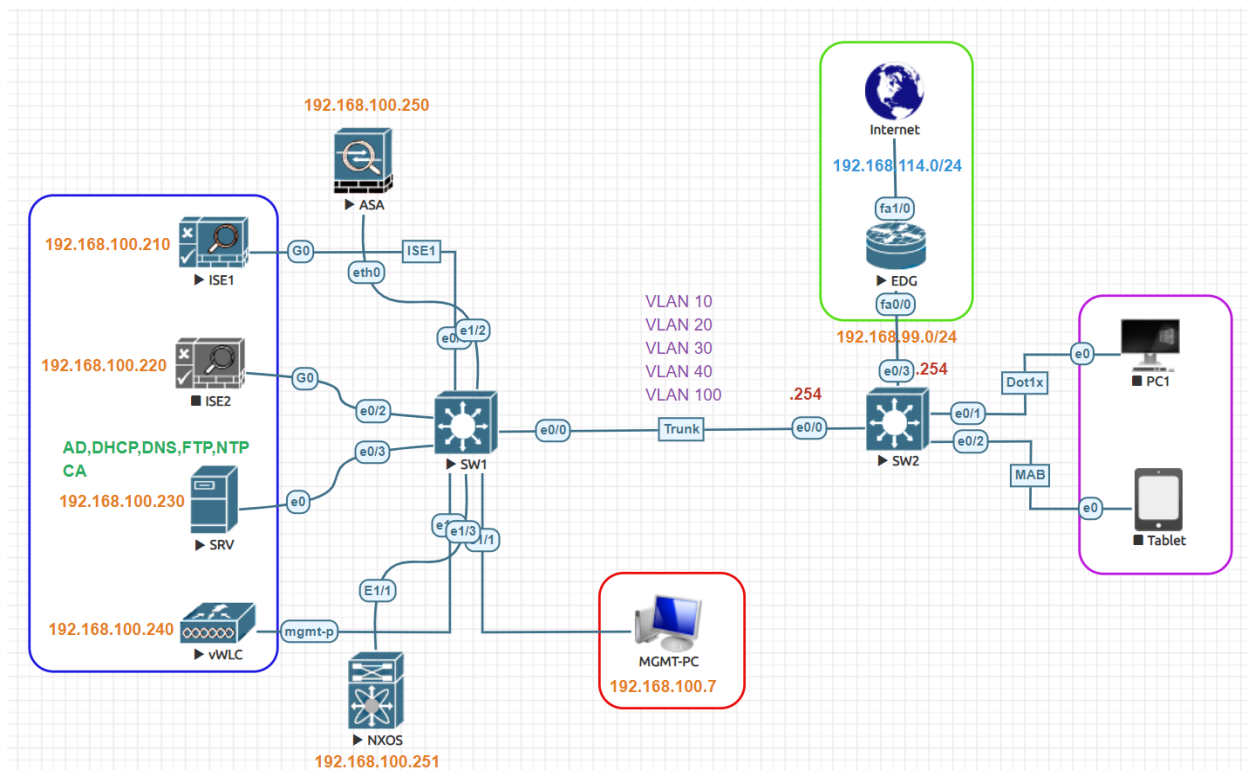


## WLC Device Administration Lab:



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 vWLC
Authentication Switch MGMT IP	192.168.100.254
vWLC TACACS Interface	MGMT Port
Network Device IP Address	192.168.100.240

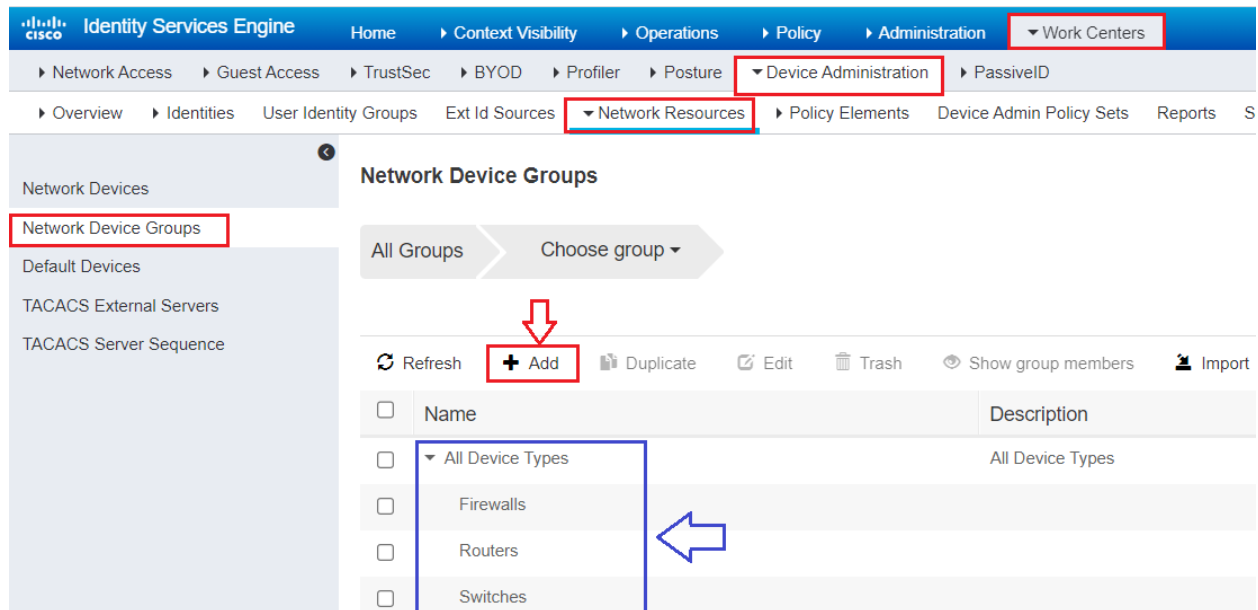
## Enable TACACS+:

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), and 'Work Centers'. The left sidebar shows 'System' (highlighted) with sub-items like 'Deployment' (highlighted), 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Backup & Restore', 'Admin Access', and 'Settings'. The main content area is titled 'Deployment Nodes List > ise1' and 'Edit Node'. The 'General Settings' tab is selected, showing fields for Hostname (ise1), FQDN (ise1.test.local), IP Address (192.168.100.210), and Node Type (Identity Services Engine (ISE)). Below these, the 'Role' is set to 'PRIMARY' with a 'Make Standalone' button. A list of services is shown with checkboxes: Administration, Monitoring, Policy Service (expanded), Enable Session Services, Include Node in Node Group (set to None), Enable Profiling Service, Enable Threat Centric NAC Service, Enable SXP Service, **Enable Device Admin Service** (checked and highlighted with a red box and an arrow), and Enable Passive Identity Service. The 'pxGrid' checkbox is also checked. At the bottom, the 'Save' button is highlighted with a red box and an arrow, next to a 'Reset' button.

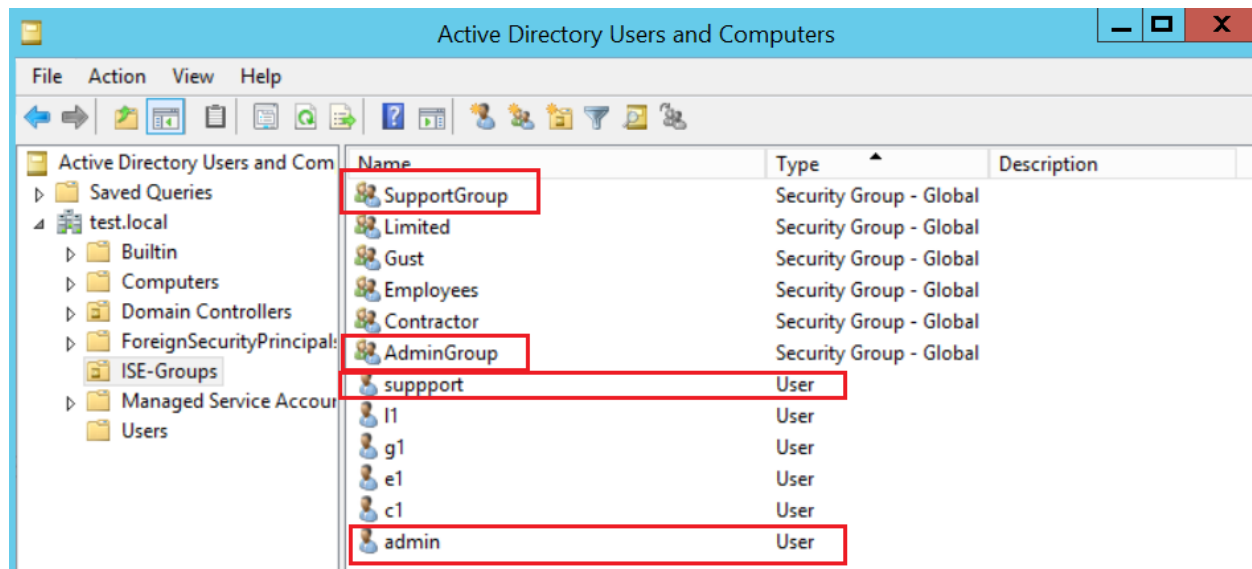
## Create Device Groups:

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



## 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**



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.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Ce

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Mana

Network Devices List > WLC1

**Network Devices**

\* Name WLC1

Description Wireless LAN Controller

IP Address \* IP : 192.168.100.240 / 32

\* Device Profile AlcatelWired

Model Name

Software Version

\* Network Device Group

Location All Locations Set To Default

IPSEC No Set To Default

Device Type WLC Set To Default

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

☐ RADIUS Authentication Settings

☒ TACACS Authentication Settings

Shared Secret Test123 Hide

Enable Single Connect Mode ☐

☒ Legacy Cisco Device

☐ TACACS Draft Compliance Single Connect Support

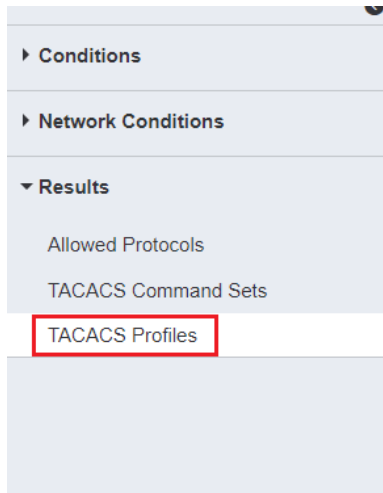
☐ SNMP Settings

☐ Advanced TrustSec Settings

Submit Cancel

## Create TACACS Profiles:

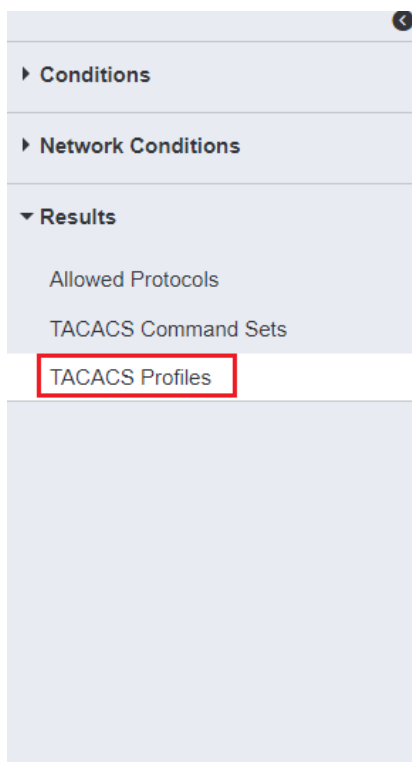
Let's create two TACACS Profiles for our Admins and Support Users. Navigate to **Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles** click **Add**.



### 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		



TACACS Profiles > WLC ALL

### TACACS Profile

Name WLC ALL

Description WLC ALL

Task Attribute View

Raw View

### Common Tasks

Common Task Type WLC

☒ All

☐ Monitor

☐ Lobby

☐ Selected

TACACS Profiles > WLC MONITOR

### TACACS Profile

Name

Description

**Task Attribute View** **Raw View**

### Common Tasks

Common Task Type

☐ All  
☒ Monitor  
☐ Lobby  
☐ Selected

Identity Services Engine Home Context Visibility Operations Policy Administration **Work Centers**

Network Access Guest Access TrustSec BYOD Profiler Posture **Device Administration** PassiveID  
 Overview Identities User Identity Groups Ext Id Sources Network Resources **Policy Elements** Device Admin Policy Sets R

### TACACS Profiles

Refresh Add Duplicate Trash Edit

<input type="checkbox"/>	Name	Type	Description
<input type="checkbox"/>	ASAAdmin Pro	Shell	
<input type="checkbox"/>	ASA Read Only	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

default Profile →

## 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		

Reset Policyset Hitcounts Reset Save

Reset Save

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

Policy Sets → Devices-Admin

Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits
✓	Default	Test_Identity_Stores		0

Options

Then, configure authorization Policies under 'Authorization Policy'.

▼ Authorization Policy (3)

				Results	
	Status	Rule Name	Conditions	Command Sets	Shell Profiles
Search					
	✓	ASA-Firewall-Admin	<div><div></div>ad.test.local-ExternalGroups EQUALS test.local/ISE-Groups/AdminGroup</div>	<div>× ASA-Admin</div> <div>+</div>	<div>ASA Admin Pro</div> <div>×</div> <div>+</div>
	✓	ASA-Firewall-Readonly	<div><div></div>ad.test.local-ExternalGroups EQUALS test.local/ISE-Groups/SupportGroup</div>	<div>× ASA-ReadOnly</div> <div>+</div>	<div>ASA Read Only</div> <div>×</div> <div>+</div>
<div></div>	✓	WLC-Admin	<div>AND</div> <div><div><div></div>ad.test.local-ExternalGroups EQUALS test.local/ISE-Groups/AdminGroup</div><div><div></div>DEVICE Device Type EQUALS All Device Types#WLC</div></div>	<div>Select from list</div> <div>+</div>	<div>WLC ALL</div> <div>×</div> <div>+</div>
<div></div>	✓	WLC-Readonly	<div>AND</div> <div><div><div></div>ad.test.local-ExternalGroups EQUALS test.local/ISE-Groups/SupportGroup</div><div><div></div>DEVICE Device Type EQUALS All Device Types#WLC</div></div>	<div>Select from list</div> <div>+</div>	<div>WLC MONITOR</div> <div>×</div> <div>+</div>
	✓	Default		<div>× DenyAllCommands</div> <div>+</div>	<div>Deny All Shell Profile</div> <div>×</div> <div>+</div>

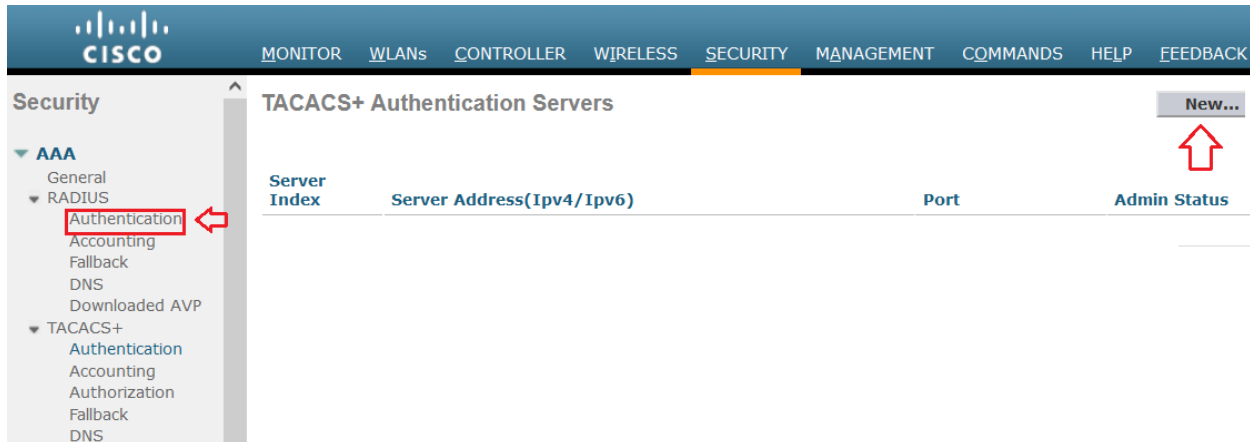
✓	WLC-Admin	AND	<div><div><div></div>ad.test.local-ExternalGroups EQUALS test.local/ISE-Groups/AdminGroup</div><div><div></div>DEVICE Device Type EQUALS All Device Types#WLC</div></div>	<div>WLC ALL</div> <div>×</div> <div>+</div>
✓	WLC-Readonly	AND	<div><div><div></div>ad.test.local-ExternalGroups EQUALS test.local/ISE-Groups/SupportGroup</div><div><div></div>DEVICE Device Type EQUALS All Device Types#WLC</div></div>	<div>WLC MONITOR</div> <div>×</div> <div>+</div>



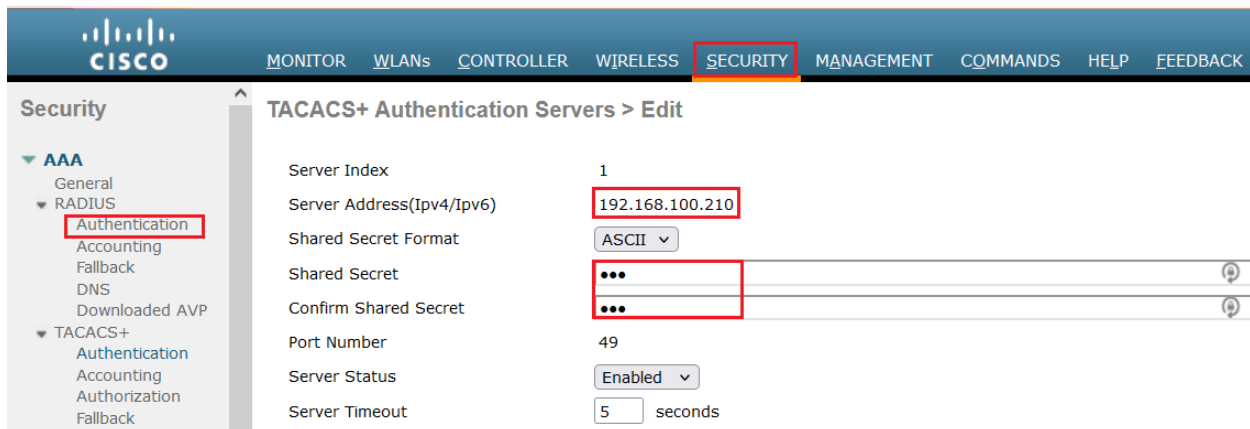
## Cisco WLC Configuration:

Now that we have all our profiles, policy sets, and rules are in place, we just need to tell the wireless controller to use TACACS+ for auth.

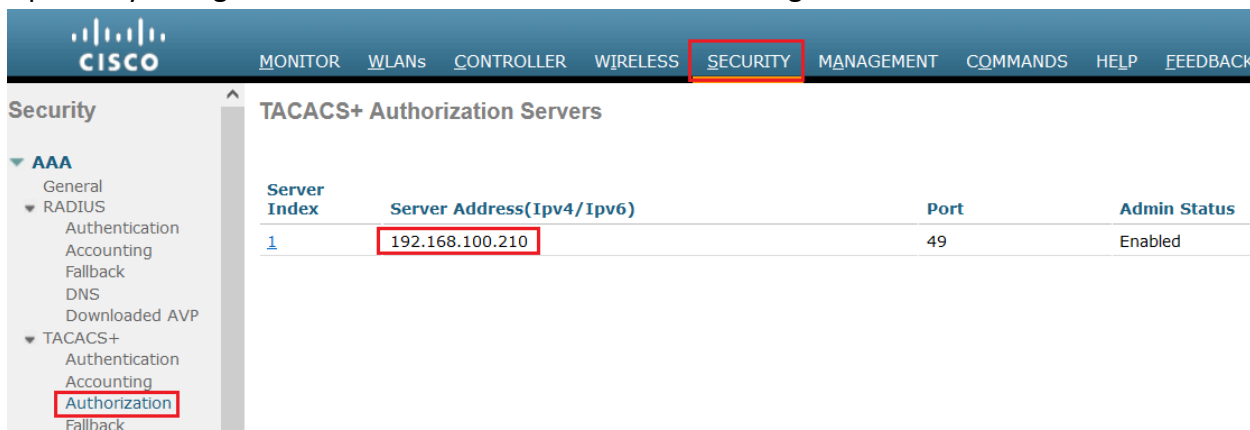
Log into your WLC web gui and navigate to **Advanced -> Security -> AAA -> TACACS+ -> Authentication** and click on **New...** in the upper right corner.



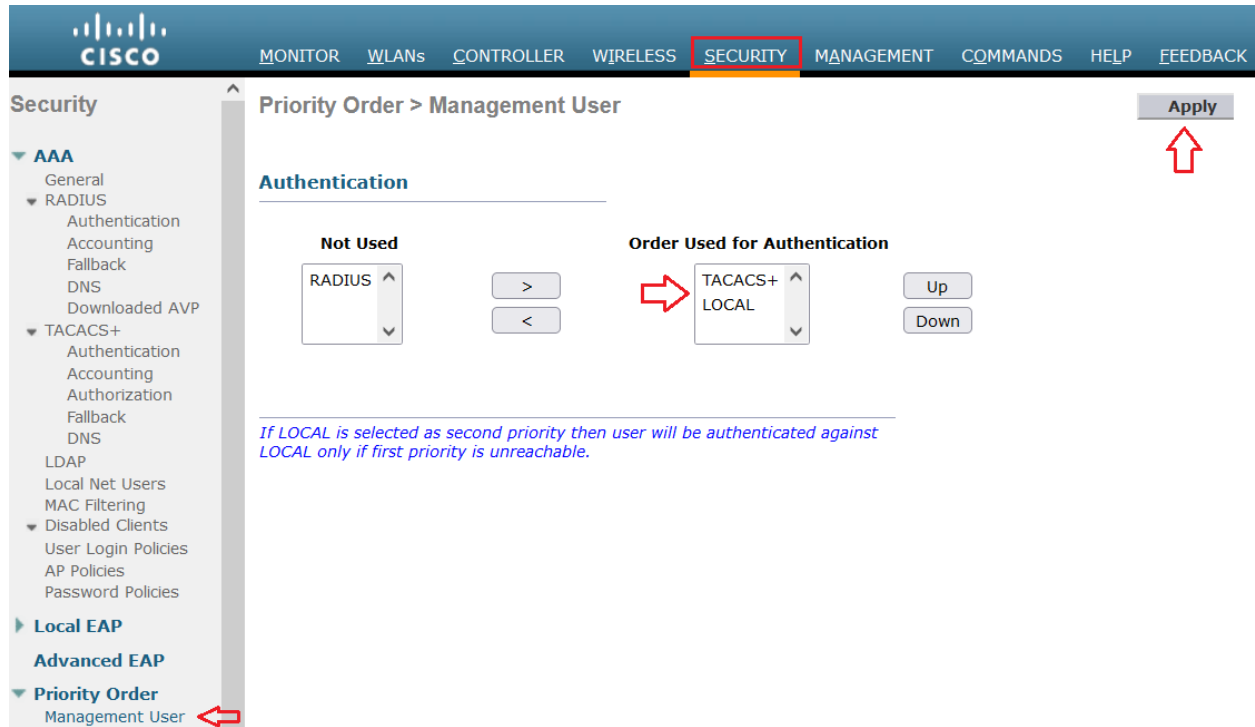
Enter the IP of your Cisco ISE server as well as your Shared Secret and click **Apply**.



Optionally configure same like authentication the Accounting and Authorization screen.



Expand **Priority Order** and move **TACACS+** to the top of the Order Used for Authentication and click **Apply**.



The screenshot shows the Cisco Security Configuration Interface. The top navigation bar includes links for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY (highlighted with a red box), MANAGEMENT, COMMANDS, HELP, and FEEDBACK. On the left, the 'Security' sidebar is expanded to show 'AAA' > 'TACACS+' > 'Authentication' > 'Priority Order' > 'Management User', with a red arrow pointing to the 'Management User' link. The main content area is titled 'Priority Order > Management User' and features an 'Apply' button in the top right corner, indicated by a red arrow. Under the 'Authentication' section, there are two columns: 'Not Used' and 'Order Used for Authentication'. The 'Not Used' column contains a dropdown menu with 'RADIUS' selected. The 'Order Used for Authentication' column contains a dropdown menu with 'TACACS+' and 'LOCAL' listed, with 'TACACS+' at the top. A red arrow points to the 'TACACS+' entry in this list. To the right of the dropdown are 'Up' and 'Down' buttons. Below these columns, a blue italicized note states: 'If LOCAL is selected as second priority then user will be authenticated against LOCAL only if first priority is unreachable.'

## Testing and Verification:

We can test our configuration by login into the Cisco WLC through GUI. Let's try using the **admin1** user credential.

192.168.100.240

This site is asking you to sign in.

Username

admin1

Password

.....

Sign in Cancel

Welcome! Please click the login button to enter your user name and password

Login

We can monitor the authentication/authorization logs on ISE **Operations > TACACS > Live Logs**. The **admin1** user was successfully authenticated and authorized to run privileged commands.

Refresh Export To

Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device ...	Network Device IP
		Identity		Authentication Policy	Authorization Policy	Ise Node	Network Device Nam	
✓		admin1	Authorization		Devices-Admin >> WLC-Admin	ise1	WLC1	192.168.100.240
✓		admin1	Authentication	Devices-Admin >> Default		ise1	WLC1	192.168.100.240
✗		admin1	Authentication	Devices-Admin >> Default		ise1	WLC1	192.168.100.240
✓		admin1	Authorization		Devices-Admin >> WLC-Admin	ise1	WLC1	192.168.100.240

Now let's try again using support account users **sup1**. The user **sup1** was successfully authenticated but wasn't authorized to run privileged commands.

https://192.168.100.240/index.html

192.168.100.240

This site is asking you to sign in.

Username

sup1

Password

.....

Sign in Cancel

Try to delete or modify something it will give authorization failed message.

https://192.168.100.240/screens/frameset.html

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs

Current Filter: [Change Filter] [Clear Filter] Create New

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status
1	WLAN	TestSSID	TestSSID	Enabled

192.168.100.240

Authorization Failed. No sufficient privileges

☐ Don't allow 192.168.100.240 to prompt you again

OK

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

The screenshot displays the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations' (highlighted), 'Policy', 'Administration', and 'Work Centers'. Below this, the 'TACACS' menu item is selected, showing options for 'RADIUS', 'Threat-Centric NAC Live Logs', 'Troubleshoot', 'Adaptive Network Control', and 'Reports'. The 'Live Logs' link is also highlighted. The main content area shows a table of logs with columns for Status, Details, Identity, Type, Authentication Policy, and Authorization Policy. Two log entries are visible, both for the identity 'sup1'.

Status	Details	Identity	Type	Authentication Policy	Authorization Policy
✓		sup1	Authorization	Authentication Policy	Devices-Admin >> WLC-Readonly
✓		sup1	Authentication	Devices-Admin >> Default	