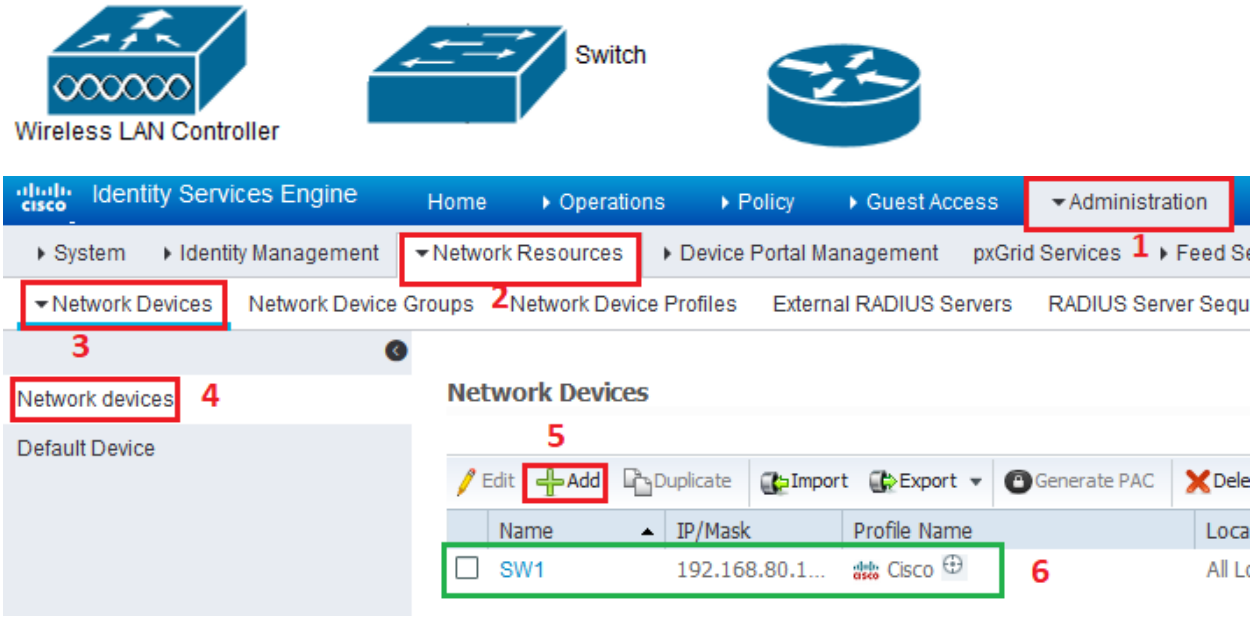
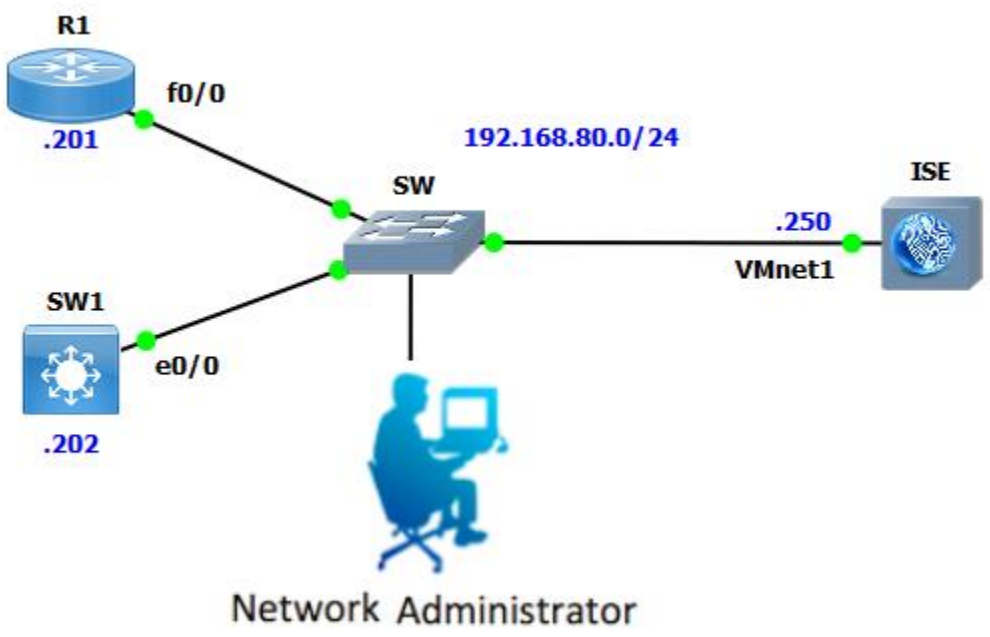
Network Access Device:

- NAD stands for Network Access Device.
- Network Access Device (NAD) is the Access Layer Device.
- NAD is basically, a device through which Endpoint is connected.
- Network Access Device (NAD) is AAA Client device.
- Any device that is going to send RADIUS authentication requests to ISE.
- NAD responsible for sending EAP authentication request to authentication server.
- NAD is Authenticator for 802.1X from a supplicant to the authentication server.
- NAD can be the device such as Switch, Router that support NAC Enforcement policies.
- Common NAD types Wired Ethernet Switches, Wireless LAN Controllers & ASA.



 Created by Ahmad Ali E-Mail: ahmadalimsc@gmail.com , Mobile: 056 430 3717

Network Diagram:



Configure Router for Authentication and Authorization:

Enable AAA new-model. Define TACACS server ISE. Configure login, enable authentications, and then use the exec and command authorizations. Assign method lists to line vty.

R1 AAA Configuration
R1(config)#aaa new-model
R1(config)#tacacs-server host 192.168.80.250 key test123
R1(config)#aaa authentication login default group tacacs+ local R1(config)#aaa authentication enable default group tacacs+ enable R1(config)#aaa authorization exec default group tacacs+ local R1(config)#aaa authorization commands 0 default group tacacs+ local R1(config)#aaa authorization commands 1 default group tacacs+ local R1(config)#aaa authorization commands 15 default group tacacs+ local R1(config)#aaa authorization config-commands
R1(config)#line vty 0 4 R1(config-line)#authorization commands 0 default R1(config-line)#authorization commands 1 default R1(config-line)#authorization commands 15 default R1(config-line)#authorization exec default R1(config-line)#login authentication default

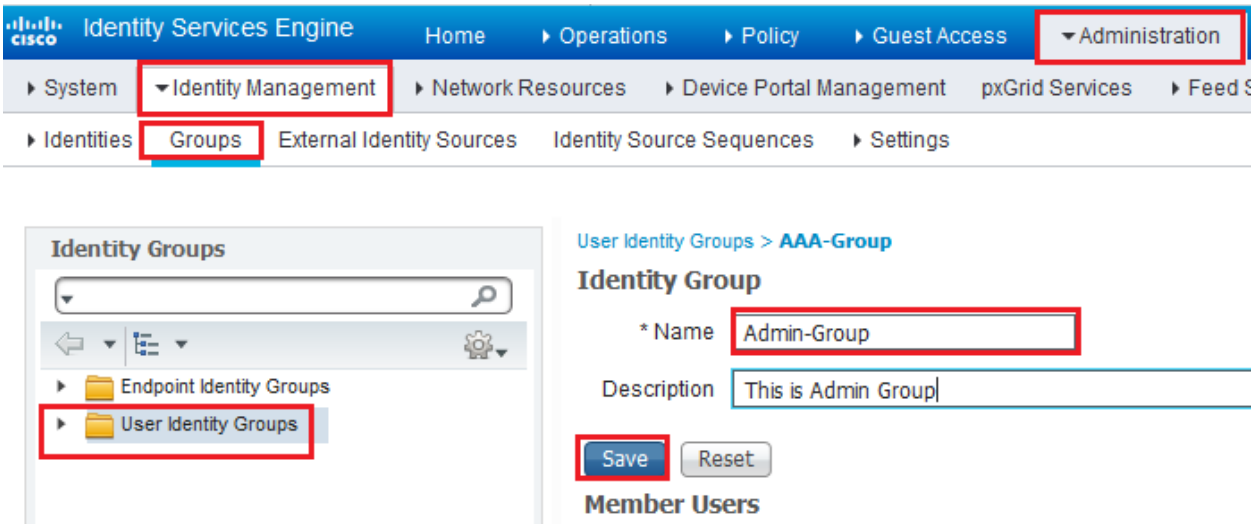
Configure Switch for Authentication and Authorization:

Enable AAA new-model. Define TACACS server ISE. Configure login, enable authentications, and then use the exec and command authorizations. Assign method lists to line vty.

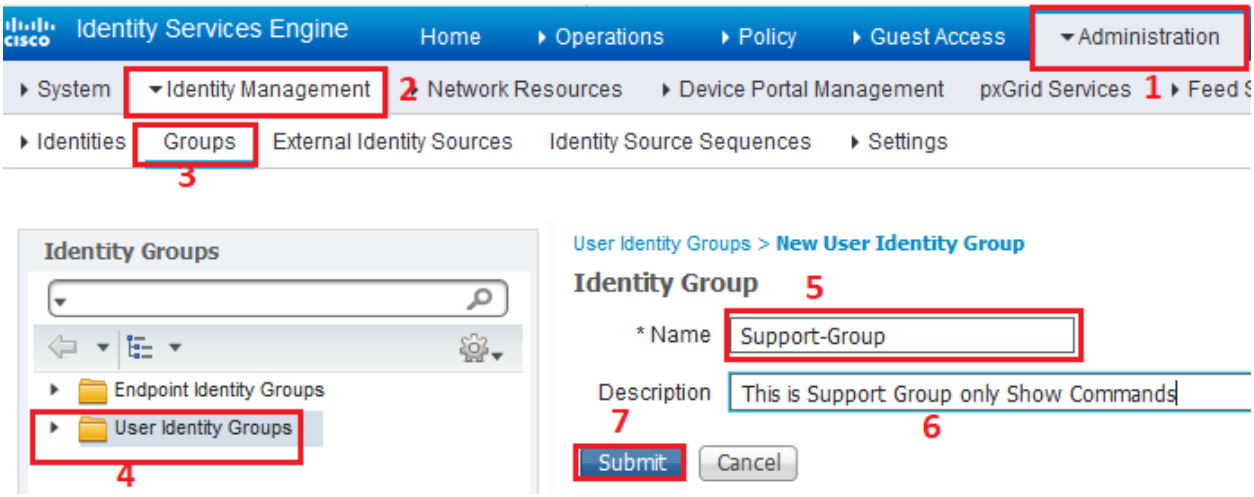
SW1 AAA Configuration
SW1(config)#aaa new-model
SW1(config)#tacacs server ISE SW1(config-server-tacacs)#address ipv4 192.168.80.250 SW1(config-server-tacacs)#key test123
SW1(config)#aaa authentication login default group tacacs+ local SW1(config)#aaa authentication enable default group tacacs+ enable SW1(config)#aaa authorization exec default group tacacs+ local SW1(config)#aaa authorization commands 0 default group tacacs+ local SW1(config)#aaa authorization commands 1 default group tacacs+ local SW1(config)#aaa authorization commands 15 default group tacacs+ local SW1(config)#aaa authorization config-commands
SW1(config)#line vty 0 4 SW1(config-line)#authorization commands 0 default SW1(config-line)#authorization commands 1 default SW1(config-line)#authorization commands 15 default SW1(config-line)#authorization exec default SW1(config-line)#login authentication default

Add Local Groups & Users:

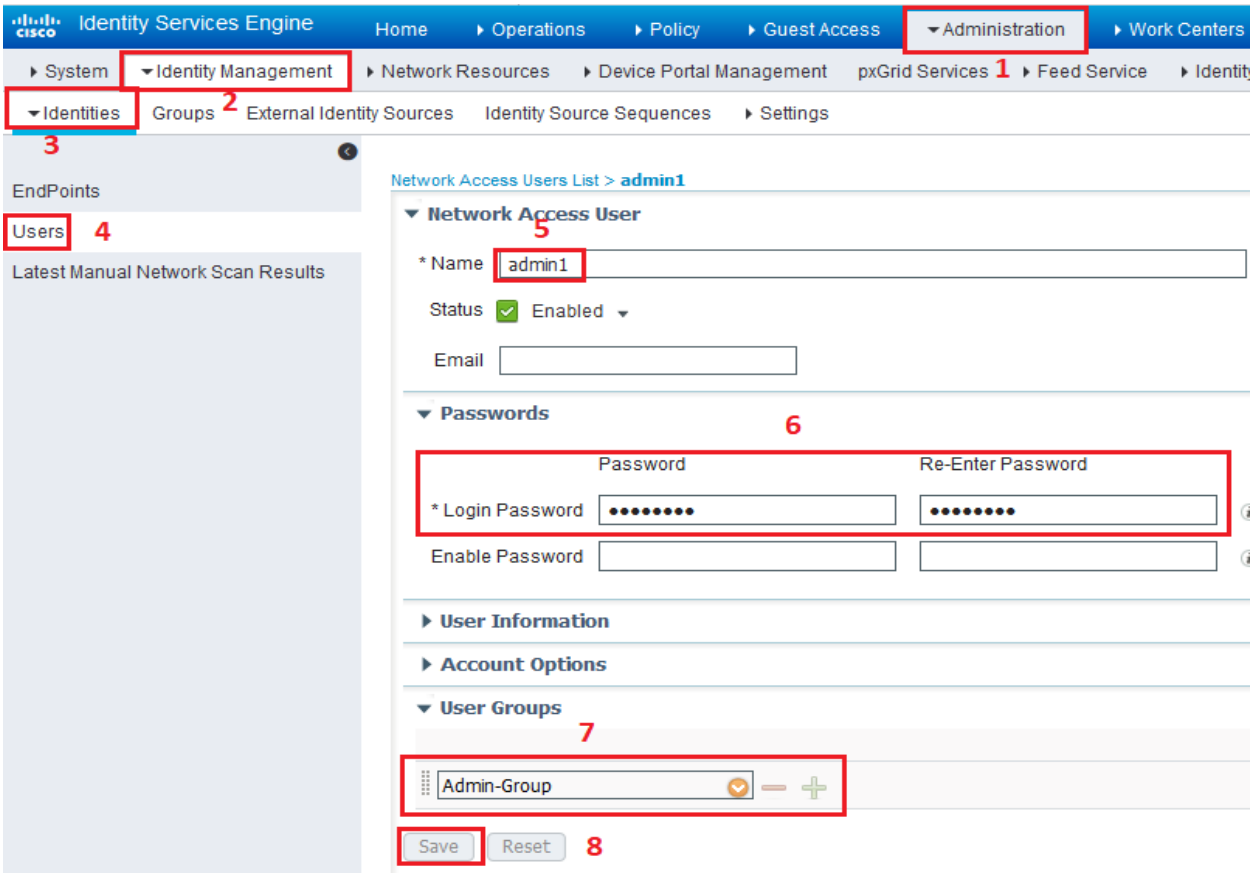
Navigate to **Administration > Identity Management > Groups > User Identity Groups**. Click **Add**. Provide Name, Description and click "**Save"** to save setting.



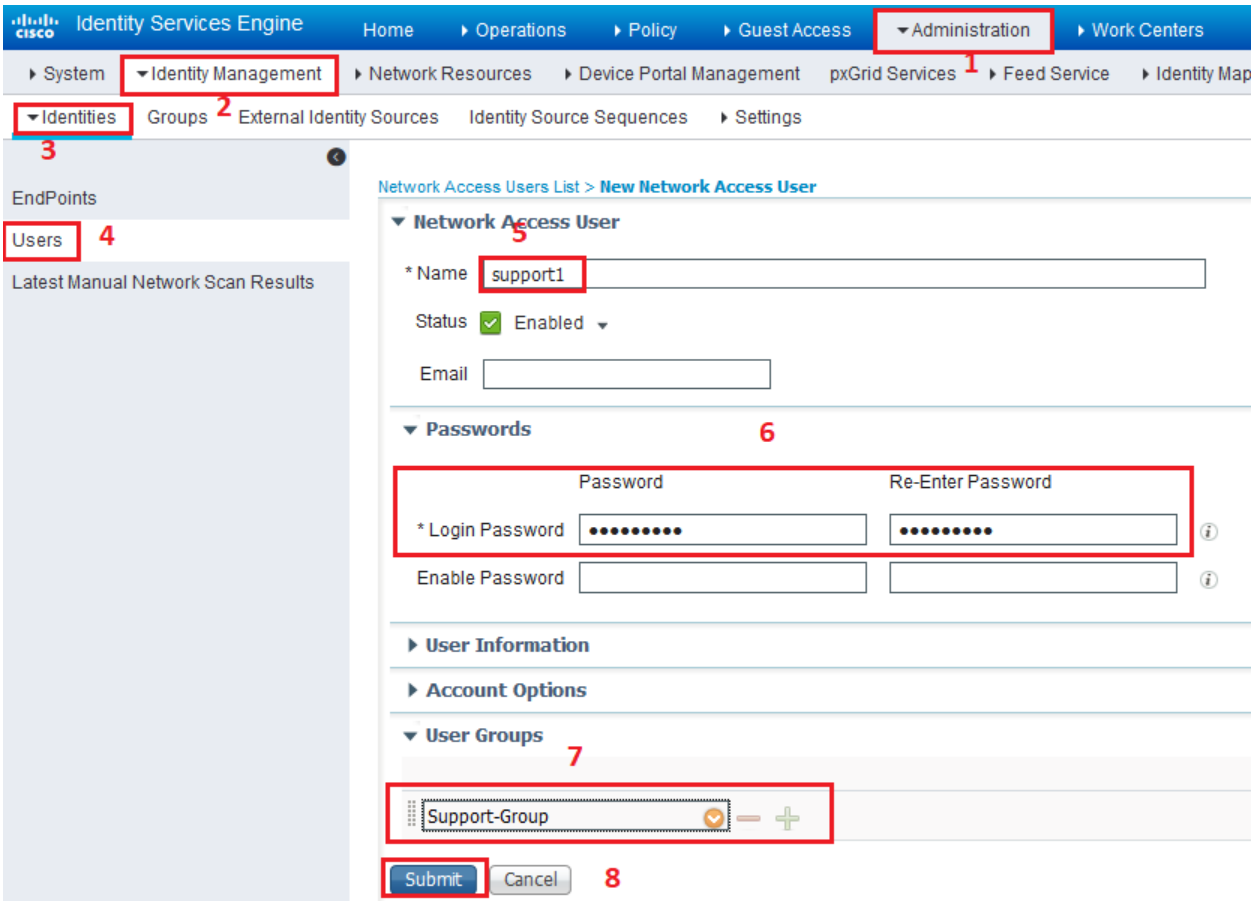
Navigate to **Administration > Identity Management > Groups > User Identity Groups**. Click **Add**. Provide Name, Description and click "**Save"** to save setting.



Navigate to **Administration > Identity Management > Identities > Users**. Click **Add**. Provide Name, Passwords and User Groups select Admin-Group and click "**Save"** to save the setting.



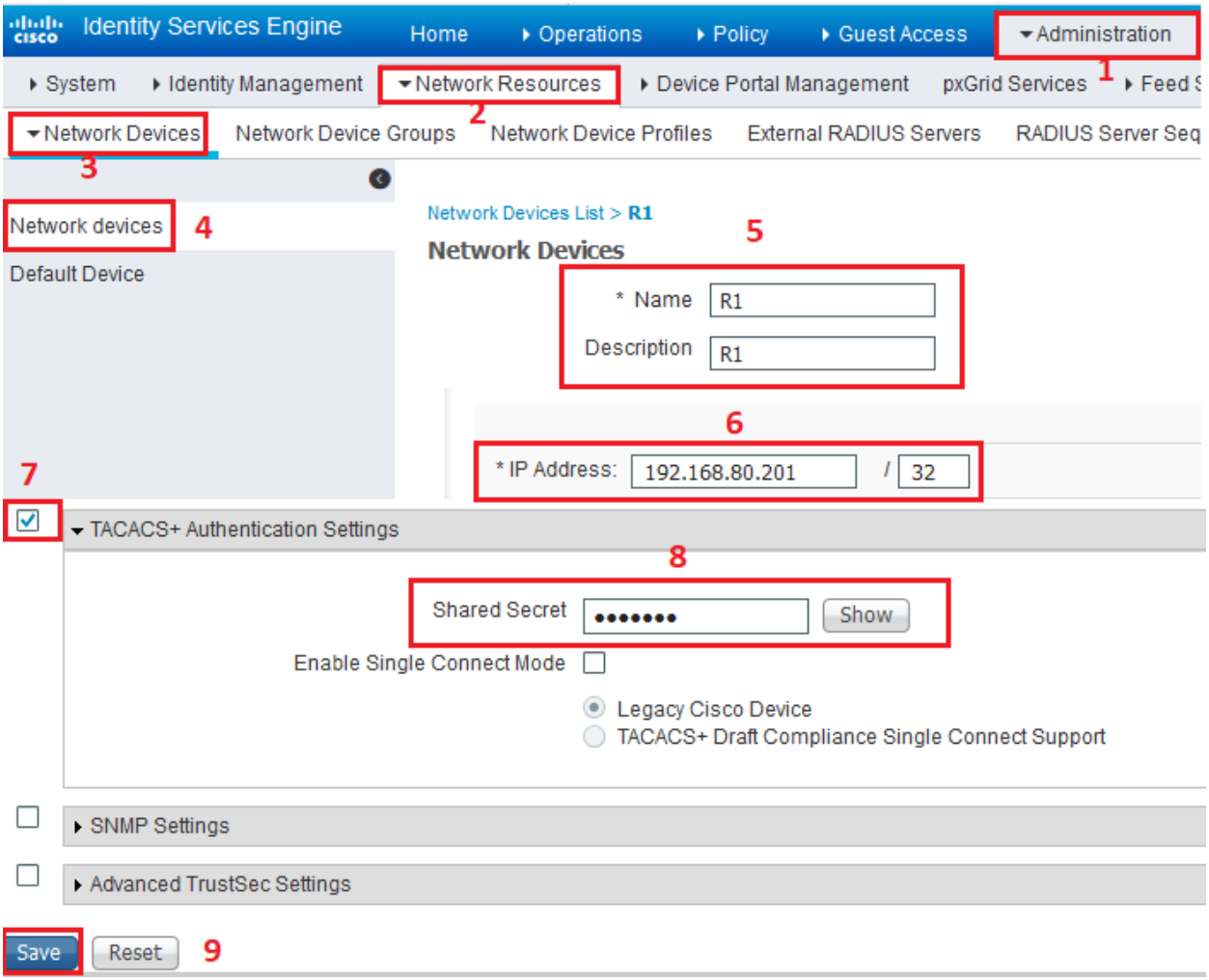
Navigate to **Administration > Identity Management > Identities > Users**. Click **Add**. Provide Name, Passwords and User Groups select Support-Group and click "**Save"** to save the setting.



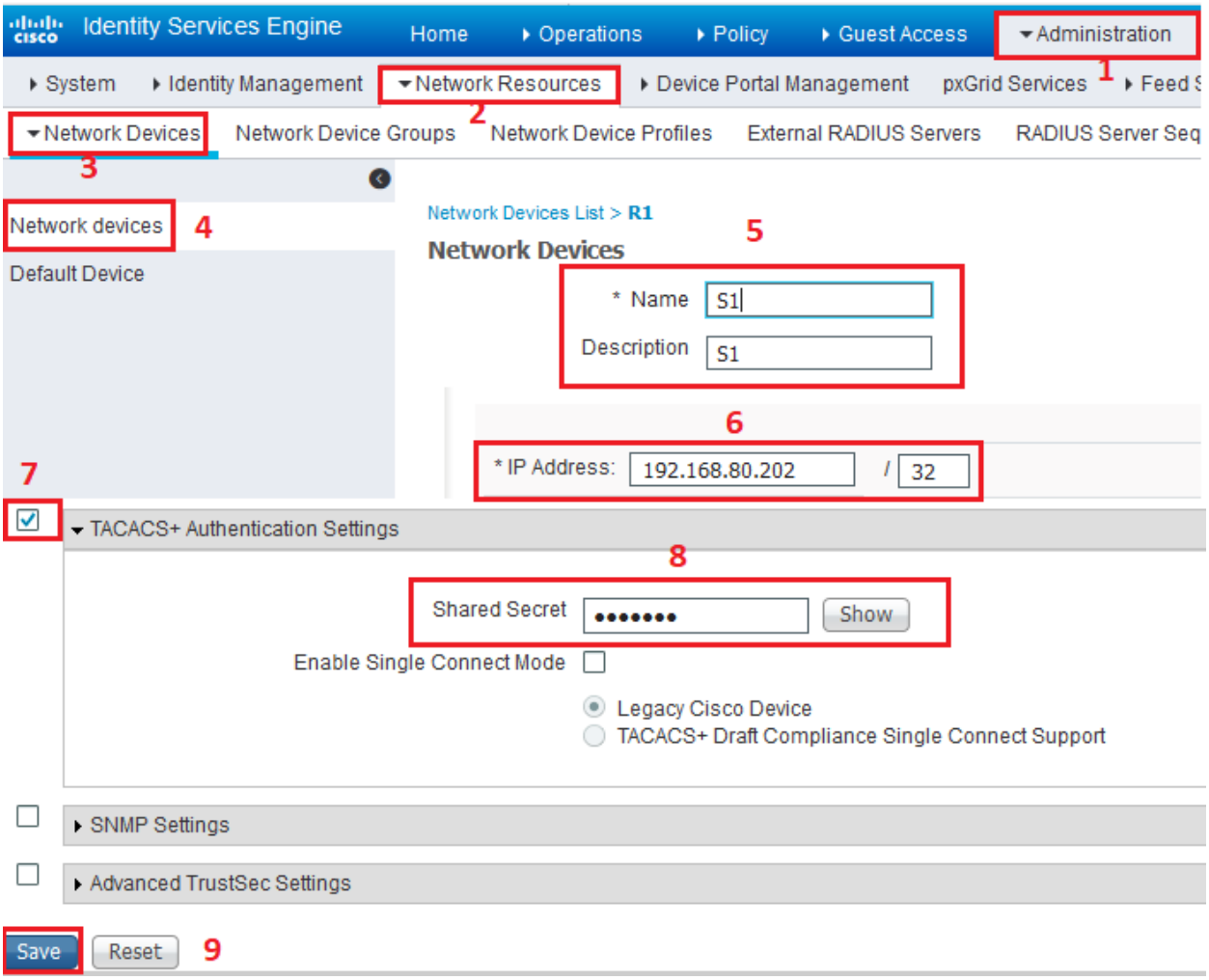
 Created by Ahmad Ali E-Mail: ahmadalimsc@gmail.com , Mobile: 056 430 3717

Add Network Device:

Navigate to **Administration > Network Resources > Network Devices**. Click **Add**. Provide Name, IP Address, select **TACACS+ Authentication Settings** checkbox and provide Shared Secret key.

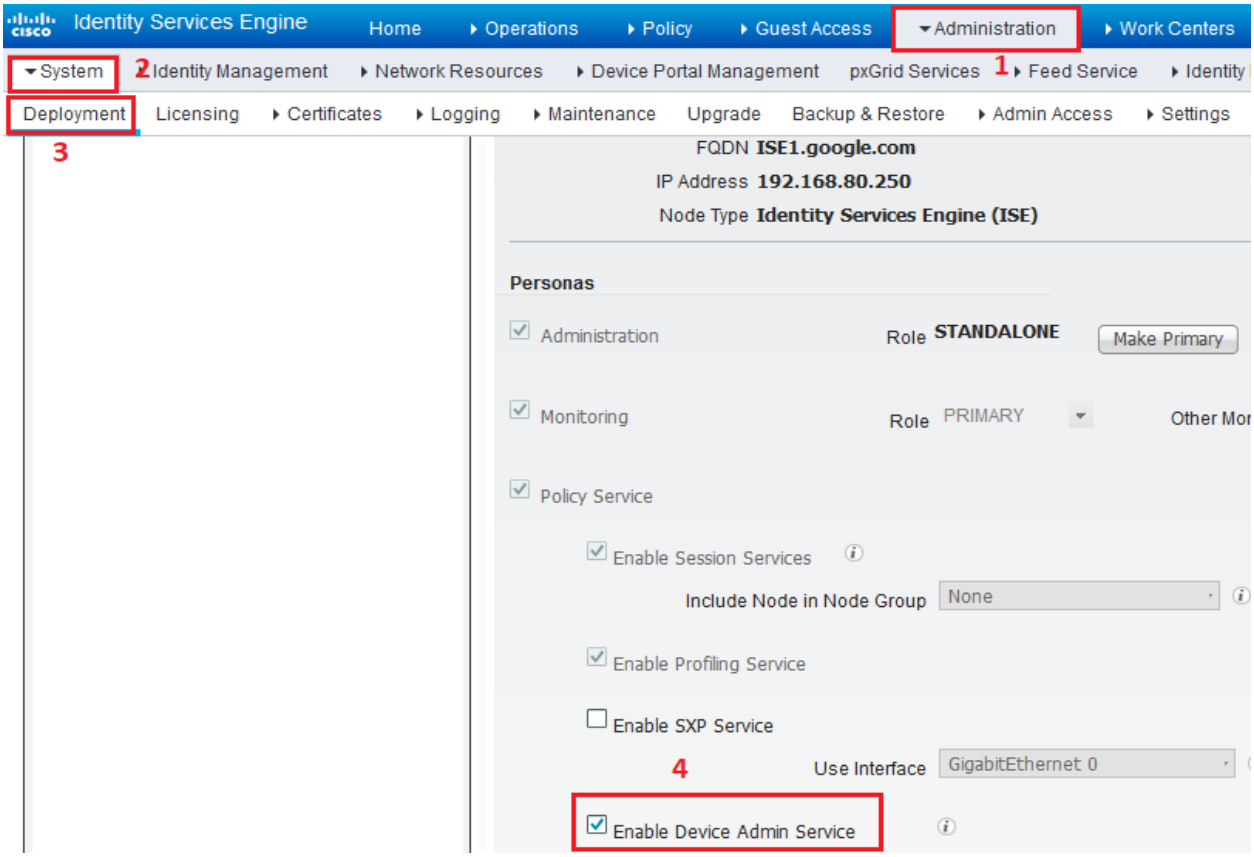


Navigate to **Administration > Network Resources > Network Devices**. Click **Add**. Provide Name, IP Address, select **TACACS+ Authentication Settings** checkbox and provide Shared Secret key.



Enable Device Admin Service:

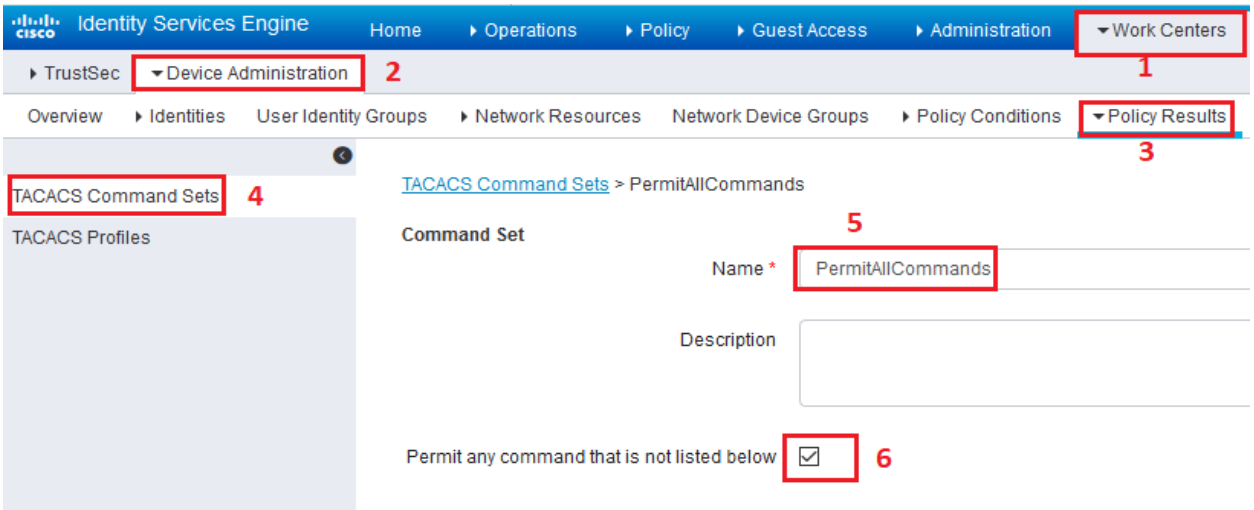
Navigate to **Administration > System > Deployment.** Select required Node. Select **Enable Device Admin Service** checkbox and click "**Save"** to save the setting:



Configuring TACACS Command Sets:

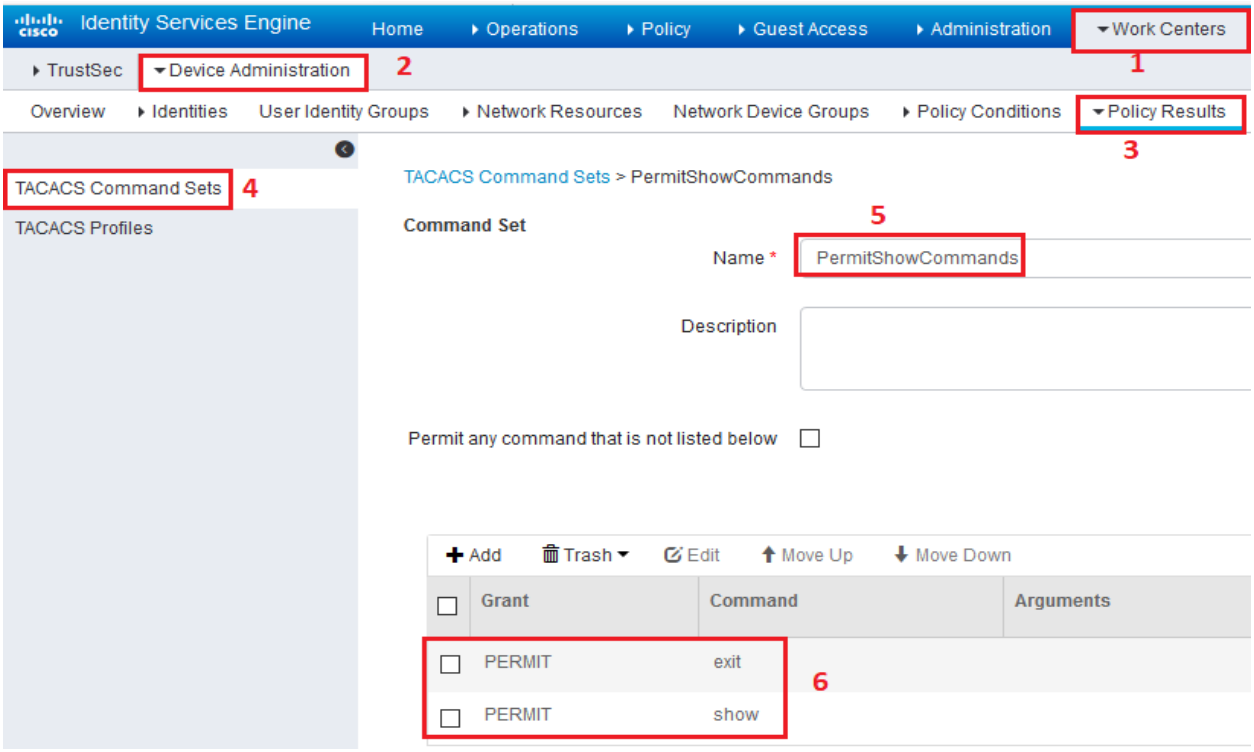
First **PermitAllCommands** for the user admin, which allow all commands on the device. Second **PermitShowCommands** for user **support**, which will allow only show commands.

1. Navigate to **Work Centers > Device Administration > Policy Results > TACACS Command Sets.** Click **Add.** Provide the Name **PermitAllCommands**, select **Permit any command that is not listed below** and click **Submit.**



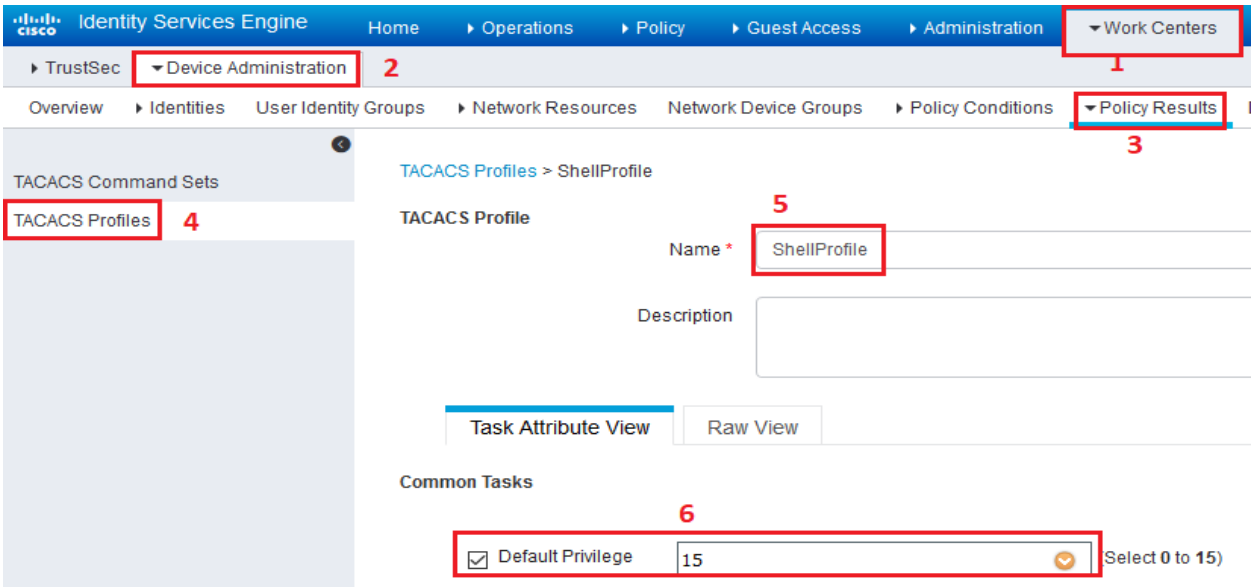
 Created by Ahmad Ali E-Mail: ahmadalimsc@gmail.com , Mobile: 056 430 3717

2. Navigate to **Work Centers > Device Administration > Policy Results > TACACS Command Sets.** Click **Add.** Provide the Name **PermitShowCommands**, click **Add** and permit **show** and **exit** commands. By default if Arguments is left blank, all arguments are be included. Click **Submit.**



Configuring TACACS Profile:

Navigate to **Work Centers > Device Administration > Policy Results > TACACS Profiles.** Click **Add.** Provide Name ShellProfile, select **Default Privilege** checkbox and enter the value of 15. Click **Submit.**

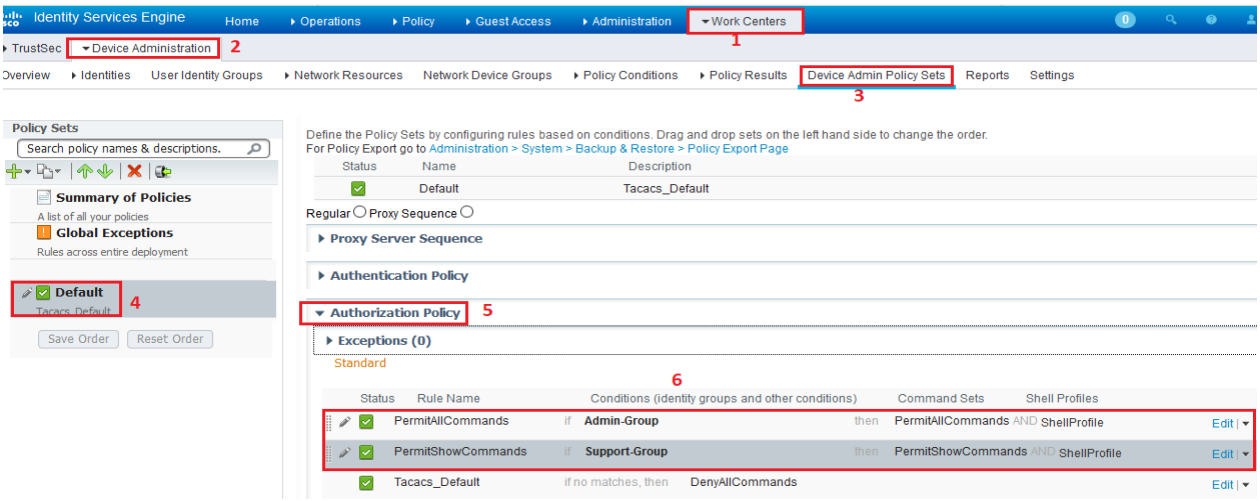


 Created by Ahmad Ali E-Mail: ahmadalimsc@gmail.com , Mobile: 056 430 3717

Configuring TACACS Authorization Policy:

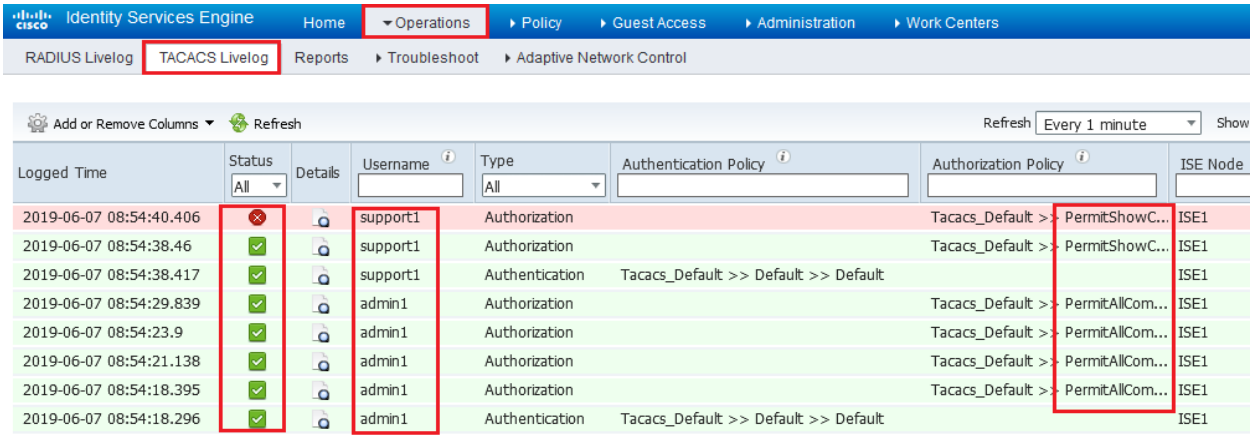
Navigate to **Work Centers > Device Administration > Policy Sets > Default > Authorization Policy > Edit > Insert New Rule Above.**

Two authorization rules are configured, first rule assigns TACACS profile **ShellProfile** and command Set **PermitAllCommands** based on Network **Admin-Group** membership. Second rule assigns TACACS profile **ShellProfile** and command Set **PermitShowCommands** based on Network **Support-Group** membership.



Verify:

Navigate to **Operations > TACACS Livelog.**



Cisco IOS Router Verification.

```
R1#telnet 192.168.80.202
Trying 192.168.80.202 ... Open
Username:support1
Password:

SW1#config t
Command authorization failed.
```