


## Network Access Device:

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

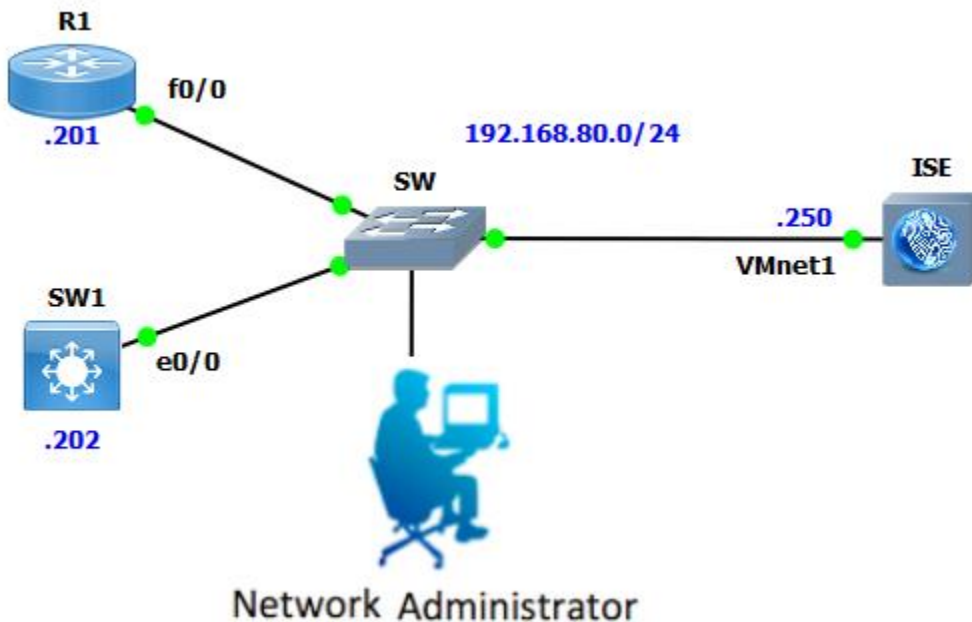


Wireless LAN Controller      Switch

The screenshot shows the Cisco Identity Services Engine (ISE) Administration interface. The navigation menu includes: Administration (1), Network Resources (2), Network Devices (3), Network Device Groups, Network Device Profiles (4), External RADIUS Servers, and RADIUS Server Sequences. The main content area displays the 'Network Devices' page (5) with a table of devices. The 'Add' button (6) is highlighted, and a table entry for 'SW1' is shown with its IP address and profile name.

Name	IP/Mask	Profile Name	Loca
SW1	192.168.80.1...	Cisco	All L

## 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.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation path is: Administration > Identity Management > Groups > User Identity Groups. The 'Groups' menu item is highlighted. The 'User Identity Groups > AAA-Group' page is displayed, showing the configuration for a new 'Identity Group'. The 'Name' field is set to 'Admin-Group' and the 'Description' field is set to 'This is Admin Group'. The 'Save' button is highlighted.

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

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation path is **Administration > Identity Management > Groups > User Identity Groups**. The **Groups** menu item is highlighted. The **User Identity Groups > New User Identity Group** page is displayed. The **Identity Group** is **5**. The **\* Name** field is **Support-Group**. The **Description** is **This is Support Group only Show Commands**. The **Submit** button is highlighted. The **EndPoints** menu item is highlighted. The **Users** menu item is highlighted. The **Latest Manual Network Scan Results** section is visible.

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.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation path is **Administration > Identity Management > Identities > Users**. The **Identities** menu item is highlighted. The **Network Access Users List > admin1** page is displayed. The **Network Access User** is **5**. The **\* Name** is **admin1**. The **Status** is **Enabled**. The **Email** field is empty. The **Passwords** section is **6**. The **\* Login Password** field is **.....**. The **Re-Enter Password** field is **.....**. The **User Information** section is expanded. The **Account Options** section is expanded. The **User Groups** section is **7**. The **Admin-Group** is selected. The **Save** button is highlighted. The **Reset** button is highlighted. The **EndPoints** menu item is highlighted. The **Latest Manual Network Scan Results** section is visible.

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.

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation path is **Administration > Identity Management > Identities > Users**. The main content area is titled **New Network Access User**. The configuration form includes the following fields and sections:

- Name:** \* Name (support1)
- Status:** Status (Enabled)
- Email:** Email
- Passwords:** \* Login Password (masked), Re-Enter Password (masked), Enable Password
- User Information:** (Collapsible section)
- Account Options:** (Collapsible section)
- User Groups:** User Groups (Support-Group)
- Buttons:** Submit, Cancel

### 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.

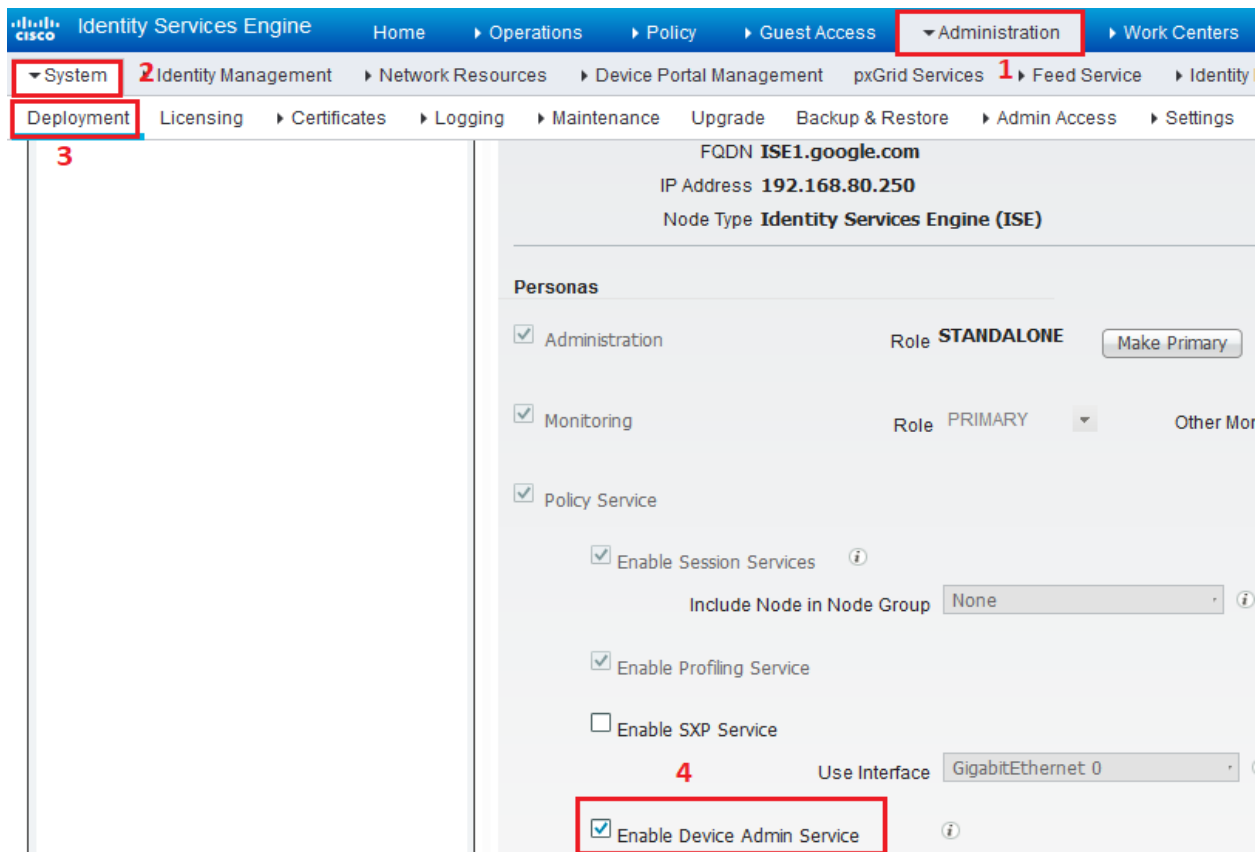
The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The navigation path is Administration > Network Resources > Network Devices. The page shows the configuration for a new network device named 'R1'. The IP address is set to 192.168.80.201 with a subnet mask of 32. The TACACS+ Authentication Settings checkbox is checked. The Shared Secret field is masked with dots. The page also includes sections for SNMP Settings and Advanced TrustSec Settings, and a Save button at the bottom.

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

The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The navigation menu at the top includes 'Administration', 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', 'pxGrid Services', and 'Feed S'. The 'Network Resources' menu is expanded, showing 'Network Devices', 'Network Device Groups', 'Network Device Profiles', 'External RADIUS Servers', and 'RADIUS Server Seq'. The 'Network Devices' section is selected, showing a list of devices with 'S1' highlighted. The configuration page for 'S1' includes fields for Name, Description, and IP Address (192.168.80.202/32). The 'TACACS+ Authentication Settings' section is expanded, showing a 'Shared Secret' field with a 'Show' button, and radio buttons for 'Legacy Cisco Device' (selected) and 'TACACS+ Draft Compliance Single Connect Support'. There are also checkboxes for 'SNMP Settings' and 'Advanced TrustSec Settings'. At the bottom, there are 'Save' and 'Reset' buttons.

### Enable Device Admin Service:

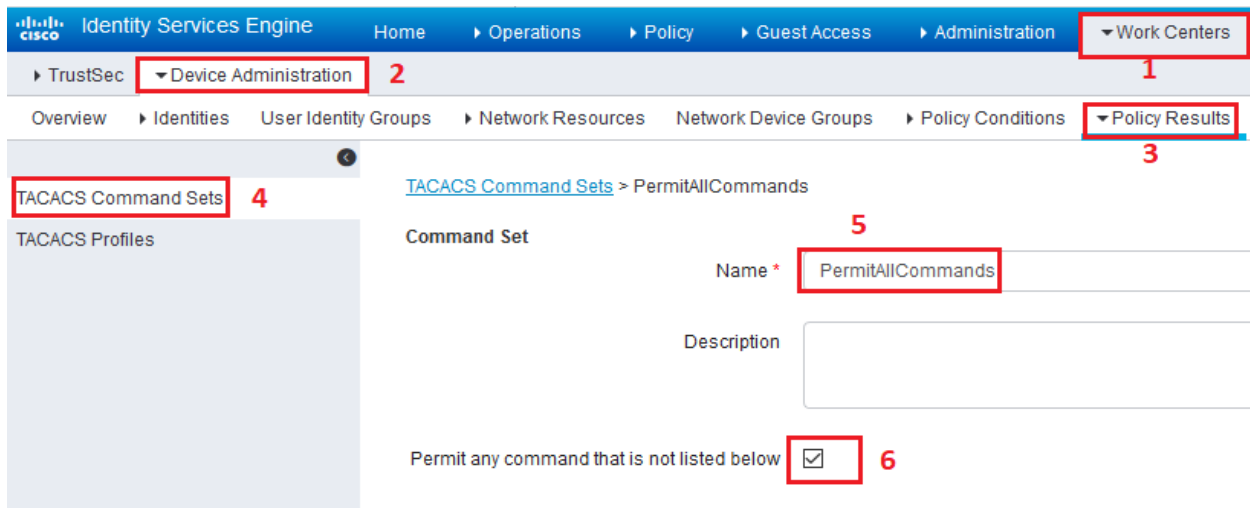
Navigate to **Administration > System > Deployment**. Select required Node. Select **Enable Device Admin Service** checkbox and click **“Save”** to save the setting:



### 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** checkbox that is not listed below and click **Submit**.



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**.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration page for TACACS Command Sets. The breadcrumb navigation is: Home > Operations > Policy > Guest Access > Administration > Work Centers > Device Administration > Policy Results > TACACS Command Sets. The 'Name' field is filled with 'PermitShowCommands'. Below the form, there is a table with columns for 'Grant', 'Command', and 'Arguments'. Two rows are highlighted: one for 'PERMIT' with 'exit' as the command, and another for 'PERMIT' with 'show' as the command.

### 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**.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration page for TACACS Profiles. The breadcrumb navigation is: Home > Operations > Policy > Guest Access > Administration > Work Centers > Device Administration > Policy Results > TACACS Profiles. The 'Name' field is filled with 'ShellProfile'. Below the form, there are tabs for 'Task Attribute View' and 'Raw View'. Under 'Common Tasks', the 'Default Privilege' checkbox is checked, and the value '15' is entered in the adjacent field.

## 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.

Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order. For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Status	Name	Description
<input checked="" type="checkbox"/>	Default	Tacacs_Default

Regular  Proxy Sequence

Proxy Server Sequence

Authentication Policy

Authorization Policy

Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Command Sets	Shell Profiles
<input checked="" type="checkbox"/>	PermitAllCommands	if Admin-Group	then PermitAllCommands AND ShellProfile	
<input checked="" type="checkbox"/>	PermitShowCommands	if Support-Group	then PermitShowCommands AND ShellProfile	
<input checked="" type="checkbox"/>	Tacacs_Default	if no matches, then	DenyAllCommands	

## Verify:

Navigate to **Operations > TACACS Livelog.**

Logged Time	Status	Details	Username	Type	Authentication Policy	Authorization Policy	ISE Node
2019-06-07 08:54:40.406	<input checked="" type="checkbox"/>		support1	Authorization		Tacacs_Default > PermitShowC...	ISE1
2019-06-07 08:54:38.46	<input checked="" type="checkbox"/>		support1	Authorization		Tacacs_Default > PermitShowC...	ISE1
2019-06-07 08:54:38.417	<input checked="" type="checkbox"/>		support1	Authentication	Tacacs_Default >> Default >> Default		ISE1
2019-06-07 08:54:29.839	<input checked="" type="checkbox"/>		admin1	Authorization		Tacacs_Default > PermitAllCom...	ISE1
2019-06-07 08:54:23.9	<input checked="" type="checkbox"/>		admin1	Authorization		Tacacs_Default > PermitAllCom...	ISE1
2019-06-07 08:54:21.138	<input checked="" type="checkbox"/>		admin1	Authorization		Tacacs_Default > PermitAllCom...	ISE1
2019-06-07 08:54:18.395	<input checked="" type="checkbox"/>		admin1	Authorization		Tacacs_Default > PermitAllCom...	ISE1
2019-06-07 08:54:18.296	<input checked="" type="checkbox"/>		admin1	Authentication	Tacacs_Default >> Default >> Default		ISE1

## 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.
  
```