

IP assignment for VPN users using an External server on ACS 5.x

On this example I am using Radius Identity Server for the authentication and the Internal database for the Authorization to add the IP information.

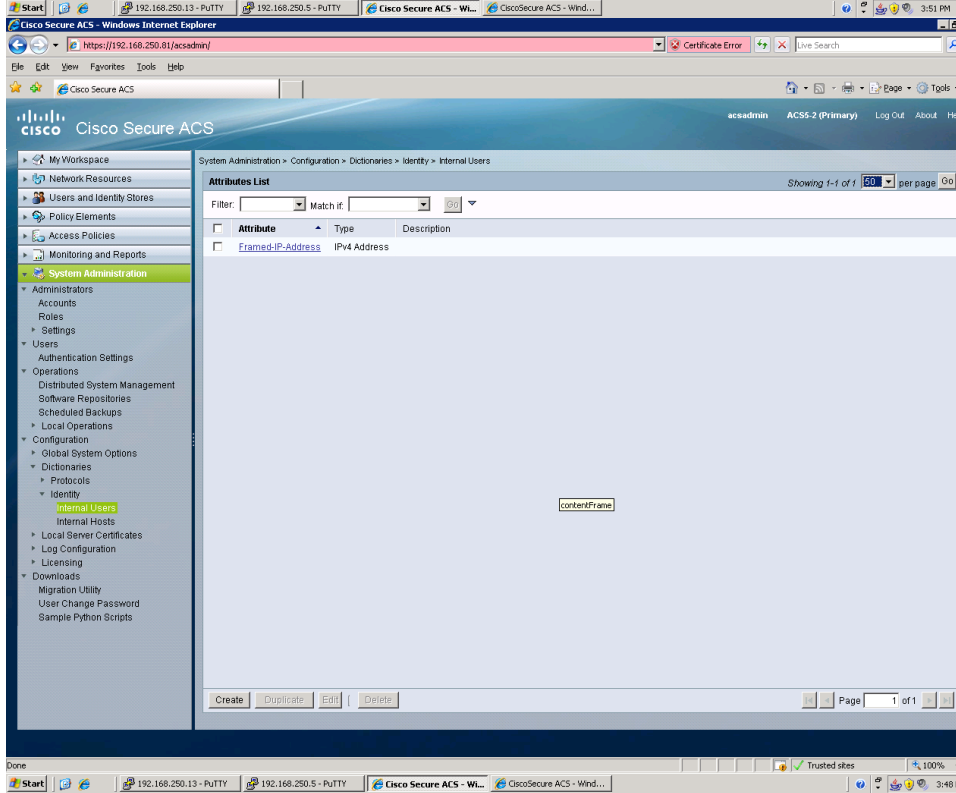
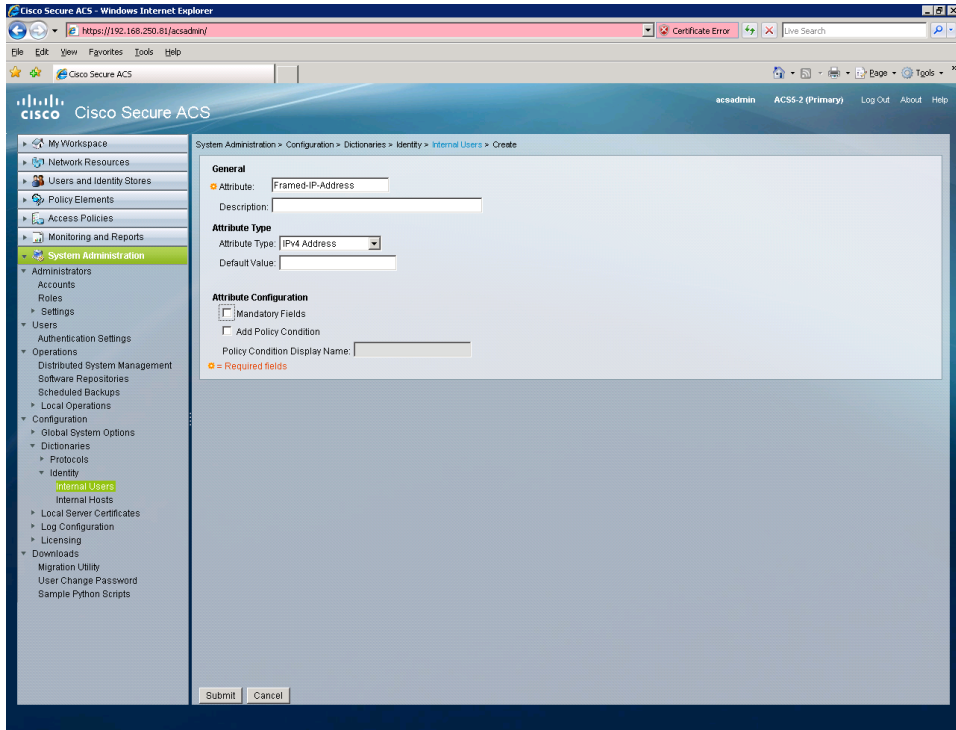
Step 1: Create the Radius Identity server that will handle the user information for the authentication.

The screenshot displays the Cisco Secure ACS 5.x web interface in a Windows Internet Explorer browser. The browser's address bar shows the URL `https://192.168.250.81/acsadmin/`. The interface includes a navigation menu on the left with categories like My Workspace, Network Resources, Users and Identity Stores, and Policy Elements. The main content area is titled "Users and Identity Stores > External Identity Stores > RADIUS Identity Servers > Edit: 'ACS4.x'".

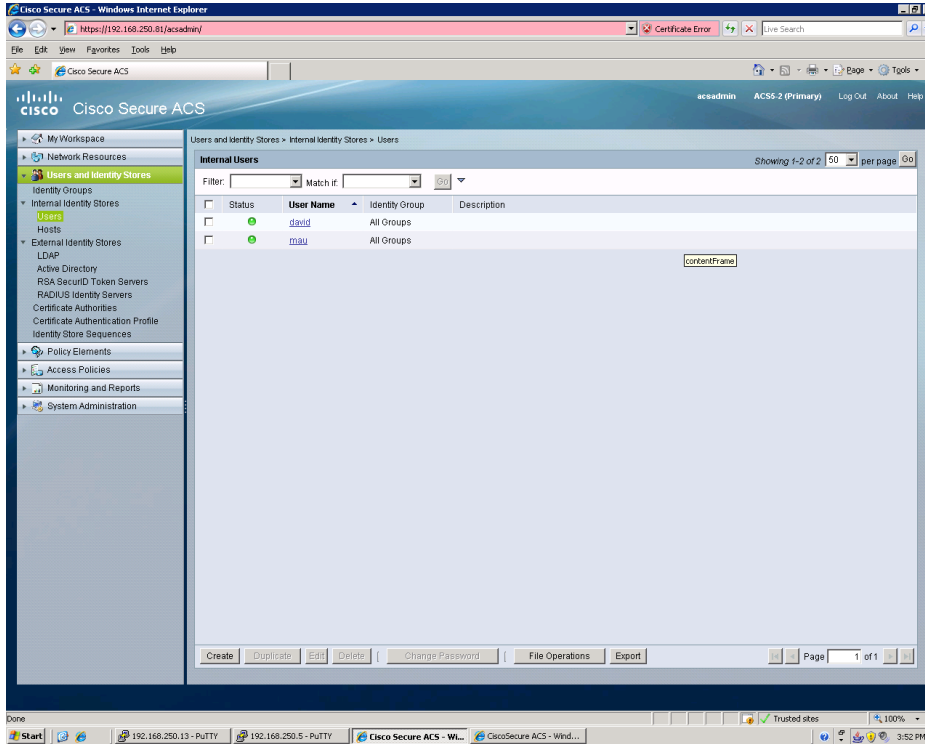
The configuration page for the RADIUS Identity Server "ACS4.x" is shown, with the "General" tab selected. The "Name" field is set to "ACS4.x". Under "Server Connection", the "Always Access Primary Server First" radio button is selected, and the "Fallback To Primary Server After" is set to 0 minutes. The "Primary Server" section has the following values: Hostname: 192.168.250.28, Shared Secret: [masked], Authentication Port: 1812, Server Timeout: 5 Seconds, and Connection Attempts: 3. The "Secondary Server" section has empty fields for Hostname, Shared Secret, Authentication Port, Server Timeout, and Connection Attempts. A legend at the bottom left of the form indicates that orange asterisks denote required fields. "Submit" and "Cancel" buttons are located at the bottom of the form.

The Windows taskbar at the bottom shows the Start button, several open applications including PuTTY and Cisco Secure ACS, and the system clock displaying 3:42 PM.

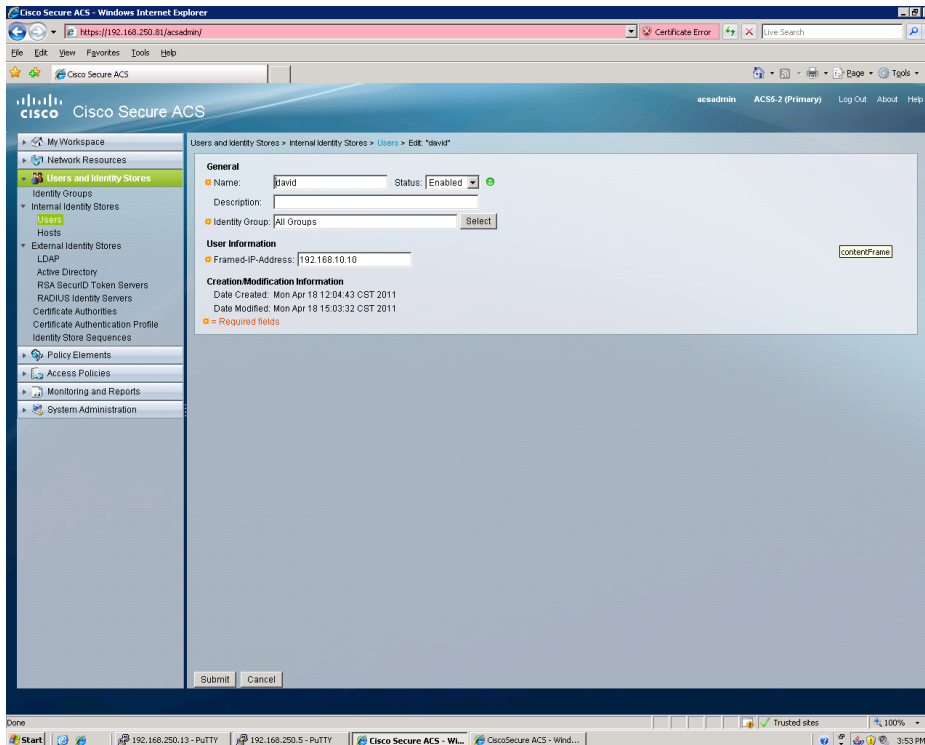
Step 2: Create a new value for the user entries that include the IP address value "IPv4 address". This configuration is done under "System Administration" / "Configuration" / "Dictionaries" / "Identity" / "Internal Users"



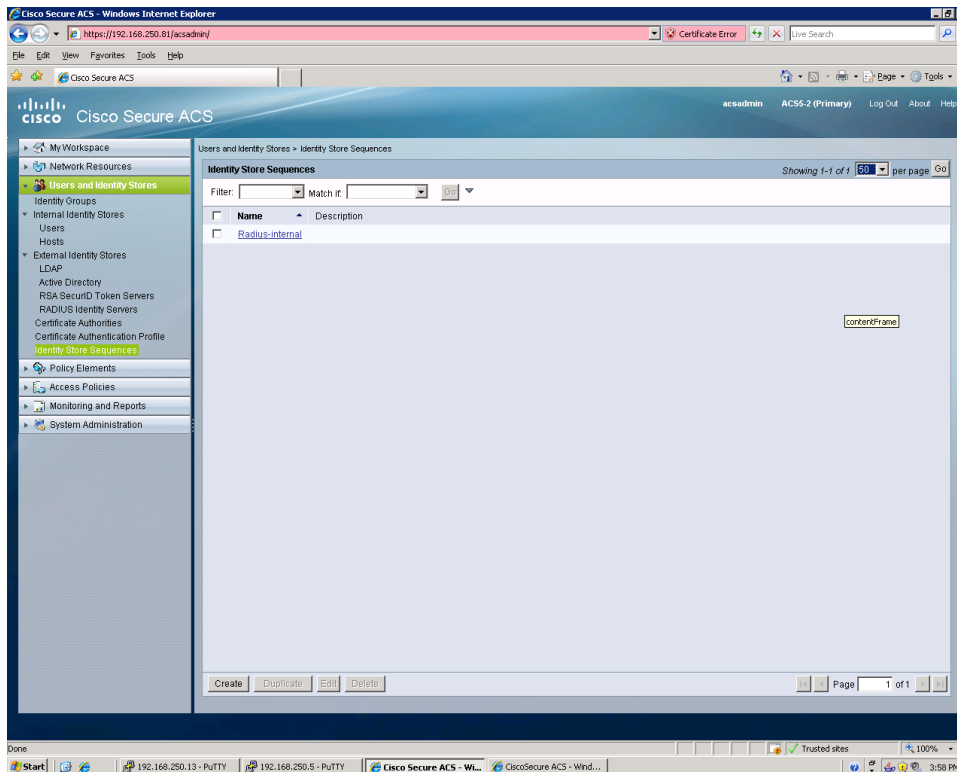
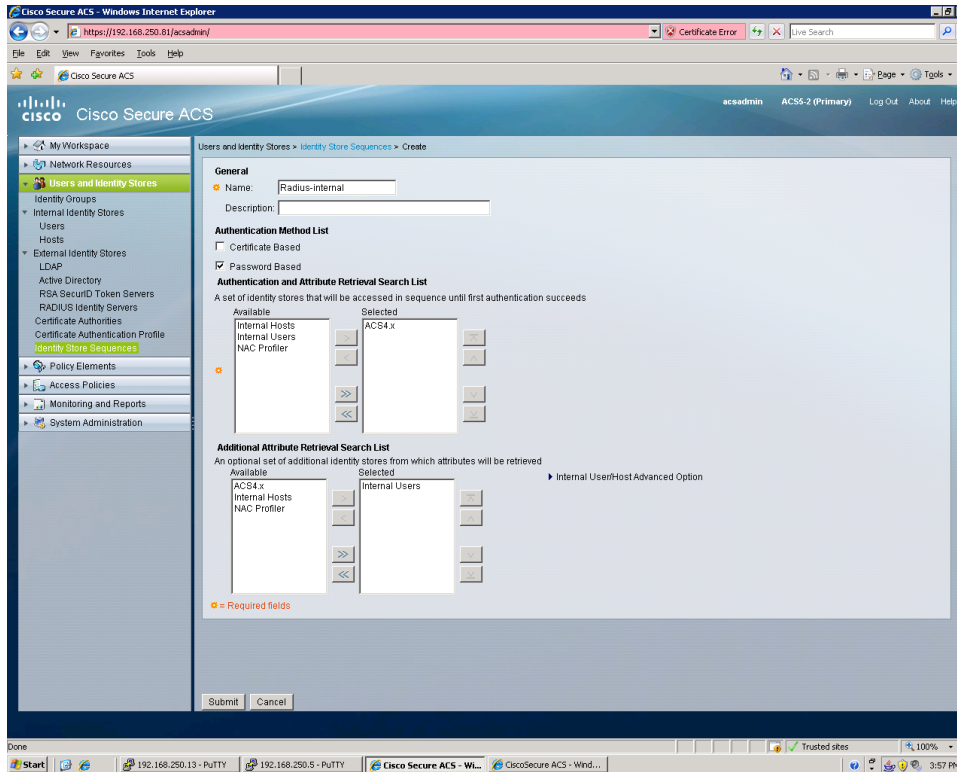
Step 3: Make sure that the user on the Radius Identity server also exist on the internal database. On this example I created two account called "David" and "Mau"



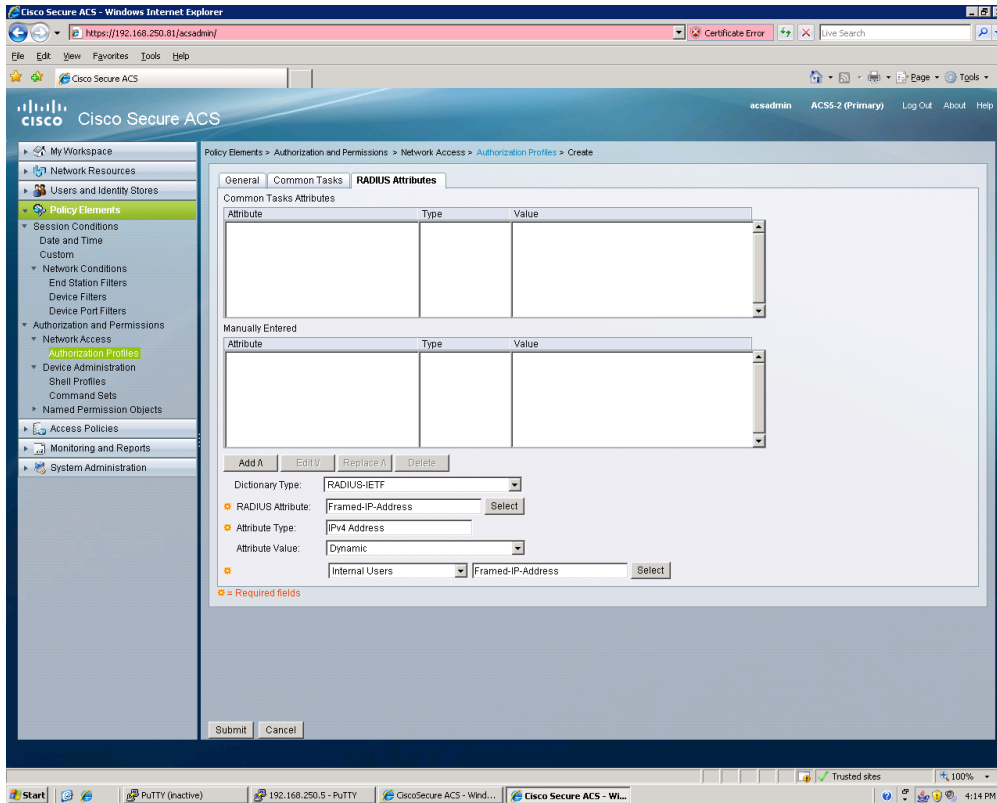
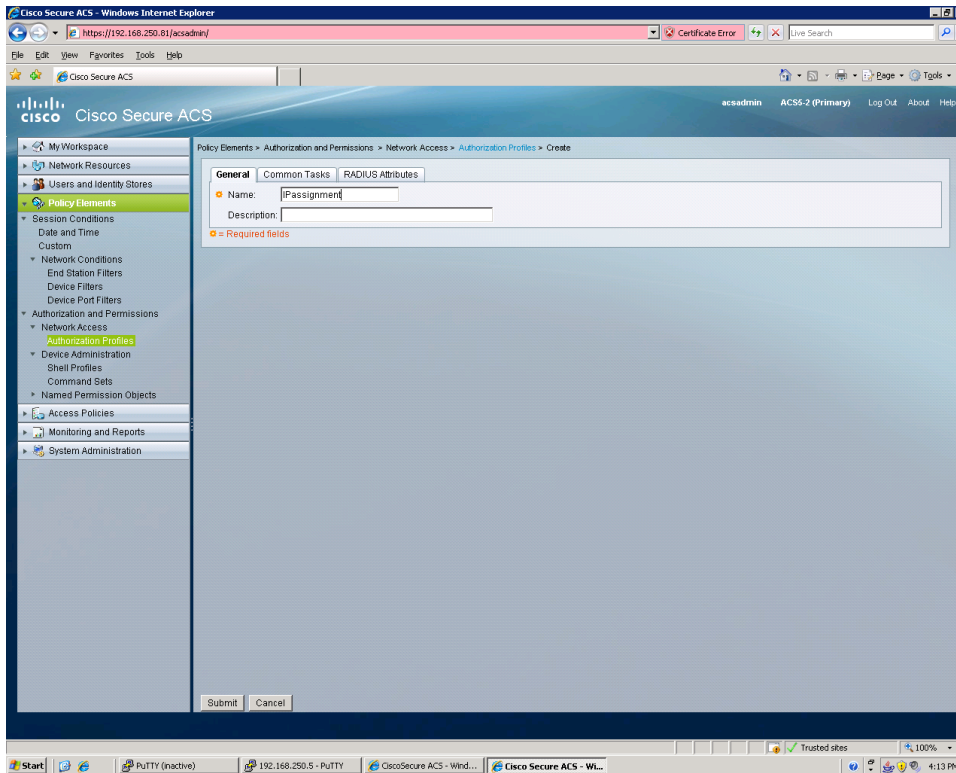
Step 4: Assign the IP address to the specific user



Step 5: Create a Identity Store Sequence in order to force the authentication to be done through the Radius Identity server and the additional attribute retrieval that contains the IP address created on the user against the Internal User database.

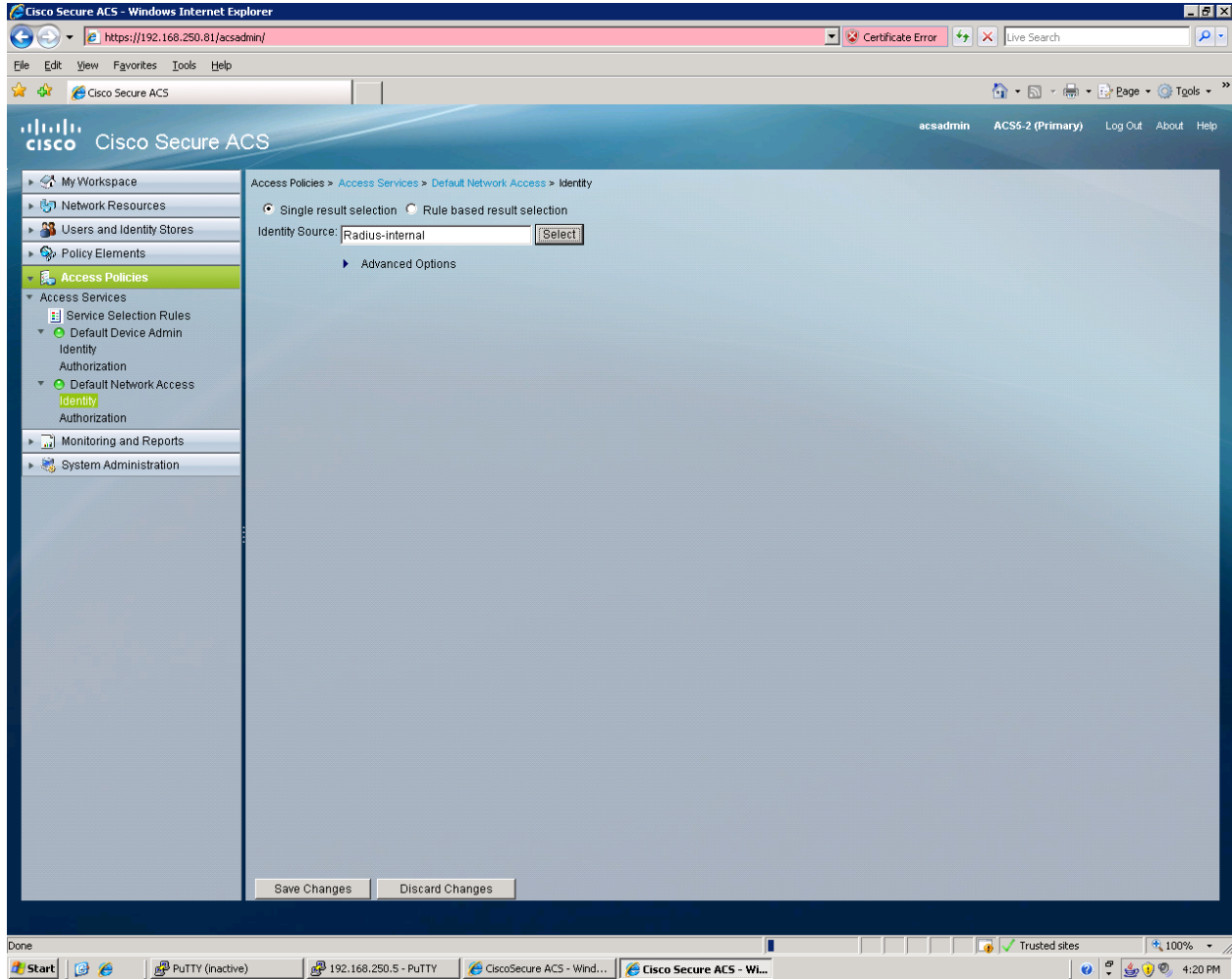


Step 6: Go into the Policy Elements / Network Access/ Authorization Profile and create a new rule

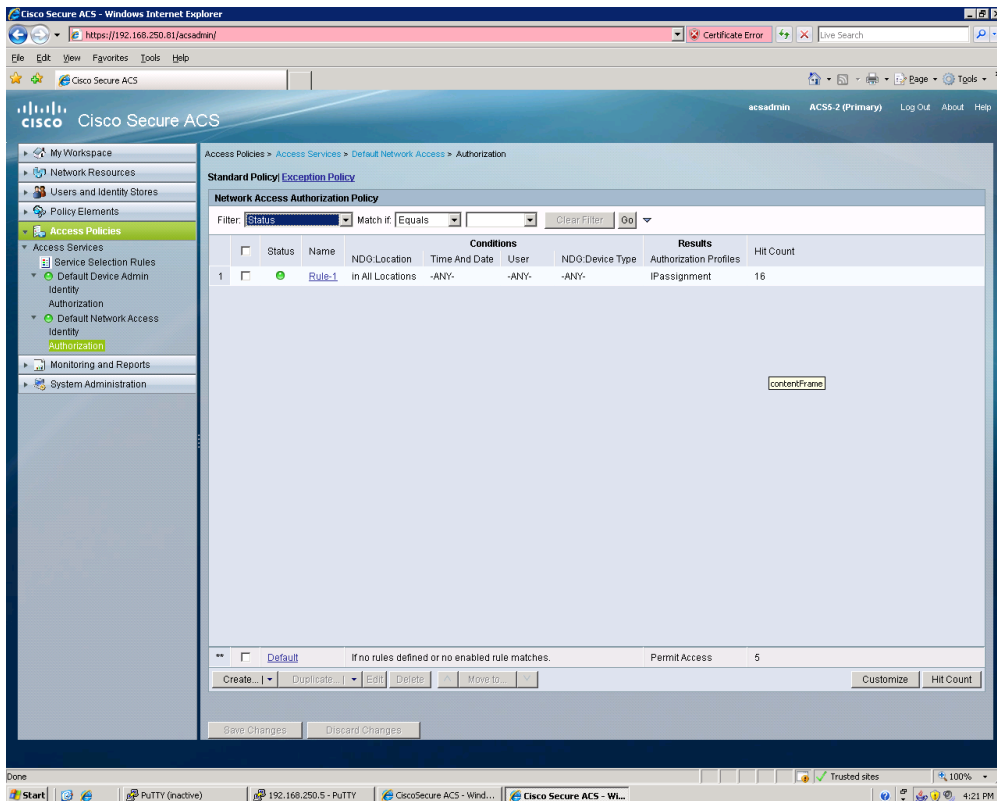
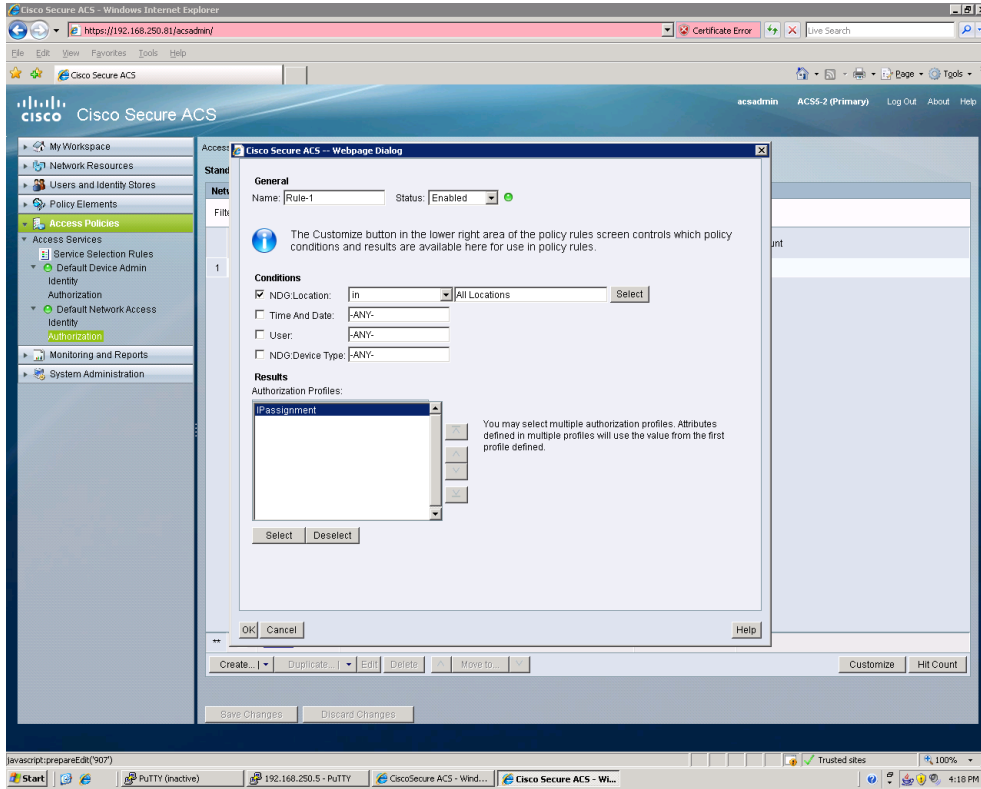


NOTE: Make sure that the new profile is using the Directory called “Radius IETF” with the attribute “Framed-IP-Address” and select the value as Dynamic using the Internal Users values and finally select the name of the attribute that was created under Step 2. On this example the name was Framed-IP-Address.

Step 7: Apply the identity store sequence into the Access Policy for the Radius Authentication so we can retrieve the authentication with the external Radius server and the authorization from the internal users.



Step 8: Create a new rule under the Authorization section of the Default Network Access or the specific Access Service that you are using and as a result rules apply the Authorization Profile.



Troubleshooting:

- a) On the ASA or VPN Server you can enable the Radius debugs to verify if the Framed IP address attribute is being sent by the ACS.

Debug aaa authentication

Debug radius

Term monitor

Example of the log:

Parsed packet data.....

Radius: Code = 2 (0x02)

Radius: Identifier = 15 (0x0F)

Radius: Length = 56 (0x0038)

Radius: Vector: 5D9D606E796D7D9690EB931F08BDAF99

Radius: Type = 1 (0x01) User-Name

Radius: Length = 5 (0x05)

Radius: Value (String) =

6d 61 75 | mau

Radius: Type = 8 (0x08) Framed-IP-Address

Radius: Length = 6 (0x06)

Radius: Value (IP Address) = 192.168.20.120 (0xC0A81478)

Radius: Type = 25 (0x19) Class

Radius: Length = 25 (0x19)

Radius: Value (String) =

43 41 43 53 3a 41 43 53 35 2d 32 2f 39 32 35 33 | CACS:ACS5-2/9253

32 37 36 38 2f 31 36 | 2768/16

rad_procpkt: ACCEPT

RADIUS_ACCESS_ACCEPT: normal termination

RADIUS_DELETE

remove_req 0xd8381bd0 session 0x113 id 15

free_rip 0xd8381bd0

radius: send queue empty

INFO: Authentication Successful

b) Verify the ACS reports to verify if the Authorization Profile is being assigned.

The screenshot displays the Cisco Secure ACS View interface in a Windows Internet Explorer browser. The address bar shows the URL <https://192.168.250.81/acsview/>. The page title is "Cisco Secure ACS View" and the user is logged in as "acsadmin". The interface includes a navigation menu on the left with categories like "Monitoring and Reports", "Alarms", "Reports", "Catalog", and "Troubleshooting". The main content area shows a report generated on April 18, 2011, at 4:25:53 PM CST. The "Authentication Summary" section includes the following details:

- Logged At: April 18, 2011 4:22:29.023 PM
- RADIUS Status: Authentication succeeded
- NAS Failure:
- Username: mau
- MAC/IP Address:
- Network Device: ASA-MAU : 192.168.250.5
- Access Service: Default Network Access
- Identity Store: ACS4 x
- Authorization Profiles: IPAssignment
- CTS Security Group:
- Authentication Method: PAP_ASCII

The "Actions" section on the right provides links for troubleshooting and configuration changes. Below the summary, the "Authentication Details" section provides further information:

- Logged At: April 18, 2011 4:22:29.023 PM
- ACS Time: April 18, 2011 4:22:29.016 PM
- ACS Instance: ACS5-2
- Authentication Method: PAP_ASCII
- EAP Authentication Method:
- EAP Tunnel Method:
- User: ACS Username: mau, RADIUS Username: mau, Calling Station ID:
- Framed IP Address: 192.168.20.120
- Host Lookup:
- Network Device: ASA-MAU, Network Device Device Type: All Device Types, Group: Location: All Locations

The browser's taskbar at the bottom shows several open windows, including "PUTTY (inactive)", "192.168.250.5 - PUTTY", and "Cisco Secure ACS - M...". The system clock indicates the time is 4:26 PM on Monday, April 18, 2011.