

Configure Posture on Catalyst 9800 WLC and ISE

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Network Diagram](#)

[AAA Configuration on 9800 WLC](#)

[WLAN Configuration](#)

[Policy Profile Configuration](#)

[Policy Tag Configuration](#)

[Policy Tag Assignment](#)

[Redirect ACL Configuration](#)

[Policy ACL Configuration](#)

[AAA Configuration and Posture Setting on ISE](#)

[Examples](#)

[Verify](#)

[Troubleshoot](#)

[Checklist](#)

[Collect Debugs](#)

[References](#)

Introduction

This document describes how to configure a posture WLAN on a Catalyst 9800 WLC and ISE through the Graphic User Interface (GUI).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- 9800 WLC general configuration
- ISE policies and profiles configuration

Components Used

The information in this document is based on these software and hardware versions:

- 9800 WLC Cisco IOS® XE Cupertino v17.9.5

- Identity Service Engine (ISE) v3.2
- Laptop Windows 10 Enterprise

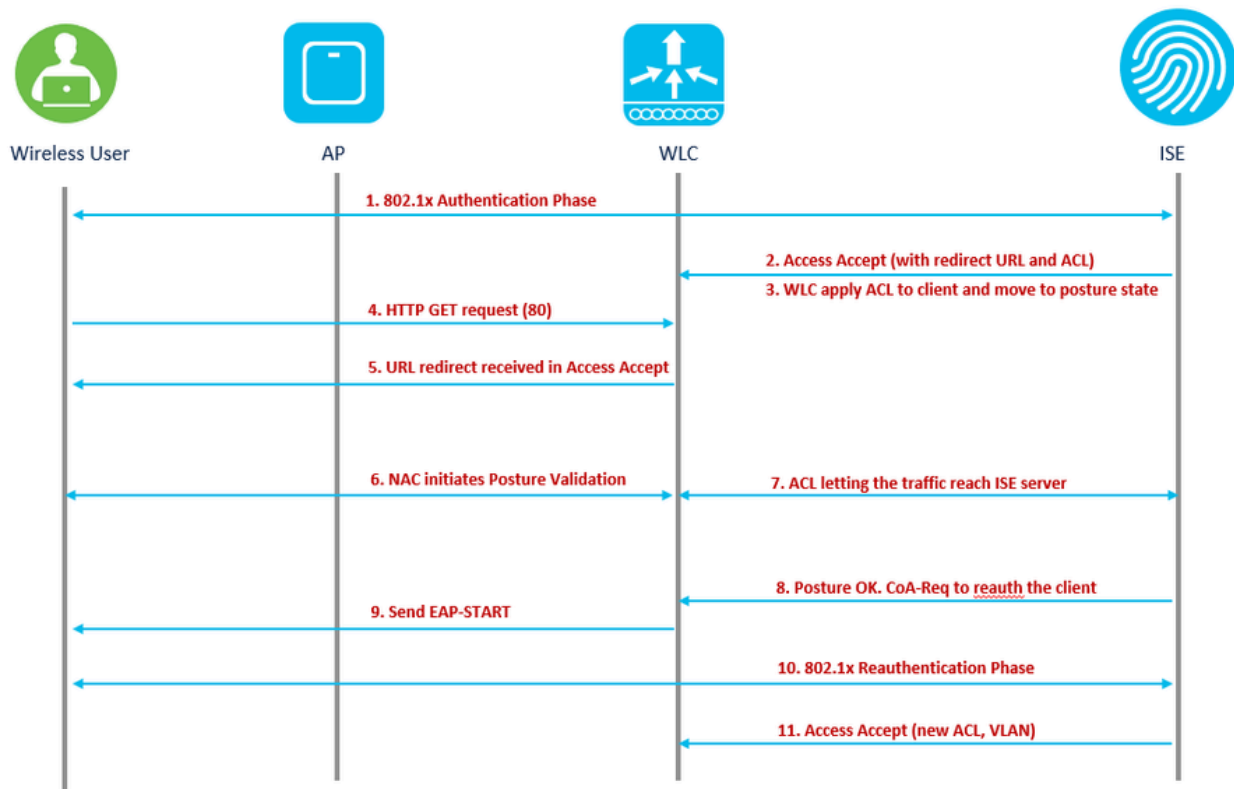
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Wireless LAN Controller RADIUS NAC and CoA Feature Flow

1. Client authenticates using dot1x authentication.
2. RADIUS Access Accept carries redirected URL for port 80 and pre-auth ACLs that includes allowing IP addresses and ports, or quarantine VLAN.
3. Client is re-directed to the URL provided in access accept, and put into a new state until posture validation is done. The client in this state talks to the ISE server and validate itself against the policies configured on the ISE NAC server.
4. NAC agent on client initiates posture validation (traffic to port 80): Agent sends HTTP discovery request to port 80 which controller redirects to URL provided in access accept. The ISE knows that client trying to reach and responds directly to client. This way the client learns about the ISE server IP and from now on, the client talks directly with the ISE server.
5. WLC allows this traffic because the ACL is configured to allow this traffic. In case of VLAN override, the traffic is bridged so that it reaches the ISE server.
6. Once ISE-client completes assessment, a RADIUS CoA-Req with reauth service is sent to the WLC. This initiates re-authentication of the client (by sending EAP-START). Once re-authentication succeeds, the ISE sends access accept with a new ACL (if any) and no URL redirect, or access VLAN.
7. WLC has support for CoA-Req and Disconnect-Req as per RFC 3576. The WLC needs to support CoA-Req for re-auth service, as per RFC 5176.
8. Instead of downloadable ACLs, pre-configured ACLs are used on the WLC. The ISE server just sends the ACL name, which is already configured in controller.
9. This design works for both VLAN and ACL cases. In case of VLAN override, we just redirect the port 80 is redirected and allows (bridge) rest of the traffic on the quarantine VLAN. For the ACL, the pre-auth ACL received in access accept is applied.

This figure provides a visual representation of this feature flow:



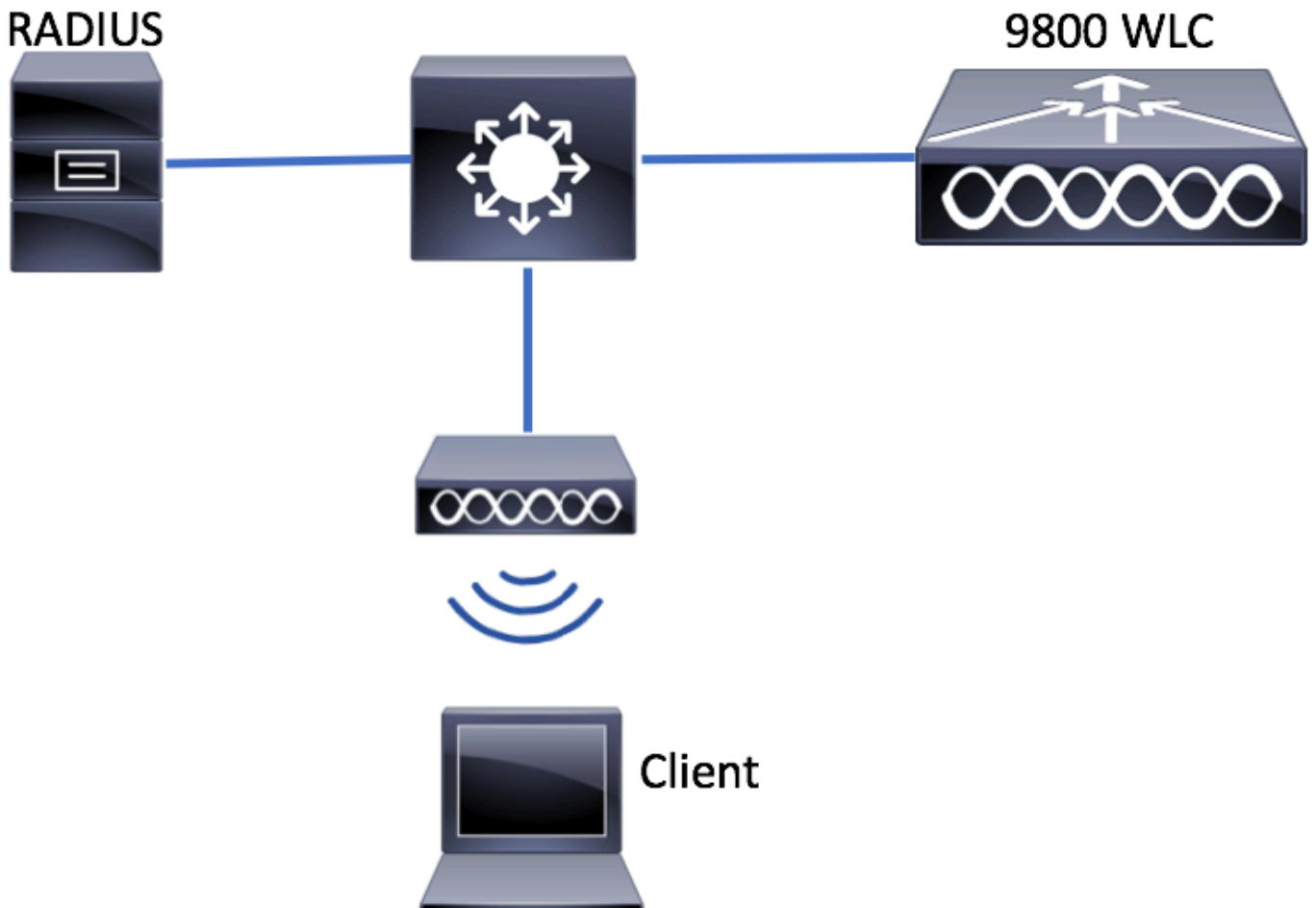
feature workflow

For this use case, an SSID which is only used for corporate users are enabled for posture. No other use cases, such as BYOD, Guest, or any others exist on this SSID.

When a wireless client connects to the Posture SSID for the first time, it must download and install the Posture Module on the redirected portal of the ISE, and finally applied with relevant ACLs based on the posture check result (Compliant/Non-Compliant).

Configure

Network Diagram



Network Diagram

AAA Configuration on 9800 WLC

Step 1. Add the ISE server to the 9800 WLC configuration. Navigate to **Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add** and enter the RADIUS server information as shown in the images. Ensure Support for CoA is enabled for posture NAC.

The screenshot shows the Cisco ISE configuration interface. On the left is a dark sidebar with menu items: Dashboard, Monitoring, Configuration (highlighted in blue), Administration, Licensing, and Troubleshooting. The main content area shows a breadcrumb path: Configuration > Security > AAA. Below this is a '+ AAA Wizard' button. Underneath is a tabbed interface with 'Servers / Groups' selected. Below the tabs are '+ Add' and '× Delete' buttons. A 'RADIUS' tab is highlighted. Under the 'RADIUS' tab, 'TACACS+' and 'LDAP' are listed. To the right, the 'Servers' tab is active, showing a table with columns 'Name' and 'Address'. The table is empty, and there is a pagination control showing '0' items and '10 items per page'.

9800 create radius server

Create AAA Radius Server

Name*	posture-radius	Support for CoA ⓘ	ENABLED <input checked="" type="checkbox"/>
Server Address*	10.124.57.141	CoA Server Key Type	Clear Text ▼
PAC Key	<input type="checkbox"/>	CoA Server Key ⓘ	•••••
Key Type	Clear Text ▼	Confirm CoA Server Key	•••••
Key* ⓘ	•••••	Automate Tester	<input type="checkbox"/>
Confirm Key*	•••••		
Auth Port	1812		
Acct Port	1813		
Server Timeout (seconds)	1-1000		
Retry Count	0-100		

[Cancel](#) [Apply to Device](#)

9800 create radius details

Step 2. Create an authentication method list. Navigate to **Configuration > Security > AAA > AAA Method List > Authentication > + Add** as shown in the image:

Cisco Catalyst 9800-CL Wireless Controller 17.9.5

Welcome sis/ Last login 04/09/2024

Configuration > Security > AAA Show Me How

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

Authentication

Authorization

Accounting

+ Add - Delete

Name	Type	Group Type
<input type="checkbox"/> default	login	local

1 10

9800 add auth list

Quick Setup: AAA Authentication

Method List Name*

Type* ▼ ⓘ

Group Type ▼ ⓘ

Fallback to local ☐

Available Server Groups

ldap
tacacs+



Assigned Server Groups

radius



Cancel

Apply to Device

9800 create auth list details

Step 3. (Optional) Create an accounting method list as shown in the image:

Dashboard

Monitoring >

Configuration >

Administration >

Licensing

Troubleshooting

Configuration > Security > AAA

Show Me How

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

Authentication

Authorization

Accounting

+ Add

× Delete

Name	Type
0	10 ▼

9800 add account list

Quick Setup: AAA Accounting



Method List Name*

POSTUREacct

Type*

identity



Available Server Groups

Assigned Server Groups

ldap
tacacs+



radius



Cancel

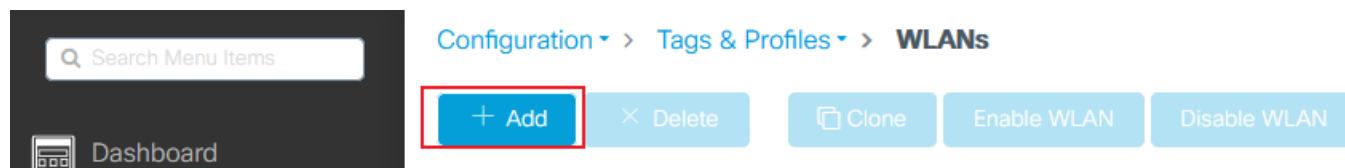


Apply to Device

9800 create acct list details

WLAN Configuration

Step 1. Create the WLAN. Navigate to **Configuration > Tags & Profiles > WLANs > + Add** and configure the network as needed:



9800 WLAN add

Step 2. Enter the WLAN general information.

Add WLAN



General

Security

Advanced

Profile Name* posture_demo

SSID* posture_demo

WLAN ID* 1

Status **ENABLED** ☒

Broadcast SSID **ENABLED** ☒

Radio Policy ⓘ

[Show slot configuration](#)

6 GHz

Status **ENABLED** ☒ ⓘ

- ✖ WPA2 Disabled
- ✖ WPA3 Enabled
- ✓ Dot11ax Enabled

5 GHz

Status **ENABLED** ☒

2.4 GHz

Status **ENABLED** ☒

802.11b/g Policy 802.11b/g ▼

↶ Cancel

📄 Apply to Device

9800 create WLAN general

Step 3. Navigate to the **Security** tab and choose the needed security method. In this case, choose '802.1x' and the AAA authentication list (that you created in Step 2. in the **AAA Configuration** section) are needed:

Add WLAN

General

Security

Advanced

Layer2

Layer3

AAA

☒ WPA + WPA2

☐ WPA2 + WPA3

☐ WPA3

☐ Static WEP

☐ None

MAC Filtering

☐

Lobby Admin Access

☐

WPA Parameters

WPA Policy

☐

GTK Randomize

☐

WPA2 Policy

☒

OSEN Policy

☐

WPA2 Encryption

AES(CCMP128)

☒

GCMP128

☐

CCMP256

☐

GCMP256

☐

Protected Management Frame

PMF

Disabled

Fast Transition

Status

Adaptive Enabled

Over the DS

☐

Reassociation Timeout *

20

Auth Key Mgmt

802.1x

☒

Easy-PSK

☐

FT + 802.1x

☐

802.1x-SHA256

☐

PSK

☐

CCKM

☐

FT + PSK

☐

PSK-SHA256

☐

Cancel

Apply to Device

9800 create WLAN security L2

Edit WLAN

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

General

Security

Advanced

Add To Policy Tags

Layer2

Layer3

AAA

Authentication List

posture-authn-list

Local EAP Authentication

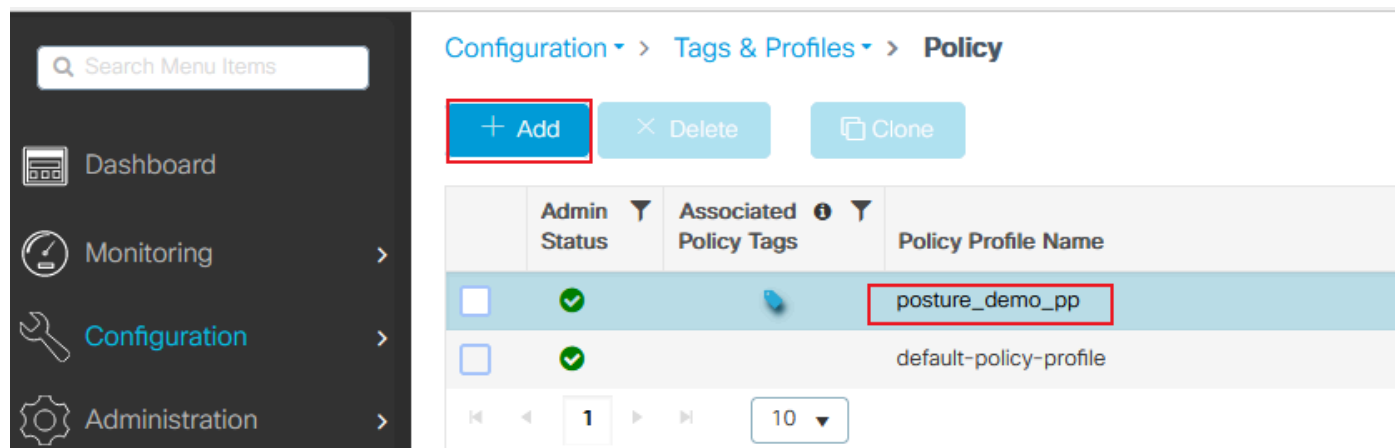
☐

9800 create WLAN security AAA

Policy Profile Configuration

Inside a Policy Profile, you can decide to assign the clients to which VLAN, among other settings (like Access Controls List (ACLs), Quality of Service (QoS), Mobility Anchor, Timers, and so on). You can either use your default policy profile or you can create a new one.

Step 1. Create a new **Policy Profile**. Navigate to **Configuration > Tags & Profiles > Policy** and create a new one:



Configuration > Tags & Profiles > Policy

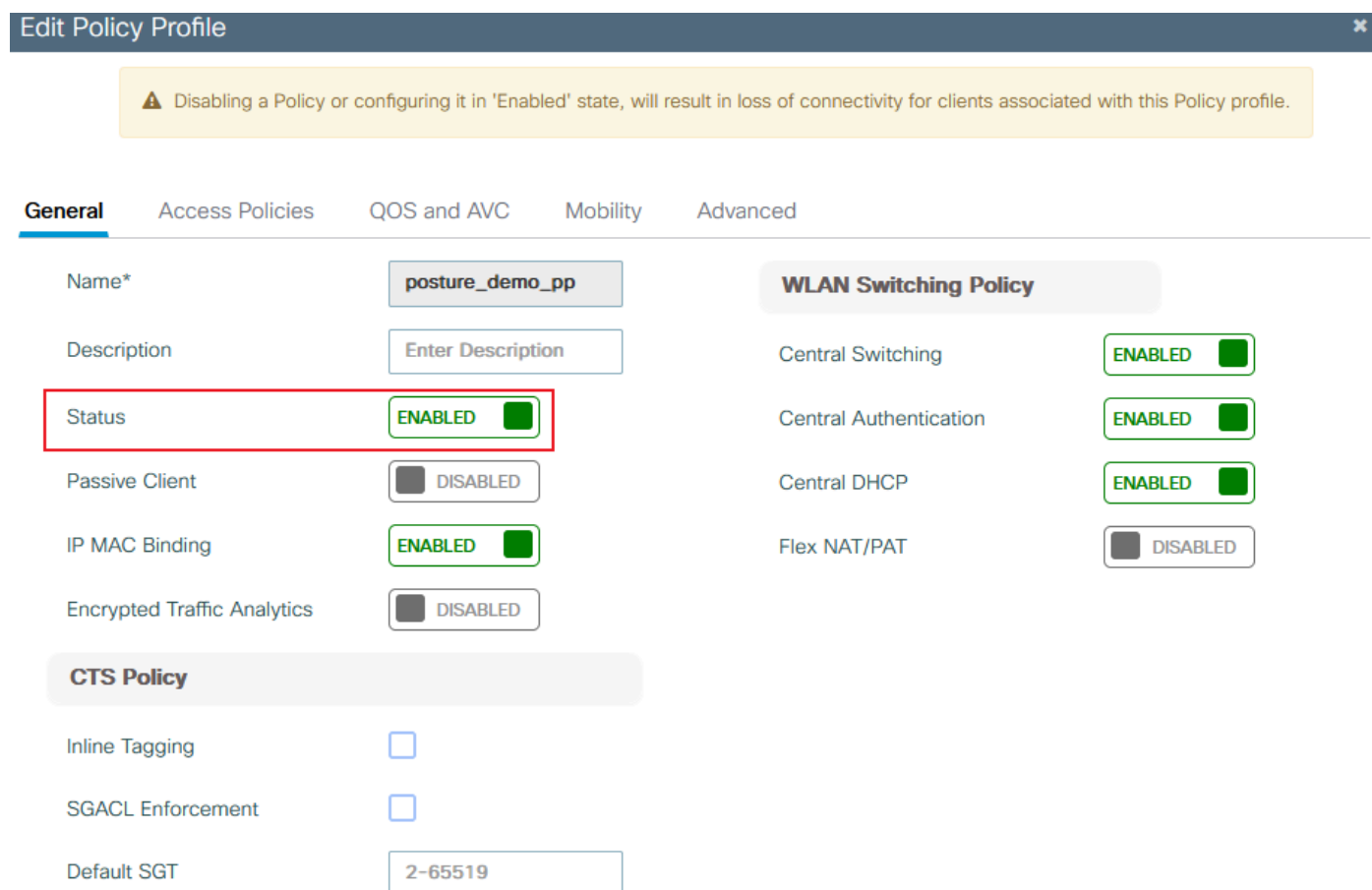
+ Add × Delete Clone

	Admin Status	Associated Policy Tags	Policy Profile Name
<input type="checkbox"/>	✓		posture_demo_pp
<input type="checkbox"/>	✓		default-policy-profile

1 10

9800 add policy profile

Ensure the profile is enabled.



Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General Access Policies QOS and AVC Mobility Advanced

Name* posture_demo_pp

Description Enter Description

Status **ENABLED**

Passive Client ☐ DISABLED

IP MAC Binding **ENABLED**

Encrypted Traffic Analytics ☐ DISABLED

WLAN Switching Policy

Central Switching **ENABLED**

Central Authentication **ENABLED**

Central DHCP **ENABLED**

Flex NAT/PAT ☐ DISABLED

CTS Policy

Inline Tagging ☐

SGACL Enforcement ☐

Default SGT 2-65519

9800 create policy profile general

Step 2. Choose the VLAN. Navigate to the **Access Policies** tab and choose the VLAN name from the drop-down or manually type the VLAN-ID. Do not configure an ACL in the policy profile:

Edit Policy Profile



⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

RADIUS Profiling

☐

HTTP TLV Caching

☐

DHCP TLV Caching

☐

WLAN Local Profiling

Global State of Device
Classification

Disabled ⓘ

Local Subscriber Policy Name

Search or Select ▼



VLAN

VLAN/VLAN Group

VLAN1072 ▼



Multicast VLAN

Enter Multicast VLAN

WLAN ACL

IPv4 ACL

Search or Select ▼



IPv6 ACL

Search or Select ▼



URL Filters ⓘ

Pre Auth

Search or Select ▼



Post Auth

Search or Select ▼



9800 create policy profile VLAN

Step 3. Configure the policy profile to accept ISE overrides (allow AAA override) and Change of Authorization (CoA) (NAC State). You can optionally specify an accounting method too:

←

General

Access Policies

QOS and AVC

Mobility

Advanced

WLAN Timeout

Session Timeout (sec)

1800

Idle Timeout (sec)

300

Idle Threshold (bytes)

0

Client Exclusion Timeout (sec)

60

Guest LAN Session Timeout

DHCP

IPv4 DHCP Required

DHCP Server IP Address

10.10.10.1

Show more >>>

AAA Policy

Allow AAA Override

NAC State

Policy Name

default-aaa-policy

Accounting List

POSTUREacct

WGB Parameters

Fabric Profile

Search or Select

Link-Local Bridging

mDNS Service Policy

default-mdns-ser ...

Clear

Hotspot Server

Search or Select

User Defined (Private) Network

Status

Drop Unicast

DNS Layer Security

DNS Layer Security Parameter Map

Not Configured

Clear

Flex DHCP Option for DNS

ENABLED

Flex DNS Traffic Redirect

IGNORE

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

Search or Select

Air Time Fairness Policies

Cancel

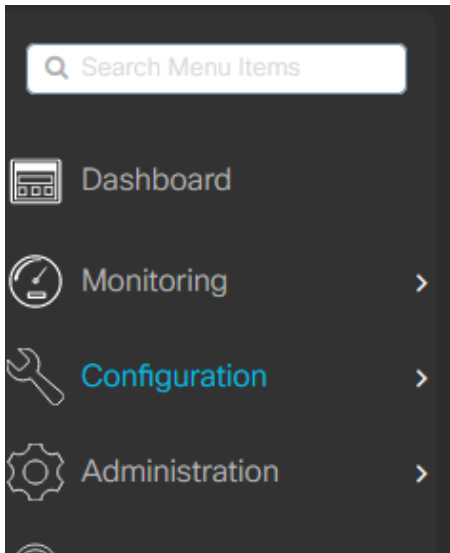
Update & Apply to Device

9800 create policy profile Advance

Policy Tag Configuration

Inside the Policy Tag is where you link your SSID with your Policy Profile. You can either create a new Policy Tag or use the default-policy tag.

Navigate to **Configuration > Tags & Profiles > Tags > Policy** and add a new one if needed as shown in the image:



Configuration > Tags & Profiles > Tags

PolicySiteRFAP

+ Add

× Delete

📄 Clone

Policy Tag Name
<input type="checkbox"/> default-policy-tag

⏪ ⏩ 1 ⏪ ⏩

10 ▼

9800 policy tag add

Link your WLAN Profile to the desired Policy Profile:

Edit Policy Tag

⚠ Changes may result in loss of connectivity for some clients that are associated to APs with this Policy Tag.

Name*

posture-policy-tag

Description

Enter Description

▼ WLAN-POLICY Maps: 1

+ Add

× Delete

WLAN Profile	Policy Profile
<input type="checkbox"/> posture_demo	posture_demo_pp

⏪ ⏩ 1 ⏪ ⏩

10 ▼

1 - 1 of 1 items

9800 policy tag details

Policy Tag Assignment

Assign the Policy Tag to the needed APs. Navigate to **Configuration > Wireless > Access Points > AP Name > General Tags** , make the needed assignment, and then click **Update & Apply** to Device .

Edit AP

General

Interfaces

High Availability

Inventory

ICap

Advanced

Support Bundle

General

Tags

AP Name*

Location*

default location

Base Radio MAC

Ethernet MAC

Admin Status

ENABLED

AP Mode

Local

⚠

Changing Tags will cause the AP to momentarily lose association with the Controller. Writing Tag Config to AP is not allowed while changing Tags.

Policy

posture-policy-tag

Site

default-site-tag

RF

default-rf-tag

9800 policy tag assignment

Redirect ACL Configuration

Navigate to **Configuration > Security > ACL > + Add** in order to create a new ACL.

The ACL used for Posture Portal Redirect has the same requirements as the CWA (Central Web Authentication).

You need to deny traffic to your ISE PSNs nodes as well as deny DNS and permit all the rest. This redirect ACL is not a security ACL but a punt ACL that defines what traffic goes to the CPU (on permits) for further treatment (like redirection) and what traffic stays on the data plane (on deny) and avoids redirection. The ACL must look like this (replace 10.124.57.141 with your ISE IP address in this example):

Edit ACL

ACL Name*

POSTURE_REDIRECT_ACL

ACL Type

IPv4 Extended

Rules

Sequence*

Action

permit

Source Type

any

Destination Type

any

Protocol

ahp

Log

☐

DSCP

None

+ Add

× Delete

	Sequence ↑	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
<input type="checkbox"/>	10	deny	any		10.124.57.141		ip	None	None	None	Disa
<input type="checkbox"/>	20	deny	10.124.57.141		any		ip	None	None	None	Disa
<input type="checkbox"/>	30	deny	any		any		udp	None	eq domain	None	Disa
<input type="checkbox"/>	40	deny	any		any		udp	eq domain	None	None	Disa
<input type="checkbox"/>	50	permit	any		any		tcp	None	eq www	None	Disa

9800 redirect ACL details

Policy ACL Configuration

In this case, you need to define separate ACLs on 9800 WLC for ISE to authorize the Compliant and Non-Compliant scenarios based on poture check result.

Configuration > Security > ACL

+ Add

× Delete

Associate Interfaces

	ACL Name	ACL Type
<input type="checkbox"/>	POSTURE_COMPLIANT_ACL	IPv4 Extended
<input type="checkbox"/>	POSTURE_NON-COMPLIANT_ACL	IPv4 Extended
<input type="checkbox"/>	POSTURE_REDIRECT_ACL	IPv4 Extended

1

10

9800 ACL general

For Compliant scenario, simply use **permit all** in this case. As another common configuration, you can also have ISE not to authorize any ACL in the compliant result, which is equivalent to **permit all** on the 9800 side:

Edit ACL

ACL Name*

POSTURE_COMPLIANT

ACL Type

IPv4 Extended

Rules

Sequence*

Action

permit

Source Type

any

Destination Type

any

Protocol

ahp

Log

☐

DSCP

None

+ Add

× Delete

	Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
<input type="checkbox"/>	10	permit	any		any		ip	None	None	None	Disable

1
10

1 - 1 of 1 items

9800 ACL - Compliant

For Non-compliant scenario, the client only allows access to certain networks, usually the remediation server (ISE itself in this case):

Edit ACL

ACL Name*

POSTURE_NON-COMP

ACL Type

IPv4 Extended

Rules

Sequence*

Action

permit

Source Type

any

Destination Type

any

Protocol

ahp

Log

☐

DSCP

None

+ Add

× Delete

	Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
<input type="checkbox"/>	10	permit	10.124.57.141		any		ip	None	None	None	Disa
<input type="checkbox"/>	20	permit	any		10.124.57.141		ip	None	None	None	Disa
<input type="checkbox"/>	30	permit	any		any		udp	None	eq domain	None	Disa
<input type="checkbox"/>	40	permit	any		any		udp	eq domain	None	None	Disa
<input type="checkbox"/>	50	deny	any		any		ip	None	None	None	Disa

1
10

1 - 5 of 5 items

9800 ACL - Non-Compliant

AAA Configuration and Posture Setting on ISE

Posture Requirement: In this example, the requirement to determine compliance is to detect whether a

specific test file exists on the desktop used to test Windows PC.

Step 1. Add WLC 9800 as NAD on the ISE. Navigate to **Administration> Network Resources> Network Devices> Add**:

The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is 'Administration > Network Resources'. The left sidebar has 'Network Devices' selected. The main area is titled 'Network Devices List > WLC9800'. Below this is the 'Network Devices' configuration form. The 'Name' field is 'WLC9800'. The 'Description' field is empty. The 'IP Address' field is '10.124.60.41' with a subnet mask of '32'. The 'Device Profile' is 'Cisco'. The 'Model Name' and 'Software Version' fields are empty. The 'Network Device Group' is 'All Locations'. The 'Location' is 'All Locations'. The 'IPSEC' is 'No'. The 'Device Type' is 'All Device Types'. There are 'Set To Default' links for 'Location', 'IPSEC', and 'Device Type'.

Add Network Device 01

The screenshot shows the 'RADIUS Authentication Settings' for the WLC9800. The breadcrumb navigation is 'Administration > Network Resources'. The left sidebar has 'Network Devices' selected. The main area is titled 'RADIUS Authentication Settings'. The 'Protocol' is 'RADIUS'. The 'Shared Secret' is '*****'. The 'CoA Port' is '1700'. The 'RADIUS DTLS Settings' section is expanded, showing 'DTLS Required' as 'No', 'Shared Secret' as 'radius/dtls', 'CoA Port' as '2083', and 'Issuer CA of ISE Certificates for CoA' as 'Select if required (optional)'. There are 'Show' and 'Set To Default' links for various fields.

Add Network Device 02

Step 2. Download Cisco Secure Client Headend Deployment Package and Compliance module on Cisco Software CCO website.

Access and search Cisco Secure Client:

Cisco Secure Client Headend Deployment Package (Windows)

06-Feb-2024

111.59 MB

[cisco-secure-client-win-5.1.2.42-webdeploy-k9.pkg](#)

[Advisories](#) 

Secure Client 5.1.2.42

ISE Posture Compliance Library - Windows / Head-end deployment (PKG). This image can be used with AnyConnect version 4.3 and later along with ISE 2.1 and later. Cisco Secure Client 5.x along with ISE 2.7 and later.

30-Jan-2023

19.59 MB

[cisco-secure-client-win-4.3.3335.6146-isecompliance-webdeploy-k9.pkg](#)

[Advisories](#) 

ISE Compliance module 4.3

Step 3. Upload Cisco Secure Client Headend Deployment Package and Compliance module package to ISE Client Provisioning. Navigate to **Work Centers> Posture> Client Provisioning> Resources** . Click **Add**, Choose **Agent resources from local disk** from the drop-down box:

Overview

Network Devices


Client Provisioning



Policy Elements


Client Provisioning Policy


Resources

Client Provisioning Portal

 Edit

 Add 

 Duplicate

 Delete

☐

Agent resources from Cisco site

☐

Agent resources from local disk

☐

Native Supplicant Profile

☐

Agent Configuration

☐

Agent Posture Profile

☐

AMP Enabler Profile

Upload Secure Client

Cisco ISE

Work Centers - Posture

Overview

Network Devices

Client Provisioning

Policy Elements

Posture Policy

Policy Sets

Troubleshoot

Reports

Settings

Client Provisioning Policy

Resources

Client Provisioning Portal

Selected 0 Total 13

Quick Filter

<input type="checkbox"/>	Name	Type	Version	Last Update	Description
<input type="checkbox"/>	CiscoTemporalAgentOSX 4.10.02051	CiscoTemporalAgentOSX	4.10.2051.0	2021/08/10 03:12:31	With CM: 4.3.1858.4353
<input type="checkbox"/>	CiscoSecureClientComplianceModuleWindows 4.3.3335.6146	CiscoSecureClientComplianceModuleWindows	4.3.3335.6146	2024/03/30 19:28:34	Cisco Secure Client Win...
<input type="checkbox"/>	Cisco-ISE-Chrome-NSP	Native Supplicant Profile	Not Applicable	2016/10/07 04:01:12	Pre-configured Native S...
<input type="checkbox"/>	CiscoAgentlessOSX 4.10.02051	CiscoAgentlessOSX	4.10.2051.0	2021/08/10 03:12:36	With CM: 4.3.1858.4353
<input type="checkbox"/>	bloomtest-Posture for Windows	AgentProfile	Not Applicable	2024/03/30 19:31:40	test windows PC for con...
<input type="checkbox"/>	AnyConnectDesktopWindows 4.10.7073.0	AnyConnectDesktopWindows	4.10.7073.0	2024/03/30 19:47:18	AnyConnect Secure Mob...
<input type="checkbox"/>	MacOsXSPWizard 2.7.0.1	MacOsXSPWizard	2.7.0.1	2021/08/10 03:12:27	Supplicant Provisioning ...
<input type="checkbox"/>	CiscoAgentlessWindows 4.10.02051	CiscoAgentlessWindows	4.10.2051.0	2021/08/10 03:12:33	With CM: 4.3.2227.6145
<input type="checkbox"/>	Cisco-ISE-NSP	Native Supplicant Profile	Not Applicable	2016/10/07 04:01:12	Pre-configured Native S...
<input type="checkbox"/>	WLC9800-windows	AgentConfig	Not Applicable	2024/04/01 17:44:50	Test for WLC9800 Wirele...
<input type="checkbox"/>	WinSPWizard 3.0.0.3	WinSPWizard	3.0.0.3	2021/08/10 03:12:27	Supplicant Provisioning ...
<input type="checkbox"/>	CiscoTemporalAgentWindows 4.10.02051	CiscoTemporalAgentWindows	4.10.2051.0	2021/08/10 03:12:28	With CM: 4.3.2227.6145
<input type="checkbox"/>	CiscoSecureClientDesktopWindows 5.1.2.042	CiscoSecureClientDesktopWindows	5.1.2.42	2024/03/30 19:20:54	Cisco Secure Client for ...

Upload Secure Client and Compliance Module successfully

Step 4. Create Agent Posture Profile Navigate to **Work Centers> Posture> Client Provisioning> Resources> Add> Agent Posture Profile:**

Cisco ISE		Work Centers - Posture				<div> <div></div> <div></div> <div></div> <div></div> </div>		
Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
Client Provisioning Policy		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
Resources		<div> <div></div> <div></div> </div>						
Client Provisioning Portal		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						
		<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>						

Cisco ISE

Work Centers · Posture

Overview

Network Devices

Client Provisioning

Policy Elements

Posture Policy

Policy Sets

Troubleshoot

Reports

Settings

Client Provisioning Policy

Resources

Client Provisioning Portal

* Select Agent Package:

CiscoSecureClientDesktopWindows 5.1

* Configuration Name:

WLC9800-windows

Description:

Test for WLC9800 Wireless dot1x

Description Value Notes

* Compliance Module

CiscoSecureClientComplianceModuleW

Cisco Secure Client Module Selection

ISE Posture

☒

VPN

☐

Zero Trust Access

☐

Network Access Manager

☐

Secure Firewall Posture

☐

Network Visibility

☐

Umbrella

☐

Start Before Logon

☐

Diagnostics and Reporting Tool

☒

Profile Selection

* ISE Posture

bloomtest-Posture for Windows

Add Agent Configuration

Step 6. Confirm the Client Provisioning portal, use default portal for testing is OK. (Please generate CSR and Apply for an SSL certificate from the CA server, and replace Certificate Group tag on this portal Settings, Otherwise, a certificate untrusted warning occurs during the test process.)

Navigate to **Work Centers> Posture> Client Provisioning> Client Provisioning Portals:**

Cisco ISE

Work Centers · Posture

Overview

Network Devices

Client Provisioning

Policy Elements

Posture Policy

Policy Sets

Troubleshoot

Reports

Settings

Client Provisioning Policy

Resources

Client Provisioning Portal

Client Provisioning Portals

You can edit and customize the default Client Provisioning portal and create additional ones

Create

Edit

Duplicate

Delete

Client Provisioning Portal (default)

Default portal and user experience used to install the posture agents and verify compliance on user's devices

Choose Client Provisioning Portal 01

Cisco ISE

Work Centers - Posture

OverviewNetwork DevicesClient ProvisioningPolicy ElementsPosture PolicyPolicy SetsTroubleshootReportsSettings

Client Provisioning PolicyResourcesClient Provisioning Portal

Portal Behavior and Flow SettingsPortal Page Customization

Portal & Page Settings

▼ Portal Settings

HTTPS port: *8443(8000 - 8999)

Bidirectional port: *8449(8000 - 8999)

Allowed Interfaces: *

For PSNs Using Physical Interfaces

☒ Gigabit Ethernet 0

☐ Gigabit Ethernet 1

☐ Gigabit Ethernet 2

☐ Gigabit Ethernet 3

☐ Gigabit Ethernet 4

☐ Gigabit Ethernet 5

For PSNs with Bonded Interfaces Configured

☒ Bond 0
Uses Gigabit Ethernet 0 as primary interface, Gigabit Ethernet 1 as backup

☐ Bond 1
Uses Gigabit Ethernet 2 as primary interface, Gigabit Ethernet 3 as backup

☐ Bond 2
Uses Gigabit Ethernet 4 as primary interface, Gigabit Ethernet 5 as backup

Certificate group tag: *

Test-CPP ▼

Configure certificates at:
[Administration > System > Certificates > System Certificates](#)

Authentication method: *

Certificate_Request_Sequence ▼

Configure authentication methods at:
[Administration > Identity Management > Identity Source Sequences](#)

Choose Client Provisioning Portal 02

Step 7. Create Client Provisioning Policy. Navigate to **Work Centers> Posture> Client Provisioning> Client Provisioning Policy > Edit> insert new policy above.**

OverviewNetwork DevicesClient ProvisioningPolicy ElementsPosture PolicyPolicy SetsTroubleshootReportsSettings

Client Provisioning PolicyResourcesClient Provisioning Portal

Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
<input checked="" type="checkbox"/> WLC9800-Windows	If Any	and Windows All	and Condition(s)	then WLC9800-windows Edit
<input checked="" type="checkbox"/> IOS	If Any	and Apple IOS All	and Condition(s)	then Cisco-ISE-NSP Edit
<input checked="" type="checkbox"/> Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP Edit
<input checked="" type="checkbox"/> Windows	If Any	and Windows All	and Condition(s)	then CiscoTemporalAgentWindows 4.10.02051 And WinSPWizard 3.0.0.3 And Cisco-ISE-NSP Edit
<input checked="" type="checkbox"/> MAC OS	If Any	and Mac OSX	and Condition(s)	then CiscoTemporalAgentOSX 4.10.02051 And MacOsXSPWizard 2.7.0.1 And Cisco-ISE-NSP Edit
<input checked="" type="checkbox"/> Chromebook	If Any	and Chrome OS All	and Condition(s)	then Cisco-ISE-Chrome-NSP Edit

Create Client Provisioning Policy

Step 8. Create File Conditions. Navigate to **Work Centers> Posture> Policy Elements> Conditions> File> File Conditions> Add:**

Overview Network Devices Client Provisioning **Policy Elements** Posture Policy Policy Sets Troubleshoot Reports Settings

File Conditions List > WLC9800-Posture-demo

File Condition

Name * WLC9800-Posture-demo

Description test for WLC9800

* Operating System Windows All

Compliance Module Any version

* File Type FileExistence

* File Path USER_DESKTOP WLC9800-Posture-Demo.txt

* File Operator Exists

Create File Condition

Step 9. Create Remediations Navigate to **Work Centers> Posture> Policy Elements> Remediations > File> Add:**

≡ Cisco ISE Work Centers · Posture

Overview Network Devices Client Provisioning **Policy Elements** Posture Policy Policy Sets Troubleshoot Reports Settings

File Remediations List > WLC9800-Posture-Demo

File Remediation

* Name WLC9800-Posture-Demo

Description your PC must have file named WLC9800-Posture-

Compliance Module Any version

Version 1.0

File Uploaded WLC9800-Posture-Demo.txt

Create File Remediation

Step 10. Create Requirement. Navigate to **Work Centers> Posture> Policy Elements> Requirements> Insert new Requirement:**

Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
----------	-----------------	---------------------	-----------------	----------------	-------------	--------------	---------	----------

Conditions	Remediations	Requirements
Application	Anti-Malware	
Anti-Spyware	Anti-Virus	
File	Firewall	
Launch Program	Link	
Patch Management	Script	
USB	Windows Server Update Servi...	
Windows Update		

Name	Operating System	Compliance Module	Posture Type	Conditions	Remediations Actions
Any_AM_Installation_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if ANY_am_mac_inst then	Message Text Only Edit
Default_AppVis_Requirement_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if Default_AppVis_Condition_Win then	Select Remediations Edit
Default_AppVis_Requirement_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if Default_AppVis_Condition_Mac then	Select Remediations Edit
Default_Hardware_Attributes_Requirement_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if Hardware_Attributes_Check then	Select Remediations Edit
Default_Hardware_Attributes_Requirement_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if Hardware_Attributes_Check then	Select Remediations Edit
Default_Firewall_Requirement_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if Default_Firewall_Condition_Win then	Default_Firewall_Remediation_Win Edit
Default_Firewall_Requirement_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if Default_Firewall_Condition_Mac then	Default_Firewall_Remediation_Mac Edit
WLC9800-Posture-Demo	for Windows All	using Any version	using Agent	met if WLC9800-Posture-demo then	WLC9800-Posture-Demo Edit

Note:
 Remediation Action is filtered based on the operating system and stealth mode selection.
 Remediation Actions are not applicable for Application Conditions (configured using the Provision By Category or Provision By Everything options), Hardware Conditions, and External Data source conditions.
 Remediations Actions are not applicable for Agentless Posture type.

Create Posture Requirement

Step 11. Create Posture Policy. Navigate to **Work Centers> Posture> Insert new policy:**

Cisco ISE	Work Centers - Posture	Q	?	?
-----------	------------------------	---	---	---

Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
----------	-----------------	---------------------	-----------------	----------------	-------------	--------------	---------	----------

Posture Policy [Guide Me](#)

Define the Posture Policy by configuring rules based on operating system and/or other conditions.

WLC9800

Status	Policy Options	Rule Name	Identity Groups	Operating Systems	Compliance Module	Posture Type	Other Conditions	Requirements
<input checked="" type="checkbox"/>	Policy Options	WLC9800-Posture-Demo	if Any	and Windows All	and Any version	and Agent	and	then WLC9800-Posture-Demo Edit

Create Posture Policy

Step 12. Create three Authorization Profiles: Posture status is Unknown; Posture status is Non-Compliant; Posture Status is Compliant. Navigate to **Policy> Policy Elements> Results> Authorizaton> Authorization Profiles> Add:**

Dictionaries	Conditions	Results
--------------	------------	---------

Authentication	Authorization	Profiling	Posture	Client Provisioning
Allowed Protocols	Authorization Profiles			
	Downloadable ACLs			

Standard Authorization Profiles

For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

[Edit](#) [+ Add](#) [Duplicate](#) [Delete](#)

<input type="checkbox"/>	Name	Profile	Description
<input type="checkbox"/>	WLC9800		
<input type="checkbox"/>	WLC9800-Posture-Compliant	Cisco	
<input type="checkbox"/>	WLC9800-Posture-NonCompliant	Cisco	
<input type="checkbox"/>	WLC9800-Posure-Unknown	Cisco	

Create Authorization Profiles 01

Dictionary

Conditions

Results

Authentication

Allowed Protocols

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > WLC9800-Posture-Unknown

Authorization Profile

* NameWLC9800-Posture-Unknown

Description

* Access TypeACCESS_ACCEPT

Network Device ProfileCisco

Service Template

Track Movement

Agentless Posture

Passive Identity Tracking

Common Tasks

Web Redirection (CWA, MDM, NSP, CPP)

Client Provisioning (Posture)

ACLPOSTURE_REDIRECT_ACL

ValueClient Provisioning Portal (def:)

Static IP/Host name/FQDN

Suppress Profiler CoA for endpoints in Logical Profile

Create Authorization Profiles 02

Dictionary

Conditions

Results

Authentication

Allowed Protocols

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > WLC9800-Posture-Compliant

Authorization Profile

* NameWLC9800-Posture-Compliant

Description

* Access TypeACCESS_ACCEPT

Network Device ProfileCisco

Service Template

Track Movement

Agentless Posture

Passive Identity Tracking

Common Tasks

Airespace ACL Name

POSTURE_COMPLIANT_ACL

Airespace IPv6 ACL Name

Create Authorization Profiles 03

Dictionarys Conditions Results

Authorization Profile

* Name WLC9800-Posture-NonComp

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement

Agentless Posture

Passive Identity Tracking

Common Tasks

Interface Template

Web Authentication (Local Web Auth)

☒ Airespace ACL Name POSTURE_NON-COMPLIANT_

Airespace IPv6 ACL Name

Advanced Attributes Settings

Step 13. Create Policy Sets. Navigate to **Policy> Policy**

Policy Sets

Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
<input checked="" type="checkbox"/>	WLC9800-Posture-Demo		AND Network Access Device IP Address EQUALS 10.124.60.41 Normalised Radius SSID CONTAINS posture_demo	Default Network Access	0		
<input checked="" type="checkbox"/>	Default	Default policy set		Default Network Access	0		

Reset Save

Create Policy Sets

Sets> Add Icon:

Step 14. Create Authentication Policy Navigate to **Policy> Policy Sets> Expand "WLC9800-Posture-Demo"> Authentication Policy> Add:**

Cisco ISE Policy - Policy Sets

Search

WLC9800-Posture-Demo AND Network Access Device IP Address EQUALS 10.124.60.41 Normalised Radius-SSID CONTAINS posture_demo Default Network Access

Authentication Policy (2)

Status	Rule Name	Conditions	Use	Hits	Actions
●	Wireless-dot1x	Wireless_802.1X	Internal Users	0	Options
●	Default		All_User_ID_Stores	0	Options

Create Authentication Policy

Step 15. Create Authorization Policy Navigate to **Policy> Policy Sets> Expand "WLC9800-Posture-Demo"> Authorization Policy> Add:**

Authorization Policy (4)

Status	Rule Name	Conditions	Results		Hits	Actions
			Profiles	Security Groups		
●	Posture-Compliant	Session PostureStatus EQUALS Compliant	WLC9800-Posture-Co...	Select from list	0	Options
●	Posture-Noncompliant	Session PostureStatus EQUALS NonCompliant	WLC9800-Posture-No...	Select from list	0	Options
●	Posture-Unknown	Session PostureStatus EQUALS Unknown	WLC9800-Posture-Unk...	Select from list	0	Options
●	Default		DenyAccess	Select from list	0	Options

Create Authorization Policy

Examples

1. Connected test SSID **posture_demo** with correct 802.1X credentials.



posture_demo
Secured

Enter your user name and password

wlc9800-user

••••••••



OK

Cancel

Network & Internet settings

Change settings, such as making a connection metered.

- If the browser has been redirected to the ISE portal URL but the page cannot be loaded, check whether the ISE domain name is not added to the DNS server, hence the client cannot resolve the portal URL. To quickly resolve this problem, check the **Static IP/Host name/FQDN** under the Authorization Profile to provide the IP address in redirect URL. However, this can be a security concern because it exposes the IP address of the ISE.

▼ Common Tasks

☒ Web Redirection (CWA, MDM, NSP, CPP) ⓘ

Client Provisioning (Posture) ▼ ACL POSTURE_REDIRECT_ACL ▼ Value Client Provisioning Portal (def: ▼

☒ Static IP/Host name/FQDN

☐ Suppress Profiler CoA for endpoints in Logical Profile

☐ Auto Smart Port

Collect Debugs

[Enable Debugs on C9800](#)

[Enable Debugs on ISE](#)

References

- [Configure CWA on Catalyst 9800 WLC and ISE - Cisco](#)
- [Wireless BYOD with Identity Services Engine](#)
- [Deploy ISE Posture](#)
- [Troubleshoot ISE Session Management and Posture](#)
- [Compare ISE Posture Redirection Flow to ISE Posture Redirectionless Flow](#)