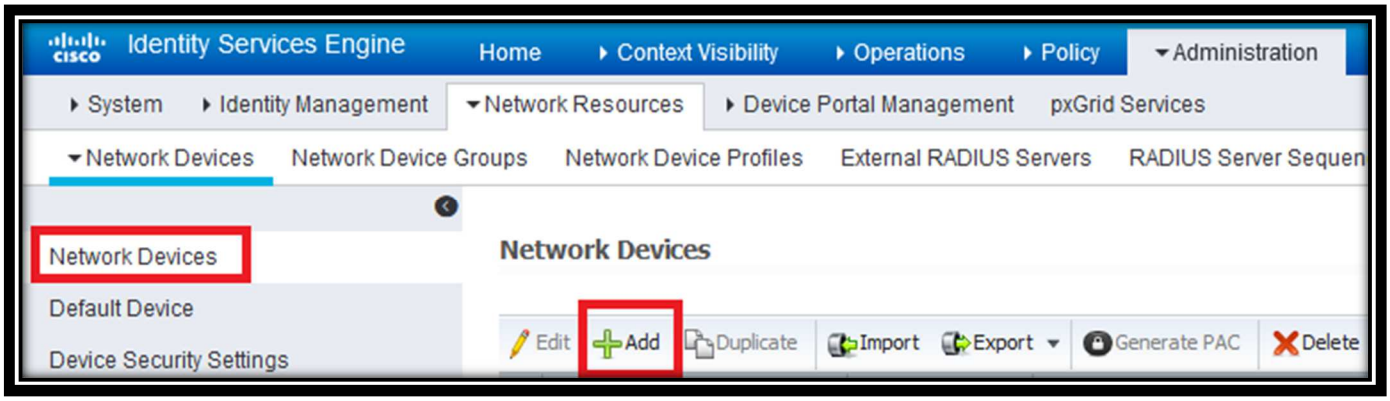
1. Connect Cisco ISE with Cisco FTD and FMC and configure Cisco FTD VPN Policy via FMC to authenticate and authorise thru Cisco ISE
2. Configure Cisco ISE parameters for VPN Authentication
3. Configure Cisco ISE parameters for Dynamic Authorisation – Authorisation Policy
4. Configure different Cisco ISE policy for each VPN user category (e.g. Vendor, Employee, etc)
5. Testing and verification of the policy

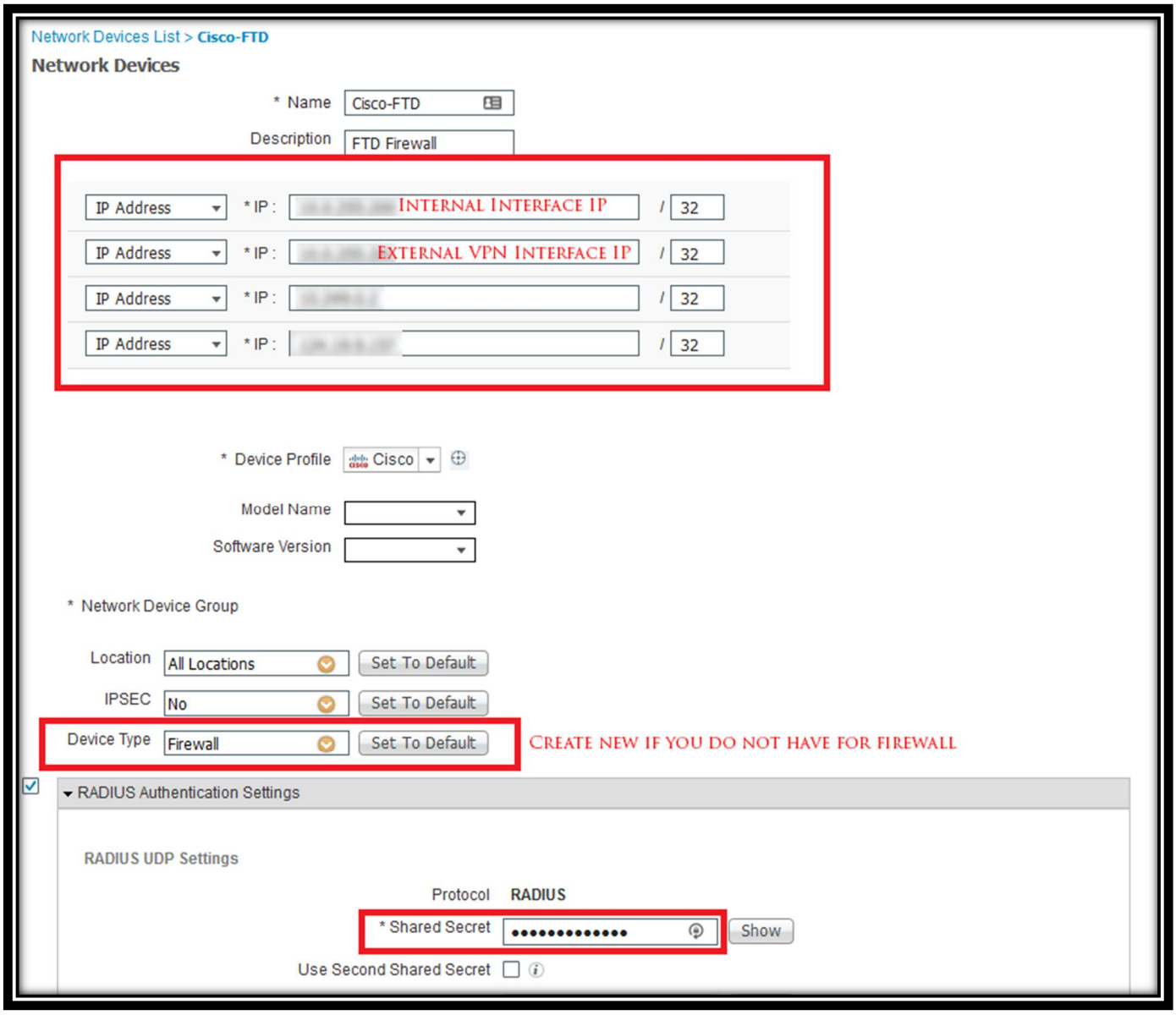
Step 1 – Connect Cisco ISE with Cisco FTD and FMC and configure Cisco FTD VPN Policy via FMC to authenticate and authorise thru Cisco ISE

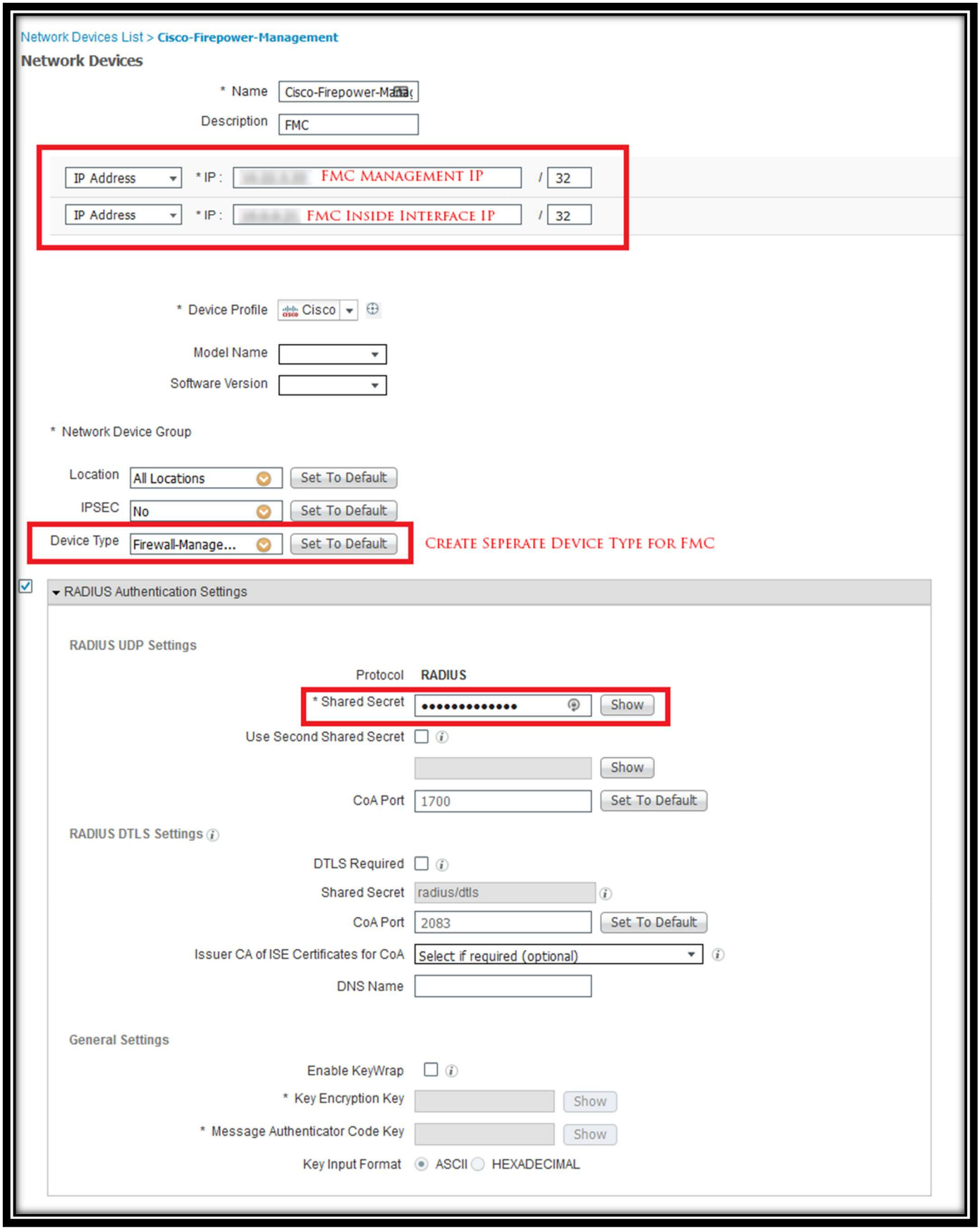
In this phase, we will configure Cisco ISE to allow AAA requests from Cisco FTD and FMC. When a VPN user connects, FTD will be sending request to ISE. Adding FMC is optional, but can be used for FMC GUI/CLI login authentication via ISE using centralised directory. You can skip this step, if FTD and FMC is already added to ISE. Also, we will configure VPN Policy to user ISE for Authentication, Authorisation and Accounting via FMC.

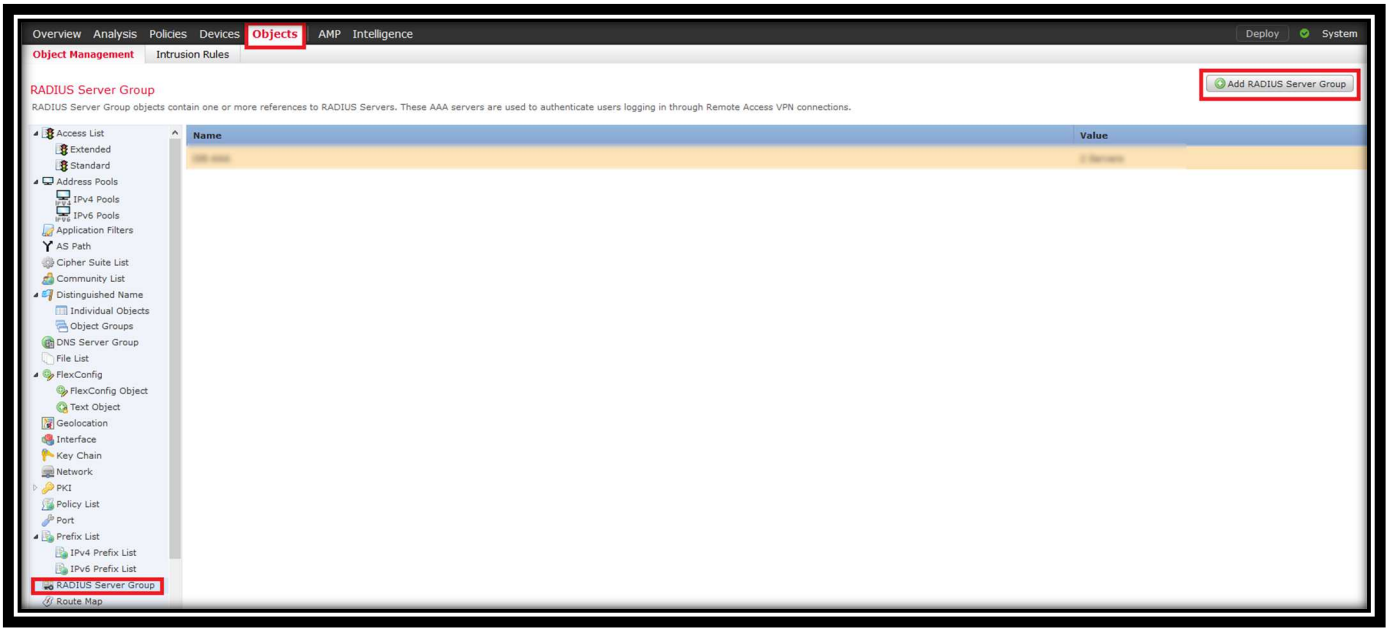
1. Login to **Cisco ISE**
2. Navigate to **Administration → Network Resources → Network Devices**
3. Click **Add**, and configure the below parameters:
    a. Name and Description – ***As you like***
    b. IP address – Configure FTD inside, and outside interface (VPN Interface) IPs. If VPN connects to a different interface, please include that interface IP as well. Because FTD will send request to ISE from interface where VPN is connected.
    c. Configure Device type, recommended to add new, so that it doesn't disturb any of your existing settings.
    d. Configure Shared Key, this key will be later used with FTD/FMC configuration of Cisco ISE in FMC
4. Follow the same above steps to add FMC.
5. Login to **Cisco Firepower Management Centre (FMC)**
6. Navigate to **Objects → RADIUS Server Group → Add New**
7. Configure the name, description and add all you **PSN ISE IP addresses**
8. Save the configuration
9. Navigate to **Device → VPN → Remote Access**
10. Open your **remote access policy**
11. Edit your **VPN policy**
12. Navigate to **AAA tab**
13. Select **ISE-AAA (RADIUS)** under your Authentication, Authorisation and Accounting Server
14. **Save** the setting and **Deploy** the Change

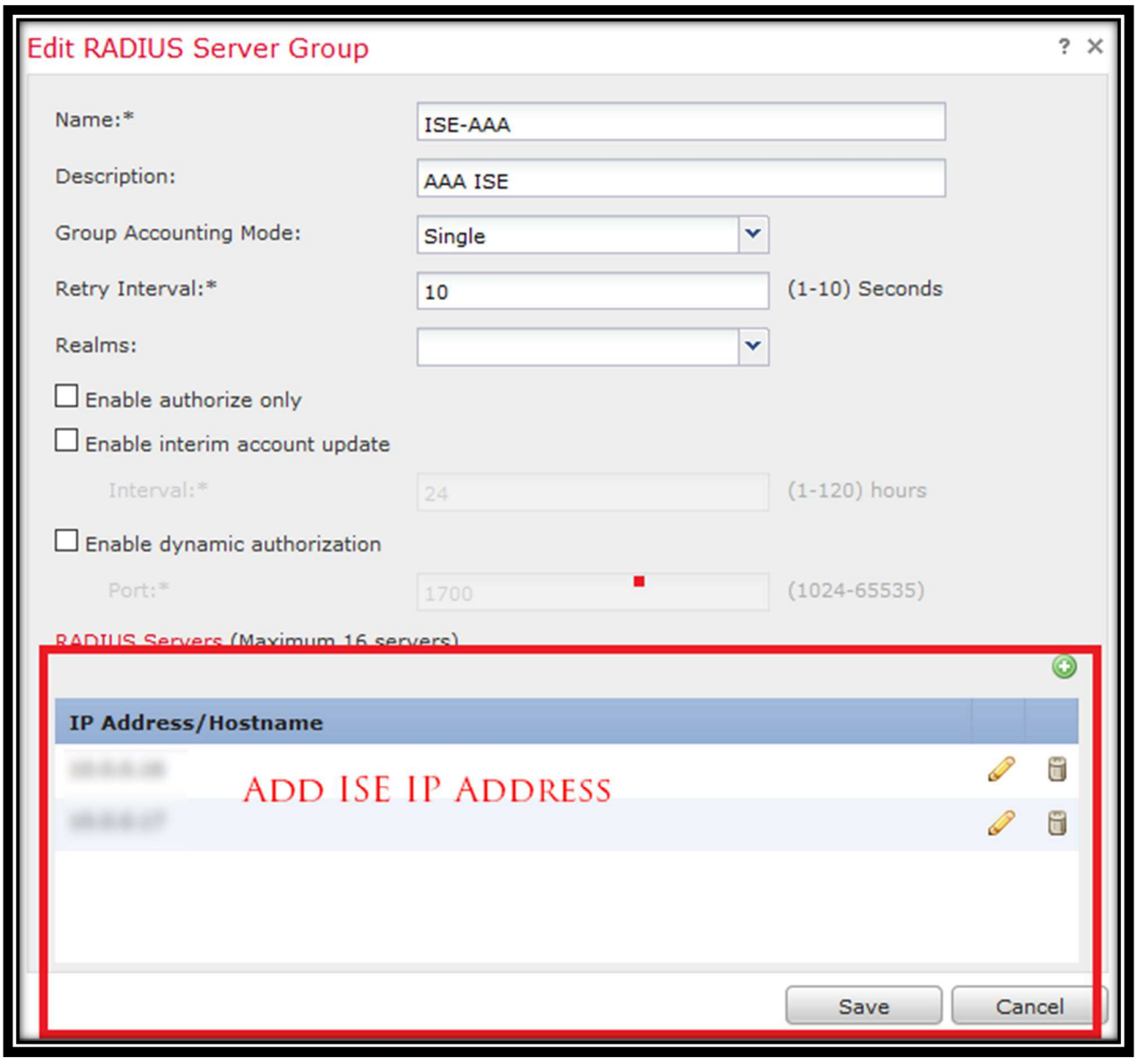


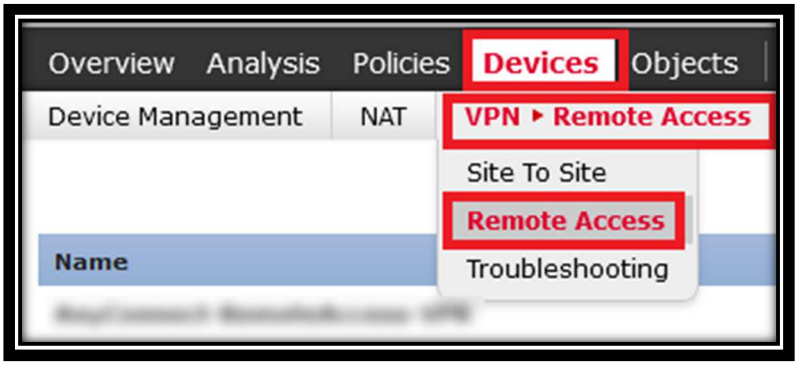


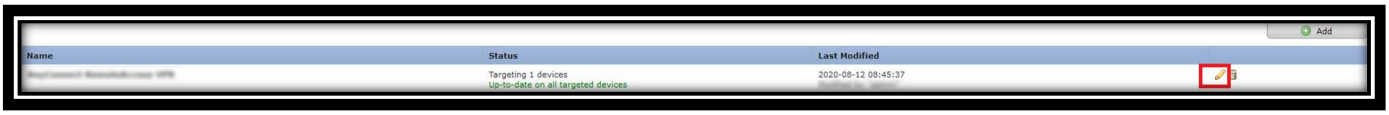


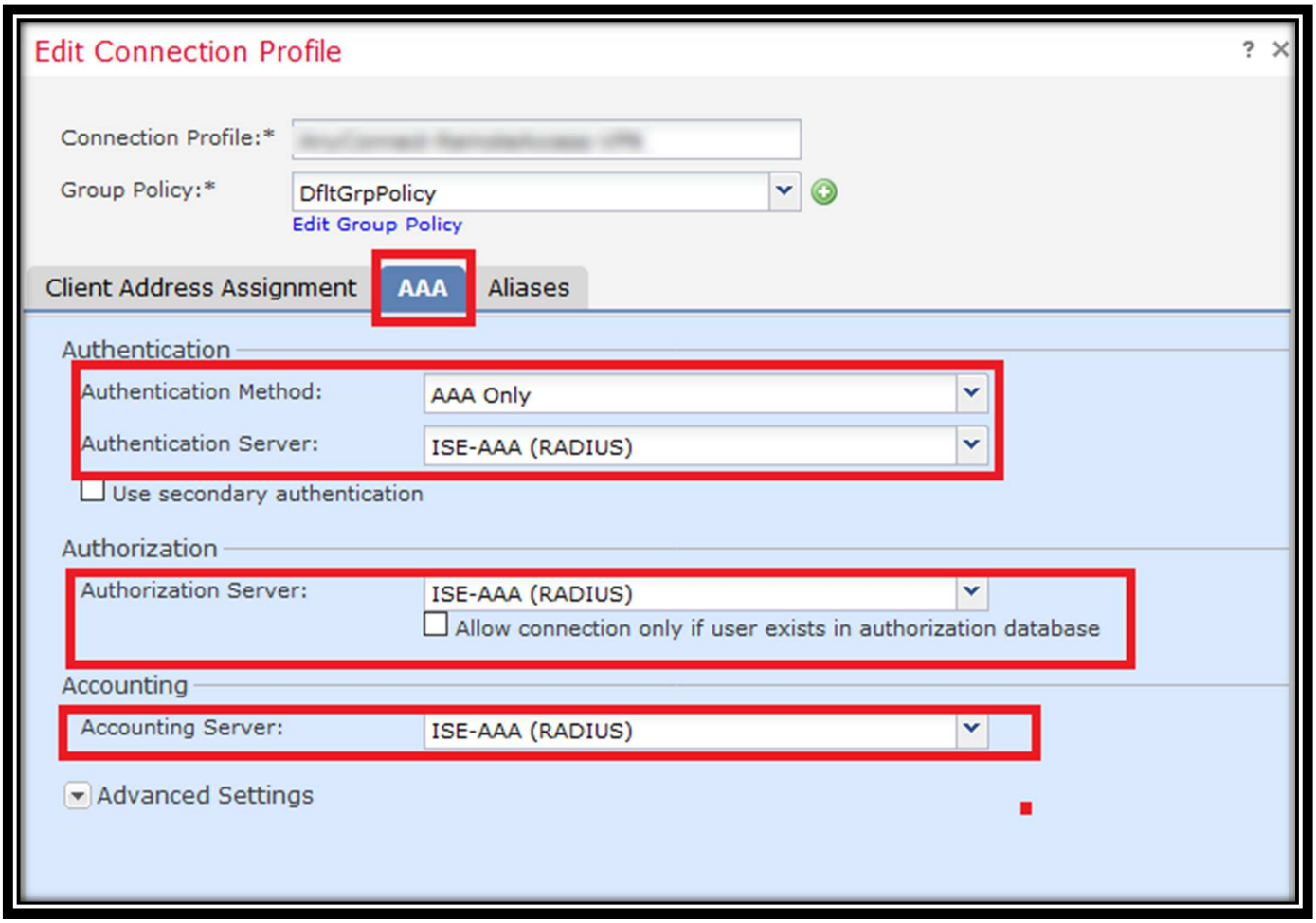












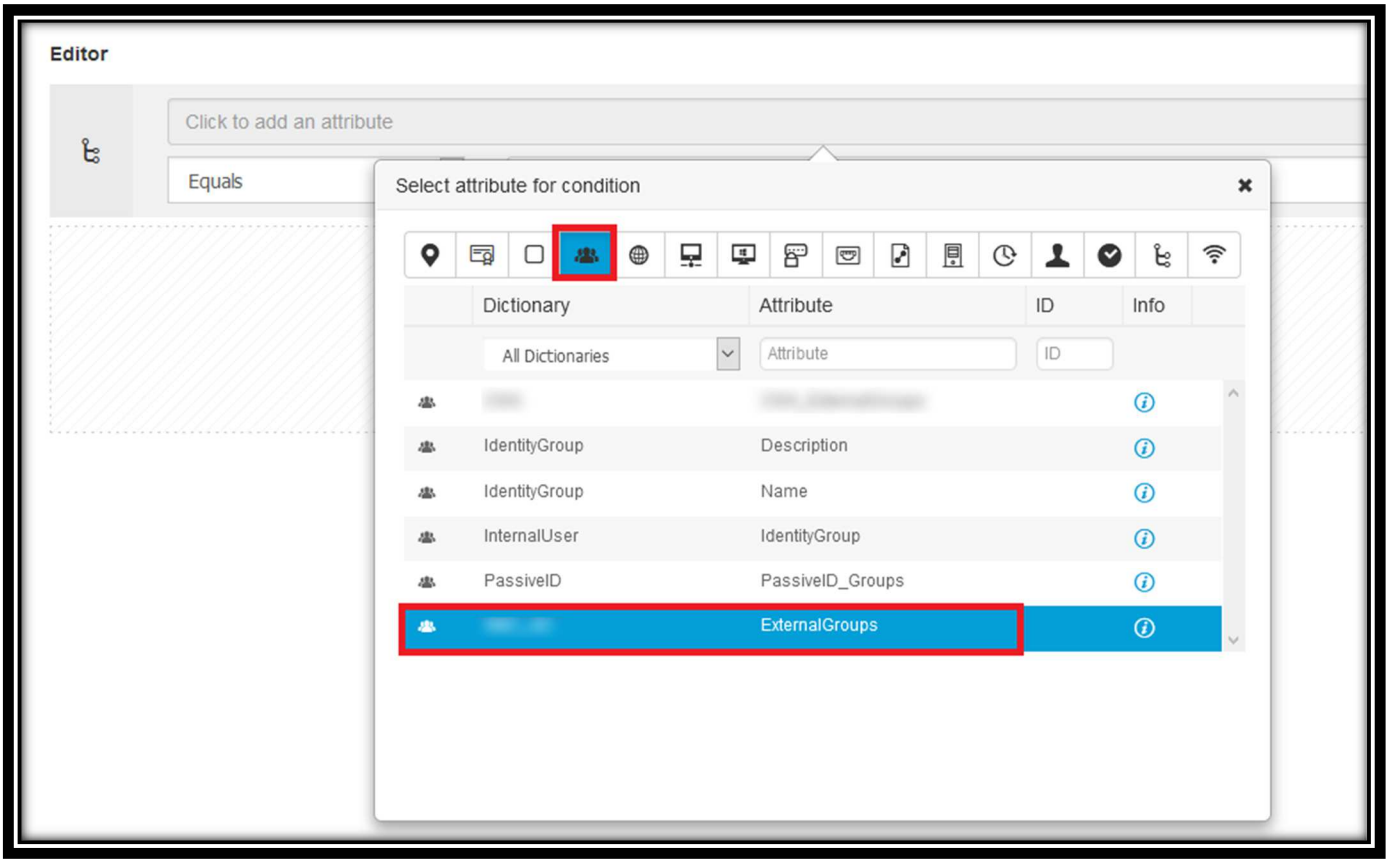
Step 2 – Configure Cisco ISE parameters for VPN Authentication

In this phase we will configure parameters used for VPN authentication in Cisco ISE policy, like AD group membership, etc. In my configuration I will use three AD Groups for Employee, Vendor and ITSupport.

1. Login to **Cisco ISE**
2. Navigate to **Policy → Policy Elements → Conditions**
3. We will create **Condition Element** for those three AD groups by selecting below:
    a. In Attribute, select **Identity → Your AD Group → Equals → <Select your AD Group>**

    Note – If you do not see AD group, you first have to add that AD group to ISE from **Administration → External Identity Source → Active Directory → <Your Directory> → Groups → Add**

    b. Similarly create **Condition Element** for other two Groups – Vendor and ITSupport



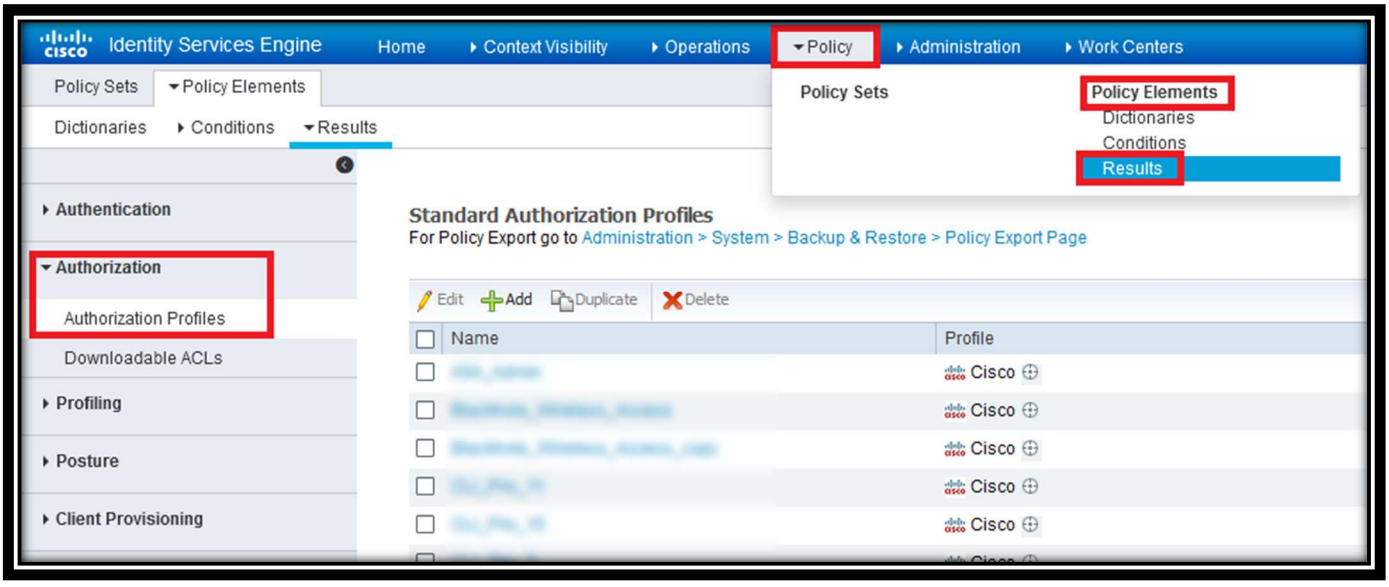

Editor
SMC_AD-ExternalGroups
Equals
AD.LOCAL\GROUP\EMPLOYEES
Set to 'Is not'
Duplicate
Save

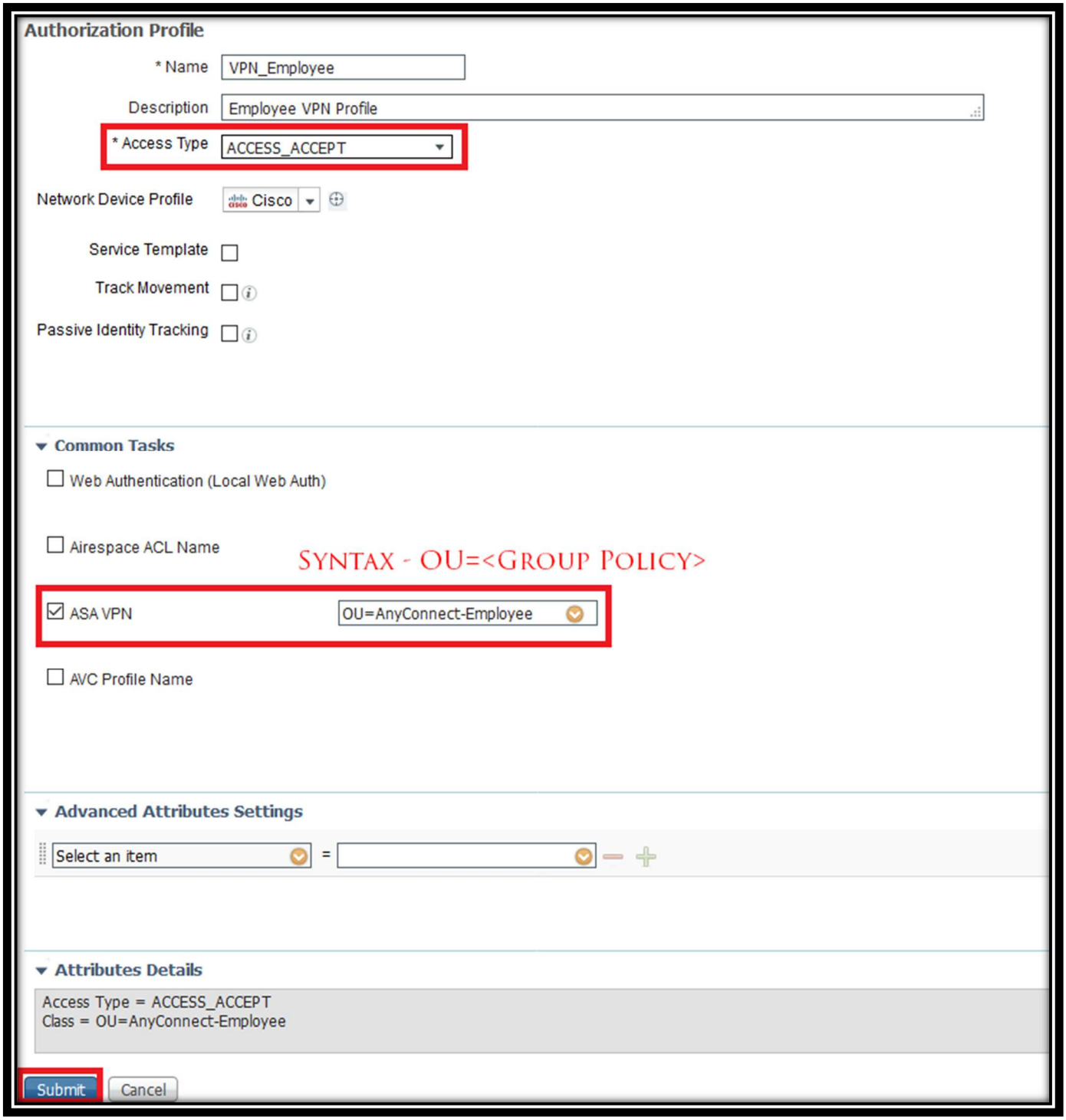

Save condition
Save as existing Library Condition (replaces current version and impact all policies that use this condition)
Select from list
Save as a new Library Condition
MemberOf_Employee
Description (optional)
Condition Description
Close
Save

Step 3 - Configure Cisco ISE parameters for Dynamic Authorisation – Authorisation Policy

In this phase, we will create resultant authorisation policy/profile when authentication and authorisation is successful. In this phase we will mention the Group Policy Name to be applied to the user.

1. Login to **Cisco ISE**
2. Navigate to **Policy → Policy Element → Results → Authorisation → Authorisation Profiles → Add**
3. Configure as below:
    a. Name and Description – ***As per your choice or naming convention***
    b. Access Type – **ACCESS_ACCEPT**
    c. Common Tasks → **ASA VPN → OU=<Group Policy Name>**
    d. Submit
4. Create for Employee, Vendor and ITSupport as per Step 3.

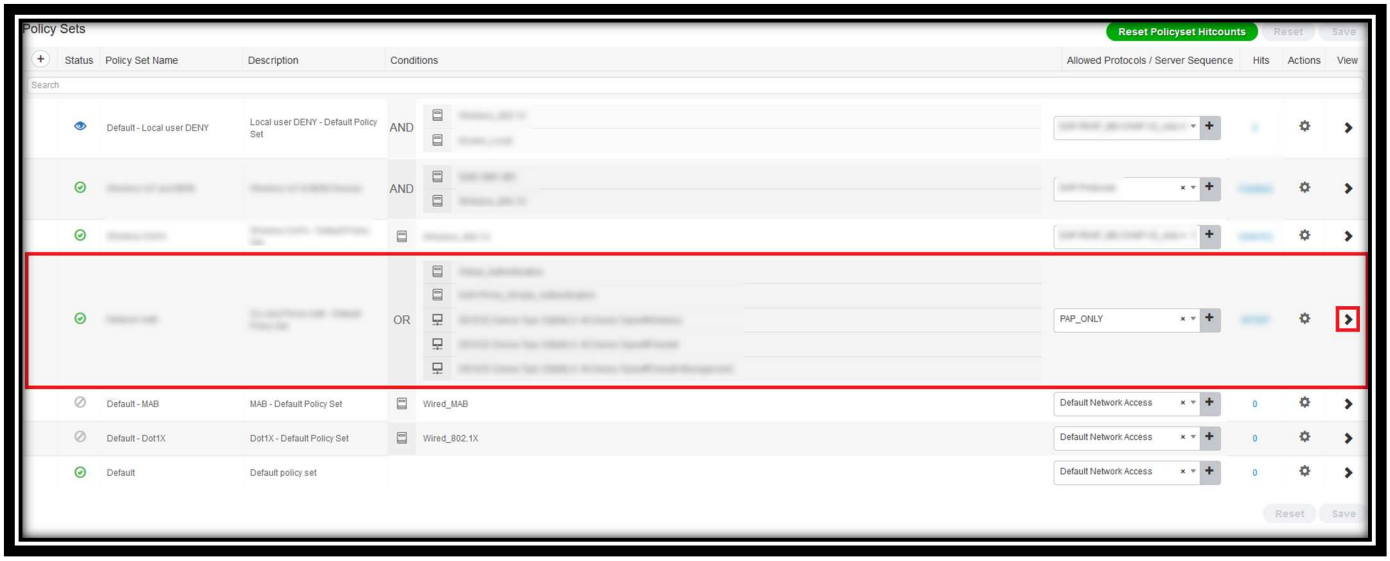


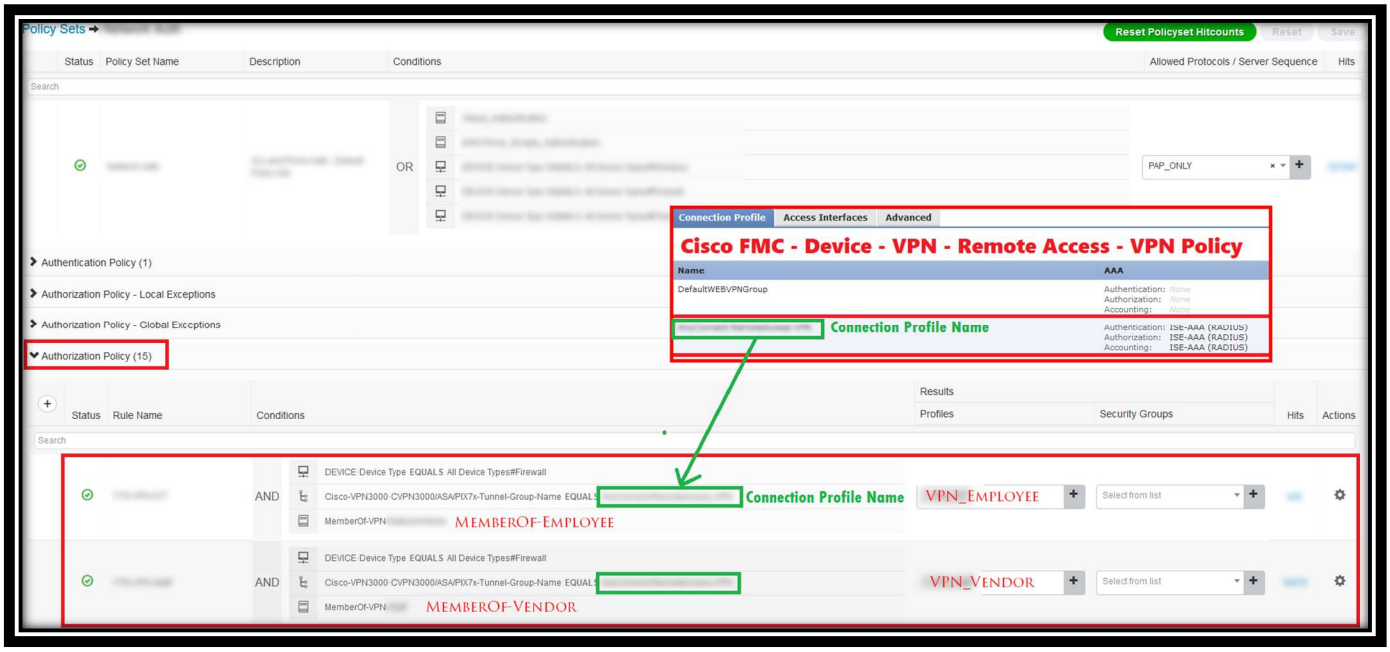


Step 4 - Configure different Cisco ISE policy for each VPN user category (e.g. Vendor, Employee, etc)

In this phase, we will create ISE policy for each VPN user.

1. Login to **Cisco ISE**
2. Navigate to **Policy → Policy Set →** *Select your main policy*
3. Add new authorisation policy at top as below:
    a. Name – **VPN-Employee**
    b. Conditions:
        i. **DEVICE – Device Type → Equals → Firewall**
        ii. **Cisco-VPN3000·CVPN3000/ASA/PIX7x-Tunnel-Group-Name → Equals →** ***<AnyConnect Remote Access Connection Profile Name>***
        iii. **MemberOf-Employee**
    c. Result → **VPN-Employee**
4. Similarly, create authorisation rules for Vendor and ITSupport, just change the MemberOf and Resultant Policy.

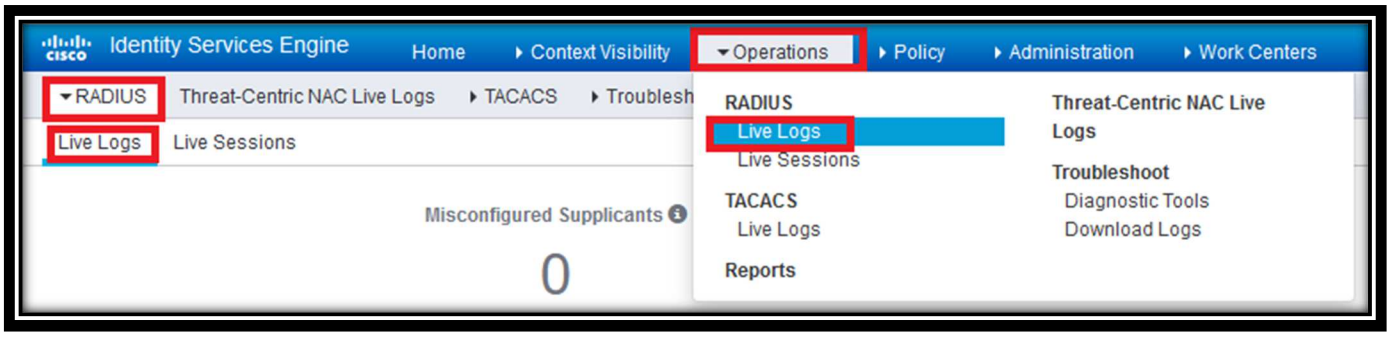


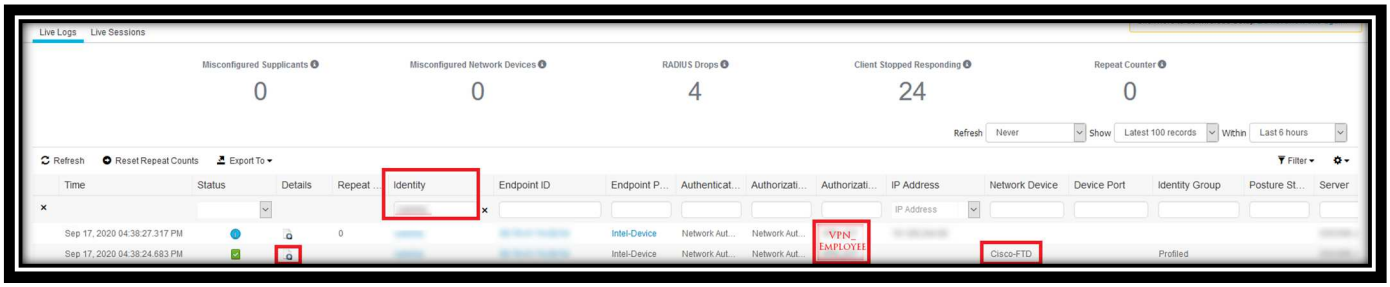


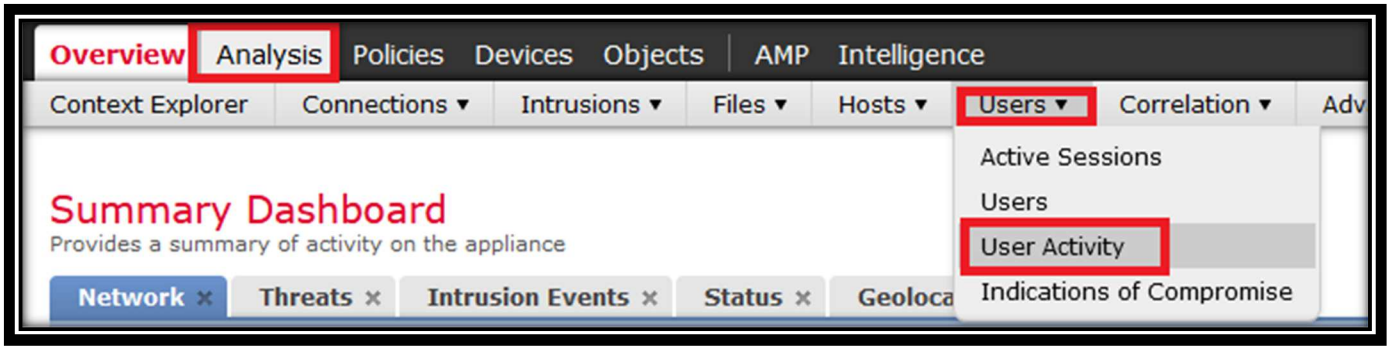
Step 5 – Testing and Verification of the policy

In this phase, we will connect via VPN and test if we getting the right policy, ACL and IP address.

1. Connect using Employee username/password group via AnyConnect
2. Login to **Cisco ISE**
3. Navigate to **Operations → Live Log**
4. Search based on the **username** to see the log
5. Find the **VPN policy log** and click the **Details column Magnifying Glass** to view details
6. In details section you can see, **resultant policy**, which rule it is hitting, AD group and all other details.
7. Login to **Cisco FMC** to verify under FMC
8. Navigate to **Analysis → Users → User Activity**
9. Search based on username
10. You will see a record of your user with **Group Policy** details.






Overview
Analysis
Policies
Devices
Objects
AMP
Intelligence
Context Explorer
Connections
Intrusions
Files
Hosts
Users
Correlation
Active Sessions
Users
User Activity
Indications of Compromise
Summary Dashboard
Provides a summary of activity on the appliance
Network
Threats
Intrusion Events
Status


User Activity
Table View of Events
Users
Search Constraints (Edit Search Save Search)
Time
Event
Username
Realm
Discovery Application
Authentication Type
IP Address
Start Port
End Port
Description
VPN Session Type
VPN Group Policy
VPN Connection Profile
VPN Client Public IP
VPN Client Country
2020-09-17 16:38:27
User Login
LDAP
2020-09-17 16:38:23
VPN User Login
Discovered Identities
LDAP
VPN Authentication
AnyConnect SSL
EMPLOYEE_GROUP_POLICY
AUS
win
Displaying rows 1–2 of 2 rows
View
Delete
View All
Delete All