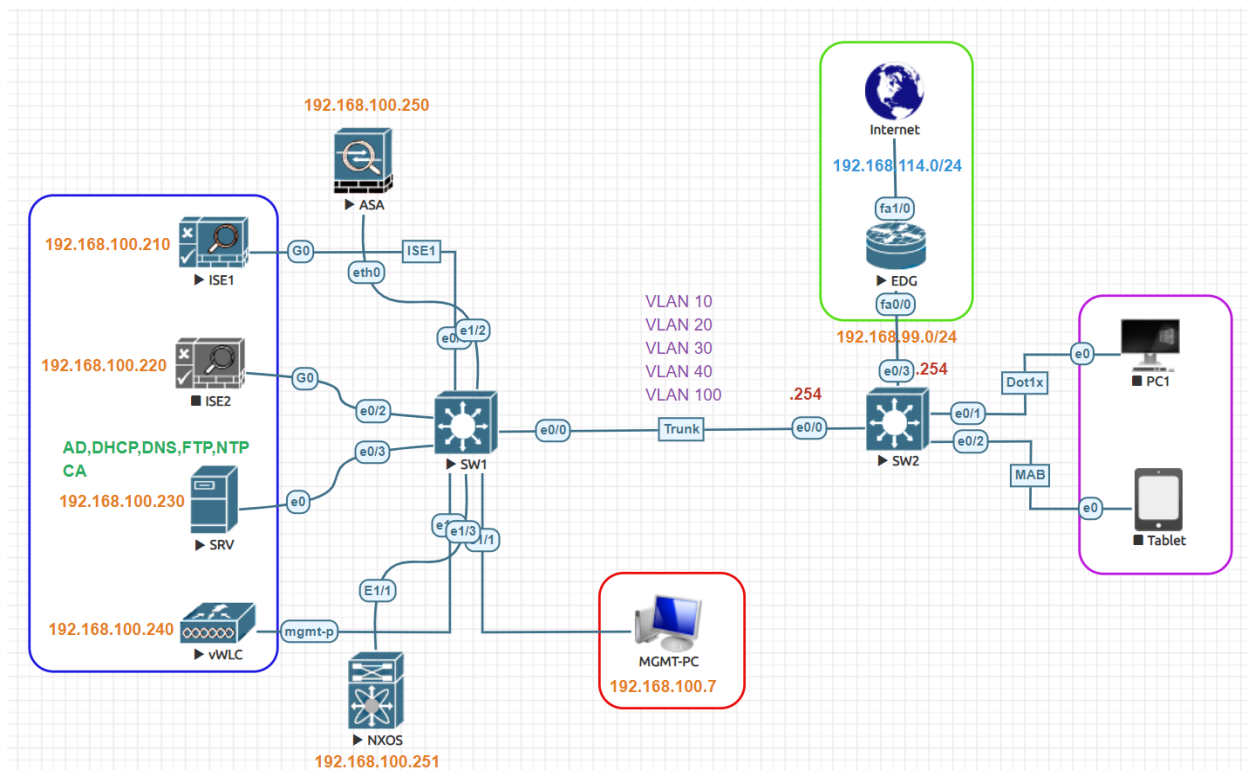


IOS Switch Device Administration Lab:



Cisco ISE Primary IP Address	192.168.100.210
Cisco ISE Secondary IP Address	192.168.100.220
AD, DNS and CA Server IP Address	192.168.100.230
Domain Name:	test.local
Admin Full Access User/Group	Admin1/AdminGroup
Support Readonly Access User/Group	Sup1/SupportGroup
Test VLAN	VLAN 100
VLAN Subnet	192.168.100.0/24
VLAN 100 Gateway	192.168.100.254
Network Device	Cisco IOS Switch
Authentication Switch MGMT IP	192.168.100.254
NXOS TACACS Interface	Ethernet 1/3
Network Device IP Address	192.168.100.254

Enable TACACS+:

Navigate to **Administration > System > Deployment > Under General Setting**, check the box **Enable Device Admin Service**. Click **Save**.

The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration' (highlighted with a red box), and 'Work Centers'. The left sidebar shows the 'System' menu (highlighted with a red box) with sub-items like 'Deployment' (highlighted with a red box) and 'PAN Failover'. The main content area is titled 'Deployment Nodes List > ise1' and shows the 'Edit Node' configuration for 'ise1'. The 'General Settings' tab is selected (highlighted with a red box). The configuration details include:

- Hostname: ise1
- FQDN: ise1.test.local
- IP Address: 192.168.100.210
- Node Type: Identity Services Engine (ISE)

Below the configuration details, the 'Role' is set to 'PRIMARY', and there is a 'Make Standalone' button. The 'Administration' checkbox is checked. The 'Monitoring' checkbox is checked. The 'Policy Service' checkbox is checked, and its sub-items are expanded:

- ☒ Enable Session Services (info icon)
- Include Node in Node Group: None (dropdown menu, info icon)
- ☒ Enable Profiling Service (info icon)
- ☐ Enable Threat Centric NAC Service (info icon)
- ☐ Enable SXP Service (info icon)
- ☒ **Enable Device Admin Service** (info icon) (highlighted with a red box and an arrow)
- ☐ Enable Passive Identity Service (info icon)

The 'pxGrid' checkbox is also checked. At the bottom, the 'Save' button is highlighted with a red box and an arrow, and the 'Reset' button is visible.

Create Device Groups:

Create device groups. We can group devices based on type or location. **Work Centers > Device Administration > Network Resources > Network Device Groups**

Network Device Groups

All Groups Choose group ▾

Refresh Add Duplicate Edit Trash Show group members

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	▼ All Device Types	All Device Types
<input type="checkbox"/>	Firewalls-Cisco	
<input type="checkbox"/>	IOS-Switches	
<input type="checkbox"/>	NX-Switches	

Create Groups and Users:

Create two groups in Active Directory and for test purpose create two users and add them to groups. Two Groups **SupportGroup** and **AdminGroup** and two users **admin1** and **sup1**

Active Directory Users and Computers

Name	Type	Description
SupportGroup	Security Group - Global	
Limited	Security Group - Global	
Gust	Security Group - Global	
Employees	Security Group - Global	
Contractor	Security Group - Global	
AdminGroup	Security Group - Global	
support	User	
l1	User	
g1	User	
e1	User	
c1	User	
admin	User	

Choose **Administration > Identity Management > External Identity Sources > Active Directory**. Click the **Groups** Tab. Click on Add and then Select Groups from Directory.

Adding Network Devices:

Work Centers > Device Administration > Network Resources > Network Devices. Click **Add**
Provide Name & IP address of Network device to be added. Select device group.

Network Devices

Default Device

Device Security Settings

Network Devices List > New Network Device

Network Devices

* Name: SW2

Description: SW2

IP Address: 192.168.100.254 / 32

* Device Profile: Cisco

Model Name: ADVENTERPRI

Software Version: 15.2

* Network Device Group

Location: All Locations

Is IPSEC Device: Is IPSEC Device

Device Type: All Device Types

Configure TACACS authentication Settings put Shared Secret Key in this case **Test123**

☐ RADIUS Authentication Settings

☒ TACACS Authentication Settings

Shared Secret: Test123

Enable Single Connect Mode: ☐

Legacy Cisco Device

TACACS Draft Compliance Single Connect Support

☐ SNMP Settings

☐ Advanced TrustSec Settings

Submit

Create Command Sets:

We will create two TACACS Command Sets for each profile. Navigate to **Work Centers > Device Administration > Policy Elements > Results > TACACS Command Sets**. Click **Add**

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The left sidebar shows a tree view with 'Conditions', 'Network Conditions', 'Results' (selected), and 'TACACS Profiles'. The main content area is titled 'TACACS Command Sets' and shows a list of command sets. A red arrow points to the '+ Add' button. The list contains three items: 'Name' (with a checkbox), 'ASA-Full-Access' (with a checkbox), and 'DenyAllCommands' (with a checkbox and 'Default C' label).

For example, we have created **IOS_Admin** which allows all commands. Check the box under Commands 'Permit any command that is not listed below' and don't add any command.

The screenshot shows the configuration page for the 'IOS_Admin' TACACS Command Set. The breadcrumb trail is 'TACACS Command Sets > IOS_Admin'. The 'Command Set' section has a 'Name' field with 'IOS_Admin' and a 'Description' field. The 'Commands' section has a checkbox labeled 'Permit any command that is not listed below' which is checked. The left sidebar shows the same tree view as the previous screenshot, with 'Results' selected and 'TACACS Command Sets' highlighted.

Another command set named **IOS_Support** is created that allows only show and few other commands. * is used for wild card.

► Conditions

► Network Conditions

▼ Results

Allowed Protocols

TACACS Command Sets

TACACS Profiles

TACACS Command Sets > IOS_Support

Command Set

Name

Description

Commands

Permit any command that is not listed below ☐

+ Add
🗑️ Trash ▼
✎ Edit
⬆ Move Up
⬇ Move Down

<input type="checkbox"/>	Grant	Command	Arguments
<input type="checkbox"/>	PERMIT	end	
<input type="checkbox"/>	PERMIT	exit	
<input type="checkbox"/>	PERMIT	show*	

Create TACACS Profiles:

Let's create two TACACS Profiles for our Admins and Support Users. Navigate to **Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles** click **Add**.

► Conditions

► Network Conditions

▼ Results

Allowed Protocols

TACACS Command Sets

TACACS Profiles

TACACS Profiles

0 Selected

🔄 Refresh

+ Add

📄 Duplicate
🗑️ Trash ▼
✎ Edit

<input type="checkbox"/>	Name	Type	Description
<input type="checkbox"/>	ASAAdmin Pro	Shell	
<input type="checkbox"/>	Default Shell Profile	Shell	Default Shell Profile
<input type="checkbox"/>	Deny All Shell Profile	Shell	Deny All Shell Profile
<input type="checkbox"/>	WLC ALL	WLC	WLC ALL
<input type="checkbox"/>	WLC MONITOR	WLC	WLC MONITOR

► Conditions

► Network Conditions

▼ Results

Allowed Protocols

TACACS Command Sets

TACACS Profiles

TACACS Profiles > IOS_AdminProfile

TACACS Profile

Name **IOS_AdminProfile**

Description

Task Attribute View

Raw View

Common Tasks

Common Task Type **Shell**

☒ Default Privilege **15** (Select 0 to 15)

☒ Maximum Privilege **15** (Select 0 to 15)

☐ Access Control List

☐ Auto Command

☐ No Escape (Select true or false)

☐ Timeout Minutes (0-9999)

☐ Idle Time Minutes (0-9999)

► Conditions

► Network Conditions

▼ Results

Allowed Protocols

TACACS Command Sets

TACACS Profiles

TACACS Profiles > IOS_SupportProfile

TACACS Profile

Name **IOS_SupportProfile**

Description

Task Attribute View

Raw View

Common Tasks

Common Task Type **Shell**

☒ Default Privilege **5** (Select 0 to 15)

☒ Maximum Privilege **7** (Select 0 to 15)

☐ Access Control List

☐ Auto Command

☐ No Escape (Select true or false)

☐ Timeout Minutes (0-9999)

☐ Idle Time Minutes (0-9999)

Device Administration Policy:

Here we will call all the items configured earlier. Navigate to **Work Centers > Device Administration > Device Admin Policy Sets** and add new policy or use default. Click small arrow button on right side of policy to expand.

Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Devices-Admin	TACACS Policy	Network Access Protocol EQUALS TACACS+	Default Device Admin			
✓	Default	Tacacs Default policy set		Default Device Admin	2		

Create **Authentication Policy** and use internal or external users in our case both.

Authentication Policy (2)

Status	Rule Name	Conditions	Use
✓	Auth-Device	Network Access Protocol EQUALS TACACS+	Test-AD Options
✓	Default		All_User_ID_Stores Options

Then, configure authorization Policies under '**Authorization Policy**'.

Authorization Policy

Policy Group	Condition	Profile
Author-AdminGroup-IOS	Test-AD: ExternalGroups EQUALS test.local/ISE/AdminGroup DEVICE: Device Type EQUALS All Device Types#IOS-Switches	IOS_AdminProfile
Author-SupportGroup-IOS	Test-AD: ExternalGroups EQUALS test.local/ISE/SupportGroup DEVICE: Device Type EQUALS All Device Types#IOS-Switches	IOS_SupportProfile

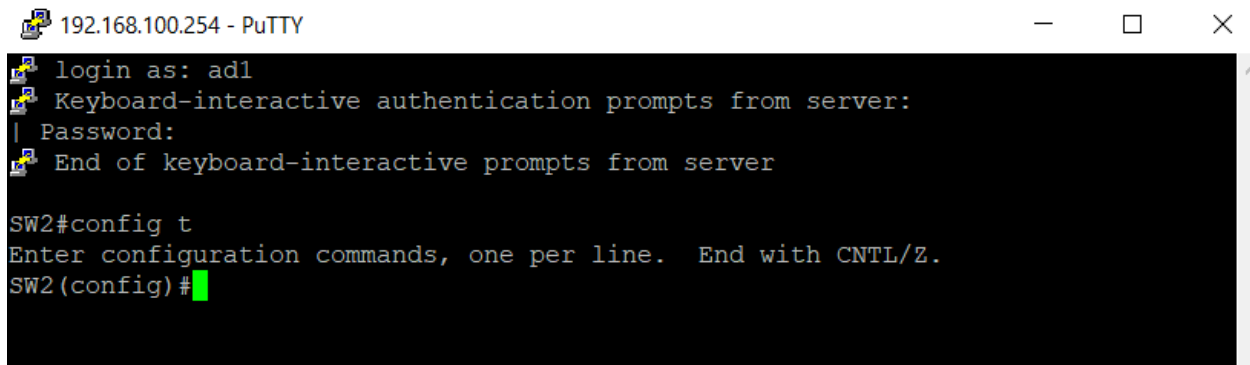
Cisco IOS Switch Configuration:

```
SW2(config)#aaa new-model
SW2(config)#tacacs server ISE
SW2(config-server-tacacs)#address ipv4 192.168.100.210
SW2(config-server-tacacs)#key Test123
SW2(config)#aaa authentication login default group tacacs+ local
SW2(config)#aaa authentication enable default group tacacs+ enable
SW2(config)#aaa authorization exec default group tacacs+ local
SW2(config)#aaa authorization commands 0 default group tacacs+ local
SW2(config)#aaa authorization commands 1 default group tacacs+ local
SW2(config)#aaa authorization commands 15 default group tacacs+ local
SW2(config)#aaa authorization config-commands
SW2(config)#aaa accounting exec default start-stop group tacacs+
SW2(config)#aaa accounting commands 0 default start-stop group tacacs+
SW2(config)#aaa accounting commands 1 default start-stop group tacacs+
SW2(config)#aaa accounting commands 15 default start-stop group tacacs+
SW2(config)#aaa accounting connection default start-stop group tacacs+

SW2(config)#line vty 0 4
SW2(config-line)#authorization commands 0 default
SW2(config-line)#authorization commands 1 default
SW2(config-line)#authorization commands 15 default
SW2(config-line)#authorization exec default
SW2(config-line)#login authentication default
SW2(config-line)#accounting exec default
SW2(config-line)#accounting commands 0 default
SW2(config-line)#accounting commands 1 default
SW2(config-line)#accounting commands 15 default
SW2(config-line)#accounting connection default
```

Testing and Verification:

We can test our configuration by login into the Cisco IOS Switch by SSH. Let's try using the **ad1** user credential.



```
192.168.100.254 - PuTTY
login as: ad1
Keyboard-interactive authentication prompts from server:
| Password:
| End of keyboard-interactive prompts from server

SW2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
SW2(config)#
```

We can monitor the authentication/authorization logs on ISE **Operations > TACACS > Live Logs**. The **ad1** user was successfully authenticated and authorized to run privileged commands.

Overview

Request Type	Authorization
Status	Pass
Session Key	ise1/428077735/91
Message Text	Device-Administration: Command Authorization succeeded
Username	ad1
Authorization Policy	Device-Policy >> Author-AdminGroup-IOS
Shell Profile	
Matched Command Set	IOS_Admin
Command From Device	configure terminal

Now let's try again using support account users **sp1**. The user **sp1** was successfully authenticated but wasn't authorized to run privileged commands.

```
192.168.100.254 - PuTTY
login as: sp1
Keyboard-interactive authentication prompts from server:
| Password:
| End of keyboard-interactive prompts from server

SW2#config t
      ^
% Invalid input detected at '^' marker.

SW2#
```

We can monitor the authentication/authorization logs on ISE **Operations > TACACS > Live Logs**.

Overview

Request Type	Authorization
Status	Pass
Session Key	ise1/428077735/94
Message Text	Device-Administration: Session Authorization succeeded
Username	sp1
Authorization Policy	Device-Policy >> Author-SupportGroup-IOS
Shell Profile	IOS_SupportProfile
Matched Command Set	
Command From Device	