

# Configurazione della postura sui switch Catalyst 9800 WLC e ISE

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazione AAA sui controller 9800 WLC](#)

[Configurazione della WLAN](#)

[Configurazione del profilo di policy](#)

[Configurazione del tag di policy](#)

[Assegnazione di un tag di policy](#)

[Configurazione degli ACL di reindirizzamento](#)

[Configurazione ACL del criterio](#)

[Configurazione AAA e impostazione della postura su ISE](#)

[Esempi](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Elenco di controllo](#)

[Raccogli debug](#)

[Riferimenti](#)

---

## Introduzione

Questo documento descrive come configurare una WLAN di postura su un Catalyst 9800 WLC e ISE tramite l'interfaccia grafica utente (GUI).

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- 9800 WLC - configurazione generale
- Configurazione di profili e policy ISE

## Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- 9800 WLC Cisco IOS® XE Cupertino v17.9.5
- Identity Service Engine (ISE) v3.2
- Notebook per Windows 10 Enterprise

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

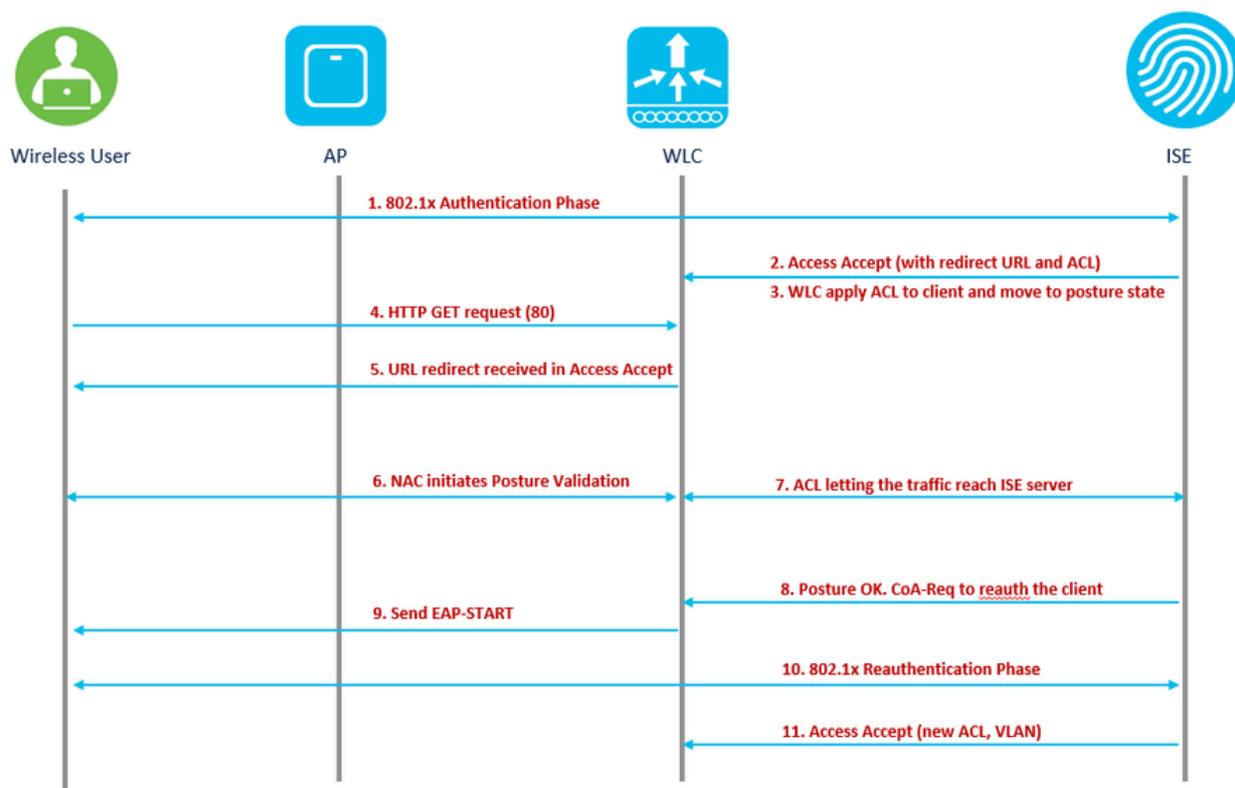
## Premesse

Flusso delle funzionalità RADIUS NAC e CoA del controller LAN wireless

1. Il client esegue l'autenticazione con dot1x.
2. L'accettazione dell'accesso RADIUS porta l'URL reindirizzato per la porta 80 e gli ACL di pre-autenticazione, che includono la possibilità di usare indirizzi IP e porte o di mettere in quarantena le VLAN.
3. Il client viene reindirizzato all'URL fornito in access accept (Accetta accesso) e messo in un nuovo stato fino a quando non viene eseguita la convalida della postura. In questo stato, il client comunica con il server ISE e si convalida rispetto alle policy configurate sul server ISE NAC.
4. L'agente NAC sul client avvia la convalida della postura (traffico verso la porta 80): L'agente invia una richiesta di individuazione HTTP alla porta 80, che il controller reindirizza all'URL specificato in Accetta. L'ISE sa che il cliente cerca di raggiungere il server ISE e risponde direttamente a quest'ultimo. In questo modo il client viene a conoscenza dell'IP del server ISE e da ora in poi comunica direttamente con il server ISE.
5. Il WLC consente questo traffico perché l'ACL è configurato per consentire questo traffico. In caso di override della VLAN, il traffico viene bloccato in modo che raggiunga il server ISE.
6. Una volta che ISE-client ha completato la valutazione, un CoA-Req RADIUS con servizio di riautenticazione viene inviato al WLC. In questo modo viene avviata la riautenticazione del client (inviando EAP-START). Se la riautenticazione ha esito positivo, ISE invia un messaggio di accettazione dell'accesso con un nuovo ACL (se presente) e senza reindirizzamento dell'URL o accesso alla VLAN.
7. Il WLC supporta CoA-Req e Disconnect-Req in base alla RFC 3576. Il WLC deve supportare CoA-Req per il servizio di riautenticazione, come da RFC 5176.
8. Anziché ACL scaricabili, sul WLC vengono utilizzati ACL preconfigurati. Il server ISE invia semplicemente il nome ACL, già configurato nel controller.

9. Questa progettazione è valida sia per le VLAN che per gli ACL. In caso di override della VLAN, è sufficiente reindirizzare la porta 80 per consentire al resto del traffico sulla VLAN di quarantena. Per l'ACL, viene applicato l'ACL di preautenticazione ricevuto in accettazione dell'accesso.

La figura seguente fornisce una rappresentazione visiva di questo flusso di funzionalità:



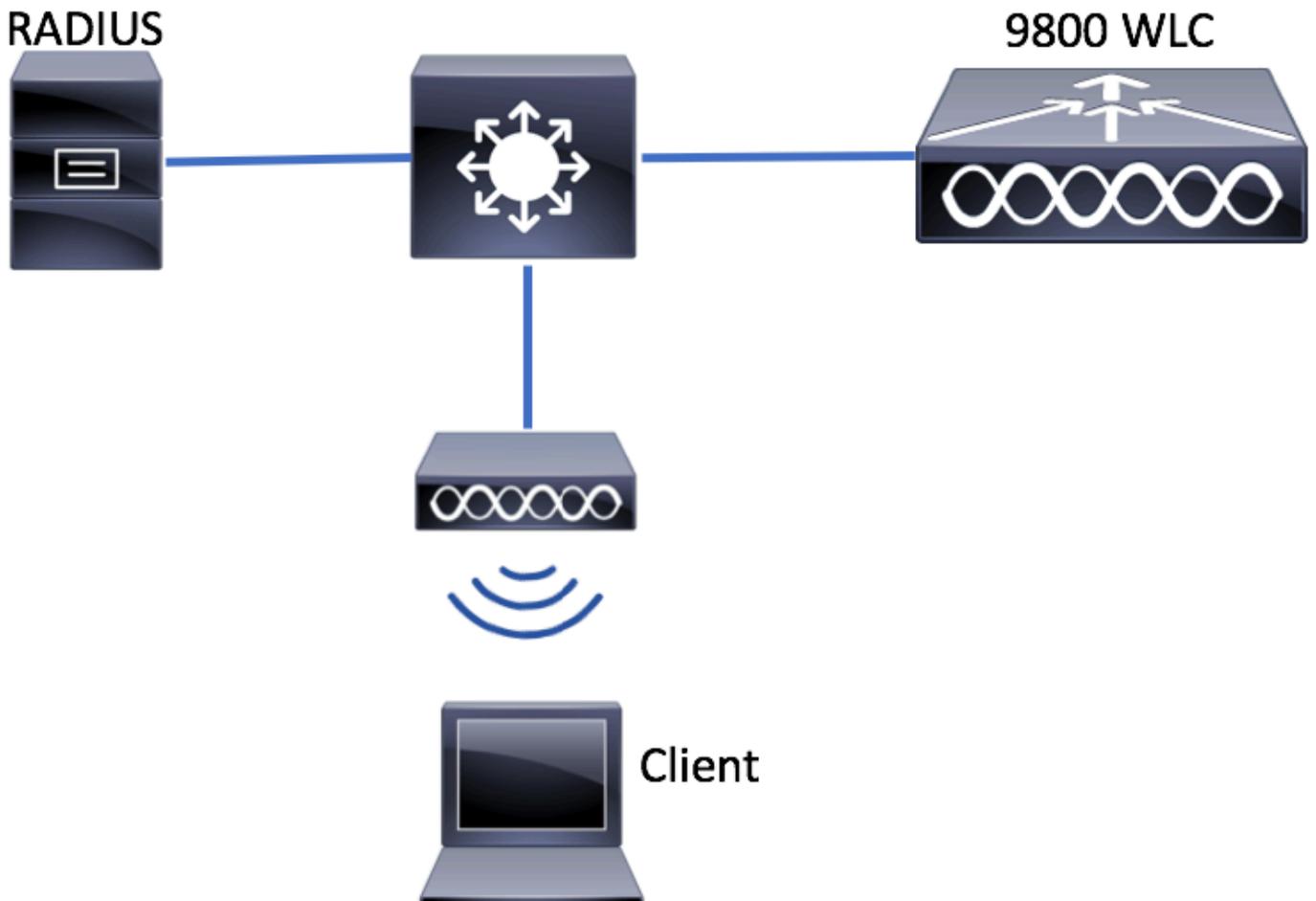
flusso di lavoro delle funzionalità

In questo caso, un SSID utilizzato solo per gli utenti aziendali è abilitato per la postura. In questo SSID non sono presenti altri scenari di utilizzo, ad esempio BYOD, Guest o altri.

Quando un client wireless si connette a Posture SSID per la prima volta, deve scaricare e installare il modulo Posture sul portale reindirizzato dell'ISE e infine deve essere applicato con gli ACL pertinenti in base al risultato della verifica della postura (conforme/non conforme).

## Configurazione

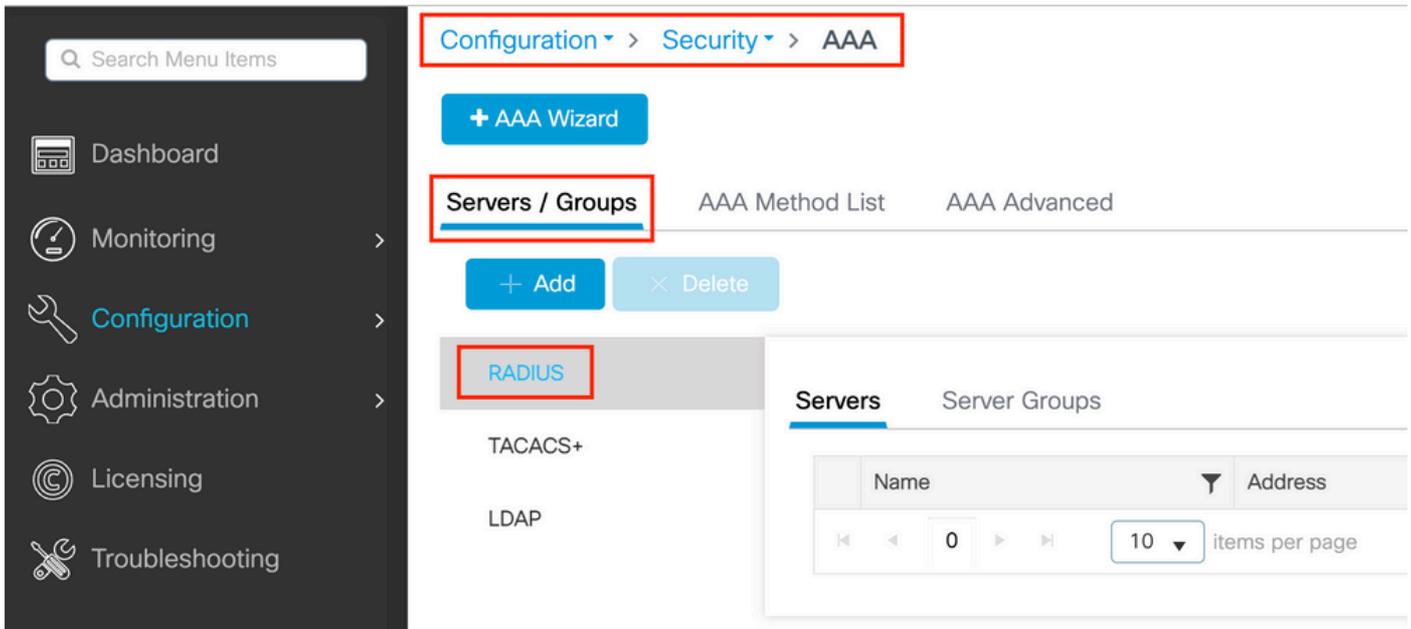
### Esempio di rete



Esempio di rete

## Configurazione AAA sui controller 9800 WLC

Passaggio 1. Aggiungere il server ISE alla configurazione WLC 9800. Passare a Configurazione > Sicurezza > AAA > Server/Gruppi > RADIUS > Server > + Aggiungi e immettere le informazioni sul server RADIUS come mostrato nelle immagini. Assicurarsi che il supporto per CoA sia abilitato per la postura NAC.



9800 create radius server

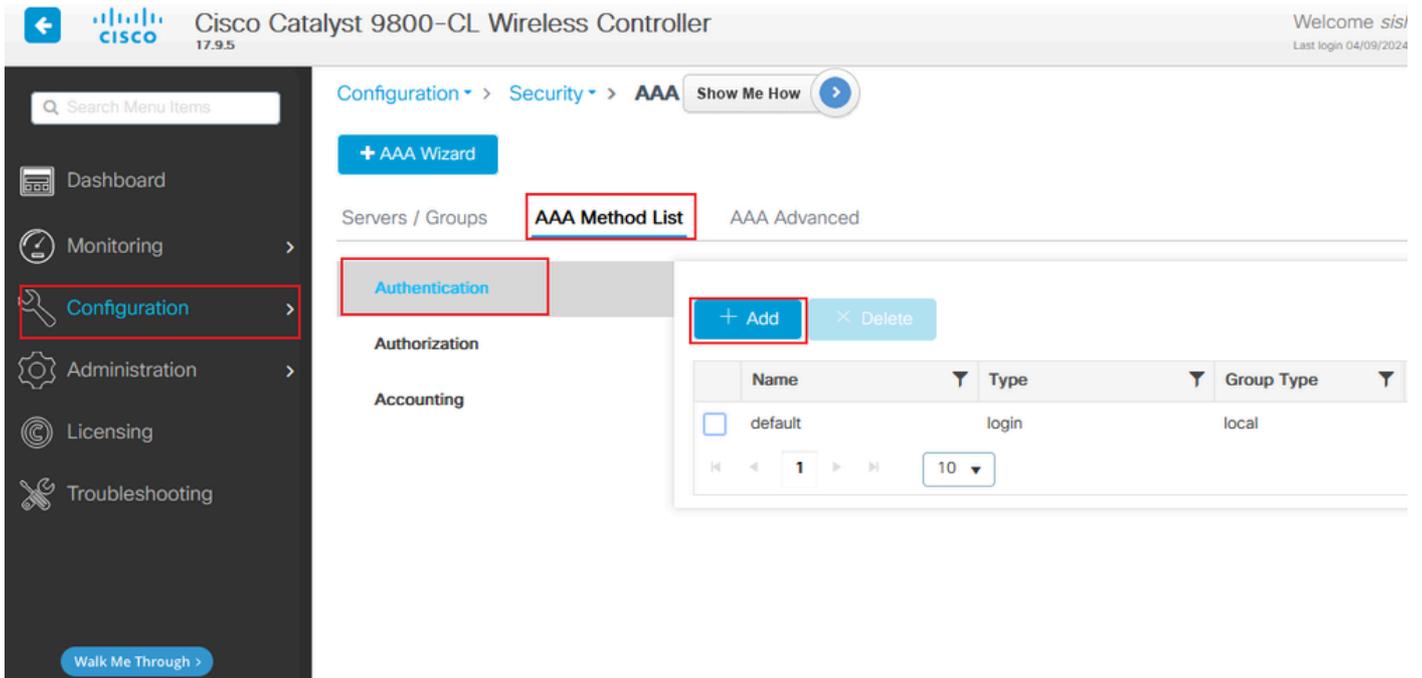
The image displays the 'Create AAA Radius Server' configuration form. The form includes the following fields and options:

- Name\*: posture-radius
- Server Address\*: 10.124.57.141
- PAC Key:
- Key Type: Clear Text
- Key\*: [masked]
- Confirm Key\*: [masked]
- Auth Port: 1812
- Acct Port: 1813
- Server Timeout (seconds): 1-1000
- Retry Count: 0-100
- Support for CoA:  ENABLED
- CoA Server Key Type: Clear Text
- CoA Server Key: [masked]
- Confirm CoA Server Key: [masked]
- Automate Tester:

At the bottom, there are 'Cancel' and 'Apply to Device' buttons.

9800 - crea dettagli raggio

Passaggio 2. Creare un elenco di metodi di autenticazione. Passare a Configurazione > Sicurezza > AAA > Elenco metodi AAA > Autenticazione > + Aggiungi come mostrato nell'immagine:



9800 add auth list

### Quick Setup: AAA Authentication

Method List Name\*

Type\*  ⓘ

Group Type  ⓘ

Fallback to local

**Available Server Groups** **Assigned Server Groups**

ldap

tacacs+

>

<

>>

<<

radius

^

^

v

v

9800 - crea dettagli elenco di autenticazione

Passaggio 3. (Facoltativo) Creare un elenco di metodi contabili come mostrato nell'immagine:



## Add WLAN



### General

### Security

### Advanced

Profile Name\*

SSID\*

WLAN ID\*

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

Cancel

Apply to Device

9800: creazione di una WLAN generale

Passaggio 3. Passare alla scheda Protezione e scegliere il metodo di protezione desiderato. In questo caso, scegliere '802.1x' e l'elenco di autenticazione AAA (creato nel passaggio 2. nella sezione Configurazione AAA) sono obbligatori:

## 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  WPA2 Policy   
GTK Randomize  OSEN Policy

### WPA2 Encryption

AES(CCMP128)  CCMP256   
GCMP128  GCMP256

### Protected Management Frame

PMF

### Fast Transition

Status

Over the DS

Reassociation Timeout \*

### Auth Key Mgmt

802.1x  PSK   
Easy-PSK  CCKM   
FT + 802.1x  FT + PSK   
802.1x-SHA256  PSK-SHA256

Cancel

Apply to Device

9800: creazione della sicurezza WLAN 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

Local EAP Authentication

9800: creazione di AAA per la sicurezza WLAN

## Configurazione del profilo di policy

All'interno di un profilo di policy, è possibile decidere di assegnare ai client la VLAN desiderata, tra le altre impostazioni (ad esempio, Access Controls List (ACL), Quality of Service (QoS), Mobility Anchor, Timer e così via). È possibile usare il profilo di policy predefinito oppure crearne uno nuovo.

Passaggio 1. Creare un nuovo Policy Profile (Profilo di policy). Passare a Configurazione > Tag e profili > Criterio e crearne uno nuovo:

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

Verificare che il profilo sia abilitato.

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

Passaggio 2. Selezionare la VLAN. Passare alla scheda Access Policies (Criteri di accesso) e scegliere il nome della VLAN dall'elenco a discesa o digitare manualmente l'ID della VLAN. Non configurare un ACL nel profilo di policy:

### 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  ⓘ

**VLAN**

VLAN/VLAN Group  ⓘ

Multicast VLAN

**WLAN ACL**

IPv4 ACL  ⓘ

IPv6 ACL  ⓘ

**URL Filters** ⓘ

Pre Auth  ⓘ

Post Auth  ⓘ

9800: creazione della VLAN del profilo della policy

Passaggio 3. Configurare il profilo di policy per accettare le sostituzioni ISE (Allow AAA Override) e le modifiche di autorizzazione, o CoA (Change of Authorization) (stato NAC). È possibile anche specificare un metodo di accounting:

⚠ 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**

**WLAN Timeout**

Session Timeout (sec)  ⓘ

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

Guest LAN Session Timeout

**DHCP**

IPv4 DHCP Required

DHCP Server IP Address

Show more >>>

**AAA Policy**

Allow AAA Override

NAC State

Policy Name  ✕ ⓘ

Accounting List  ✕ ⓘ

**WGB Parameters**

Fabric Profile   ⓘ

Link-Local Bridging

mDNS Service Policy  ⓘ [Clear](#)

Hotspot Server  ⓘ

**User Defined (Private) Network**

Status

Drop Unicast

**DNS Layer Security**

DNS Layer Security Parameter Map  ⓘ [Clear](#)

Flex DHCP Option for DNS  **ENABLED**

Flex DNS Traffic Redirect  **IGNORE**

**WLAN Flex Policy**

VLAN Central Switching

Split MAC ACL  ⓘ

**Air Time Fairness Policies**

Cancel

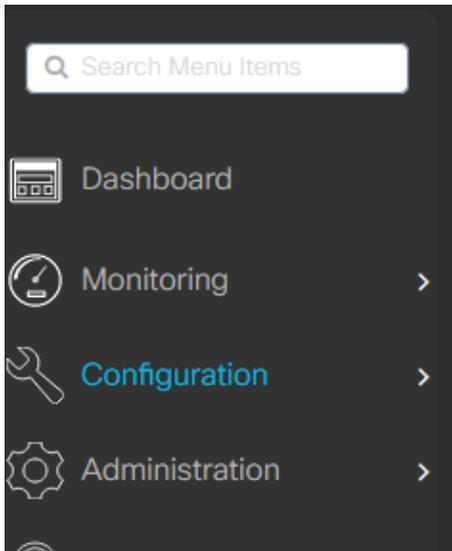
Update & Apply to Device

9800 create policy profile Advance

## Configurazione del tag di policy

Il tag di policy permette di collegare l'SSID al profilo di policy. È possibile creare un nuovo tag o utilizzare il tag predefinito.

Passare a Configurazione > Tag e profili > Tag > Criteri e aggiungerne uno nuovo, se necessario, come mostrato nell'immagine:



**Policy** Site RF AP

**+ Add** **× Delete** **Clone**

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

1 10

9800 policy tag add

Associare il profilo WLAN al profilo di policy desiderato:

**Edit Policy Tag**

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

Name\*

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

Dettagli tag criteri 9800

### Assegnazione di un tag di policy

Assegnare il tag di policy agli access point desiderati. Selezionare Configurazione > Wireless > Access Point > Nome access point > Tag generali , effettuare l'assegnazione necessaria, quindi fare clic su Aggiorna e applica al dispositivo.

Edit AP ✕

General
Interfaces
High Availability
Inventory
ICap
Advanced
Support Bundle

**General**

AP Name\*

Location\*

Base Radio MAC

Ethernet MAC

Admin Status ENABLED

AP Mode

**Tags**

⚠ 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

Site

RF

9800 assegnazione di tag ai criteri

## Configurazione degli ACL di reindirizzamento

Per creare un nuovo ACL, selezionare Configurazione > Sicurezza > ACL > + Aggiungi.

L'ACL utilizzato per il reindirizzamento del portale delle posture ha gli stessi requisiti di CWA (Central Web Authentication).

È necessario bloccare il traffico diretto ai nodi ISE PSN e al DNS; tutto il resto del traffico può essere autorizzato. Questo ACL di reindirizzamento non è un ACL di sicurezza, ma un ACL punt che definisce il traffico diretto alla CPU (sui permessi) per un ulteriore trattamento (come il reindirizzamento) e il traffico rimanente sul piano dati (su rifiuto) e impedisce il reindirizzamento. L'ACL deve avere questo aspetto (sostituire 10.124.57.141 con l'indirizzo IP ISE nell'esempio):

**Edit ACL** ✕

ACL Name\*  ACL Type

**Rules**

Sequence\*  Action

Source Type

Destination Type

Protocol

Log  DSCP

	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

Dettagli ACL di reindirizzamento 9800

## Configurazione ACL del criterio

In questo caso, è necessario definire ACL separati su 9800 WLC per ISE per autorizzare gli scenari di conformità e non conformità in base ai risultati del controllo di postura.

[Configuration](#) > [Security](#) > **ACL**

	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 - Generale

Per lo scenario conforme, utilizzare semplicemente consenti tutto in questo caso. Come altra configurazione comune, l'ISE può decidere di non autorizzare alcun ACL nel risultato conforme, il che equivale a permettere tutto sul lato 9800:

**Edit ACL** ✕

ACL Name\*  ACL Type

**Rules**

Sequence\*

Action

Source Type

Destination Type

Protocol

Log

DSCP

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 - 1 of 1 items

9800 ACL - Conforme

In uno scenario non conforme, il client consente l'accesso solo a determinate reti, in genere il server di monitoraggio e aggiornamento (in questo caso ISE):

**Edit ACL** ✕

ACL Name\*  ACL Type

**Rules**

Sequence\*

Action

Source Type

Destination Type

Protocol

Log

DSCP

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 - 5 of 5 items

9800 ACL - Non conforme

Configurazione AAA e impostazione della postura su ISE

Requisito postura: In questo esempio, il requisito per determinare la conformità è rilevare se un file di test specifico esiste sul desktop utilizzato per testare il PC Windows.

Passaggio 1. Aggiungere WLC 9800 come AND sull'ISE. Selezionare Amministrazione > Risorse di rete > Dispositivi di rete > Aggiungi:

The screenshot shows the Cisco ISE Administration interface for adding a new network device. The breadcrumb trail is Administration > Network Resources > Network Devices > Add. The device name is set to WLC9800. The IP address is 10.124.60.41 with a subnet mask of 32. The device profile is set to Cisco. Other fields like Model Name, Software Version, Location, IPSEC, and Device Type are set to their default values.

Field	Value	Action
Name	WLC9800	
Description		
IP Address	10.124.60.41 / 32	
Device Profile	Cisco	
Model Name		
Software Version		
Network Device Group		
Location	All Locations	Set To Default
IPSEC	No	Set To Default
Device Type	All Device Types	Set To Default

Aggiungi dispositivo di rete 01

The screenshot shows the RADIUS Authentication Settings configuration page. The 'RADIUS Authentication Settings' section is highlighted with a red box. The 'RADIUS UDP Settings' section is also highlighted with a red box. The 'Shared Secret' field is highlighted with a red box and contains a masked value. The 'CoA Port' field is highlighted with a red box and is set to 1700. The 'RADIUS DTLS Settings' section is also highlighted with a red box. The 'DTLS Required' checkbox is unchecked. The 'Shared Secret' field is set to radius/dtls. The 'CoA Port' field is set to 2083. The 'Issuer CA of ISE Certificates for CoA' dropdown is set to 'Select if required (optional)'. The 'DNS Name' field is empty.

Section	Field	Value	Action
RADIUS Authentication Settings	Protocol	RADIUS	
	Shared Secret	*****	Show
	Use Second Shared Secret	<input type="checkbox"/>	
RADIUS UDP Settings	CoA Port	1700	Set To Default
	Second Shared Secret		Show
RADIUS DTLS Settings	DTLS Required	<input type="checkbox"/>	
	Shared Secret	radius/dtls	
	CoA Port	2083	Set To Default
	Issuer CA of ISE Certificates for CoA	Select if required (optional)	
	DNS Name		

Aggiungi dispositivo di rete 02

Passaggio 2. Scaricare il pacchetto di distribuzione e il modulo di conformità dell'headend Cisco Secure Client sul sito Web CCO per il software Cisco.

## Accesso e ricerca in 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.  
[cisco-secure-client-win-4.3.3335.6146-isecompliance-webdeploy-k9.pkg](#)  
[Advisories](#)

ISE Compliance Module 4.3

Passaggio 3. Caricare il pacchetto del pacchetto di distribuzione headend Cisco Secure Client e il pacchetto del modulo di conformità in ISE Client Provisioning. Passare a Centri di lavoro> Postura> Provisioning client> Risorse. Fare clic su Aggiungi, Scegliere Risorse agente dal disco locale dalla casella a discesa:

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

Edit + Add Duplicate Delete Quick Filter

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 ...

Caricamento del client sicuro e del modulo di conformità completato

Passaggio 4. Crea profilo postura agente Passare a Centri di lavoro> Postura> Provisioning client> Risorse> Aggiungi> Profilo postura agente:

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

ISE Posture Agent Profile Settings > bloomtest-Posture for Windows

Agent Posture Profile

Name \*  
bloomtest-Posture for Windows

Description:  
test windows PC for connecting WLC9800

Agent Behavior

Parameter	Value	Description
Enable debug log	No	Enables the debug log on the agent
Operate on non-802.1X wireless	No	Enables the agent to operate on non-802.1X wireless networks.
Enable signature check	No	Check the signature of executables before running them.
Log file size	5 MB	The maximum agent log file size
Remediation timer	4 mins	If the user fails to remediate within this specified time, mark them as non-compliant.
Stealth Mode	Disabled	Agent can act as either clientless or standard mode. When stealth mode is enabled, it runs as a service without any user interface.
Enable notifications in stealth mode	Disabled	Display user notifications even when in Stealth mode.

Profilo postura agente

Passaggio 5. Creare la configurazione dell'agente Passare a Centri di lavoro> Postura> Provisioning client> Risorse> Aggiungi> Configurazione agente:

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	<input checked="" type="checkbox"/>
VPN	<input type="checkbox"/>
Zero Trust Access	<input type="checkbox"/>
Network Access Manager	<input type="checkbox"/>
Secure Firewall Posture	<input type="checkbox"/>
Network Visibility	<input type="checkbox"/>
Umbrella	<input type="checkbox"/>
Start Before Logon	<input type="checkbox"/>
Diagnostics and Reporting Tool	<input checked="" type="checkbox"/>

Profile Selection

\* ISE Posture bloomtest-Posture for Windows

Aggiungi configurazione agente

Passaggio 6. Verificare che il portale di provisioning client sia corretto. Utilizzare il portale predefinito per il testing. (Generare CSR e richiedere un certificato SSL dal server CA e sostituire il tag Gruppo di certificati in queste impostazioni del portale. In caso contrario, durante il processo di test verrà visualizzato un avviso di certificato non attendibile.)

Passare a Centri di lavoro> Postura> Provisioning client> Portali provisioning client:

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

Scegli portale di provisioning client 01

Client Provisioning Policy  
Resources  
Client Provisioning Portal

**Portal Behavior and Flow Settings** Portal Page Customization

Portal & Page Settings

Portal Settings

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

Bidirectional port:\* **8449** (8000 - 8999)

Allowed Interfaces:\*

For PSNs Using Physical Interfaces	For PSNs with Bonded Interfaces Configured
<input checked="" type="checkbox"/> Gigabit Ethernet 0	<input checked="" type="checkbox"/> Bond 0 Uses Gigabit Ethernet 0 as primary interface, Gigabit Ethernet 1 as backup
<input type="checkbox"/> Gigabit Ethernet 1	<input type="checkbox"/> Bond 1 Uses Gigabit Ethernet 2 as primary interface, Gigabit Ethernet 3 as backup
<input type="checkbox"/> Gigabit Ethernet 2	<input type="checkbox"/> Bond 2 Uses Gigabit Ethernet 4 as primary interface, Gigabit Ethernet 5 as backup
<input type="checkbox"/> Gigabit Ethernet 3	
<input type="checkbox"/> Gigabit Ethernet 4	
<input type="checkbox"/> Gigabit Ethernet 5	

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](#)

Scegli portale di provisioning client 02

Passaggio 7. Creazione dei criteri di provisioning client. Passare a Centri di lavoro> Postura> Provisioning client> Criterio di provisioning client > Modifica> inserire un nuovo criterio sopra.

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

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 <a href="#">Edit</a> ▼
<input checked="" type="checkbox"/> IOS	If Any	and Apple IOS All	and Condition(s)	then Cisco-ISE-NSP <a href="#">Edit</a> ▼
<input checked="" type="checkbox"/> Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP <a href="#">Edit</a> ▼
<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 <a href="#">Edit</a> ▼
<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 <a href="#">Edit</a> ▼
<input checked="" type="checkbox"/> Chromebook	If Any	and Chrome OS All	and Condition(s)	then Cisco-ISE-Chrome-NSP <a href="#">Edit</a> ▼

Crea criterio di provisioning client

Passaggio 8. Creazione delle condizioni del file. Passare a Centri di lavoro> Postura> Elementi della policy> Condizioni> File > Condizioni file> Aggiungi:

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

Crea condizione file

Passaggio 9. Creazione di soluzioni Passare a Centri di lavoro> Postura> Elementi dei criteri> Risoluzioni > File> Aggiungi:

≡ 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

Crea risoluzione file

Passaggio 10. Creazione del fabbisogno. Passare a Centri di lavoro> Postura> Elementi criteri> Requisiti> Inserisci nuovo requisito:

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

Remediations

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

Requirements

- Allowed Protocols
- Authorization Profiles
- Downloadable ACLs

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 <a href="#">Edit</a>
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 <a href="#">Edit</a>
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 <a href="#">Edit</a>
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 <a href="#">Edit</a>
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 <a href="#">Edit</a>
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 <a href="#">Edit</a>
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 <a href="#">Edit</a>
WLC9800-Posture-Demo	for Windows All	using Any version	using Agent	met if WLC9800-Posture-demo then	WLC9800-Posture-Demo <a href="#">Edit</a>

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.

Crea requisito postura

Passaggio 11. Creazione dei criteri di postura. Passare a Centri di lavoro> Postura> Inserisci nuovo criterio:

Cisco ISE Work Centers - Posture

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	with WLC9800-Posture-Demo <a href="#">Edit</a>

Crea criterio di postura

Passaggio 12. Creare tre profili di autorizzazione: Stato della postura sconosciuto; lo stato della postura non è conforme; Lo stato della postura è conforme. Passare a Criterio> Elementi dei criteri> Risultati> Autorizzazione> Profili di autorizzazione> Aggiungi:

Dictionaries Conditions **Results**

Authentication

- Allowed Protocols

Authorization

- Authorization Profiles
- Downloadable ACLs

Profiling

Posture

Client Provisioning

### Standard Authorization Profiles

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

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

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

## Crea profili di autorizzazione 01

Dictionarys Conditions **Results**

Authentication > Allowed Protocols

Authorization > Authorization Profiles > Downloadable ACLs

Profiling >

Posture >

Client Provisioning >

Authorization Profiles > WLC9800-Posture-Unknown

### Authorization Profile

\* Name: WLC9800-Posture-Unknown

Description:

\* Access Type: ACCESS\_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement:  ⓘ

Agentless Posture:  ⓘ

Passive Identity Tracking:  ⓘ

Common Tasks

Voice Domain Permission

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

Client Provisioning (Posture):  ACL: POSTURE\_REDIRECT\_ACL Value: Client Provisioning Portal (def: )

Static IP/Port name/FQDN

Suppress Profiler CoA for endpoints in Logical Profile

## Crea profili di autorizzazione 02

Dictionarys Conditions **Results**

Authentication > Allowed Protocols

Authorization > Authorization Profiles > Downloadable ACLs

Profiling >

Posture >

Client Provisioning >

Authorization Profiles > WLC9800-Posture-Compliant

### Authorization Profile

\* Name: WLC9800-Posture-Compliant

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\_COMPLIANT\_ACL

Airespace IPv6 ACL Name

## Crea profili di autorizzazione 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

Passaggio 13. Creazione di set di criteri. Passa a Criterio > Criterio

Policy Sets Reset [Reset Policyset Hitcounts](#) [Save](#)

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
<span style="color: green;">●</span>	WLC9800-Posture-Demo		AND <ul style="list-style-type: none"> <li>Network Access Device IP Address EQUALS 10.124.60.41</li> <li>Normalised Radius-SSID CONTAINS posture_demo</li> </ul>	Default Network Access	0	<a href="#">⚙️</a>	<a href="#">➔</a>
<span style="color: green;">●</span>	Default	Default policy set		Default Network Access	0	<a href="#">⚙️</a>	<a href="#">➔</a>

[Reset](#) [Save](#)

Crea set di criteri

Sets> Aggiungi icona:

Passaggio 14. Creazione del criterio di autenticazione Passare a Criterio> Set di criteri> Espandere "WLC9800-Posture-Demo"> Criteri di autenticazione> Aggiungi:

Cisco ISE Policy - Policy Sets

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

Crea criterio di autenticazione

Passaggio 15. Creazione del criterio di autorizzazione Passare a Criterio> Set di criteri> Espandere "WLC9800-Posture-Demo"> Criterio di autorizzazione> Aggiungere:

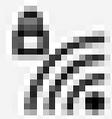
Authorization Policy (4)

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

Crea criterio di autorizzazione

## Esempi

1. Test connesso SSID posture\_demo con credenziali 802.1X corrette.



posture\_demo  
Secured

Enter your user name and password

wlc9800-user

••••••••



OK

Cancel

## Network & Internet settings

Change settings, such as making a connection metered.



- Se il browser è stato reindirizzato all'URL del portale ISE ma non è possibile caricare la pagina, verificare se il nome di dominio ISE non è stato aggiunto al server DNS e il client non è in grado di risolvere l'URL del portale. Per risolvere rapidamente il problema, controllare il nome IP/host statico/FQDN nel profilo di autorizzazione per fornire l'indirizzo IP nell'URL di reindirizzamento. Tuttavia, questo problema può riguardare la sicurezza in quanto espone l'indirizzo IP dell'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

## Raccogli debug

[Abilita debug su C9800](#)

[Abilita debug su ISE](#)

## Riferimenti

- [Configurazione di CWA su Catalyst 9800 WLC e ISE - Cisco](#)
- [BYOD wireless con Identity Services Engine](#)
- [Implementazione della postura ISE](#)
- [Risoluzione dei problemi di gestione e postura delle sessioni ISE](#)
- [Confronta il flusso di reindirizzamento della postura ISE con il flusso di reindirizzamento della postura ISE](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).