Cisco DNA Center SD-Access Guest Automation

Revised: June 1, 2021

SD-Access Guest Automation for CWA, EWA, and Hotspot SSIDs

This guide explains how Cisco DNA Center configures Central Web Authentication (CWA), External Web Authentication (EWA), and hotspot SSIDs on Cisco AireOS and Polaris-based wireless LAN controllers (Cisco Catalyst 9800 and embedded wireless on Cisco Catalyst 9000 platforms).

This guide is based on Cisco DNA Center 1.3.0.8; examples and steps will differ based on your Cisco DNA Center version.

Prerequisites

Before you start using Cisco SD-Access guest automation, note the following prerequisites:

- You must understand how to use Cisco DNA Center to design a wired and wireless SD-Access solution.
- You must understand how to design, discover, provision, and add fabric to a wireless LAN controller.
- Refer to the Cisco Software-Defined Access Compatibility Matrix for the supported Cisco DNA Center and wireless LAN controller platform versions.
- SD-Access guest automation uses the following components:
    - Cisco DNA Center to automate guest workflows.
    - Cisco DNA Center configures the wireless LAN controller (WLC) and Cisco ISE for portal configurations, along with authorization policies.

Configure SD-Access Guest Automation

The SD-Access guest automation configuration steps are same for both Cisco Catalyst 9800 (IOS) and Cisco AireOS WLC.

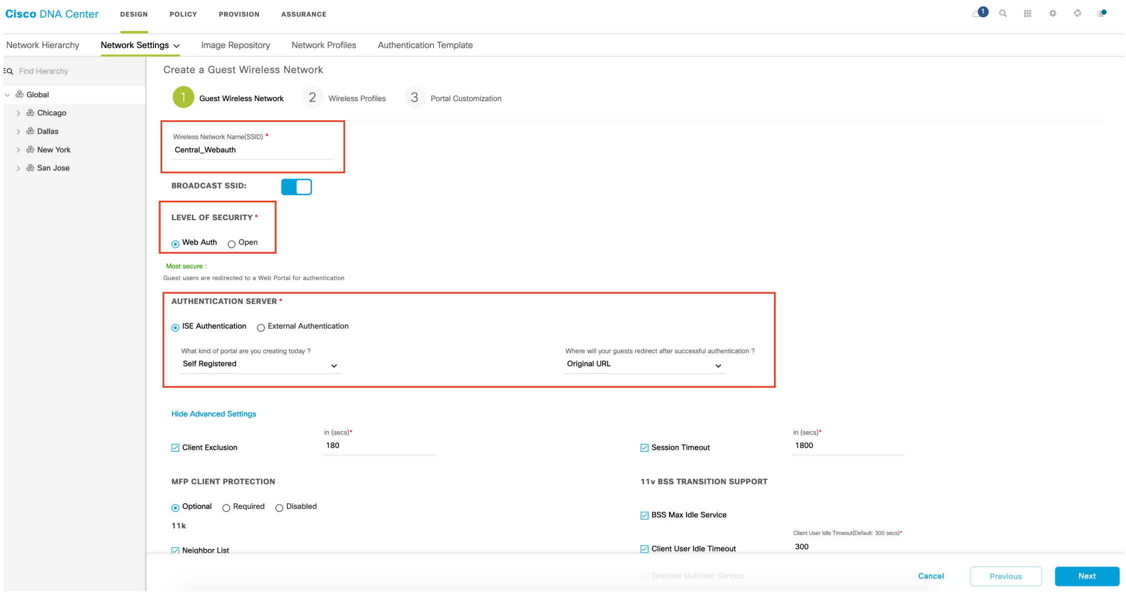
Configure CWA

Procedure

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon and choose **Design** > **Network Settings** > **Wireless**.

Step 2 To add a new SSID under **Guest Wireless**, click **Add** and complete the following fields:

- **Wireless Network Name (SSID)**: Enter the name of the wireless network.
- **LEVEL OF SECURITY**: Click the **Web Auth** radio button.
- **AUTHENTICATION SERVER**: Click the **ISE Authentication** radio button.



Create a Guest Wireless Network

Wireless Network Name(SSID) *
Central_Webauth

BROADCAST SSID:

LEVEL OF SECURITY *
● Web Auth ○ Open

Most secure :
Guest users are redirected to a Web Portal for authentication

AUTHENTICATION SERVER *
● ISE Authentication ○ External Authentication

What kind of portal are you creating today ?
Self Registered

Where will your guests redirect after successful authentication ?
Original URL

☑ Client Exclusion in (secs)* 180

☑ Session Timeout in (secs)* 1800

MFP CLIENT PROTECTION
● Optional ○ Required ○ Disabled

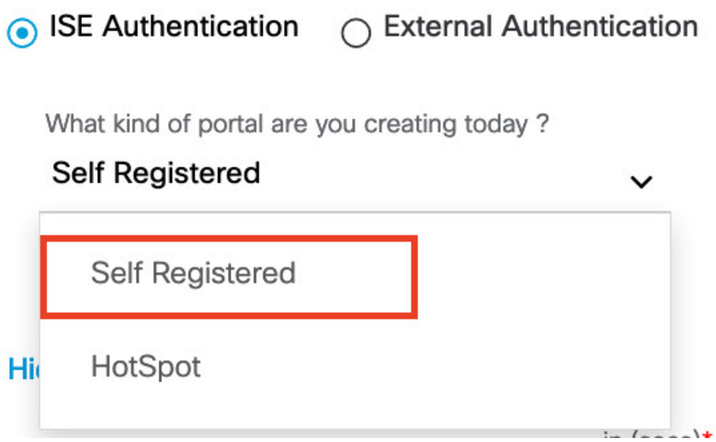
11k
☑ Neighbor List

11v BSS TRANSITION SUPPORT
☑ BSS Max Idle Service

☑ Client User Idle Timeout
Client User Idle Timeout(Default: 300 secs)* 300

☑ Directed Multicast Service

From the drop-down list for the kind of portal, choose **Self Registered**.



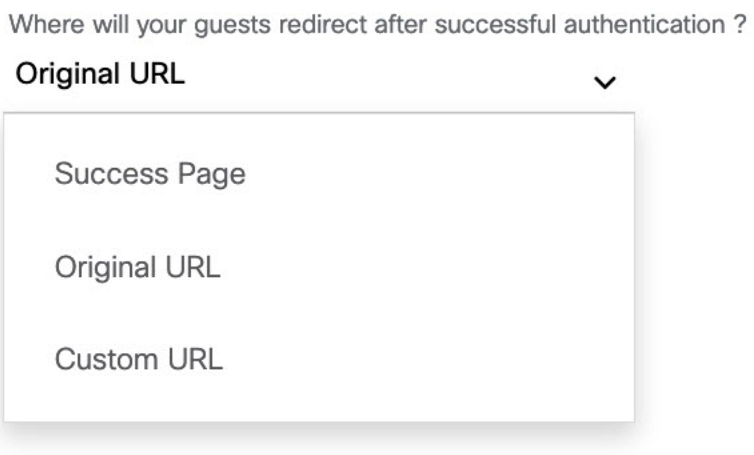
● ISE Authentication ○ External Authentication

What kind of portal are you creating today ?
Self Registered

Self Registered
HotSpot

in (secs)*

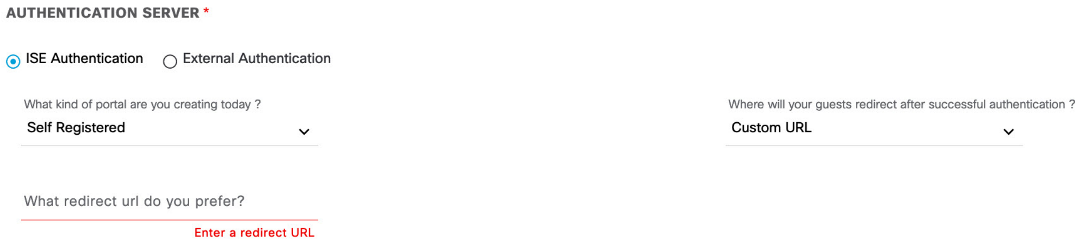
From the drop-down list for guest redirection after authentication, choose **Original URL**, **Success Page**, or **Custom URL**. To specify a redirection URL after authentication, choose **Custom URL** and enter the custom redirect URL.



Where will your guests redirect after successful authentication ?

Original URL

- Success Page
- Original URL
- Custom URL



AUTHENTICATION SERVER *

● ISE Authentication ○ External Authentication

What kind of portal are you creating today ?
Self Registered

Where will your guests redirect after successful authentication ?
Custom URL

What redirect url do you prefer?

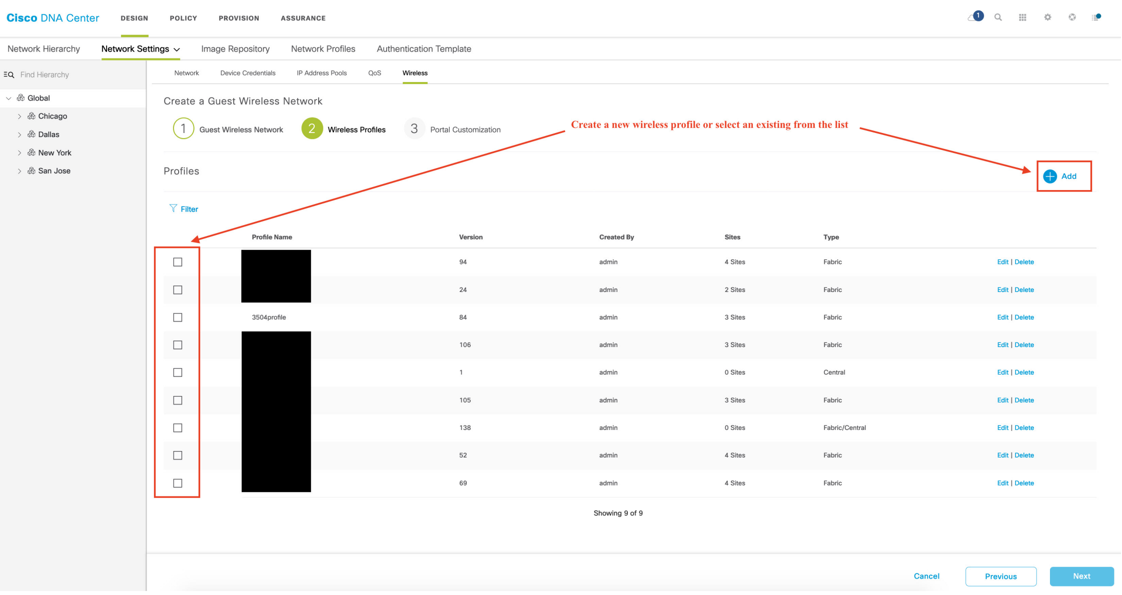
Enter a redirect URL

- Modify the additional settings as necessary.

Step 3 Click **Next**.

Step 4 To configure wireless profiles, do one of the following:

- Create a wireless profile.
- Select an existing wireless profile, where enterprise SSIDs are already broadcast on the required sites.



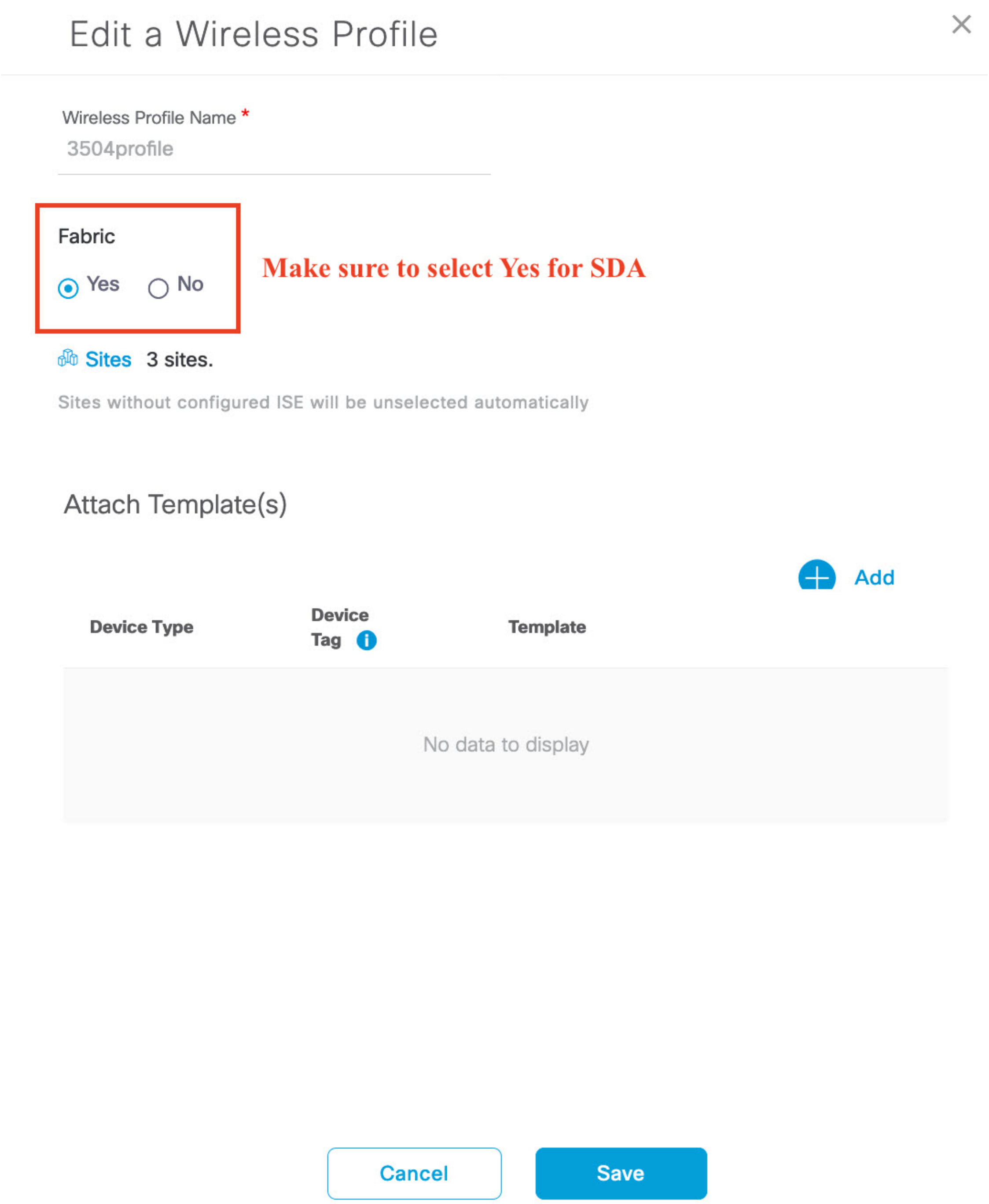
	Profile Name	Version	Created By	Sites	Type	
□	[redacted]	94	admin	4 Sites	Fabric	Edit | Delete
□	[redacted]	24	admin	2 Sites	Fabric	Edit | Delete
□	3504profile	84	admin	3 Sites	Fabric	Edit | Delete
□	[redacted]	106	admin	3 Sites	Fabric	Edit | Delete
□	[redacted]	1	admin	0 Sites	Central	Edit | Delete
□	[redacted]	105	admin	3 Sites	Fabric	Edit | Delete
□	[redacted]	138	admin	0 Sites	Fabric/Central	Edit | Delete
□	[redacted]	52	admin	4 Sites	Fabric	Edit | Delete
□	[redacted]	69	admin	4 Sites	Fabric	Edit | Delete

Showing 9 of 9

After you select the wireless profile, a dialog box appears for editing the wireless profile, where you can define the fabric or nonfabric capabilities for the SSID.

Step 5 To deploy SD-Access, under **Fabric**, click the **Yes** radio button.

If necessary, select more templates under **Attach Template(s)**.



Edit a Wireless Profile

Wireless Profile Name *

3504profile

Fabric

● Yes ○ No

Make sure to select Yes for SDA

Sites 3 sites.

Sites without configured ISE will be unselected automatically

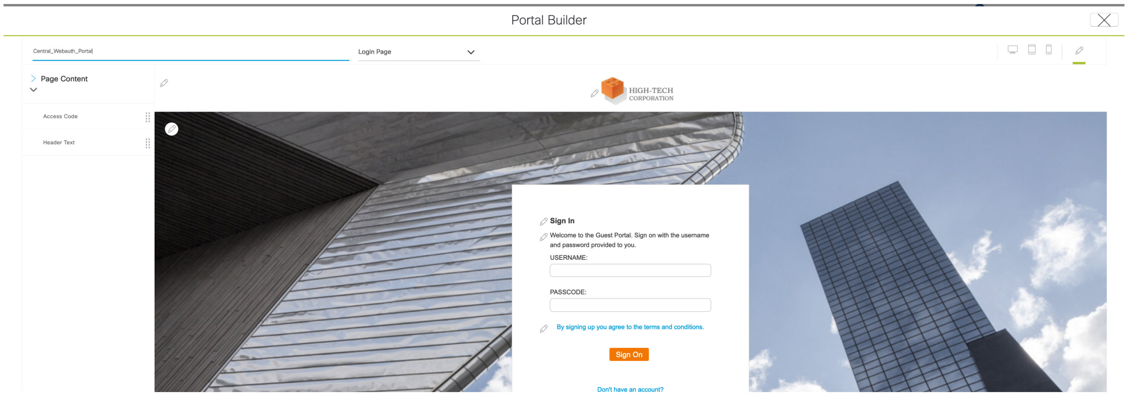
Attach Template(s)

Device Type	Device Tag	Template

No data to display

Step 6 Click **Next**.

Step 7 To add a new portal, click **Add**.



Portal Builder

Central_Webauth_Portal

Login Page

Page Content

Access Code

Header Text

Sign In

Welcome to the Guest Portal. Sign on with the username and password provided to you.

USERNAME:

PASSCODE:

By signing up you agree to the terms and conditions.

Sign On

Don't have an account?

Create a new portal for each CWA SSID; you cannot reuse the portals. Then customize the portal creation where you can configure a custom portal within Cisco DNA Center GUI or select a default template.

Note This step is automated and does not require any additional configuration on Cisco ISE. Based on the portal configuration, a new self-registered portal is configured on Cisco ISE for the SSID created. However, the existing portals are not affected.

Step 8 Click **Finish** and reprovision the WLC on the **Provision** window.

Reprovisioning the WLC pushes the following configurations on each node:

- SSID is configured on the WLC and remains in disabled state as the IP Pool is not yet assigned.
- The portal that is created in Step 7, on page 6 is configured on Cisco ISE under **Workstation** > **Guest Access** > **Portals and Components** with the same name provided during Step 7, on page 6.
- Authorization profile based on the portal name, which has the CWA portal redirection URL when the client is in **Web Auth** pending state.
- Two authorization policies; one for redirecting CWA clients to the previously mentioned authorization profile after MAC authorization and one for success profile.

What to do next

Assign IP pool for the SSID. See Assign IP Pool for SSID, on page 13.

Configure Hotspot

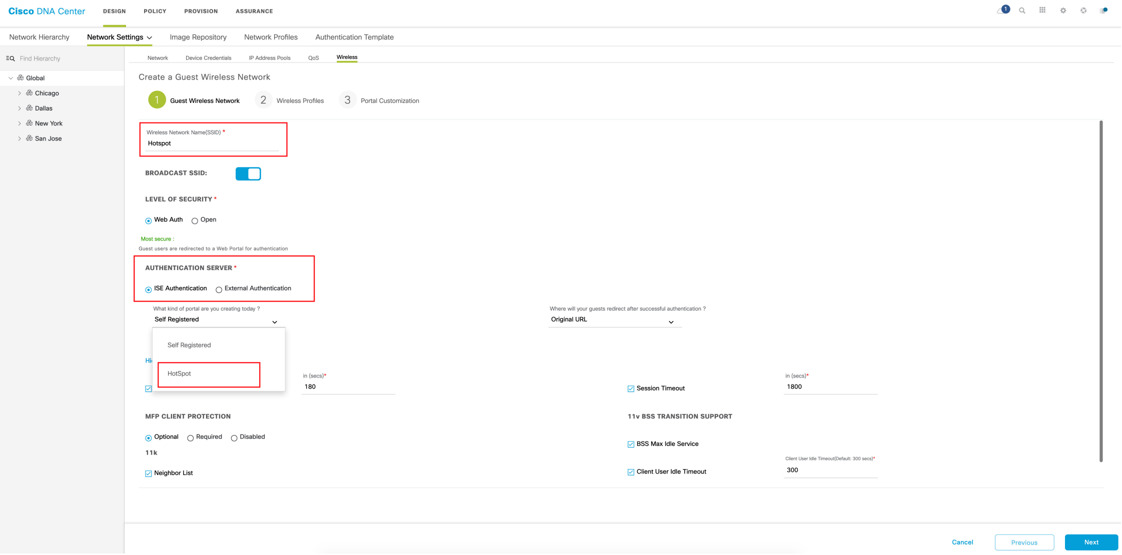
Procedure

Step 1 From the Cisco DNA Center GUI, click the **Menu** icon and choose **Design** > **Network Settings** > **Wireless**.

Step 2 To add a new SSID under **Guest Wireless**, click **Add** and complete the following fields:

- **Wireless Network Name (SSID)**: Enter the name of the wireless network.
- **LEVEL OF SECURITY**: Click the **Web Auth** radio button.

- **AUTHENTICATION SERVER**: Click the **ISE Authentication** radio button.



Create a Guest Wireless Network

1 Guest Wireless Network 2 Wireless Profiles 3 Portal Customization

Wireless Network Name(SSID) * Hotspot

BROADCAST SSID: on

LEVEL OF SECURITY *

● Web Auth ○ Open

Most secure : Guest users are redirected to a Web Portal for authentication

AUTHENTICATION SERVER *

● ISE Authentication ○ External Authentication

What kind of portal are you creating today ? Self Registered

Self Registered

HotSpot

Where will your guests redirect after successful authentication ? Original URL

in (secs)* 180

☑ Session Timeout in (secs)* 1800

MFP CLIENT PROTECTION

● Optional ○ Required ○ Disabled

11k

☑ Neighbor List

11v BSS TRANSITION SUPPORT

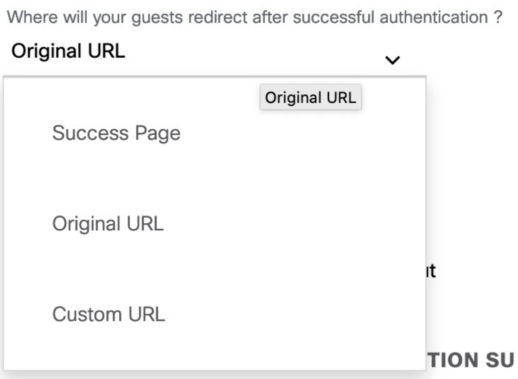
☑ BSS Max Idle Service

☑ Client User Idle Timeout Client User Idle Timeout(Default: 300 secs)* 300

From the drop-down list for the kind of portal, choose **HotSpot**.

From the drop-down list for guest redirection after authentication, choose **Original URL**, **Success Page**, or **Custom URL**. To specify where the redirection should happen after authentication, choose **Custom URL** and enter the custom redirect URL.

Redirect options are same as CWA



Where will your guests redirect after successful authentication ?

Original URL

Original URL

Success Page

Original URL

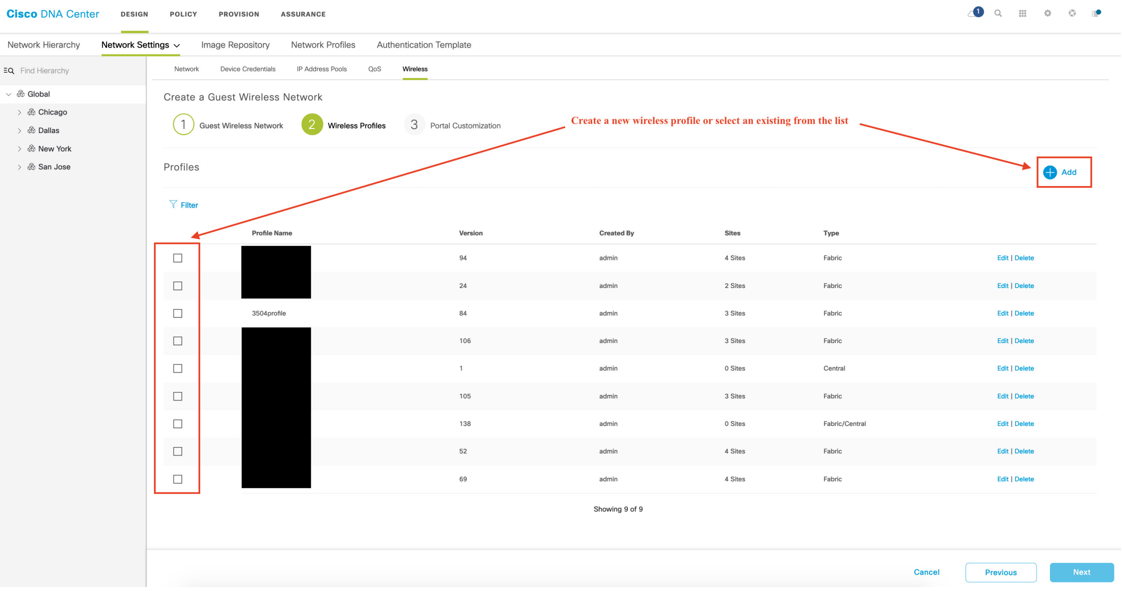
Custom URL

- Modify the additional settings as necessary.

Step 3 Click **Next**.

Step 4 To configure wireless profiles, do one of the following:

- Create a wireless profile.
- Select an existing wireless profile where enterprise SSIDs are already broadcast on the required sites.



Create a Guest Wireless Network

Create a new wireless profile or select an existing from the list

Profiles

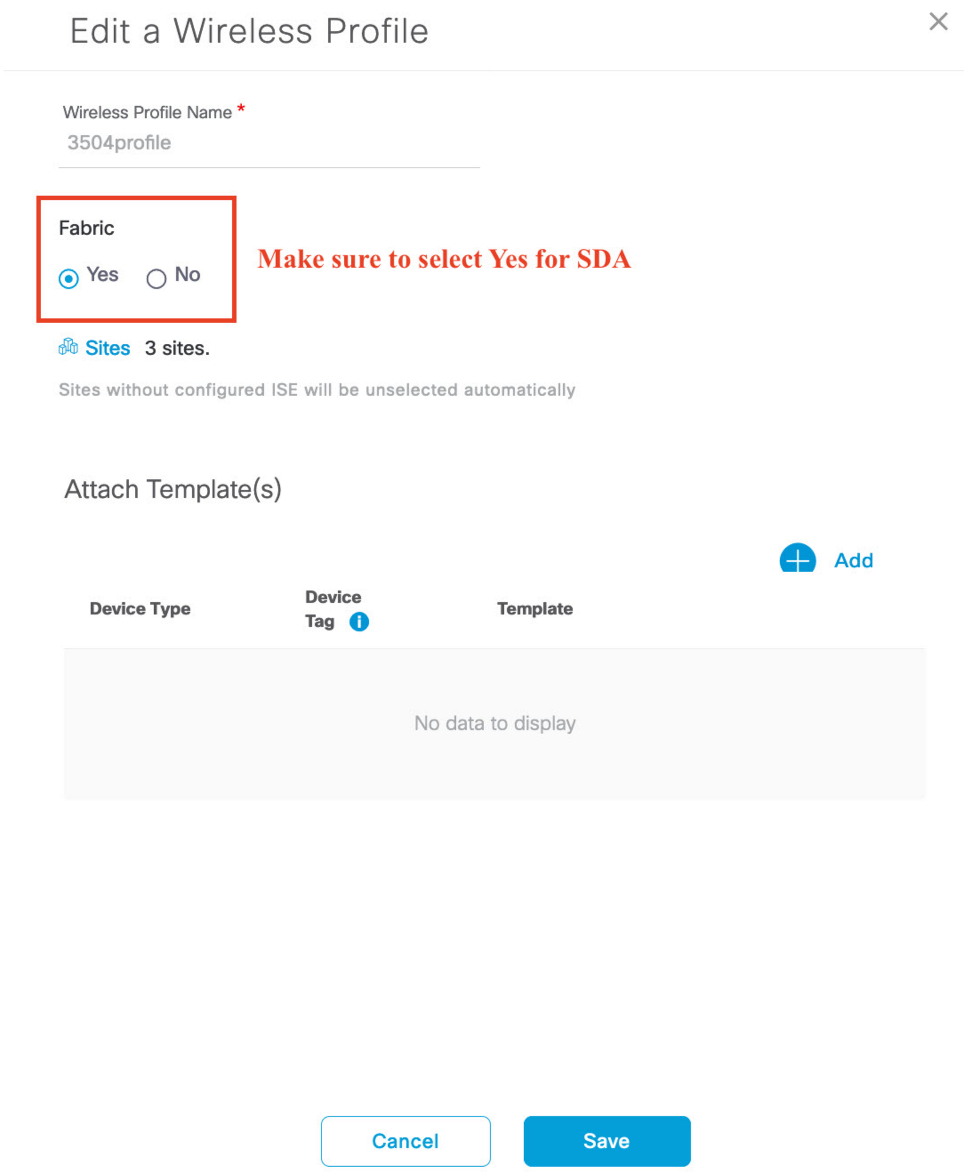
	Profile Name	Version	Created By	Sites	Type	
□	[redacted]	94	admin	4 Sites	Fabric	Edit | Delete
□	[redacted]	24	admin	2 Sites	Fabric	Edit | Delete
□	3504profile	84	admin	3 Sites	Fabric	Edit | Delete
□	[redacted]	106	admin	3 Sites	Fabric	Edit | Delete
□	[redacted]	1	admin	0 Sites	Central	Edit | Delete
□	[redacted]	105	admin	3 Sites	Fabric	Edit | Delete
□	[redacted]	138	admin	0 Sites	Fabric/Central	Edit | Delete
□	[redacted]	52	admin	4 Sites	Fabric	Edit | Delete
□	[redacted]	69	admin	4 Sites	Fabric	Edit | Delete

Showing 9 of 9

After you select the wireless profile, a dialog box appears for editing the wireless profile, where you can define the fabric or nonfabric capabilities for the SSID.

Step 5 To deploy SDA, click the **Yes** radio button under **Fabric**.

If necessary, select more templates under **Attach Template(s)**.



Edit a Wireless Profile

Wireless Profile Name *
3504profile

Fabric
● Yes ○ No

Make sure to select Yes for SDA

Sites 3 sites.

Sites without configured ISE will be unselected automatically

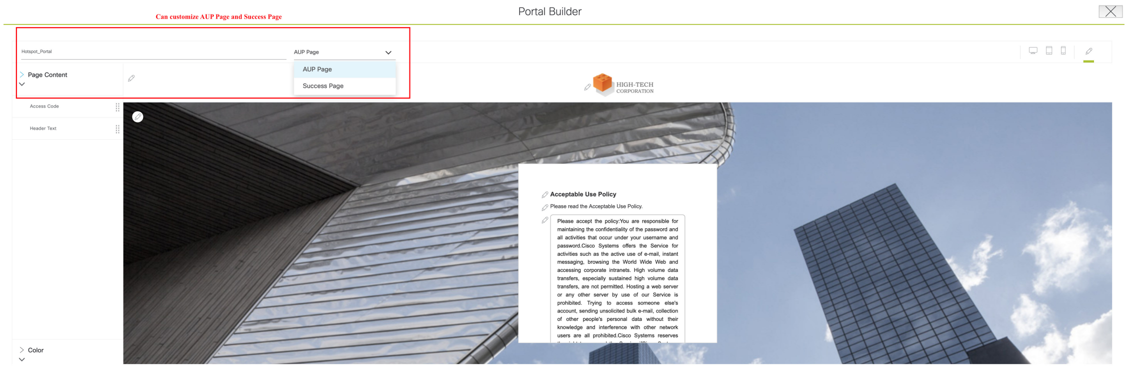
Attach Template(s)

Device Type	Device Tag	Template
No data to display		

Step 6 Click **Next**.

Step 7 To customize the portal, do one of the following:

- Configure a custom portal within Cisco DNA Center GUI.
- Select a default template.



Acceptable Use Policy

Please read the Acceptable Use Policy.

Please accept the policy:You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited.Cisco Systems reserves

Note This step is automated and does not require any additional configuration on Cisco ISE. Based on the portal configuration, a new hotspot portal is configured on Cisco ISE for the SSID created. However, existing portals are not affected.

Step 8 Click **Finish** and reprovision the WLC on the **Provision** window.

Reprovisioning the WLC pushes the following configurations on each node:

- SSID is configured on the WLC and remains in disabled state as the IP Pool is not yet assigned.
- The portal that is created in Step 6, on page 10 is configured on Cisco ISE under **Workstation** > **Guest Access** > **Portals and Components** with the same name provided during Step 6, on page 10.
- Authorization profile based on the portal name, which has the hotspot portal redirection URL when the client is in **Web Auth** pending state.
- Two authorization policies; one for redirecting hotspot clients to the previously mentioned authorization profile after MAC authorization and one for success profile.

What to do next

Assign IP pool for the SSID. See Assign IP Pool for SSID, on page 13.

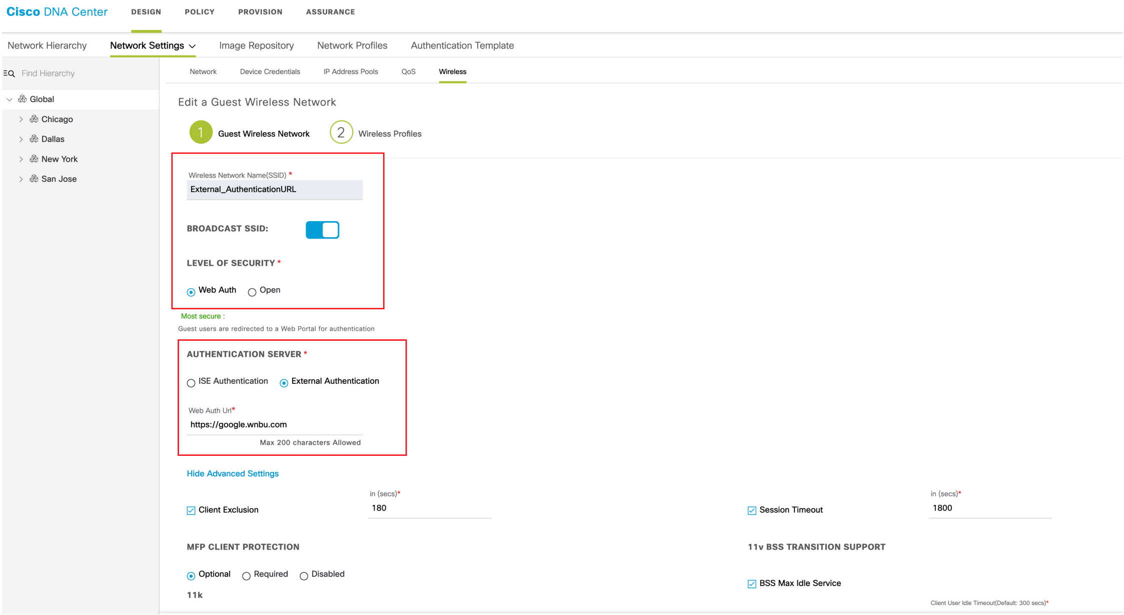
Configure EWA

Procedure

Step 1 From the Cisco DNA Center GUI, click the **Menu** icon and choose **Design** > **Network Settings** > **Wireless**.

Step 2 To add a new SSID under **Guest Wireless**, click **Add** and complete the following fields:

- **Wireless Network Name (SSID)**: Enter the name of the wireless network.
- **LEVEL OF SECURITY**: Click the **Web Auth** radio button.
- **AUTHENTICATION SERVER**: Click the **External Authentication** radio button and enter the external web URL where the authentication portal is hosted.



Edit a Guest Wireless Network

1 Guest Wireless Network 2 Wireless Profiles

Wireless Network Name(SSID) *: External_AuthenticationURL

BROADCAST SSID: on

LEVEL OF SECURITY *

● Web Auth ○ Open

Most secure :
Guest users are redirected to a Web Portal for authentication

AUTHENTICATION SERVER *

○ ISE Authentication ● External Authentication

Web Auth Url*: https://google.wnbu.com

Max 200 characters Allowed

Hide Advanced Settings

☑ Client Exclusion in (secs)*: 180

☑ Session Timeout in (secs)*: 1800

MFP CLIENT PROTECTION

● Optional ○ Required ○ Disabled

11k

11v BSS TRANSITION SUPPORT

☑ BSS Max Idle Service

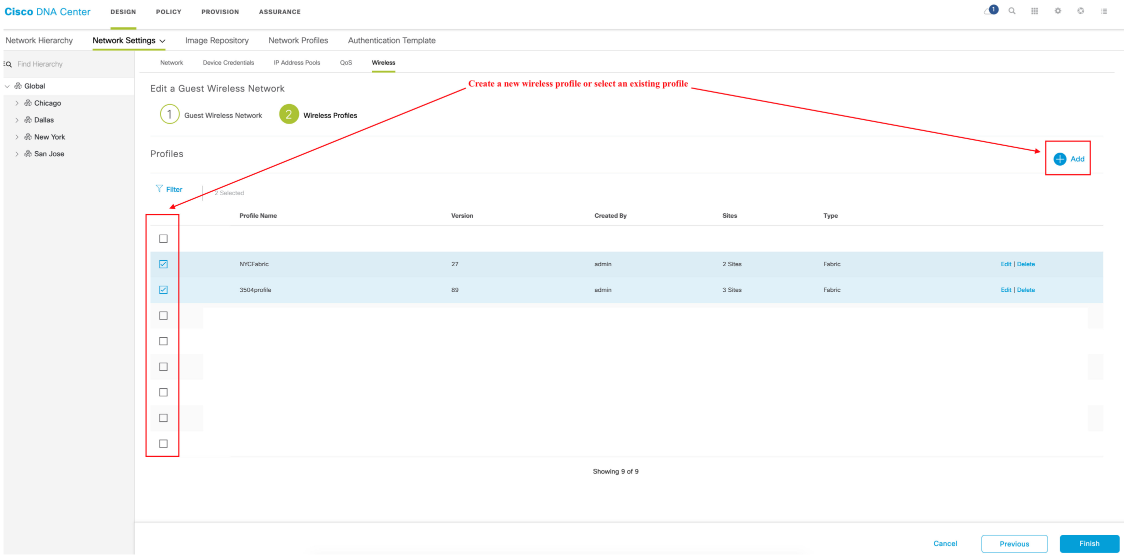
Client User Idle Timeout(Default: 300 secs)*

- Modify the additional settings as necessary.

Step 3 Click **Next**.

Step 4 To configure wireless profiles, do one of the following:

- Create a wireless profile.
- Select an existing wireless profile where enterprise SSIDs are already broadcast on the required sites.



Edit a Guest Wireless Network

1 Guest Wireless Network 2 Wireless Profiles

Create a new wireless profile or select an existing profile

Profiles

2 Selected

	Profile Name	Version	Created By	Sites	Type	
□						
☑	NYCFabric	27	admin	2 Sites	Fabric	Edit | Delete
☑	3504profile	89	admin	3 Sites	Fabric	Edit | Delete
□						
□						
□						
□						
□						
□						

Showing 9 of 9

After you select the wireless profile, a dialog box appears for editing the wireless profile, where you can define the fabric or nonfabric capabilities for the SSID.

Step 5 To deploy SDA, click the **Yes** radio button under **Fabric**.

If necessary, select more templates under **Attach Template(s)**.

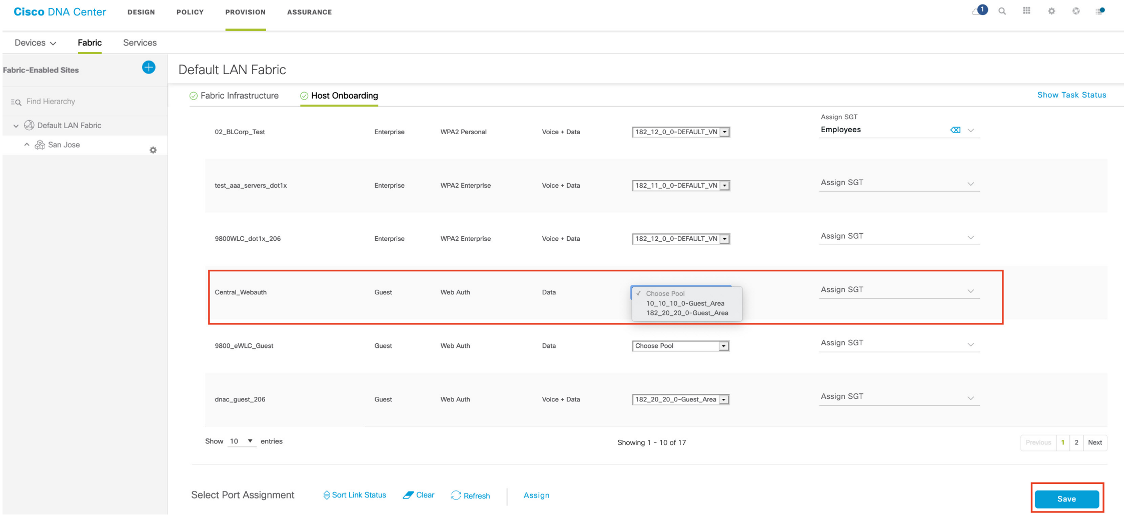
Step 6 Click **Finish**.

What to do next

Assign IP pool for the SSID. See Assign IP Pool for SSID, on page 13.

Assign IP Pool for SSID

To enable the CWA, hotspot, and EWA SSIDs on the WLC, assign an IP pool for the SSID on the **Host Onboarding** page.



02_BLCorp_Test	Enterprise	WPA2 Personal	Voice + Data	182_12_0_0-DEFAULT_VN	Assign SGT Employees
test_aaa_servers_dot1x	Enterprise	WPA2 Enterprise	Voice + Data	182_11_0_0-DEFAULT_VN	Assign SGT
9800WLC_dot1x_206	Enterprise	WPA2 Enterprise	Voice + Data	182_12_0_0-DEFAULT_VN	Assign SGT
Central_Webauth	Guest	Web Auth	Data	✓ Choose Pool 10_10_10_0-Guest_Area 182_20_20_0-Guest_Area	Assign SGT
9800_eWLC_Guest	Guest	Web Auth	Data	Choose Pool	Assign SGT
dnac_guest_206	Guest	Web Auth	Voice + Data	182_20_20_0-Guest_Area	Assign SGT

Show 10 entries

Showing 1 - 10 of 17

Verify Configuration on the Cisco AireOS WLC

Example: CWA

The following is a sample WLC SSID configuration:

```
(sdawlc3504) >show wlan 22

WLAN Identifier.................................. 22
Profile Name..................................... Central_We_Global_F_7e2e5fab
Network Name (SSID).............................. Central_Webauth
Status........................................... Enabled
MAC Filtering.................................... Enabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Enabled
Network Admission Control
Client Profiling Status
    Radius Profiling ............................ Disabled
     DHCP ....................................... Disabled
     HTTP ....................................... Disabled
    Local Profiling ............................. Enabled
     DHCP ....................................... Enabled (Auto)
     HTTP ....................................... Enabled (Auto)
  Radius-NAC State............................... Enabled
  SNMP-NAC State................................. Disabled
  Quarantine VLAN................................ 0
```

```
Maximum Clients Allowed.......................... Unlimited
Security Group Tag............................... Unknown(0)
Maximum number of Clients per AP Radio........... 200
ATF Policy....................................... 0
Number of Active Clients......................... 0
Exclusionlist Timeout............................ 180 seconds
Session Timeout.................................. 1800 seconds
User Idle Timeout................................ 300 seconds
Sleep Client..................................... disable
Sleep Client Timeout............................. 720 minutes
Sleep Client Auto Auth Feature................... Enabled
Web Auth Captive Bypass Mode..................... None
User Idle Threshold.............................. 0 Bytes
NAS-identifier................................... none
CHD per WLAN..................................... Enabled
Webauth DHCP exclusion........................... Disabled
Interface........................................ management
Multicast Interface.............................. Not Configured
WLAN IPv4 ACL.................................... unconfigured
WLAN IPv6 ACL.................................... unconfigured
WLAN Layer2 ACL.................................. unconfigured
WLAN URL ACL..................................... unconfigured
mDNS Status...................................... Disabled
mDNS Profile Name................................ default-mdns-profile
DHCP Server...................................... Default
Central NAT Peer-Peer Blocking................... Unknown
DHCP Address Assignment Required................. Disabled
Static IP client tunneling....................... Disabled
Tunnel Profile................................... Unconfigured
EoGRE Override VLAN state........................ disable
EoGRE Override VLAN ID........................... 0
PMIPv6 Mobility Type............................. none
    PMIPv6 MAG Profile........................... Unconfigured
    PMIPv6 Default Realm......................... Unconfigured
    PMIPv6 NAI Type.............................. Hexadecimal
    PMIPv6 MAG location.......................... WLC
Quality of Service............................... Silver
Per-SSID Rate Limits............................. Upstream      Downstream
Average Data Rate................................   0             0
Average Realtime Data Rate.......................   0             0
Burst Data Rate..................................   0             0
Burst Realtime Data Rate.........................   0             0
Per-Client Rate Limits........................... Upstream      Downstream
Average Data Rate................................   0             0
Average Realtime Data Rate.......................   0             0
Burst Data Rate..................................   0             0
Burst Realtime Data Rate.........................   0             0
Scan Defer Priority.............................. 4,5,6
Scan Defer Time.................................. 100 milliseconds
WMM.............................................. Allowed
WMM UAPSD Compliant Client Support............... Disabled
Media Stream Multicast-direct.................... Disabled
CCX - AironetIe Support.......................... Disabled
CCX - Gratuitous ProbeResponse (GPR)............. Disabled
CCX - Diagnostics Channel Capability............. Disabled
Dot11-Phone Mode (7920).......................... Disabled
Wired Protocol................................... 802.1P (Tag=0)
Passive Client Feature........................... Disabled
Peer-to-Peer Blocking Action..................... Disabled
Radio Policy..................................... All
DTIM period for 802.11a radio.................... 1
DTIM period for 802.11b radio.................... 1
Radius Servers
   Authentication................................ 192.168.2.193 1812 *
   Accounting.................................... 192.168.2.193 1813 *
      Interim Update............................. Enabled
      Interim Update Interval.................... 0
      Framed IPv6 Acct AVP ...................... Prefix
   Authorization ACA............................. Disabled
   Accounting ACA................................ Disabled
   Dynamic Interface............................. Disabled
   Dynamic Interface Priority.................... wlan
Local EAP Authentication......................... Disabled
Radius NAI-Realm................................. Disabled
Radius Authentication caching.................... Disabled
Mu-Mimo.......................................... Enabled
Security

   802.11 Authentication:........................ Open System
   FT Support.................................... Disabled
   Static WEP Keys............................... Disabled
   802.1X........................................ Disabled
   Wi-Fi Protected Access (WPA/WPA2)............. Disabled
   Wi-Fi Direct policy configured................ Disabled
   EAP-Passthrough............................... Disabled
   CKIP ......................................... Disabled
   Web Based Authentication...................... Disabled
   Web Authentication Timeout.................... 300
   Web-Passthrough............................... Disabled
   Mac-auth-server............................... 0.0.0.0
   Web-portal-server............................. 0.0.0.0
   qrscan-des-key................................
   Conditional Web Redirect...................... Disabled
   Splash-Page Web Redirect...................... Disabled
   Auto Anchor................................... Disabled
   FlexConnect Local Switching................... Disabled
   FlexConnect Central Association............... Disabled
   flexconnect Central Dhcp Flag................. Disabled
   flexconnect nat-pat Flag...................... Disabled
   flexconnect Dns Override Flag................. Disabled
   flexconnect PPPoE pass-through................ Disabled
   flexconnect local-switching IP-source-guar.... Disabled
   FlexConnect Vlan based Central Switching ..... Disabled
   FlexConnect Local Authentication.............. Disabled
   FlexConnect Learn IP Address.................. Enabled
   Fleconnect Post-Auth IPv4 ACL................. Unconfigured
   Fleconnect Post-Auth IPv6 ACL................. Unconfigured
   Client MFP.................................... Optional but inactive (WPA2 not configured)
   PMF........................................... Disabled
   PMF Association Comeback Time................. 1
   PMF SA Query RetryTimeout..................... 200
   Tkip MIC Countermeasure Hold-down Timer....... 60
   Eap-params.................................... Not Applicable
AVC Visibilty.................................... Disabled
AVC Profile Name................................. None
OpenDns Profile Name............................. None
OpenDns Wlan Mode................................ ignore
OpenDns Wlan Dhcp Option 6....................... enable
Flow Monitor Name................................ None
Split Tunnel Configuration
    Split Tunnel................................. Disabled
Call Snooping.................................... Disabled
Roamed Call Re-Anchor Policy..................... Disabled
SIP CAC Fail Send-486-Busy Policy................ Enabled
SIP CAC Fail Send Dis-Association Policy......... Disabled
KTS based CAC Policy............................. Disabled
Assisted Roaming Prediction Optimization......... Disabled
802.11k Neighbor List............................ Enabled
```

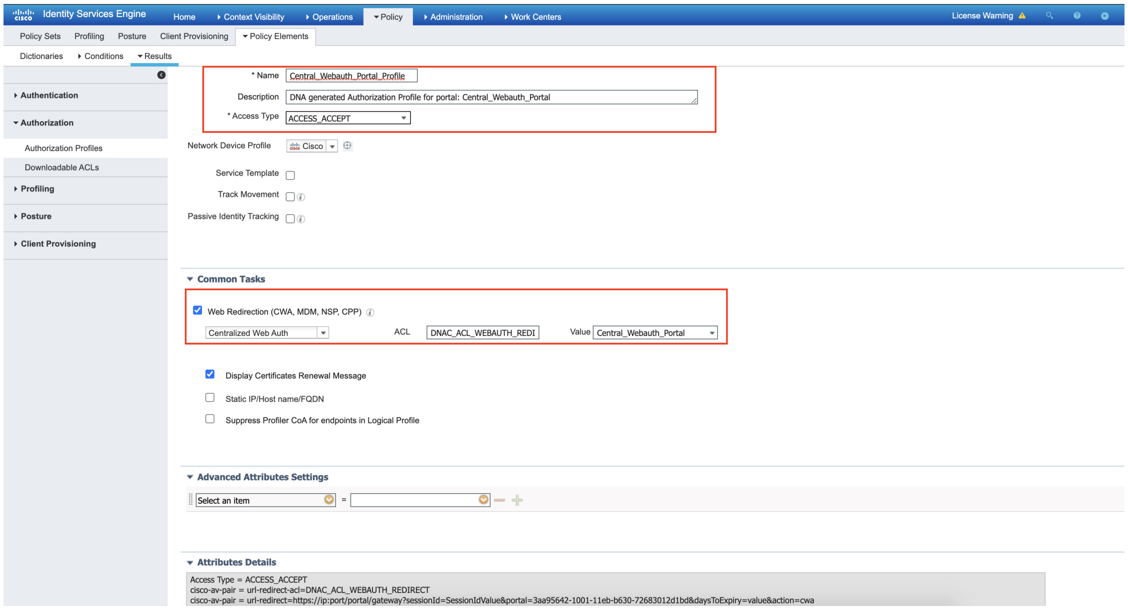
```
802.11k Neighbor List Dual Band.................. Disabled
802.11v Directed Multicast Service............... Enabled
802.11v BSS Max Idle Service..................... Enabled
802.11v BSS Transition Service................... Enabled
802.11v BSS Transition Disassoc Imminent......... Disabled
802.11v BSS Transition Disassoc Timer............ 200
802.11v BSS Transition OpRoam Disassoc Timer..... 40
DMS DB is empty
Band Select...................................... Disabled
Load Balancing................................... Disabled
Multicast Buffer................................. Disabled
Universal Ap Admin............................... Disabled
Broadcast Tagging................................ Disabled
PRP.............................................. Disabled
Fast Receive..................................... Disabled

 Mobility Anchor List
 WLAN ID     IP Address            Status                             Priority
 -------     ---------------       ------                             --------

802.11u........................................ Disabled

MSAP Services.................................. Disabled

Local Policy
----------------
Priority  Policy Name
--------  ---------------

Lync State ...................................... Disabled
Audio QoS Policy................................. Silver
Video QoS Policy................................. Silver
App-Share QoS Policy............................. Silver
File Transfer QoS Policy......................... Silver
Lync State ...................................... Disabled
Audio QoS Policy................................. Silver
Video QoS Policy................................. Silver
App-Share QoS Policy............................. Silver
File Transfer QoS Policy......................... Silver
File Transfer QoS Policy......................... Silver
QoS Fastlane Status.............................. Disable
Selective Reanchoring Status..................... Disable
Lobby Admin Access............................... Disabled

 Fabric Status
--------------

Fabric status.................................... Enabled
Vnid Name........................................ 182_20_20_0-Guest_Area
Vnid............................................. 8196
Applied SGT Tag.................................. 0
Peer Ip Address.................................. 0.0.0.0
Flex Acl Name....................................
Flex IPv6 Acl Name...............................
Flex Avc Policy Name.............................

U3-Interface................................... Disable

U3-Reporting Interval.......................... 30
```

The following is a sample WLC ACL configuration:

```
(sdawlc3504) >show flexconnect acl detailed DNAC_ACL_WEBAUTH_REDIRECT

                   Source                        Destination               Source Port  Dest Port
```

```
Index        IP Address/Netmask              IP Address/Netmask        Prot   Range       Range     DSCP  Action
------ ------------------------------- ------------------------------- ---- ----------- ----------- -----
-------
     1    192.168.5.10/255.255.255.255         0.0.0.0/0.0.0.0           17    67-67       68-68     Any Permit

     2         0.0.0.0/0.0.0.0           192.168.5.10/255.255.255.255   17    68-68       67-67     Any Permit

     3         1.2.3.4/255.255.255.255         0.0.0.0/0.0.0.0           17    53-53        0-65535  Any Permit

     4         0.0.0.0/0.0.0.0                1.2.3.4/255.255.255.255   17     0-65535    53-53     Any Permit

     5         1.2.3.4/255.255.255.255         0.0.0.0/0.0.0.0            6    53-53        0-65535  Any Permit

     6         0.0.0.0/0.0.0.0                1.2.3.4/255.255.255.255    6     0-65535    53-53     Any Permit

     7    192.168.5.10/255.255.255.255         0.0.0.0/0.0.0.0           17    53-53        0-65535  Any Permit

     8         0.0.0.0/0.0.0.0           192.168.5.10/255.255.255.255   17     0-65535    53-53     Any Permit

     9    192.168.5.10/255.255.255.255         0.0.0.0/0.0.0.0            6    53-53        0-65535  Any Permit

    10         0.0.0.0/0.0.0.0           192.168.5.10/255.255.255.255    6     0-65535    53-53     Any Permit

    11   192.168.2.193/255.255.255.255         0.0.0.0/0.0.0.0          Any     0-65535     0-65535  Any Permit

    12         0.0.0.0/0.0.0.0          192.168.2.193/255.255.255.255  Any     0-65535     0-65535  Any Permit
No URL rules are configured for this Flexconnect Acl.
```

The following sample shows a Cisco ISE authorization profile:



* Name: Central_Webauth_Portal_Profile

Description: DNA generated Authorization Profile for portal: Central_Webauth_Portal

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Passive Identity Tracking □

Common Tasks

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

Centralized Web Auth — ACL: DNAC_ACL_WEBAUTH_REDI — Value: Central_Webauth_Portal

☑ Display Certificates Renewal Message

□ Static IP/Host name/FQDN

□ Suppress Profiler CoA for endpoints in Logical Profile

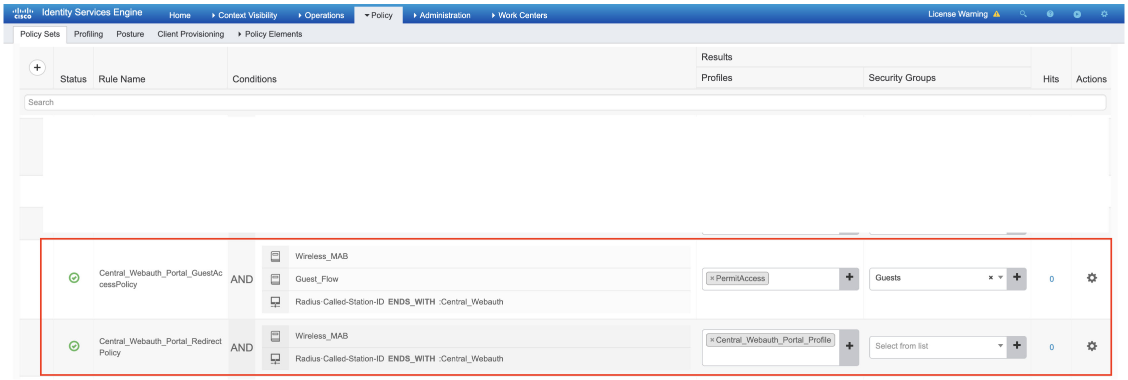
Advanced Attributes Settings

Select an item =

Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-acl=DNAC_ACL_WEBAUTH_REDIRECT
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=3aa95642-1001-11eb-b630-72683012d1bd&daysToExpiry=value&action=cwa
```

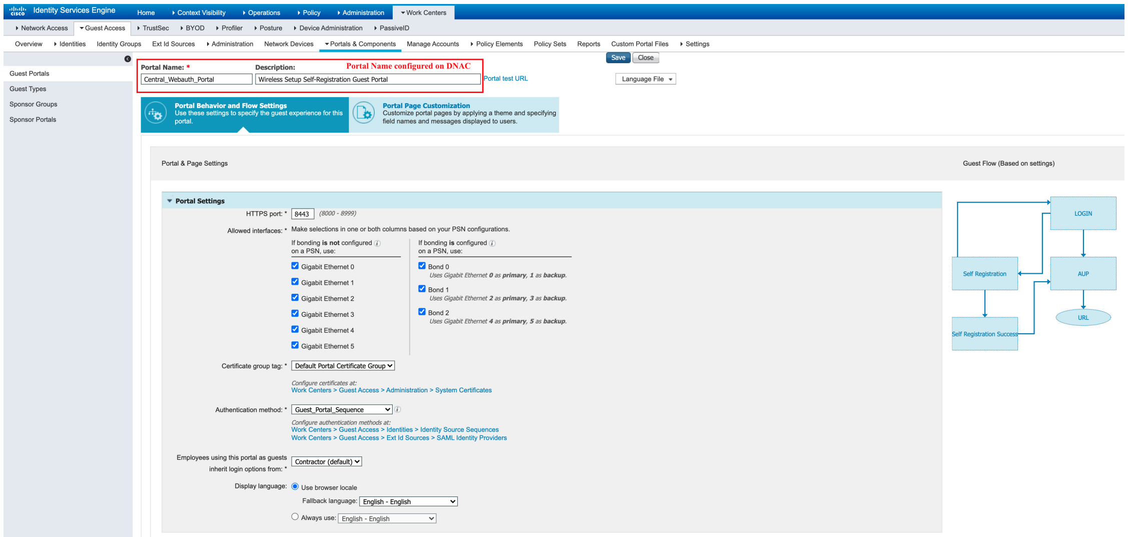
The following sample shows Cisco ISE authorization policies:



Status	Rule Name	Conditions	Results: Profiles	Results: Security Groups	Hits	Actions
✓	Central_Webauth_Portal_GuestAccessPolicy	AND Wireless_MAB Guest_Flow Radius·Called-Station-ID ENDS_WITH :Central_Webauth	× PermitAccess	Guests	0	⚙
✓	Central_Webauth_Portal_Redirect Policy	AND Wireless_MAB Radius·Called-Station-ID ENDS_WITH :Central_Webauth	× Central_Webauth_Portal_Profile	Select from list	0	⚙

The following sample shows a Cisco ISE portal that is pushed by the Cisco DNA Center:

Note After creating the portal, you cannot modify it from the Cisco DNA Center. Also, the Cisco DNA Center does not update the portal. However, you can modify the portal on Cisco ISE after the initial configuration push.



Portal Name: * Central_Webauth_Portal

Description: Wireless Setup Self-Registration Guest Portal

Portal Name configured on DNAC

Portal Behavior and Flow Settings
Use these settings to specify the guest experience for this portal.

Portal Page Customization
Customize portal pages by applying a theme and specifying field names and messages displayed to users.

Portal & Page Settings

Portal Settings

HTTPS port: * 8443 *(8000 - 8999)*

Allowed interfaces: * Make selections in one or both columns based on your PSN configurations.

If bonding **is not** configured on a PSN, use:

- ☑ Gigabit Ethernet 0
- ☑ Gigabit Ethernet 1
- ☑ Gigabit Ethernet 2
- ☑ Gigabit Ethernet 3
- ☑ Gigabit Ethernet 4
- ☑ Gigabit Ethernet 5

If bonding **is** configured on a PSN, use:

- ☑ Bond 0 *Uses Gigabit Ethernet **0** as **primary**, **1** as **backup**.*
- ☑ Bond 1 *Uses Gigabit Ethernet **2** as **primary**, **3** as **backup**.*
- ☑ Bond 2 *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

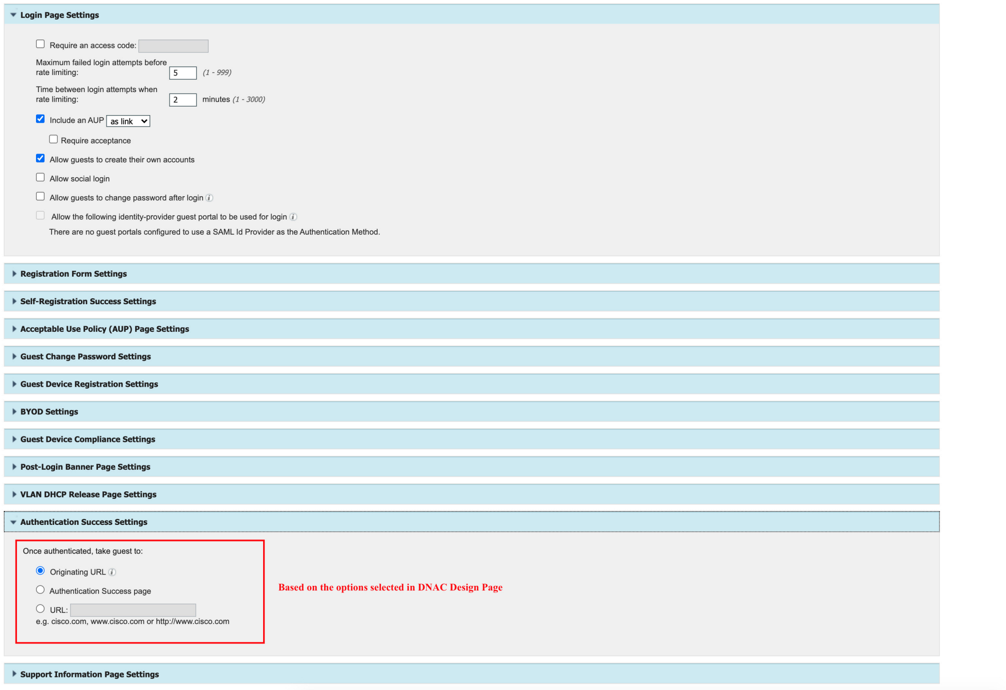
Configure authentication methods at:
Work Centers > Guest Access > Identities > Identity Source Sequences
Work Centers > Guest Access > Ext Id Sources > SAML Identity Providers

Employees using this portal as guests inherit login options from: * Contractor (default)

Display language: ● Use browser locale

Fallback language: 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 social login

☐ Allow guests to change password after login

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

There are no guest portals configured to use a SAML Id Provider as the Authentication Method.

▶ Registration Form Settings

▶ Self-Registration Success Settings

▶ Acceptable Use Policy (AUP) Page Settings

▶ Guest Change Password Settings

▶ Guest Device Registration Settings

▶ BYOD Settings

▶ Guest Device Compliance Settings

▶ Post-Login Banner Page Settings

▶ VLAN DHCP Release Page Settings

▼ Authentication Success Settings

Once authenticated, take guest to:

● Originating URL

○ Authentication Success page

○ URL:

e.g. cisco.com, www.cisco.com or http://www.cisco.com

Based on the options selected in DNAC Design Page

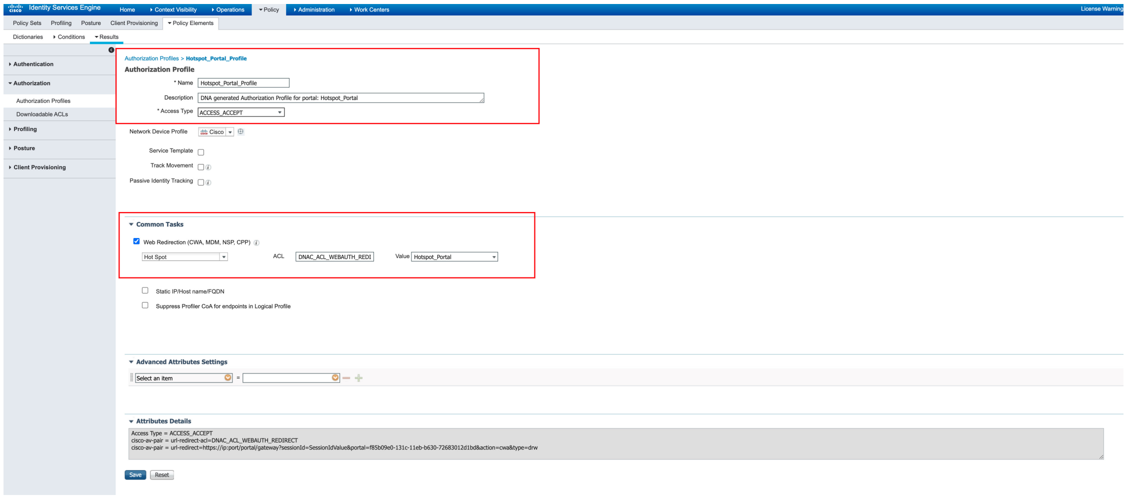
▶ Support Information Page Settings

Example: Hotspot

The following is a sample WLC ACL configuration:

```
(sdawlc3504) >show flexconnect acl detailed DNAC_ACL_WEBAUTH_REDIRECT

                   Source                         Destination              Source Port  Dest Port
Index         IP Address/Netmask              IP Address/Netmask       Prot    Range       Range     DSCP  Action
------ ------------------------------- ------------------------------- ---- ----------- ----------- -----
-------
     1    192.168.5.10/255.255.255.255        0.0.0.0/0.0.0.0            17    67-67        68-68       Any Permit

     2         0.0.0.0/0.0.0.0           192.168.5.10/255.255.255.255   17    68-68        67-67       Any Permit

     3         1.2.3.4/255.255.255.255        0.0.0.0/0.0.0.0            17    53-53         0-65535    Any Permit

     4         0.0.0.0/0.0.0.0                1.2.3.4/255.255.255.255   17      0-65535    53-53       Any Permit

     5         1.2.3.4/255.255.255.255        0.0.0.0/0.0.0.0             6    53-53         0-65535    Any Permit

     6         0.0.0.0/0.0.0.0                1.2.3.4/255.255.255.255    6      0-65535    53-53       Any Permit

     7    192.168.5.10/255.255.255.255        0.0.0.0/0.0.0.0            17    53-53         0-65535    Any Permit

     8         0.0.0.0/0.0.0.0           192.168.5.10/255.255.255.255   17      0-65535    53-53       Any Permit

     9    192.168.5.10/255.255.255.255        0.0.0.0/0.0.0.0             6    53-53         0-65535    Any Permit

    10         0.0.0.0/0.0.0.0           192.168.5.10/255.255.255.255    6      0-65535    53-53       Any Permit

    11   192.168.2.193/255.255.255.255        0.0.0.0/0.0.0.0           Any     0-65535      0-65535    Any Permit

    12         0.0.0.0/0.0.0.0          192.168.2.193/255.255.255.255  Any     0-65535      0-65535    Any Permit

No URL rules are configured for this Flexconnect Acl.
```

The following sample shows a Cisco ISE authorization profile:



Authorization Profiles > Hotspot_Portal_Profile

Authorization Profile

* Name: Hotspot_Portal_Profile

Description: DNA generated Authorization Profile for portal: Hotspot_Portal

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Passive Identity Tracking □

Common Tasks

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

Hot Spot   ACL: DNAC_ACL_WEBAUTH_REDI   Value: Hotspot_Portal

□ Static IP/Host name/FQDN

□ Suppress Profiler CoA for endpoints in Logical Profile

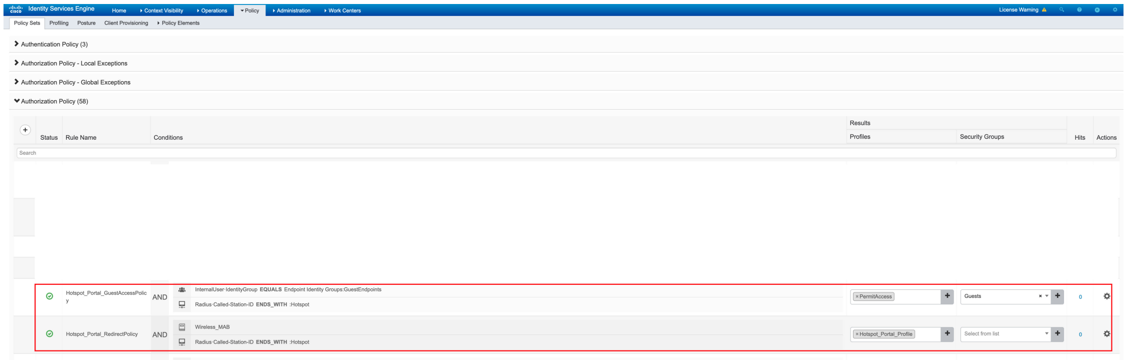
Advanced Attributes Settings

Select an item =

Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-acl=DNAC_ACL_WEBAUTH_REDIRECT
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=f85b09e0-131c-11eb-b630-72683012d1bd&action=cwa&type=drw
```

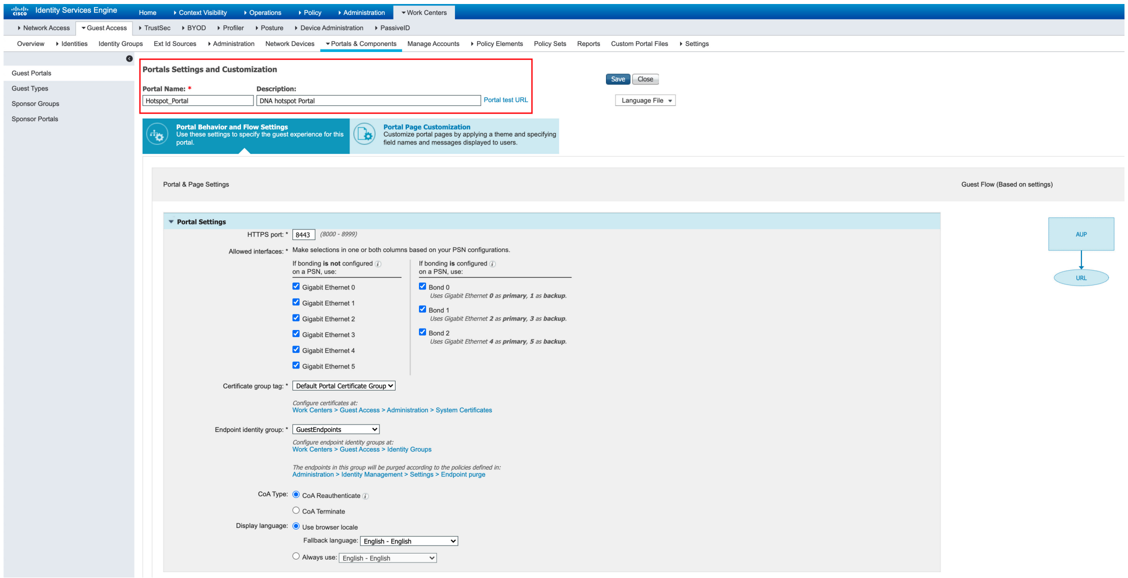
The following sample shows Cisco ISE authorization policies:



Status	Rule Name		Conditions	Results Profiles	Security Groups	Hits	Actions
✓	Hotspot_Portal_GuestAccessPolicy	AND	InternalUser·IdentityGroup EQUALS Endpoint Identity Groups:GuestEndpoints Radius·Called-Station-ID ENDS_WITH :Hotspot	PermitAccess	Guests	0	
✓	Hotspot_Portal_RedirectPolicy	AND	Wireless_MAB Radius·Called-Station-ID ENDS_WITH :Hotspot	Hotspot_Portal_Profile	Select from list	0	

The following sample shows a Cisco ISE portal that is pushed by the Cisco DNA Center:

Note After creating the portal, you cannot modify it from Cisco DNA Center. Also, the Cisco DNA Center does not update the portal. However, you can modify the portal on Cisco ISE after the initial configuration push.



Portals Settings and Customization

Portal Name: * Hotspot_Portal

Description: DNA hotspot Portal

Portal test URL

Portal Behavior and Flow Settings
Use these settings to specify the guest experience for this portal.

Portal Page Customization
Customize portal pages by applying a theme and specifying field names and messages displayed to users.

Portal & Page Settings

Portal Settings

HTTPS port: * 8443 (8000 - 8999)

Allowed interfaces: * Make selections in one or both columns based on your PSN configurations.

If bonding **is not** configured on a PSN, use:

- ☑ Gigabit Ethernet 0
- ☑ Gigabit Ethernet 1
- ☑ Gigabit Ethernet 2
- ☑ Gigabit Ethernet 3
- ☑ Gigabit Ethernet 4
- ☑ Gigabit Ethernet 5

If bonding **is** configured on a PSN, use:

- ☑ Bond 0
  *Uses Gigabit Ethernet **0** as **primary**, **1** as **backup**.*
- ☑ Bond 1
  *Uses Gigabit Ethernet **2** as **primary**, **3** as **backup**.*
- ☑ Bond 2
  *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

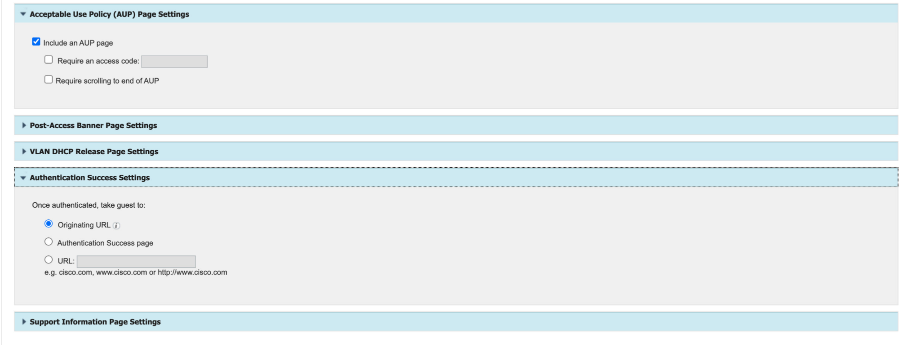
Endpoint identity group: * GuestEndpoints

Configure endpoint identity groups at:
Work Centers > Guest Access > Identity Groups

The endpoints in this group will be purged according to the policies defined in:
Administration > Identity Management > Settings > Endpoint purge

CoA Type: ● CoA Reauthenticate ○ CoA Terminate

Display language: ● Use browser locale
Fallback language: English - English
○ Always use: English - English



Acceptable Use Policy (AUP) Page Settings

☑ Include an AUP page
□ Require an access code:
□ Require scrolling to end of AUP

Post-Access Banner Page Settings

VLAN DHCP Release Page Settings

Authentication Success Settings

Once authenticated, take guest to:
● Originating URL
○ Authentication Success page
○ URL:
e.g. cisco.com, www.cisco.com or http://www.cisco.com

Support Information Page Settings

Example: EWA

The following is a sample WLC SSID configuration:

```
WLAN Identifier.................................. 21
Profile Name..................................... External_A_Global_F_0c2bc41f
Network Name (SSID).............................. External_AuthenticationURL
Status........................................... Enabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Enabled
Network Admission Control
Client Profiling Status
    Radius Profiling ............................ Disabled
     DHCP ....................................... Disabled
     HTTP ....................................... Disabled
    Local Profiling ............................. Enabled
     DHCP ....................................... Enabled
     HTTP ....................................... Enabled
  Radius-NAC State............................... Disabled
  SNMP-NAC State................................. Disabled
  Quarantine VLAN................................ 0
Maximum Clients Allowed.......................... Unlimited
Security Group Tag............................... Unknown(0)
Maximum number of Clients per AP Radio........... 200
```

```
ATF Policy....................................... 0
Number of Active Clients......................... 0
Exclusionlist Timeout............................ 180 seconds
Session Timeout.................................. 1800 seconds
User Idle Timeout................................ 300 seconds
Sleep Client..................................... disable
Sleep Client Timeout............................. 720 minutes
Sleep Client Auto Auth Feature................... Enabled
Web Auth Captive Bypass Mode..................... None
User Idle Threshold.............................. 0 Bytes
NAS-identifier................................... none
CHD per WLAN..................................... Enabled
Webauth DHCP exclusion........................... Disabled
Interface........................................ management
Multicast Interface.............................. Not Configured
WLAN IPv4 ACL.................................... unconfigured
WLAN IPv6 ACL.................................... unconfigured
WLAN Layer2 ACL.................................. unconfigured
WLAN URL ACL..................................... unconfigured
mDNS Status...................................... Disabled
mDNS Profile Name................................ default-mdns-profile
DHCP Server...................................... Default
Central NAT Peer-Peer Blocking................... Unknown
DHCP Address Assignment Required................. Disabled
Static IP client tunneling....................... Disabled
Tunnel Profile................................... Unconfigured
EoGRE Override VLAN state........................ disable
EoGRE Override VLAN ID........................... 0
PMIPv6 Mobility Type............................. none
    PMIPv6 MAG Profile........................... Unconfigured
    PMIPv6 Default Realm......................... Unconfigured
    PMIPv6 NAI Type.............................. Hexadecimal
    PMIPv6 MAG location.......................... WLC
Quality of Service............................... Silver
Per-SSID Rate Limits............................. Upstream      Downstream
Average Data Rate................................   0             0
Average Realtime Data Rate.......................   0             0
Burst Data Rate..................................   0             0
Burst Realtime Data Rate.........................   0             0
Per-Client Rate Limits........................... Upstream      Downstream
Average Data Rate................................   0             0
Average Realtime Data Rate.......................   0             0
Burst Data Rate..................................   0             0
Burst Realtime Data Rate.........................   0             0
Scan Defer Priority.............................. 4,5,6
Scan Defer Time.................................. 100 milliseconds
WMM.............................................. Allowed
WMM UAPSD Compliant Client Support............... Disabled
Media Stream Multicast-direct.................... Disabled
CCX - AironetIe Support.......................... Disabled
CCX - Gratuitous ProbeResponse (GPR)............. Disabled
CCX - Diagnostics Channel Capability............. Disabled
Dot11-Phone Mode (7920).......................... Disabled
Wired Protocol................................... 802.1P (Tag=0)
Passive Client Feature........................... Disabled
Peer-to-Peer Blocking Action..................... Disabled
Radio Policy..................................... All
DTIM period for 802.11a radio.................... 1
DTIM period for 802.11b radio.................... 1
Radius Servers
   Authentication................................ 192.168.2.193 1812 *
   Accounting.................................... 192.168.2.193 1813 *
      Interim Update............................. Enabled
      Interim Update Interval.................... 0
      Framed IPv6 Acct AVP ...................... Prefix
   Authorization ACA............................. Disabled
   Accounting ACA................................ Disabled
   Dynamic Interface............................. Disabled
   Dynamic Interface Priority.................... wlan
Local EAP Authentication......................... Disabled
Radius NAI-Realm................................. Disabled
Radius Authentication caching.................... Disabled
Mu-Mimo.......................................... Enabled
Security

   802.11 Authentication:........................ Open System
   FT Support.................................... Disabled
   Static WEP Keys............................... Disabled
   802.1X........................................ Disabled
   Wi-Fi Protected Access (WPA/WPA2/WPA3)........ Disabled
   Wi-Fi Direct policy configured................ Disabled
   EAP-Passthrough............................... Disabled
   CKIP ......................................... Disabled
   Web Based Authentication...................... Enabled
   Web Authentication Timeout.................... 300
        IPv4 ACL........................................ Unconfigured
        IPv6 ACL........................................ Unconfigured
        Web-Auth Flex ACL............................... EXT_REDIRECT_ACL_91.195.241.136
        Web-Auth Flex IPV6 ACL.......................... EXT_RE_ACL_IPV6_91.195.241.136
        Web Authentication server precedence:
        1............................................... radius
        Web-Auth done locally on AP:.................... NO
   Web-Passthrough............................... Disabled
   Mac-auth-server............................... 0.0.0.0
   Web-portal-server............................. 0.0.0.0
   qrscan-des-key................................
   Conditional Web Redirect...................... Disabled
   Splash-Page Web Redirect...................... Disabled
   Auto Anchor................................... Disabled
   FlexConnect Local Switching................... Disabled
   FlexConnect Central Association............... Disabled
   flexconnect Central Dhcp Flag................. Disabled
   flexconnect nat-pat Flag...................... Disabled
   flexconnect Dns Override Flag................. Disabled
   flexconnect PPPoE pass-through................ Disabled
   flexconnect local-switching IP-source-guar.... Disabled
   FlexConnect Vlan based Central Switching ..... Disabled
   FlexConnect Local Authentication.............. Disabled
   FlexConnect Learn IP Address.................. Enabled
   Flexconnect Post-Auth IPv4 ACL................ Unconfigured
   Flexconnect Post-Auth IPv6 ACL................ Unconfigured
   Client MFP.................................... Optional but inactive (WPA2 not configured)
   PMF........................................... Disabled
   PMF Association Comeback Time................. 1
   PMF SA Query RetryTimeout..................... 200
   Tkip MIC Countermeasure Hold-down Timer....... 60
   Eap-params.................................... Not Applicable
AVC Visibilty.................................... Disabled
AVC Profile Name................................. None
OpenDns Profile Name............................. None
OpenDns Wlan Mode................................ ignore
OpenDns Wlan Dhcp Option 6....................... enable
Flow Monitor Name................................ None
Split Tunnel Configuration
    Split Tunnel................................. Disabled
Call Snooping.................................... Disabled
Roamed Call Re-Anchor Policy..................... Disabled
SIP CAC Fail Send-486-Busy Policy................ Enabled
SIP CAC Fail Send Dis-Association Policy......... Disabled
KTS based CAC Policy............................. Disabled
Assisted Roaming Prediction Optimization......... Disabled
802.11k Neighbor List............................ Enabled
802.11k Neighbor List Dual Band.................. Disabled
802.11v Directed Multicast Service............... Enabled
802.11v BSS Max Idle Service..................... Enabled
802.11v BSS Transition Service................... Enabled
802.11v BSS Transition Disassoc Imminent......... Disabled
802.11v BSS Transition Disassoc Timer............ 200
802.11v BSS Transition OpRoam Disassoc Timer..... 40
802.11v BSS Transition Neigh List Dual Band...... Disabled
DMS DB is empty
Band Select...................................... Disabled
Load Balancing................................... Disabled
Multicast Buffer................................. Disabled
Universal Ap Admin............................... Disabled
Broadcast Tagging................................ Disabled
PRP.............................................. Disabled
Fast Receive..................................... Disabled
11ax Downlink MU-MIMO............................ Enabled
11ax Uplink MU-MIMO.............................. Enabled
11ax Downlink OFDMA.............................. Enabled
11ax Uplink OFDMA................................ Enabled
Wifi Alliance Multiband Operation................ Disabled
11ax Target Wake Time............................ Enabled

 Mobility Anchor List
 WLAN ID     IP Address            Status                             Priority
 -------     ---------------       ------                             --------

802.11u........................................ Disabled

MSAP Services.................................. Disabled

Local Policy
----------------
Priority  Policy Name
--------  ---------------

Lync State ...................................... Disabled
Audio QoS Policy................................. Silver
Video QoS Policy................................. Silver
App-Share QoS Policy............................. Silver
File Transfer QoS Policy......................... Silver
Lync State ...................................... Disabled
Audio QoS Policy................................. Silver
Video QoS Policy................................. Silver
App-Share QoS Policy............................. Silver
File Transfer QoS Policy......................... Silver
File Transfer QoS Policy......................... Silver
QoS Fastlane Status.............................. Disable
Selective Reanchoring Status..................... Disable
Lobby Admin Access............................... Disabled

 Fabric Status
--------------

Fabric status.................................... Enabled
Vnid Name........................................ 182_20_20_0-Guest_Area
Vnid............................................. 8196
Applied SGT Tag.................................. 0
Peer Ip Address.................................. 0.0.0.0
Flex Acl Name....................................
Flex IPv6 Acl Name...............................
Flex Avc Policy Name.............................

U3-Interface................................... Disable

U3-Reporting Interval.......................... 30
```

The following is a sample WLC ACL configuration. ACL is created based on DHCP, DNS, and Cisco ISE or external AAA server added for configured sites.

```
                   Source                        Destination                Source Port  Dest Port
Index        IP Address/Netmask             IP Address/Netmask        Prot   Range       Range    DSCP  Action
------ ------------------------------- ------------------------------- ---- ----------- ----------- -----
-------
     1    192.168.5.10/255.255.255.255         0.0.0.0/0.0.0.0          17    67-67       68-68     Any Permit

     2         0.0.0.0/0.0.0.0           192.168.5.10/255.255.255.255   17    68-68       67-67     Any Permit

     3         1.2.3.4/255.255.255.255         0.0.0.0/0.0.0.0          17    53-53        0-65535  Any Permit

     4         0.0.0.0/0.0.0.0                1.2.3.4/255.255.255.255   17     0-65535    53-53     Any Permit

     5         1.2.3.4/255.255.255.255         0.0.0.0/0.0.0.0           6    53-53        0-65535  Any Permit

     6         0.0.0.0/0.0.0.0                1.2.3.4/255.255.255.255    6     0-65535    53-53     Any Permit

     7    192.168.5.10/255.255.255.255         0.0.0.0/0.0.0.0          17    53-53        0-65535  Any Permit

     8         0.0.0.0/0.0.0.0           192.168.5.10/255.255.255.255   17     0-65535    53-53     Any Permit

     9    192.168.5.10/255.255.255.255         0.0.0.0/0.0.0.0           6    53-53        0-65535  Any Permit

    10         0.0.0.0/0.0.0.0           192.168.5.10/255.255.255.255    6     0-65535    53-53     Any Permit

    11  91.195.241.136/255.255.255.255         0.0.0.0/0.0.0.0         Any     0-65535     0-65535  Any Permit

    12         0.0.0.0/0.0.0.0         91.195.241.136/255.255.255.255  Any     0-65535     0-65535  Any Permit

No URL rules are configured for this Flexconnect Acl.
```

Note There is no configuration push for EWA SSID on Cisco ISE.

Verify Configuration on Cisco Catalyst 9800 Series WLC (IOS-Based)

Example: CWA

The following is a sample WLC SSID configuration:

```
wireless profile fabric Central_We_Global_F_7e2e5fab
 client-l2-vnid 8193
 description Central_We_Global_F_7e2e5fab

wireless profile policy Central_We_Global_F_7e2e5fab
 aaa-override
 no central dhcp
 no central switching
 description Central_We_Global_F_7e2e5fab
 dhcp-tlv-caching
 exclusionlist timeout 180
 fabric Central_We_Global_F_7e2e5fab
 http-tlv-caching
 nac
 service-policy input silver-up
 service-policy output silver
 no shutdown
 wlan Central_We_Global_F_7e2e5fab policy Central_We_Global_F_7e2e5fab

wlan Central_We_Global_F_7e2e5fab 26 Central_Webauth
 mac-filtering default
 no security ft adaptive
 no security wpa
 no security wpa wpa2 ciphers aes
 no security wpa akm dot1x
 no shutdown
```

The following is a sample WLC ACL and Default-flex-profile configuration:

```
Extended IP access list DNAC_ACL_WEBAUTH_REDIRECT
    1 deny udp host 192.168.5.10 eq bootps any eq bootpc
    2 deny udp any eq bootpc host 192.168.5.10 eq bootps
    3 deny udp host 192.168.5.10 eq domain any range 0 65535
    4 deny udp any range 0 65535 host 192.168.5.10 eq domain
    5 deny tcp host 192.168.5.10 eq domain any range 0 65535
    6 deny tcp any range 0 65535 host 192.168.5.10 eq domain
    7 deny ip host 192.168.2.193 any
    8 deny ip any host 192.168.2.193
    9 permit tcp any range 0 65535 any eq www
    10 permit tcp any range 0 65535 any eq 443

wireless profile flex default-flex-profile
 acl-policy DNAC_ACL_WEBAUTH_REDIRECT
  central-webauth
```

The Cisco ISE configurations are same as the Cisco AireOS WLC configurations.

Example: Hotspot

The following is a sample WLC SSID configuration:

```
wireless profile fabric Hotspot_Global_F_e42ed6d8
 client-l2-vnid 8196
 description Hotspot_Global_F_e42ed6d8

wireless profile policy Hotspot_Global_F_e42ed6d8
 aaa-override
 no central dhcp
 no central switching
 description Hotspot_Global_F_e42ed6d8
 dhcp-tlv-caching
 exclusionlist timeout 180
 fabric Hotspot_Global_F_e42ed6d8
 http-tlv-caching
 nac
 service-policy input silver-up
 service-policy output silver
 no shutdown
 wlan Hotspot_Global_F_e42ed6d8 policy Hotspot_Global_F_e42ed6d8

wlan Hotspot_Global_F_e42ed6d8 25 Hotspot
 mac-filtering default
 no security ft adaptive
 no security wpa
 no security wpa wpa2 ciphers aes
 no security wpa akm dot1x
```

The following is a sample WLC ACL and Default-flex-profile configuration:

Note Hotspot uses the same ACL that the CWA uses.

```
Extended IP access list DNAC_ACL_WEBAUTH_REDIRECT
    1 deny udp host 192.168.5.10 eq bootps any eq bootpc
    2 deny udp any eq bootpc host 192.168.5.10 eq bootps
    3 deny udp host 192.168.5.10 eq domain any range 0 65535
    4 deny udp any range 0 65535 host 192.168.5.10 eq domain
    5 deny tcp host 192.168.5.10 eq domain any range 0 65535
    6 deny tcp any range 0 65535 host 192.168.5.10 eq domain
    7 deny ip host 192.168.2.193 any
    8 deny ip any host 192.168.2.193
    9 permit tcp any range 0 65535 any eq www
    10 permit tcp any range 0 65535 any eq 443

wireless profile flex default-flex-profile
 acl-policy DNAC_ACL_WEBAUTH_REDIRECT
  central-webauth
```

Example: EWA

The following is a sample WLC SSID configuration:

```
wireless profile fabric External_A_Global_F_0c2bc41f
 client-l2-vnid 8193
 description External_A_Global_F_0c2bc41f

wireless profile policy External_A_Global_F_0c2bc41f
 aaa-override
 no central dhcp
 no central switching
 description External_A_Global_F_0c2bc41f
 dhcp-tlv-caching
 exclusionlist timeout 180
 fabric External_A_Global_F_0c2bc41f
 http-tlv-caching
 service-policy input silver-up
 service-policy output silver
 no shutdown
 wlan External_A_Global_F_0c2bc41f policy External_A_Global_F_0c2bc41f

wlan External_A_Global_F_0c2bc41f 28 External_AuthenticationURL
 ip access-group web EXT_REDIRECT_ACL_91.195.241.136
 no security ft adaptive
 no security wpa
 no security wpa wpa2 ciphers aes
 no security wpa akm dot1x
 security web-auth
 security web-auth authentication-list dnac-cts-list
 security web-auth parameter-map https---google-wnbu-com
 no shutdown
```

The following is a sample WLC ACL configuration:

```
Extended IP access list EXT_REDIRECT_ACL_91.195.241.136
    1 permit udp host 192.168.5.10 eq bootps any eq bootpc
    2 permit udp any eq bootpc host 192.168.5.10 eq bootps
    3 permit udp host 192.168.5.10 eq domain any range 0 65535
    4 permit udp any range 0 65535 host 192.168.5.10 eq domain
    5 permit tcp host 192.168.5.10 eq domain any range 0 65535
    6 permit tcp any range 0 65535 host 192.168.5.10 eq domain
    7 permit ip host 91.195.241.136 any
    8 permit ip any host 91.195.241.136

wireless profile flex default-flex-profile
 acl-policy EXT_REDIRECT_ACL_192.168.2.193
 description "default flex profile"
```

Troubleshoot: Client CWA Debugging

Complete the following steps to find out at what stage the issue occurs:

Before you begin

You must use Cisco DNA Center to deploy CWA in SD-Access. After deployment, the Cisco DNA Center deploys authorization policy, authentication policy, and authorization profile on the Cisco ISE. Manually configure the identities for authentication similar to the configuration for Dot1x.

Procedure

Step 1 Verify if the client is getting the IP address and moving to **Web Auth** pending and do one of the following:

- If yes, go to Step 2, on page 28.
- If no, then the issue is at initial joining stage.
  - Check the configuration on WLC and Access Point (AP).
  - Check if the ACL is being pushed on AP and matches the ACL on the WLC. If the ACL is not pushed correctly, reload the AP and check if it is an interim state, where the configuration is not pushed. After confirming on one AP, make sure to provision the APs through Cisco DNA Center.

Step 2 Verify if the client is able to load the redirect page and do one of the following:

- If yes, go to Step 3, on page 28.
- If no, then the issue may be at multiple places.
  - Check the configuration on WLC and AP.
  - Check if the ACL is being pushed on AP and matches the ACL on the WLC. If the ACL is not pushed correctly, reload the AP and check if it is an interim state where the configuration is not pushed. After confirming on one AP, make sure to provision the APs through Cisco DNA Center.
  - Check the reachability from WLC to Cisco ISE and the switch, where the AP is connected to Cisco ISE. Make sure that there is no firewall in between.
  - Check if the DNS is configured correctly.

Step 3 Verify if the client is able to see the web page, but the issue is with logging in and moving to success.

Make sure to double check the configurations in Step 1, on page 28 and Step 2, on page 28.

Make sure that the authorization profile, authentication policy, and authorization policy are correct.

Check the Cisco ISE live logs.

Make sure that the username and password are correctly configured in the Cisco ISE identities.

If everything looks good, collect the following debugs on the WLC and AP:

- Debugs on WLC:
    - Run the following **show** commands for Cisco AireOS and Polaris:

      Cisco AireOS- **show run-config**, **show wlan summary**, **show wlan** *ID_for_Guest*, **show flexconnect acl summary** , and **show flexconnect acl detailed** *ACL_from_previous_command*

      Polaris/IOS-**show running**, **show tech-support wireless**, **show wlan summary**, **show wlan id** *ID_for_guest*, **show ap name** *AP_name* **config general**, **show running-config | sec ACL**, **show wireless profile flex summary**, and **show wireless profile flex detailed** *profile_name_from_above*

    - Enable the following debugs on Cisco AireOS and Polaris:

      Cisco AireOS-**debug client** *client_mac*, **debug aaa all enable**. Reproduce the issue. Collect console, SSH, or telnet logs.

      Polaris (Cisco Catalyst 9300, Cisco Catalyst 9400, and Cisco Catalyst 9500 platforms)-Use the **set platform software trace wncd switch active r0 all-modules debug** command. Reproduce the issue. Use the **show platform software trace message wncd switch active R0 reverse | redirect flash:***filename* command. Request platform software trace archive. Collect both files from flash.

- Debugs on AP:
    - Collect the ACL information using the **show ip access-lists**
    - Collect the following debug information from AP using the **debug capwap client avc all**, **debug capwap client acl**, **debug client** *client mac*, **debug dot11 client level info address** *mac*, **debug dot11 client level events address** *mac*, and **debug flexconnect pmk** commands.

- Packet captures from AP uplink port on the switch.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.