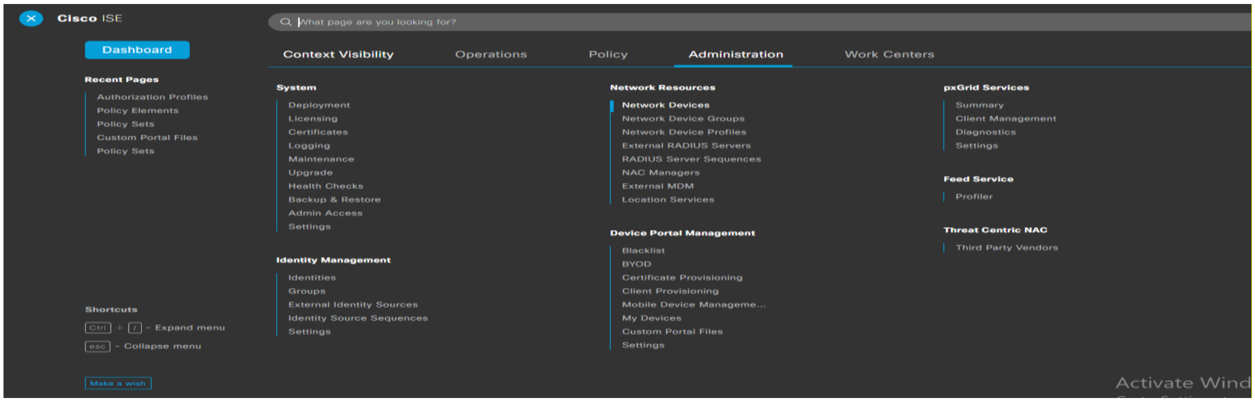
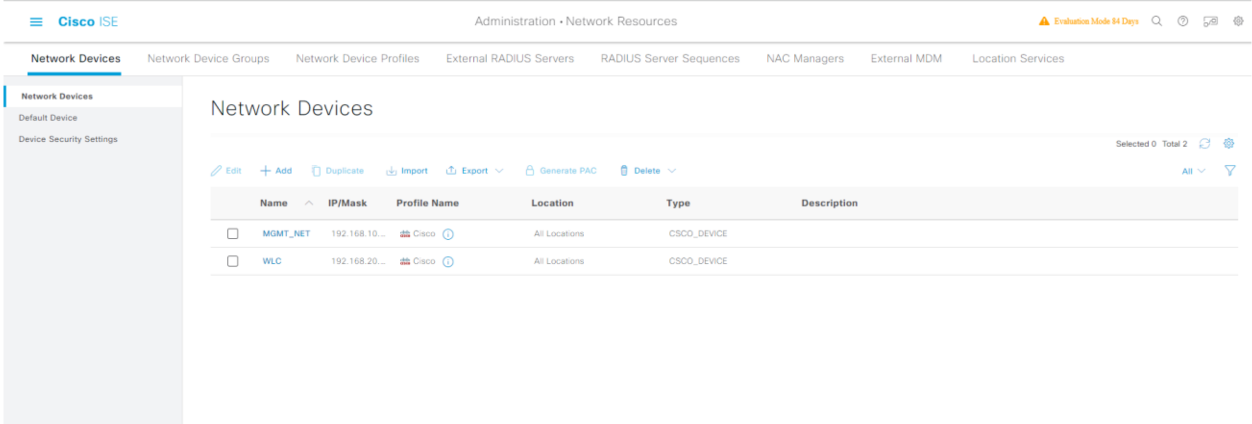
Project Name: Cisco ISE integration with Cisco WLC for an Government organization

Cisco ISE configuration

After login to ISE, we will get a **Dashboard** like below. To add integrated network devices with ISE, we have to select **Administration -> Network Resources** -> **Network Devices** tab.

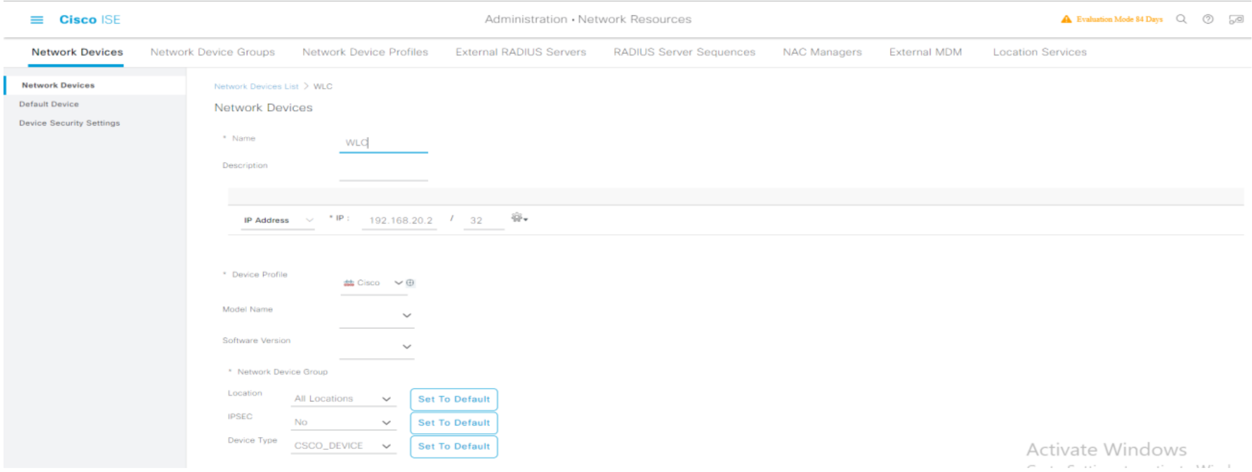


Click on ‘**Network Devices** and **Add** new devices like below:



	Name	IP/Mask	Profile Name	Location	Type	Description
□	MGMT_NET	192.168.10...	Cisco	All Locations	CSCO_DEVICE	
□	WLC	192.168.20...	Cisco	All Locations	CSCO_DEVICE	

Set **Name, Device Profile, IP Address and Device** type like below:



Network Devices

* Name: WLC

Description:

IP Address · * IP : 192.168.20.2 / 32

* Device Profile: Cisco

Model Name:

Software Version:

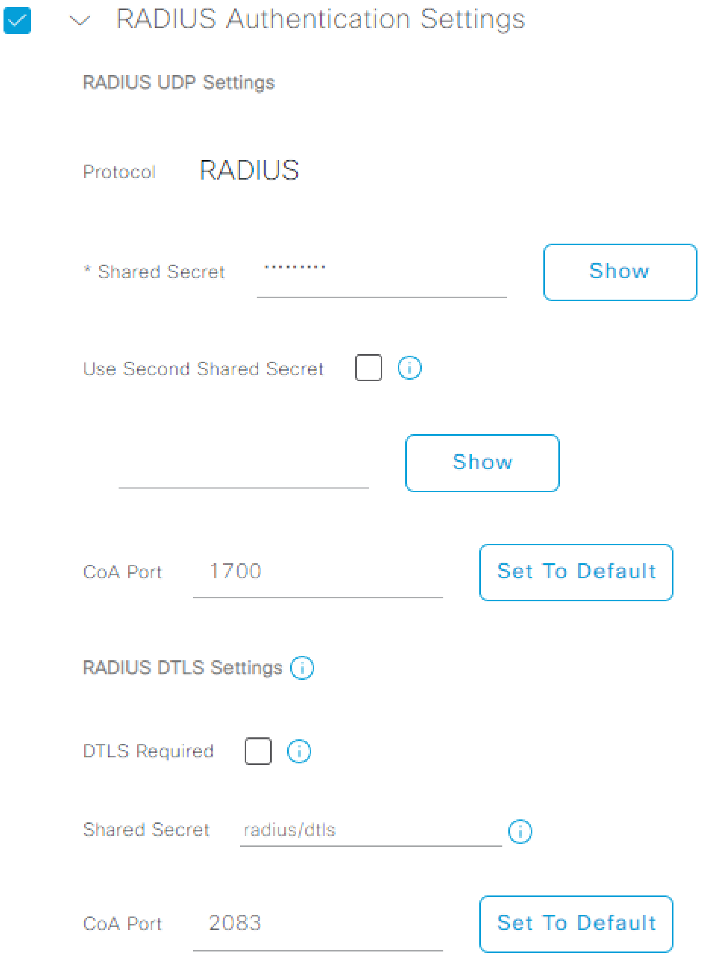
* Network Device Group

Location: All Locations — Set To Default

IPSEC: No — Set To Default

Device Type: CSCO_DEVICE — Set To Default

Configuring RADIUS settings. Same shared secret key needs to be set for WLC and ISE integration. Ports are set by default and Save it.



☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

* Shared Secret ········· Show

Use Second Shared Secret □

Show

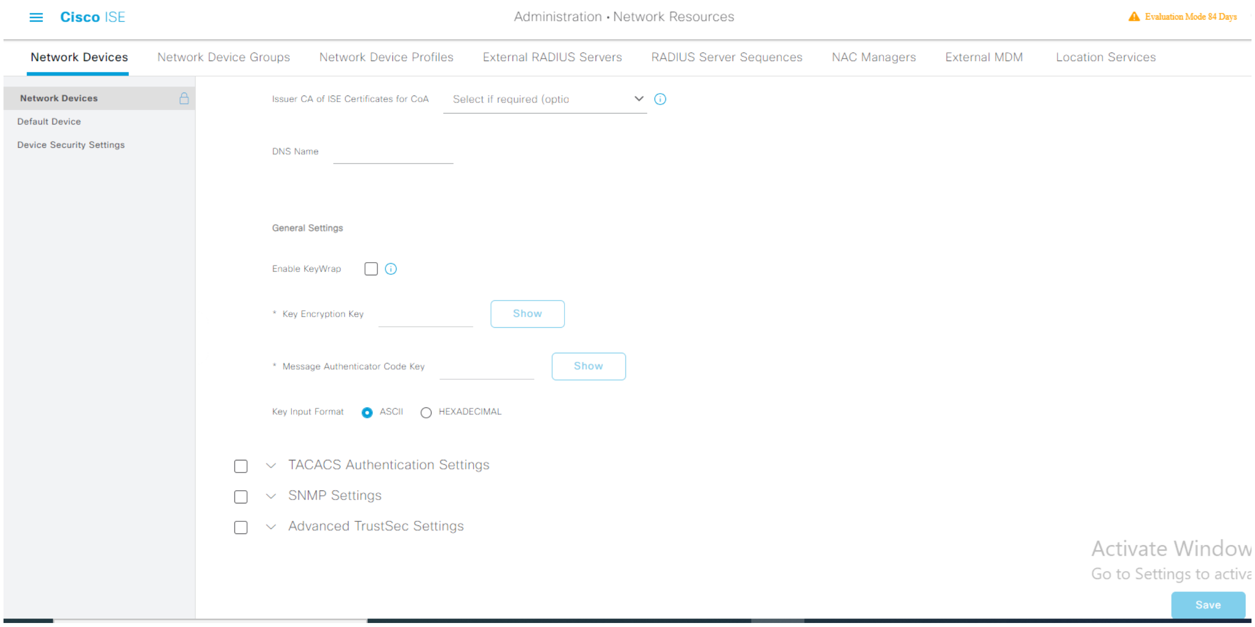
CoA Port 1700 Set To Default

RADIUS DTLS Settings

DTLS Required □

Shared Secret radius/dtls

CoA Port 2083 Set To Default



Issuer CA of ISE Certificates for CoA: Select if required (optio

DNS Name

General Settings

Enable KeyWrap □

* Key Encryption Key [Show]

* Message Authenticator Code Key [Show]

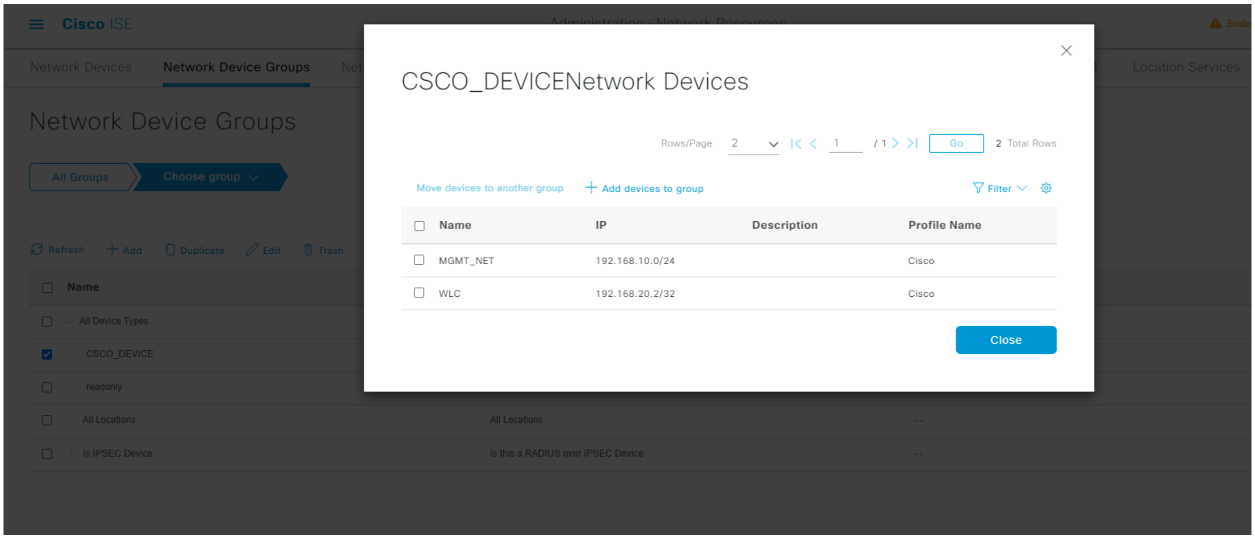
Key Input Format ● ASCII ○ HEXADECIMAL

□ TACACS Authentication Settings

□ SNMP Settings

□ Advanced TrustSec Settings

If there are multiple devices with same profile or category, we can add those devices in a common group.



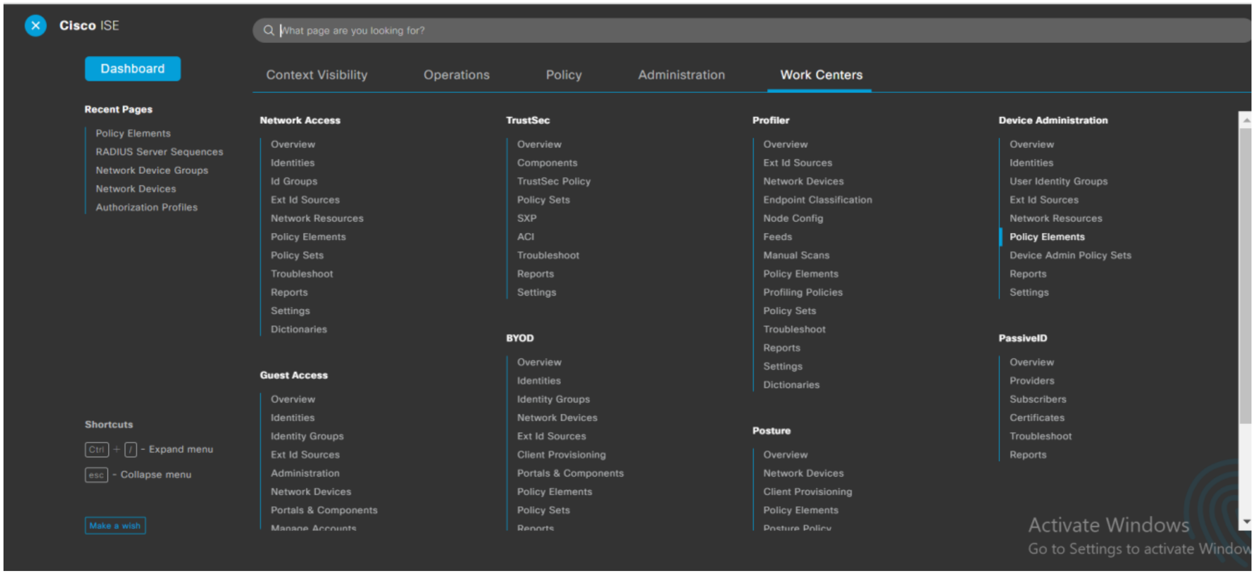
□	Name		
□	All Device Types		
☑	CSCO_DEVICE		
□	readonly		
□	All Locations	All Locations	--
□	Is IPSEC Device	Is this a RADIUS over IPSEC Device	--

CSCO_DEVICENetwork Devices

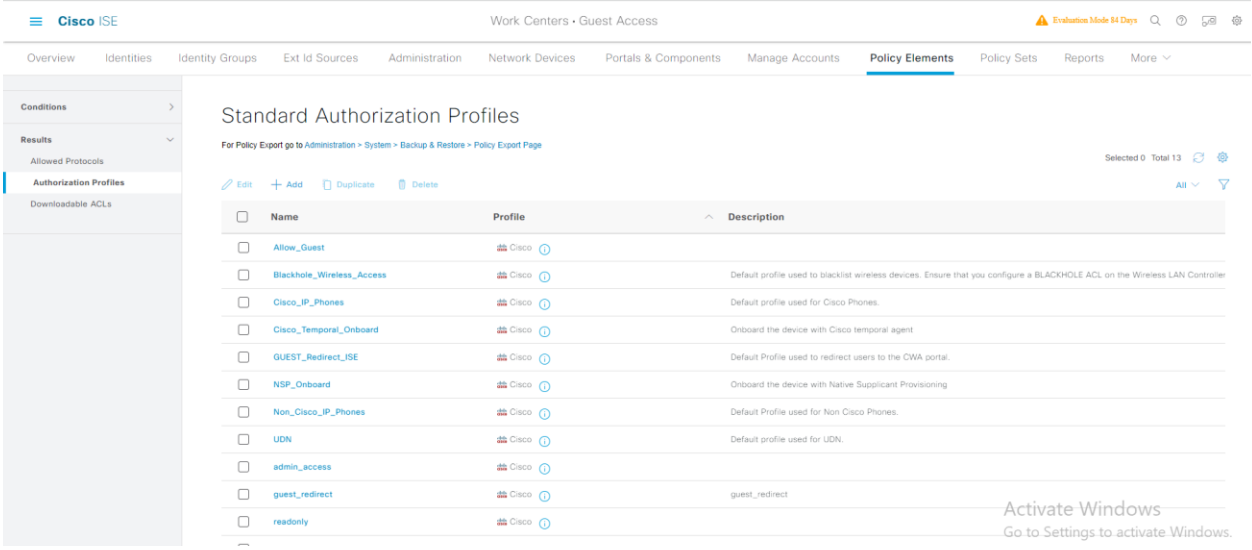
Rows/Page 2 | 1 / 1 | 2 Total Rows

□	Name	IP	Description	Profile Name
□	MGMT_NET	192.168.10.0/24		Cisco
□	WLC	192.168.20.2/32		Cisco

Click on **Work Centers -> Guest Access -> Policy Elements**



Then we need to create Authorization **Profiles.** For this purpose, we created two **Authorization profiles** named **Allow_Guest** to allow any ip after authentication and authorization of SSID and another profile is **GUEST_Redirect_ISE** to redirect a page containing Sign-on form and Registration Form while connecting to that SSID.



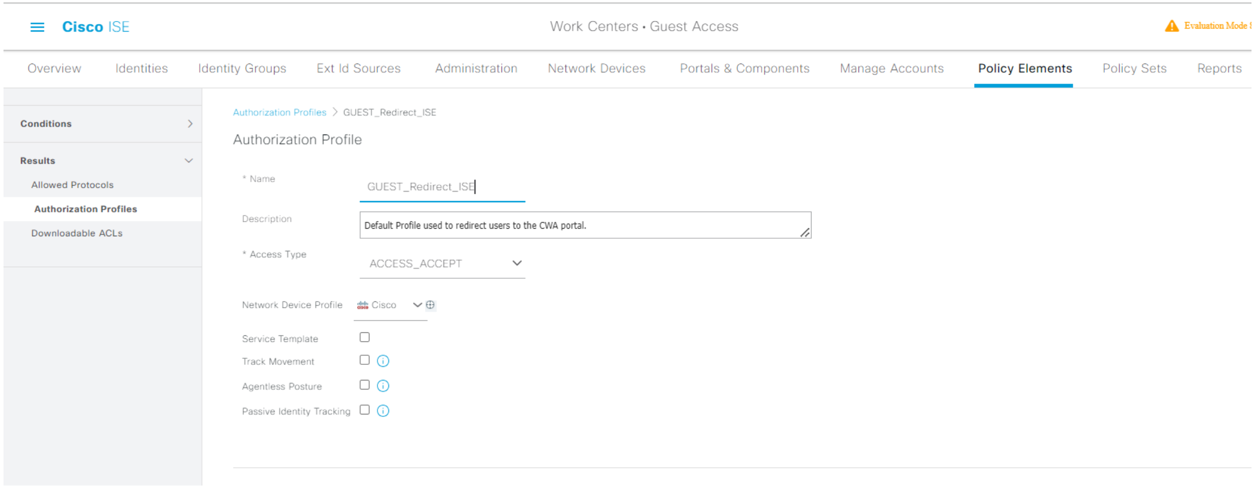
Standard Authorization Profiles

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Selected 0 Total 13

□	Name	Profile	Description
□	Allow_Guest	Cisco	
□	Blackhole_Wireless_Access	Cisco	Default profile used to blacklist wireless devices. Ensure that you configure a BLACKHOLE ACL on the Wireless LAN Controller
□	Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.
□	Cisco_Temporal_Onboard	Cisco	Onboard the device with Cisco temporal agent
□	GUEST_Redirect_ISE	Cisco	Default Profile used to redirect users to the CWA portal.
□	NSP_Onboard	Cisco	Onboard the device with Native Supplicant Provisioning
□	Non_Cisco_IP_Phones	Cisco	Default Profile used for Non Cisco Phones.
□	UDN	Cisco	Default profile used for UDN.
□	admin_access	Cisco	
□	guest_redirect	Cisco	guest_redirect
□	readonly	Cisco	

Let’s have an example to create **Authorization Profile** like below:



Authorization Profile

* Name: GUEST_Redirect_ISE

Description: Default Profile used to redirect users to the CWA portal.

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

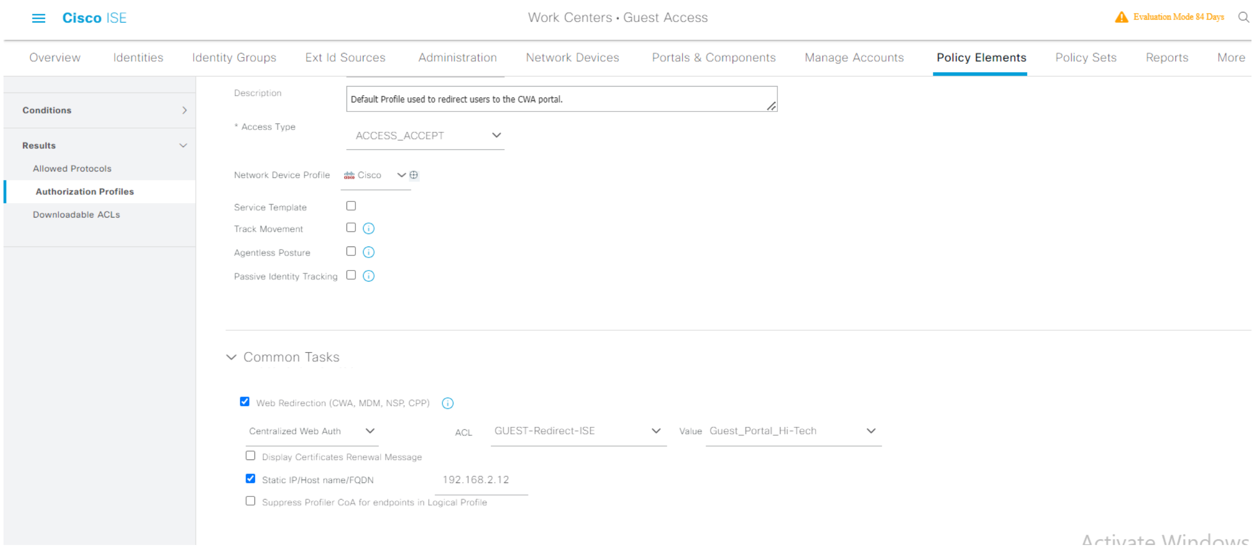
Track Movement □

Agentless Posture □

Passive Identity Tracking □

In **Common Tasks**, we need to select Web Redirection as **‘Centralized Web Auth’** and provide the same ACL defined in WLC. Also we need to select the Value which we will show later where it was created.

Finally need to give the static IP (ISE-192.168.2.12) so that it can redirect to this page when connected to SSID.



Description: Default Profile used to redirect users to the CWA portal.

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Agentless Posture □

Passive Identity Tracking □

Common Tasks

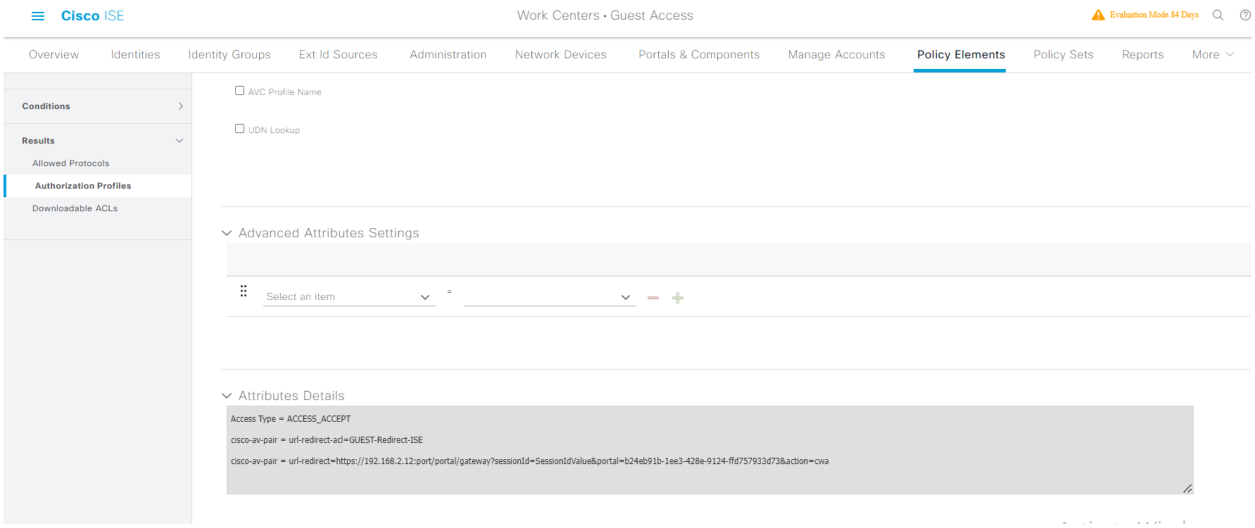
☑ Web Redirection (CWA, MDM, NSP, CPP)

Centralized Web Auth   ACL: GUEST-Redirect-ISE   Value: Guest_Portal_Hi-Tech

□ Display Certificates Renewal Message

☑ Static IP/Host name/FQDN: 192.168.2.12

□ Suppress Profiler CoA for endpoints in Logical Profile



□ AVC Profile Name

□ UDN Lookup

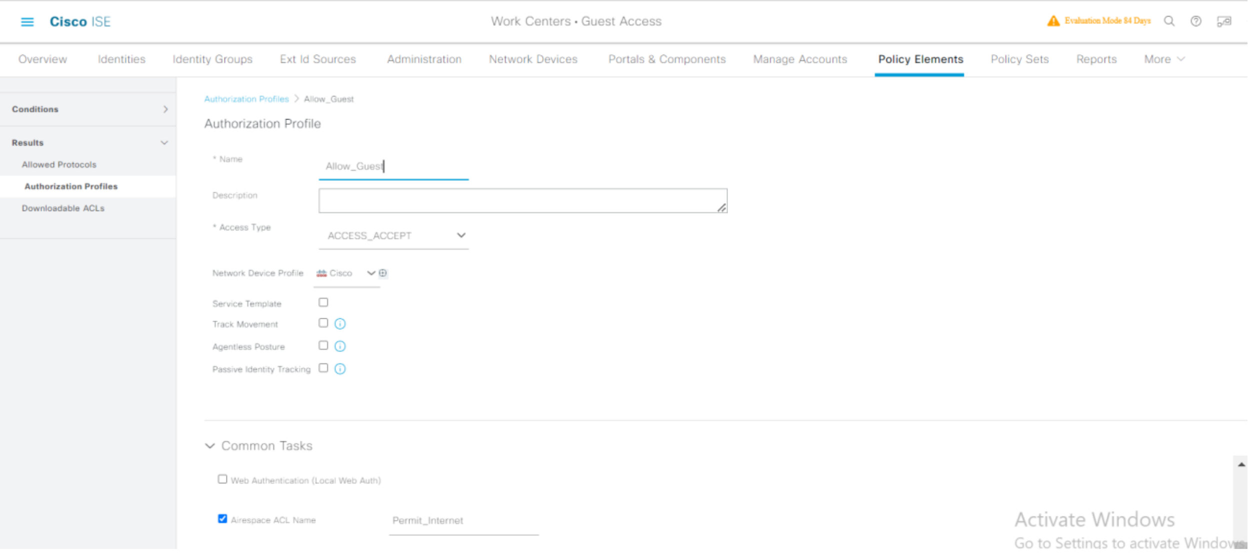
Advanced Attributes Settings

Select an item =

Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-acl=GUEST-Redirect-ISE
cisco-av-pair = url-redirect=https://192.168.2.12:port/portal/gateway?sessionId=SessionIdValue&portal=b24eb91b-1ee3-428e-9124-ffd757933d73&action=cwa
```

Same task need to be done for another Authorization profile for ‘**Allow_Guest’**



Authorization Profile

* Name: Allow_Guest

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Agentless Posture □

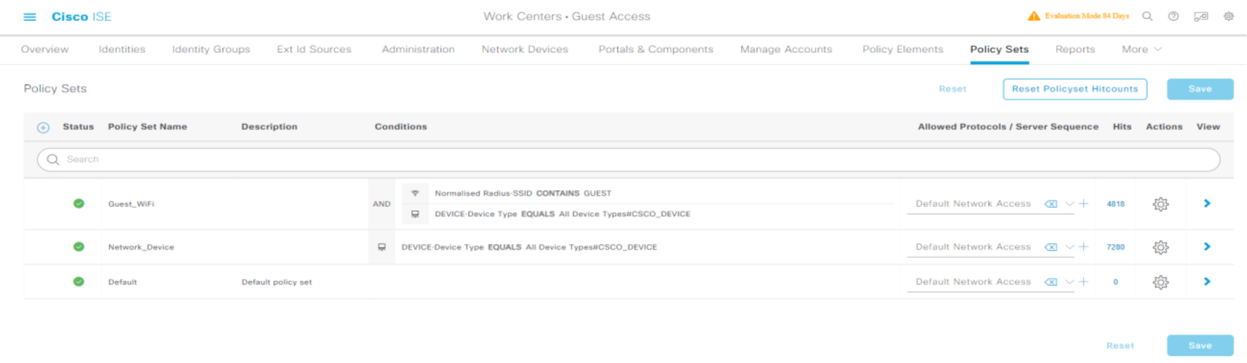
Passive Identity Tracking □

Common Tasks

□ Web Authentication (Local Web Auth)

☑ Airespace ACL Name: Permit_Internet

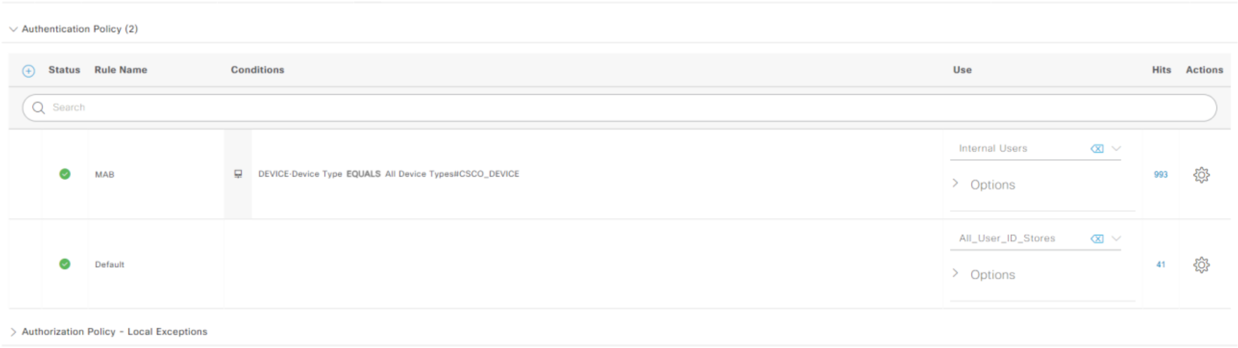
Then we have to create a policy sets from **Policy Sets** tab named **Guest_WiFi**. Here we have to apply some conditions like below:



Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Guest_WiFi		AND Normalised Radius·SSID CONTAINS GUEST DEVICE·Device Type EQUALS All Device Types#CSCO_DEVICE	Default Network Access	4818	⚙	>
✓	Network_Device		DEVICE·Device Type EQUALS All Device Types#CSCO_DEVICE	Default Network Access	7280	⚙	>
✓	Default	Default policy set		Default Network Access	0	⚙	>

Also need to create **Authentication Policy (MAB)** and **Authorization Policy (Wifi_Redirect_Portal and WIFI_Guest)** from the newly created policy set. Here also conditions need to be applied as well.

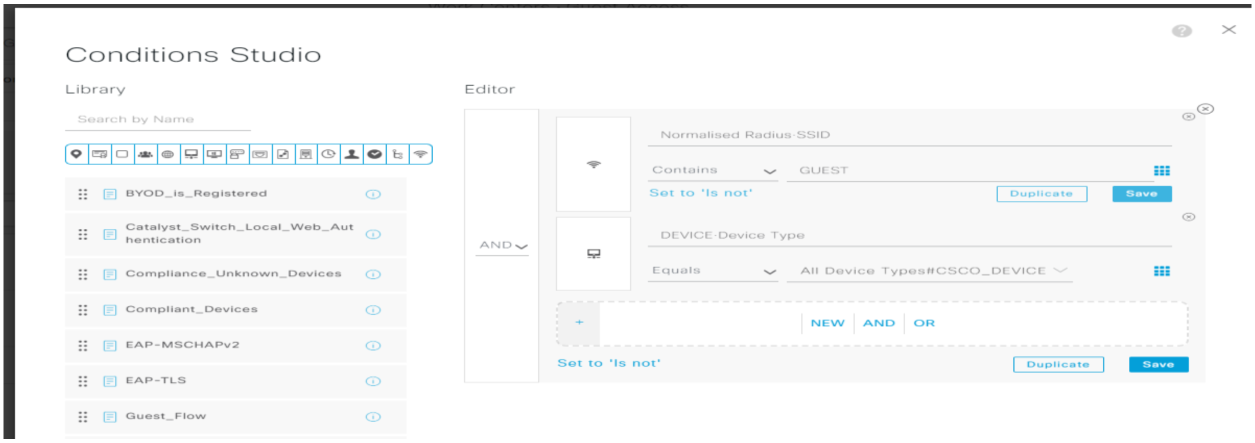


Authentication Policy (2)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	MAB	DEVICE·Device Type EQUALS All Device Types#CSCO_DEVICE	Internal Users	993	⚙
✓	Default		All_User_ID_Stores	41	⚙

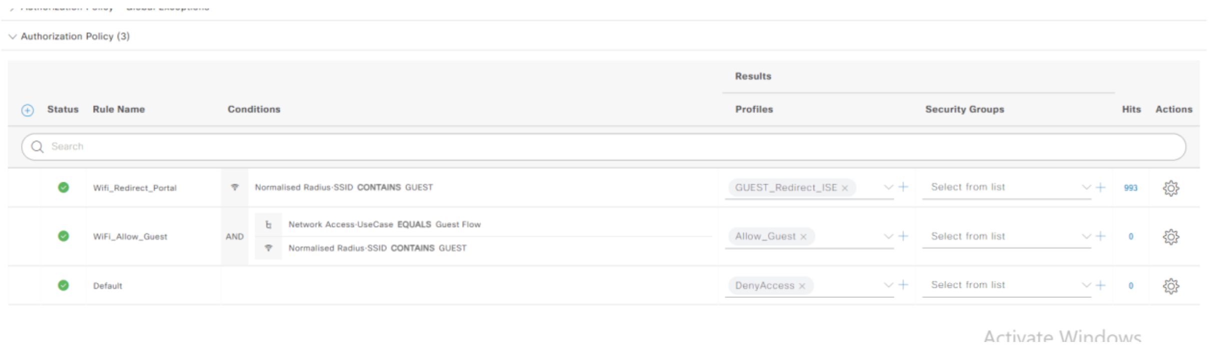
Authorization Policy - Local Exceptions

Here is the sample below how to create Condition Studio. Based on requirement we need to create **Conditions Studio**. We must select items for which conditions will be applied. Here we have selected the SSID contains **GUEST** for which users will get authenticated via RADIUS (ISE). And also, we need to select Device Type like for which devices the condition should be applied of ISE.



Normalised Radius·SSID
Contains GUEST

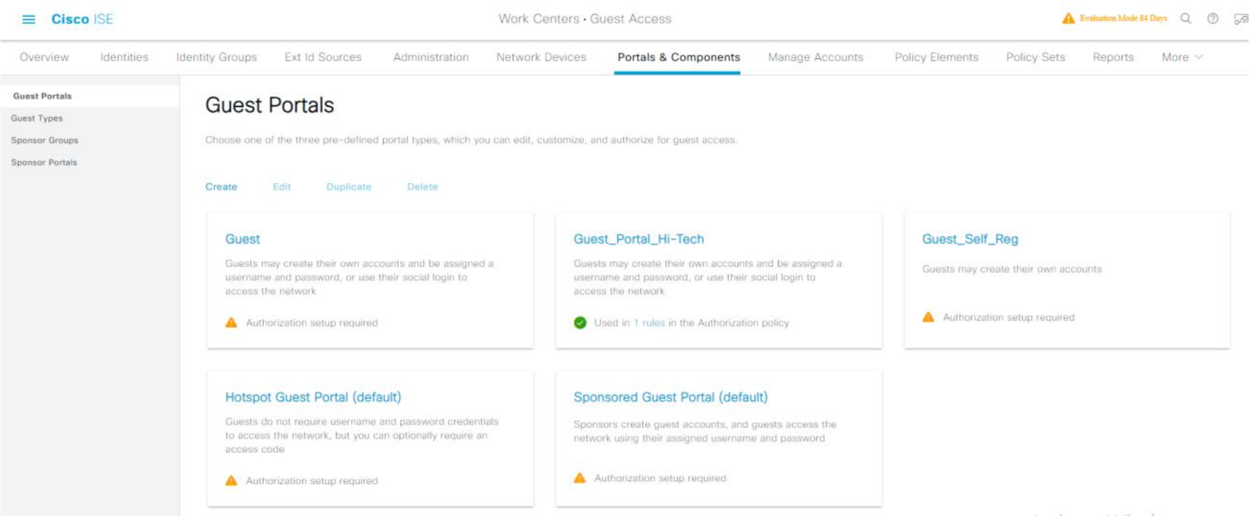
DEVICE·Device Type
Equals All Device Types#CSCO_DEVICE



Authorization Policy (3)

Status	Rule Name	Conditions		Results: Profiles	Results: Security Groups	Hits	Actions
✓	Wifi_Redirect_Portal		Normalised Radius·SSID **CONTAINS** GUEST	GUEST_Redirect_ISE	Select from list	993	⚙
✓	WiFi_Allow_Guest	AND	Network Access·UseCase **EQUALS** Guest Flow Normalised Radius·SSID **CONTAINS** GUEST	Allow_Guest	Select from list	0	⚙
✓	Default			DenyAccess	Select from list	0	⚙

Then we created a profile for ‘**Portal & Components’** named **Guest_Portal_Hi-Tech’**



Guest Portals

Choose one of the three pre-defined portal types, which you can edit, customize, and authorize for guest access.

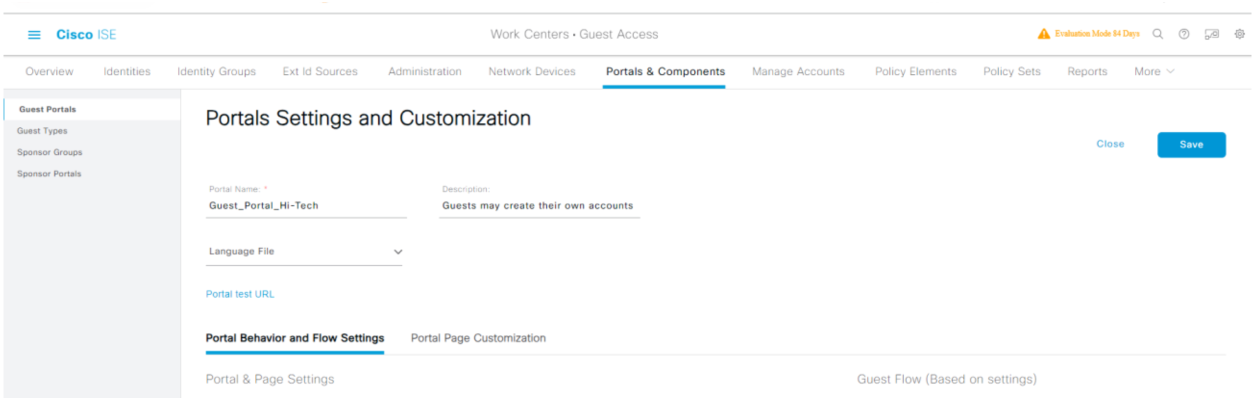
Guest
Guests may create their own accounts and be assigned a username and password, or use their social login to access the network
Authorization setup required

Guest_Portal_Hi-Tech
Guests may create their own accounts and be assigned a username and password, or use their social login to access the network
Used in 1 rules in the Authorization policy

Guest_Self_Reg
Guests may create their own accounts
Authorization setup required

Hotspot Guest Portal (default)
Guests do not require username and password credentials to access the network, but you can optionally require an access code
Authorization setup required

Sponsored Guest Portal (default)
Sponsors create guest accounts, and guests access the network using their assigned username and password
Authorization setup required



Portals Settings and Customization

Portal Name: * Guest_Portal_Hi-Tech

Description: Guests may create their own accounts

Language File

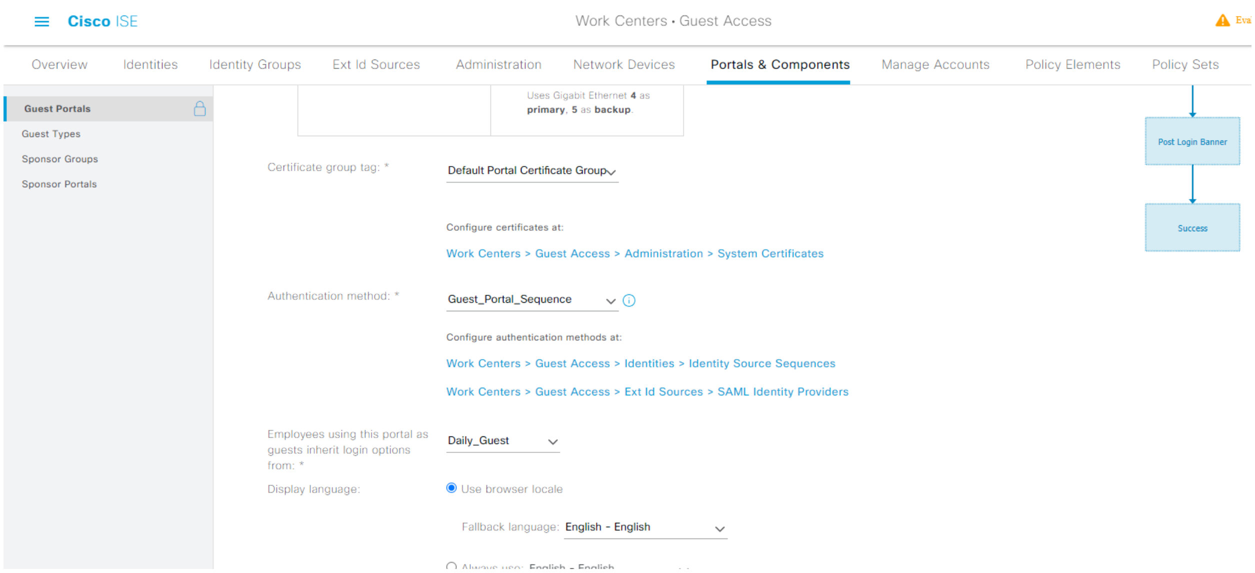
Portal test URL

Portal Behavior and Flow Settings | Portal Page Customization

Portal & Page Settings

Guest Flow (Based on settings)

We have created a policy for the newly created group called **Daily_Guest** who can get for a limited time and also can fill up the form by his own and can change the password after first login.



Uses Gigabit Ethernet **4** as **primary**, **5** as **backup**.

Certificate group tag: * Default Portal Certificate Group

Configure certificates at:

Work Centers > Guest Access > Administration > System Certificates

Authentication method: * Guest_Portal_Sequence

Configure authentication methods at:

Work Centers > Guest Access > Identities > Identity Source Sequences

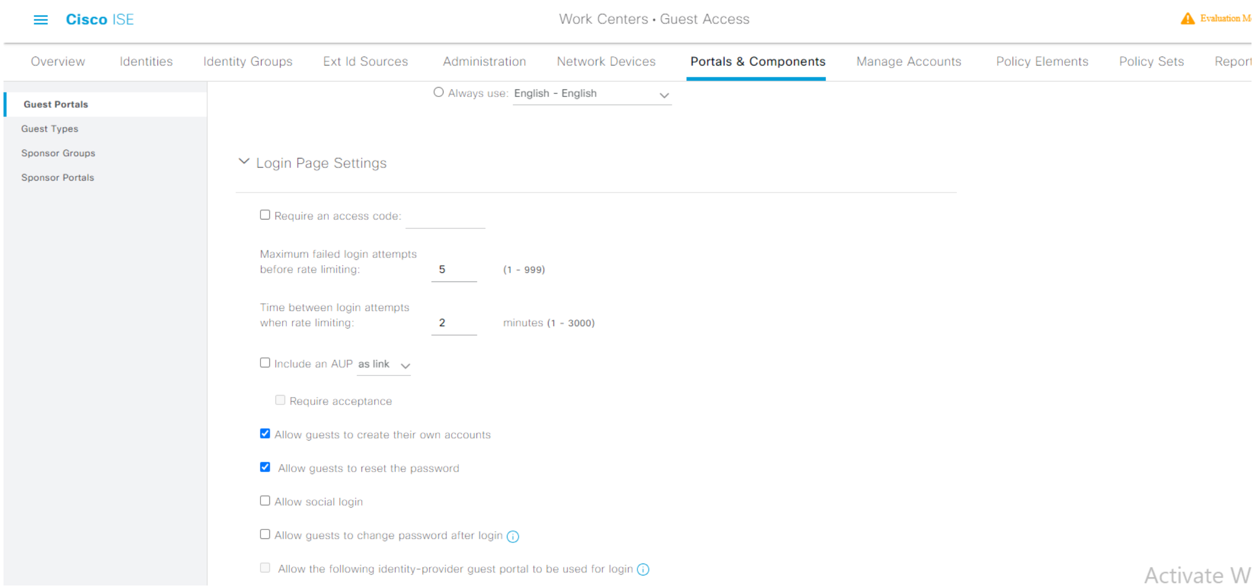
Work Centers > Guest Access > Ext Id Sources > SAML Identity Providers

Employees using this portal as guests inherit login options from: * Daily_Guest

Display language: ● Use browser locale

Fallback language: English - English

○ Always use: English - English



○ Always use: English - English

Login Page Settings

□ Require an access code:

Maximum failed login attempts before rate limiting: 5 (1 - 999)

Time between login attempts when rate limiting: 2 minutes (1 - 3000)

□ Include an AUP as link

□ Require acceptance

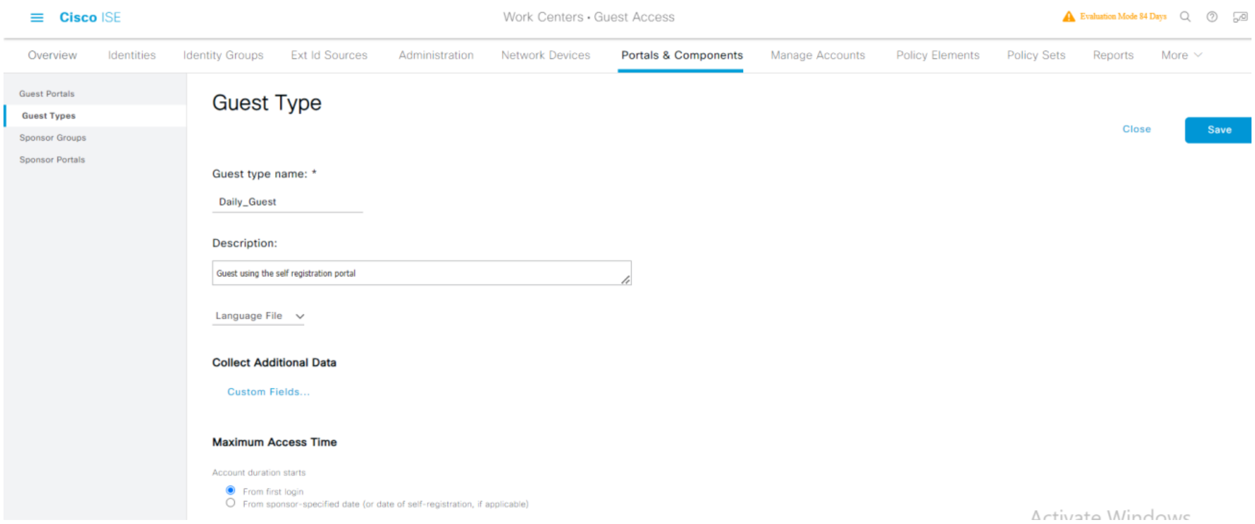
☑ Allow guests to create their own accounts

☑ Allow guests to reset the password

□ Allow social login

□ Allow guests to change password after login

□ Allow the following identity-provider guest portal to be used for login



Guest Type

Guest type name: *

Daily_Guest

Description:

Guest using the self registration portal

Language File

Collect Additional Data

Custom Fields...

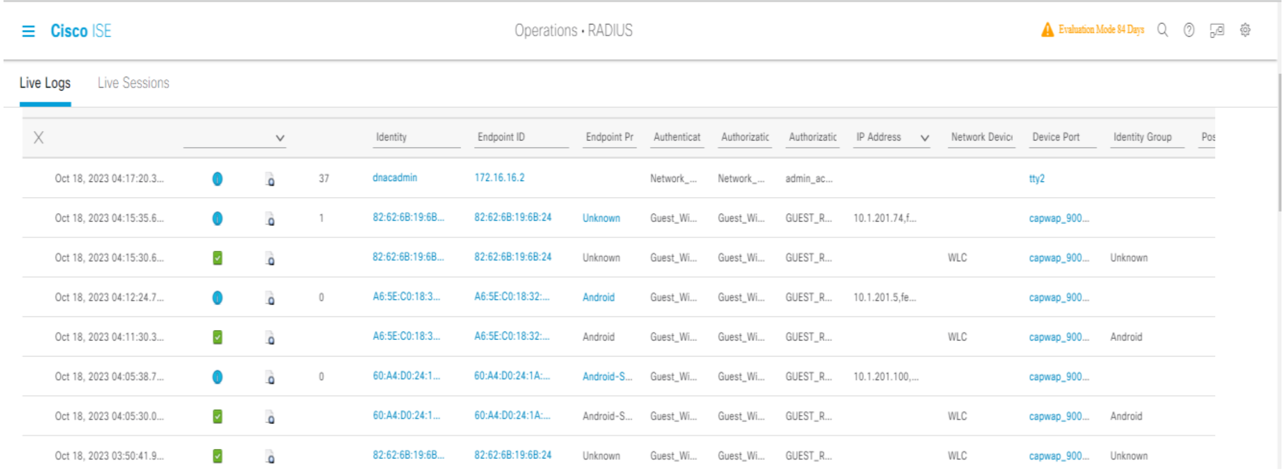
Maximum Access Time

Account duration starts

● From first login

○ From sponsor-specified date (or date of self-registration, if applicable)

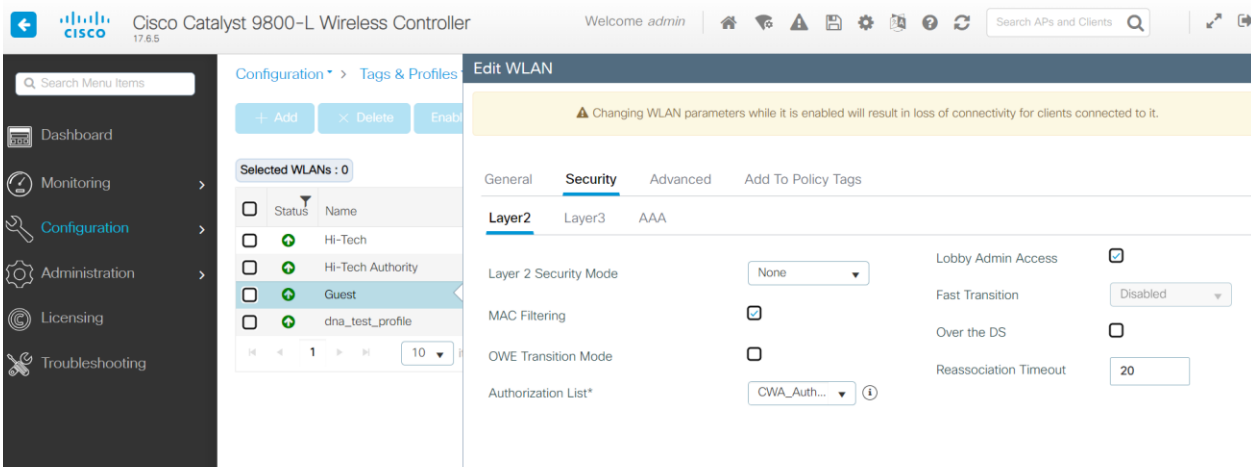
To see the log or live session, we need to go **Operations -> RADIUS -> Live Logs** like below. We can see MAC address and IP address of the users who have joined GUEST SSID are authenticated and authorized from ISE.



X				Identity	Endpoint ID	Endpoint Pr	Authenticat	Authorizatic	Authorizatic	IP Address	Network Devic	Device Port	Identity Group	Pos
Oct 18, 2023 04:17:20.3...	●		37	dnacadmin	172.16.16.2		Network_...	Network_...	admin_ac...			tty2		
Oct 18, 2023 04:15:35.6...	●		1	82:62:6B:19:6B...	82:62:6B:19:6B:24	Unknown	Guest_Wi...	Guest_Wi...	GUEST_R...	10.1.201.74,f...		capwap_900...		
Oct 18, 2023 04:15:30.6...	✓			82:62:6B:19:6B...	82:62:6B:19:6B:24	Unknown	Guest_Wi...	Guest_Wi...	GUEST_R...		WLC	capwap_900...	Unknown	
Oct 18, 2023 04:12:24.7...	●		0	A6:5E:C0:18:3...	A6:5E:C0:18:32:...	Android	Guest_Wi...	Guest_Wi...	GUEST_R...	10.1.201.5,fe...		capwap_900...		
Oct 18, 2023 04:11:30.3...	✓			A6:5E:C0:18:3...	A6:5E:C0:18:32:...	Android	Guest_Wi...	Guest_Wi...	GUEST_R...		WLC	capwap_900...	Android	
Oct 18, 2023 04:05:38.7...	●		0	60:A4:D0:24:1...	60:A4:D0:24:1A:...	Android-S...	Guest_Wi...	Guest_Wi...	GUEST_R...	10.1.201.100,...		capwap_900...		
Oct 18, 2023 04:05:30.0...	✓			60:A4:D0:24:1...	60:A4:D0:24:1A:...	Android-S...	Guest_Wi...	Guest_Wi...	GUEST_R...		WLC	capwap_900...	Android	
Oct 18, 2023 03:50:41.9...	✓			82:62:6B:19:6B...	82:62:6B:19:6B:24	Unknown	Guest_Wi...	Guest_Wi...	GUEST_R...		WLC	capwap_900...	Unknown	

Cisco WLC Part :

As a WLAN named GUEST is already created and assign a vlan for that SSID, we had to enable MAC Filter and assign the Authorization list created from WLC. **Configuration -> Tags & Profiles**



Cisco Catalyst 9800-L Wireless Controller 17.6.5

Welcome *admin*

Configuration > Tags & Profiles

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

Selected WLANs : 0

□	Status	Name
□	●	Hi-Tech
□	●	Hi-Tech Authority
□	●	Guest
□	●	dna_test_profile

General | **Security** | Advanced | Add To Policy Tags

Layer2 | Layer3 | AAA

Layer 2 Security Mode: None

MAC Filtering: ☑

OWE Transition Mode: □

Authorization List*: CWA_Auth...

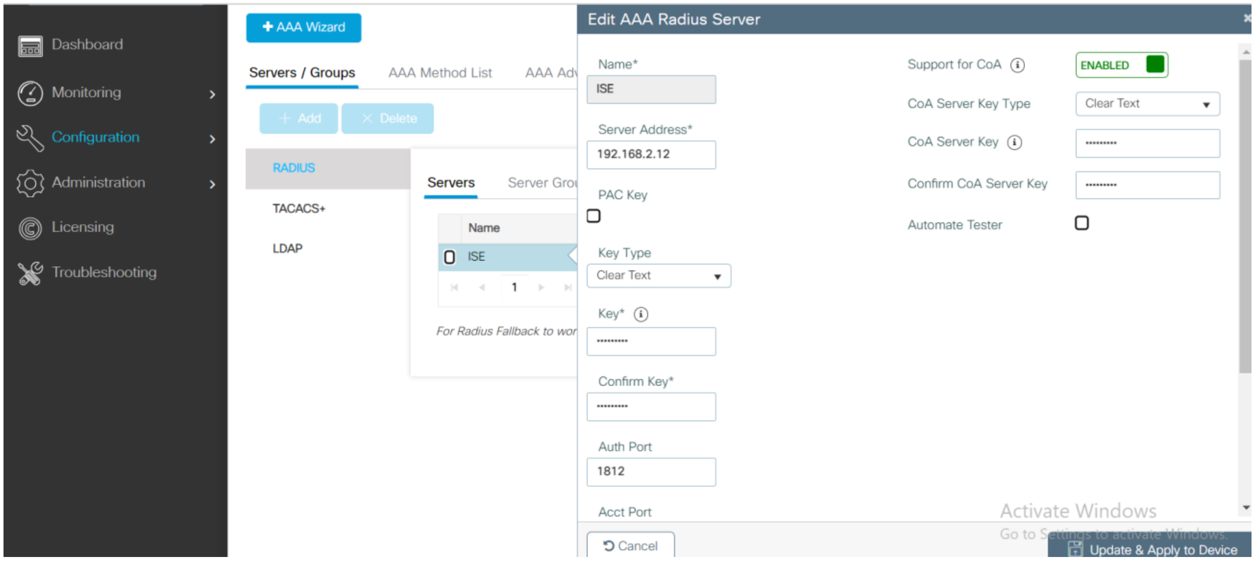
Lobby Admin Access: ☑

Fast Transition: Disabled

Over the DS: □

Reassociation Timeout: 20

To integrate WLC with ISE, we had to select Radius server as ISE ip and enable Support for CoA. Same key need to be used which was provided in ISE. **Configuration -> Security -> AAA**



Edit AAA Radius Server

Name*: ISE

Server Address*: 192.168.2.12

PAC Key: □

Key Type: Clear Text

Key*: ••••••••••

Confirm Key*: ••••••••••

Auth Port: 1812

Acct Port

Support for CoA: ENABLED

CoA Server Key Type: Clear Text

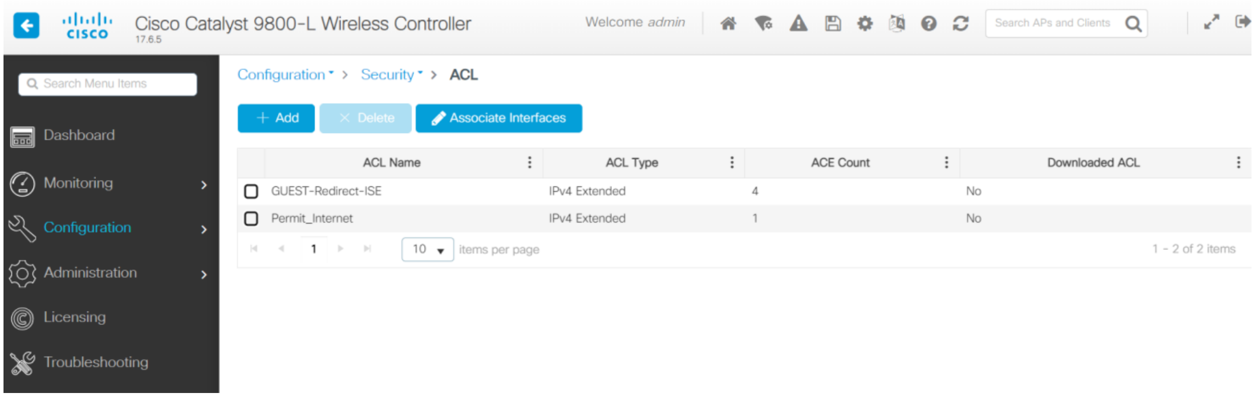
CoA Server Key: ••••••••••

Confirm CoA Server Key: ••••••••••

Automate Tester: □

For Radius Fallback to wor

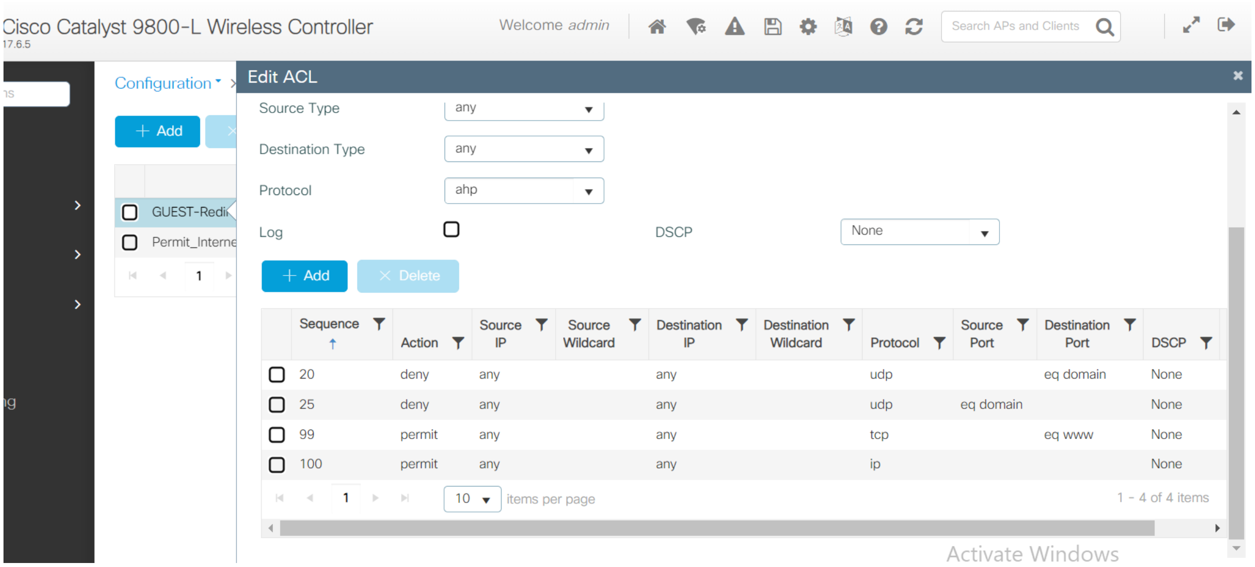
Finally we had to create two ACLs from **Configuration -> Security -> ACL** which was applied for the web redirection and getting the access to the network.



	ACL Name	ACL Type	ACE Count	Downloaded ACL
□	GUEST-Redirect-ISE	IPv4 Extended	4	No
□	Permit_Internet	IPv4 Extended	1	No

1 | 10 items per page | 1 - 2 of 2 items

We had to give same ACL name in ISE so that when user will hit the GUEST SSID, it will get authenticated and authorized in ISE and will allow access to the user on the basis of ACL.



Source Type: any

Destination Type: any

Protocol: ahp

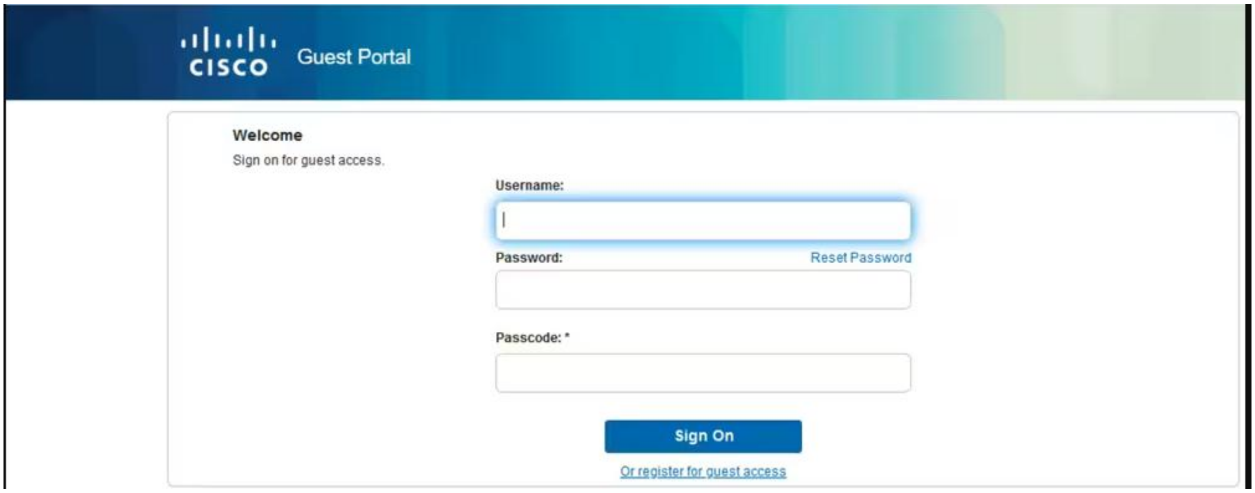
Log: □

DSCP: None

	Sequence ↑	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP
□	20	deny	any		any		udp		eq domain	None
□	25	deny	any		any		udp	eq domain		None
□	99	permit	any		any		tcp		eq www	None
□	100	permit	any		any		ip			None

1 | 10 items per page | 1 - 4 of 4 items

After completing all these process, user will get below page while trying to browse the internet using GUEST SSID.



Guest Portal

Welcome

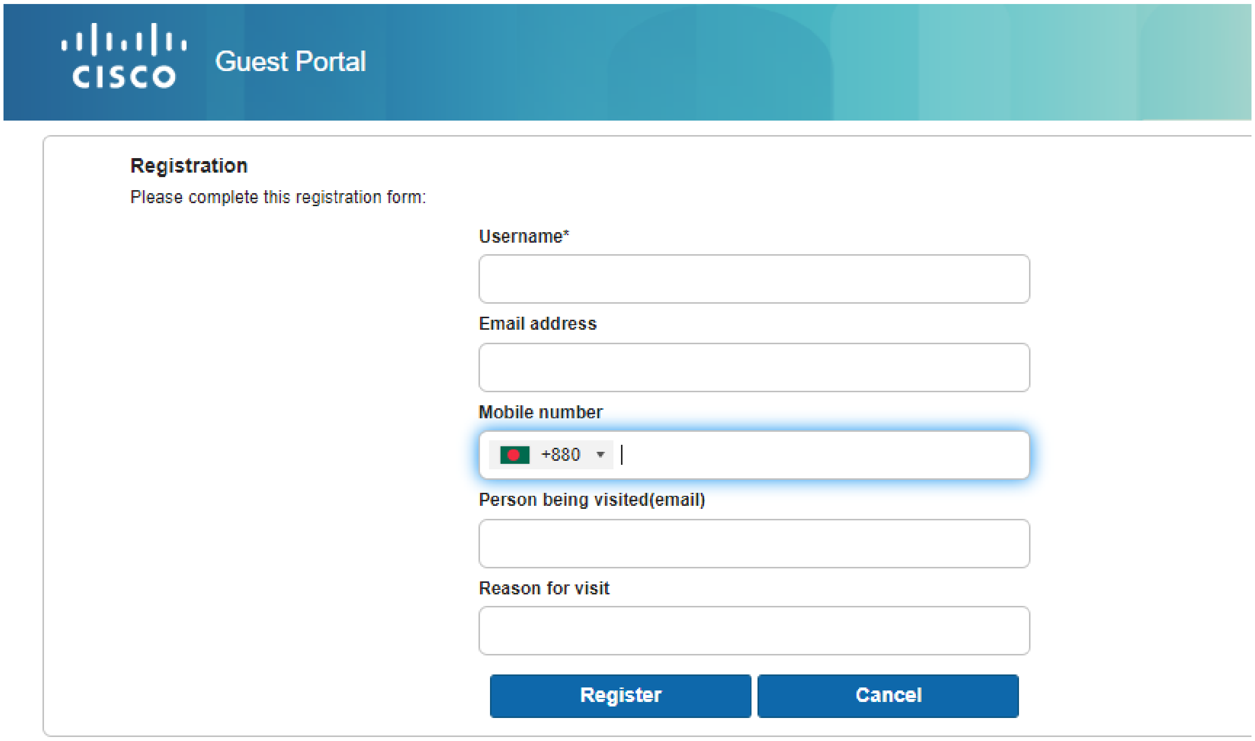
Sign on for guest access.

Username:

Password: Reset Password

Passcode: *

Then the guest user needs to fill up the form containing and he will get a temporary password after giving the username and password they will get the access of internet.



Guest Portal

Registration

Please complete this registration form:

Username*

Email address

Mobile number

+880

Person being visited(email)

Reason for visit