

Configureren van houding op Catalyst 9800 WLC en ISE

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[AAA-configuratie op 9800 WLC](#)

[WLAN-configuratie](#)

[Configuratie van beleidsprofiel](#)

[Configuratie van beleidstag](#)

[Toewijzing van beleidstags](#)

[Configuratie ACL-omleiding](#)

[Configuratie van ACL-beleid](#)

[AAA-configuratie en -instelling op ISE](#)

[Voorbeelden](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Checklist](#)

[Debugs verzamelen](#)

[Referenties](#)

Inleiding

Dit document beschrijft hoe u een houding WLAN op een Catalyst 9800 WLC en ISE kunt configureren via de grafische gebruikersinterface (GUI).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Algemene configuratie 9800 WLC
- ISE-beleid en profielconfiguratie

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- 980 WLC Cisco IOS® XE koper v17.9.5
- Identity Service Engine (ISE) v3.2
- Laptop Windows 10 Enterprise

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

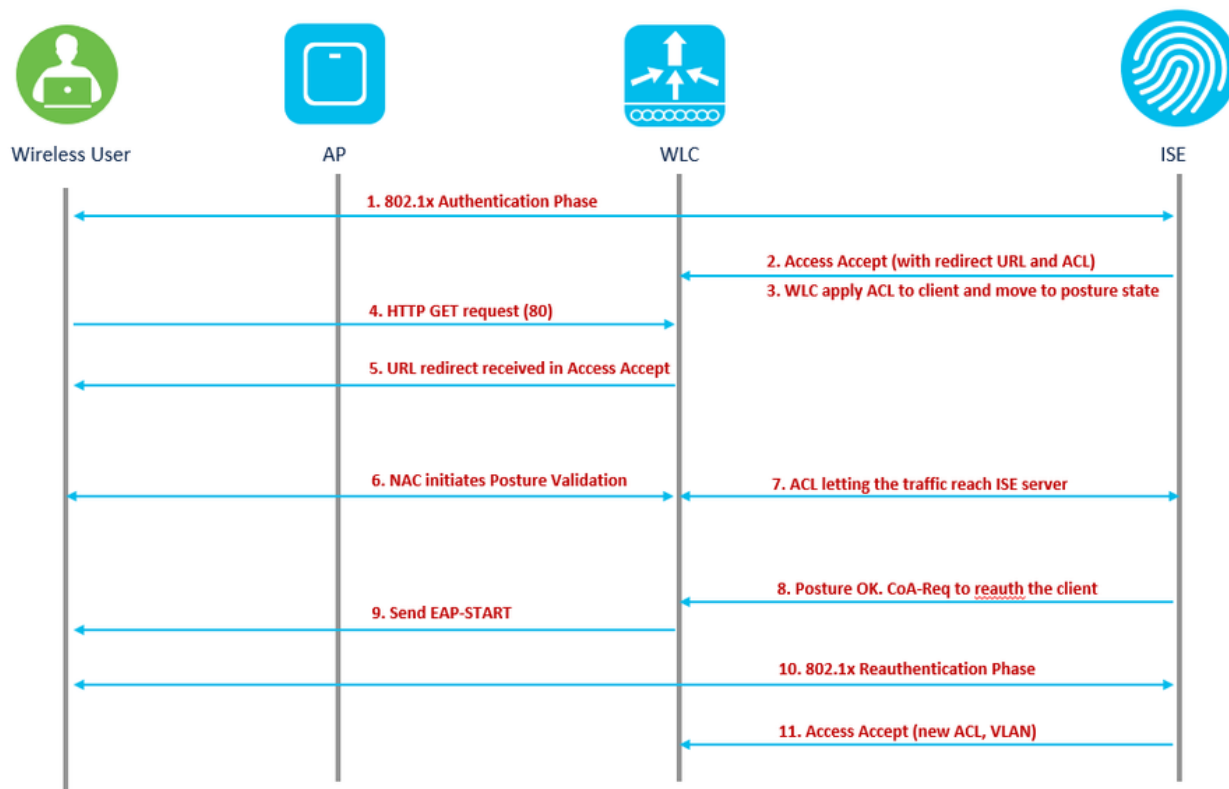
Achtergrondinformatie

Functiestroom voor draadloze LAN-controller voor RADIUS, NAC en CoA

1. Client verifieert met behulp van dot1x-verificatie.
2. RADIUS-toegangsgoedkeuring bevat omgeleide URL voor poort 80 en pre-auth ACL's die het toestaan van IP-adressen en poorten of quarantaine-VLAN omvatten.
3. De client wordt omgeleid naar de URL die in toegang accepteert wordt geleverd en wordt in een nieuwe status geplaatst tot de posture validatie is uitgevoerd. De client in deze staat praat met de ISE-server en valideert zichzelf tegen de beleidsregels die op de ISE NAC-server zijn geconfigureerd.
4. NAC-agent op client initieert posture-validatie (verkeer naar poort 80): Agent stuurt HTTP-detectieaanvraag naar poort 80 die controller omleidt naar URL die in toegang wordt verstrekt accepteert. De ISE weet dat de klant probeert te bereiken en direct op de klant reageert. Op deze manier leert de client over de ISE-server IP en van nu af aan spreekt de client direct met de ISE-server.
5. WLC staat dit verkeer toe omdat ACL wordt gevormd om dit verkeer toe te staan. In het geval van VLAN-overschrijving wordt het verkeer overbrugd zodat het de ISE-server bereikt.
6. Zodra de ISE-client de evaluatie heeft voltooid, wordt een RADIUS CoA-Req met basisservice naar de WLC verzonden. Hiermee wordt de verificatie van de client opnieuw gestart (door EAP-START te verzenden). Zodra de herverificatie slaagt, stuurt de ISE toegang accepteren met een nieuwe ACL (indien van toepassing) en geen URL doorsturen, of toegang tot VLAN.
7. WLC ondersteunt CoA-Req en Disconnect-Req zoals in RFC 3576. De WLC moet CoA-Req ondersteunen voor opnieuw opstarten, zoals per RFC 5176.
8. In plaats van downloadbare ACL's worden voorgeconfigureerde ACL's op de WLC gebruikt. De ISE-server verstuurt alleen de ACL-naam, die al in controller is geconfigureerd.
9. Dit ontwerp werkt voor zowel VLAN- als ACL-cases. In het geval van VLAN override, we

gewoon de poort 80 wordt omgeleid en staat (bridge) rest van het verkeer op het quarantine VLAN toe. Voor ACL wordt de pre-auth ACL die in toegang wordt ontvangen, toegepast.

Dit cijfer geeft een visuele weergave van deze functiestroom:



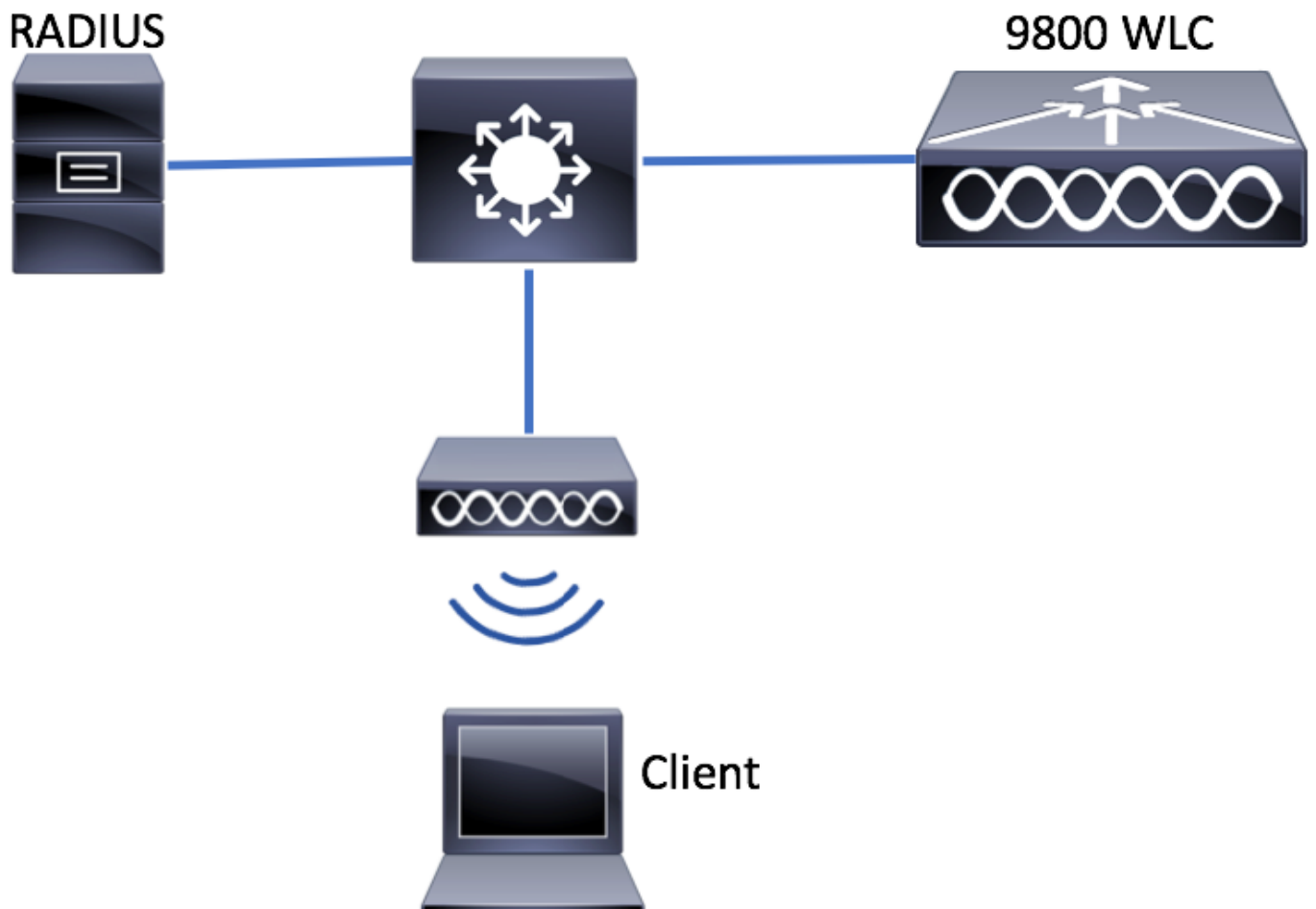
kenmerkenworkflow

Voor dit gebruiksgesval, wordt een SSID die slechts voor collectieve gebruikers wordt gebruikt toegelaten voor houding. Er bestaan geen andere gebruikscases, zoals BYOD, Guest, of andere op deze SSID.

Wanneer een draadloze client voor de eerste keer verbinding maakt met de Posture SSID, moet hij de Posture Module downloaden en installeren op het omgeleide portaal van de ISE, en uiteindelijk toegepast met relevante ACL's gebaseerd op het resultaat van de posture check (conform/niet-conform).

Configureren

Netwerkdigram



Netwerkdigram

AAA-configuratie op 9800 WLC

Stap 1. Voeg de ISE-server toe aan de 9800 WLC-configuratie. Ga naar Configuratie > Beveiliging > AAA > Servers/groepen > RADIUS > Servers > + Voeg de RADIUS-serverinformatie toe en voer deze in zoals in de afbeeldingen. Zorg ervoor dat ondersteuning voor CoA is ingeschakeld voor postuur NAC.

- Dashboard
- Monitoring
- Configuration
- Administration
- Licensing
- Troubleshooting

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add × Delete

RADIUS

TACACS+

LDAP

Servers Server Groups

Name	Address
0 10 items per page	

9800 straalserver maken

Create AAA Radius Server

Name* posture-radius

Server Address* 10.124.57.141

PAC Key ☐

Key Type Clear Text

Key*

Confirm Key*

Auth Port 1812

Acct Port 1813

Server Timeout (seconds) 1-1000

Retry Count 0-100

Support for CoA ☒

CoA Server Key Type Clear Text

CoA Server Key

Confirm CoA Server Key

Automate Tester ☐

Cancel

Apply to Device

De 9800 genereert radiusdetails

Stap 2. Maak een lijst met verificatiemethoden. Navigeer naar Configuratie > Beveiliging > AAA > AAA-methodelijst > Verificatie > + Toevoegen zoals in de afbeelding:

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
☐ default	login	local

1 10

Walk Me Through >

9800 controlelijst toevoegen

Quick Setup: AAA Authentication

Method List Name* posture-authn-list

Type* dot1x ⓘ

Group Type group ⓘ

Fallback to local ☐

Available Server Groups

Assigned Server Groups

radius

Cancel Apply to Device

9800 controlegegevens maken

Stap 3. (Optioneel) Maak een lijst met boekhoudmethoden zoals in de afbeelding:

- 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 rekeninglijst toevoegen

Quick Setup: AAA Accounting

Method List Name*

POSTUREacct

Type*

identity

Available Server Groups

Assigned Server Groups

ldap
tacacs+

radius

[Cancel](#)

[Apply to Device](#)

9800 maken lijst met wijzigingen

WLAN-configuratie

Stap 1. Maak het WLAN. Navigeren naar Configuratie > Tags en profielen > WLAN's > + Het netwerk toevoegen en configureren als dat nodig is:

- Dashboard

Configuration > Tags & Profiles > **WLANs**

[+ Add](#)

[× Delete](#)

[Clone](#)

[Enable WLAN](#)

[Disable WLAN](#)

9800 WLAN-add

Stap 2. Voer de algemene informatie van WLAN in.

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 maakt WLAN-algemeen

Stap 3. Navigeer naar het tabblad Beveiliging en kies de gewenste beveiligingsmethode. Kies in dit geval '802.1x' en kies de AAA-verificatielijst (die u in Stap 2 hebt gemaakt. in het gedeelte AAA Configuration) die nodig is:

Layer2 Layer3 AAA

 Cancel

 Apply to Device

Edit WLAN

General **Security** Advanced Add To Policy Tags

Configuratie van beleidsprofiel

Binnen een beleidsprofiel kunt u beslissen de clients toe te wijzen aan wie VLAN, onder andere instellingen (zoals ACL's (toegangscontrolelijst), Quality of Service (QoS), mobiliteitsanker, timers enzovoort). U kunt uw standaardbeleidsprofiel gebruiken of u kunt een nieuw profiel maken.

Stap 1. Maak een nieuw beleidsprofiel. Navigeren naar Configuratie > Tags & profielen > Beleid en een nieuwe maken:

Configuration > Tags & Profiles > Policy

+ Add Delete Clone

	Admin Status	Associated Policy Tags	Policy Profile Name
☐	✓		posture_demo_pp
☐	✓		default-policy-profile

1 10

9800 beleidsprofiel toevoegen

Zorg ervoor dat het profiel is ingeschakeld.

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 algemeen beleidsprofiel maken

Stap 2. Kies VLAN. Navigeer naar het tabblad Toegangsbeleid en kies de VLAN-naam in de vervolgkeuzelijst of typ handmatig de VLAN-ID. Configureer geen ACL in het beleidsprofiel:

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 beleidsprofiel VLAN maken

Stap 3. Configureer het beleidsprofiel om ISE-overschrijvingen (AAA-overschrijving toestaan) en wijzigingen van autorisatie (CoA) (NAC-status) te accepteren. U kunt optioneel ook een boekhoudmethode opgeven:

⚠ 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)

1800

i

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 x ▼

Accounting List

POSTUREacct x ▼

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

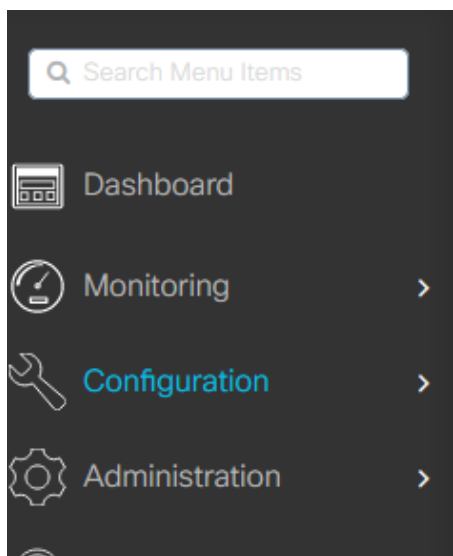
Update & Apply to Device

9800 beleidsprofiel maken Vooruitgang

Configuratie van beleidstag

Binnen de Policy Tag is waar u uw SSID koppelt aan uw Policy Profile. U kunt een nieuwe Policy Tag maken of de standaard-policy tag gebruiken.

Navigeer naar Configuration > Tags & profielen > Tags > Policy en voeg indien nodig een nieuwe toe zoals in de afbeelding:



Configuration > Tags & Profiles > Tags

Policy

Site

RF

AP

+ Add

× Delete

Clone

Policy Tag Name

default-policy-tag

1

10

9800 beleidstag toevoegen

Koppel uw WLAN-profiel aan het gewenste beleidsprofiel:

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



posture_demo

posture_demo_pp

1

10

1 - 1 of 1 items

9800 beleidstag - gegevens

Toewijzing van beleidstags

Wijs de beleidstag toe aan de benodigde toegangspunten. Navigeer naar Configuration > Wireless > Access points > AP-naam > General Tags, maak de benodigde toewijzing en klik vervolgens op Update & Apply op apparaat .

Edit AP

General

Interfaces

High Availability

Inventory

ICap

Advanced

Support Bundle

General

AP Name*

Location*

Base Radio MAC

Ethernet MAC

Admin Status

AP Mode

default location

ENABLED

Local

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

posture-policy-tag

Site

default-site-tag

RF

default-rf-tag

9800 beleidstag toewijzing

Configuratie ACL-omleiding

Navigeer naar Configuratie > Beveiliging > ACL > + Toevoegen om een nieuwe ACL te maken.

De ACL die wordt gebruikt voor Posture Portal Redirect heeft dezelfde vereisten als de CWA (Central Web Verification).

U moet verkeer naar uw ISE-PSN-knooppunten ontkennen en DNS weigeren en alle rest toestaan. Deze omleiden ACL is geen security ACL maar een punt ACL die bepaalt welk verkeer naar de CPU gaat (op vergunningen) voor verdere behandeling (zoals omleiding) en welk verkeer op het dataplatform blijft (op ontkennen) en omleiding vermijdt. De ACL moet er zo uitzien (vervang in dit voorbeeld 10.124.57.141 door uw ISE-IP-adres):

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
☐	10	deny	any		10.124.57.141		ip	None	None	None	Disa
☐	20	deny	10.124.57.141		any		ip	None	None	None	Disa
☐	30	deny	any		any		udp	None	eq domain	None	Disa
☐	40	deny	any		any		udp	eq domain	None	None	Disa
☐	50	permit	any		any		tcp	None	eq www	None	Disa

9800 omleiding ACL-gegevens

Configuratie van ACL-beleid

In dit geval moet u op 9800 WLC afzonderlijke ACL's definiëren voor ISE om de compatibele en niet-conforme scenario's te autoriseren op basis van het resultaat van de beeldcontrole.

Configuration > Security > ACL

+ Add

× Delete

Associate Interfaces

	ACL Name	ACL Type
☐	POSTURE_COMPLIANT_ACL	IPv4 Extended
☐	POSTURE_NON-COMPLIANT_ACL	IPv4 Extended
☐	POSTURE_REDIRECT_ACL	IPv4 Extended

⏪

⏩

1

⏪

⏩

10

9800 ACL - algemeen

Voor Volgzaam scenario, gebruik gewoon vergunning allen in dit geval. Als een andere gemeenschappelijke configuratie, kunt u ook ISE hebben om geen ACL in het volgzaam resultaat toe te staan, dat gelijkwaardig is om allen aan de 9800 kant toe te staan:

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
☐	10	permit	any		any		ip	None	None	None	Disable

1

10

1 - 1 of 1 items

9800 ACL - conform

Voor niet-conforme scenario's verleent de client alleen toegang tot bepaalde netwerken, doorgaans de herstelserver (in dit geval ISE zelf):

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
☐	10	permit	10.124.57.141		any		ip	None	None	None	Disa
☐	20	permit	any		10.124.57.141		ip	None	None	None	Disa
☐	30	permit	any		any		udp	None	eq domain	None	Disa
☐	40	permit	any		any		udp	eq domain	None	None	Disa
☐	50	deny	any		any		ip	None	None	None	Disa

1

10

1 - 5 of 5 items

9800 ACL - niet-conform

AAA-configuratie en -instelling op ISE

Posture-vereiste: In dit voorbeeld is het vereiste om te bepalen of aan de voorwaarden wordt voldaan, om te detecteren of er een specifiek testbestand op het bureaublad bestaat dat wordt gebruikt om Windows PC te testen.

Stap 1. Voeg WLC 9800 toe als NAD op de ISE. Navigeren naar Beheer> Netwerkbronnen> Netwerkkaparameters> Toevoegen:

Cisco ISE Administration - Network Resources

Network Devices | Network Device Groups | Network Device Profiles | External RADIUS Servers | RADIUS Server Sequences | NAC Managers | External MDM | pxGrid Direct Connectors

Network Devices List > WLC9800

Network Devices

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](#)

Netwerkkaparaat toevoegen 10

Cisco ISE Administration - Network Resources

Network Devices | Network Device Groups | Network Device Profiles | External RADIUS Servers | RADIUS Server Sequences | NAC Managers | External MDM | pxGrid Direct Connectors

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

Shared Secret: [Show](#)

☐ Use Second Shared Secret

Second Shared Secret: [Show](#)

CoA Port: 1700 [Set To Default](#)

RADIUS DTLS Settings

☐ DTLS Required

Shared Secret: radius/dtls

CoA Port: 2083 [Set To Default](#)

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

DNS Name:

Netwerkkaparaat toevoegen 02

Stap 2. Download het Cisco Secure Client Head-end implementatiepakket en de compliance-module op de Cisco Software CCO-website.

Cisco Secure-client voor toegang en zoeken:

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-nalevingsmodule 4.3

Stap 3. Upload het Cisco Secure Client Head-end implementatiepakket en het compliance-modulepakket naar ISE-clientprovisioning. Navigeren naar werkcentra> houding> clientprovisioning> resources . Klik op Toevoegen en kies resources van de agent op de lokale schijf in de vervolgkeuzelijst.

OverviewNetwork DevicesClient ProvisioningPolicy Elements

Client Provisioning Policy

Resources

Client Provisioning Portal

EditAddDuplicateDelete

☐

Agent resources from Cisco site

☐

Agent resources from local disk

☐

Native Supplicant Profile

☐

Agent Configuration

☐

Agent Posture Profile

☐

AMP Enabler Profile

Beveiligde client voor uploaden

Cisco ISE

Work Centers - Posture

OverviewNetwork DevicesClient ProvisioningPolicy ElementsPosture PolicyPolicy SetsTroubleshootReportsSettings

Client Provisioning Policy

Resources

Client Provisioning Portal

Selected 0 Total 13

Quick Filter

Edit

+ Add

Duplicate

Delete

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

Beveiligde client en nalevingsmodule uploaden is geslaagd

Stap 4. Een profiel voor de posterijen van de agent maken Navigeer naar werkcentra> een houding > clientprovisioning> resources> toevoegen> een posterieprofiel voor de agent:

Cisco ISE		Work Centers - Posture																														
Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings																								
Client Provisioning Policy		ISE Posture Agent Profile Settings > bloomtest-Posture for Windows																														
Resources		Agent Posture Profile Name * bloomtest-Posture for Windows Description: test windows PC for connecting WLC9800																														
Client Provisioning Portal		Agent Behavior <table> <tr> <th>Parameter</th><th>Value</th><th>Description</th></tr> <tr> <td>Enable debug log</td><td>No</td><td>Enables the debug log on the agent</td></tr> <tr> <td>Operate on non-802.1X wireless</td><td>No</td><td>Enables the agent to operate on non-802.1X wireless networks.</td></tr> <tr> <td>Enable signature check</td><td>No</td><td>Check the signature of executables before running them.</td></tr> <tr> <td>Log file size</td><td>5 MB</td><td>The maximum agent log file size</td></tr> <tr> <td>Remediation timer</td><td>4 mins</td><td>If the user fails to remediate within this specified time, mark them as non-compliant.</td></tr> <tr> <td>Stealth Mode</td><td>Disabled</td><td>Agent can act as either clientless or standard mode. When stealth mode is enabled, it runs as a service without any user interface.</td></tr> <tr> <td>Enable notifications in stealth mode</td><td>Disabled</td><td>Display user notifications even when in Stealth mode.</td></tr> </table>							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.
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.																														

Profiel van Agent

Stap 5. Agent Configuration maken Navigeer naar werkcentra> Wachtwoord> Clientprovisioning> Resources> Add> Agent Configuration:

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

Configuratie van Add Agent

Stap 6. Bevestig het portaal voor clientprovisioning, gebruik standaardprotocol voor testen is OK. (Genereer CSR en pas een SSL-certificaat toe vanaf de CA-server, en vervang de tag Certificaatgroep op deze profielinstellingen. Anders treedt tijdens het testproces een niet-vertrouwde waarschuwing voor een certificaat op.)

Navigeren naar werkcentra> houding> clientprovisioning> clientprovisioningportalen:

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

Kies client provisioningportal 10

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

☒ 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](#)

Kies client provisioningportal 02

Stap 7. Maak een clientprovisioningbeleid aan. Navigeren naar werkcentra> Houding> Clientprovisioning> Beleid voor clientprovisioning > Bewerken> Nieuwe beleid invoegen hierboven.

Client Provisioning Policy

Resources

Client 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
WLC9800-Windows	If Any	and Windows All	and Condition(s)	this WLC9800-windows Edit
IOS	If Any	and Apple iOS All	and Condition(s)	then Cisco-ISE-NSP Edit
Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP Edit
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
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
Chromebook	If Any	and Chrome OS All	and Condition(s)	then Cisco-ISE-Chrome-NSP Edit

Beleid voor clientprovisioning maken

Stap 8. Bestandsvoorwaarden maken. Navigeer naar werkcentra> houding> beleidsonderdelen>

voorwaarden> bestand> voorwaarden van bestand> toevoegen:

The screenshot shows the Cisco ISE Policy Elements configuration page for a File Condition. The left sidebar lists various conditions, with 'File' selected. The main area shows the configuration for 'WLC9800-Posture-demo'. The following fields are highlighted with red boxes:

- Name: WLC9800-Posture-demo
- Description: test for WLC9800
- * Operating System: Windows All
- * File Type: FileExistence
- * File Path: USER_DESKTOP, WLC9800-Posture-Demo.txt
- * File Operator: Exists

Bestandsvoorwaarde maken

Stap 9. Maak herstelbewerkingen Navigeren naar werkcenters> Houding> Beleidselementen> Herstelingen > Bestand > Toevoegen:

The screenshot shows the Cisco ISE Policy Elements configuration page for a File Remediation. The left sidebar lists various remediations, with 'Remediations' selected. The main area shows the configuration for 'WLC9800-Posture-Demo'. The following fields are highlighted with red boxes:

- * 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

Bestandsherstel maken

Stap 10. Vereiste aanmaken. Navigeren naar werkcentra> Positie> Beleidselementen> Vereisten>

Nieuwe eis invoegen:

Overview

Network Devices

Client Provisioning

Policy Elements

Posture Policy

Policy Sets

Troubleshoot

Reports

Settings

Conditions

Remediations

Requirements

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.

Posture-vereiste maken

Stap 11. Maak een posteriebeleid aan. Navigeren naar werkcentra> Houding> Nieuwe policy invoegen:

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
☒	Policy Options	WLC9800-Posture-Demo	if Any	and Windows All	and Any version	and Agent	and	then WLC9800-Posture-Demo Edit

Posturebeleid maken

Stap 12. Maak drie autorisatieprofielen: Posterstatus is onbekend; de status van de houding niet-conform is; Posterstatus is conform. Navigeer naar Beleid> Beleidselementen> Resultaten> Verificatie> Vergunningsprofielen> Toevoegen:

DictionariesConditionsResults

AuthenticationAllowed Protocols

AuthorizationAuthorization ProfilesDownloadable ACLs

Profiling

Posture

Client Provisioning

Standard Authorization Profiles

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

EditAddDuplicateDelete

☐	Name	Profile	Description
☐	WLC9800	X	
☐	WLC9800-Posture-Compliant	Cisco ⓘ	
☐	WLC9800-Posture-NonCompliant	Cisco ⓘ	
☐	WLC9800-Posure-Unknown	Cisco ⓘ	

Autorisatieprofielen maken 10

DictionariesConditionsResults

AuthenticationAllowed Protocols

AuthorizationAuthorization ProfilesDownloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > WLC9800-Posure-Unknown

Authorization Profile

* NameWLC9800-Posure-Unknown

Description

* Access TypeACCESS_ACCEPT

Network Device ProfileCisco ⓘ

Service Template☐

Track Movement☐ ⓘ

Agentless Posture☐ ⓘ

Passive Identity Tracking☐ ⓘ

Common Tasks

☐ Voice Domain Permission

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

Client Provisioning (Posture)ACLPOSTURE_REDIRECT_ACLValueClient Provisioning Portal (def: ⓘ

☐ Static IP/Host name/FQDN

☐ Suppress Profiler CoA for endpoints in Logical Profile

Autorisatieprofielen maken 02

Dictionary

Conditions

Authentication

Allowed Protocols

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Results

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)

Airspace ACL Name

POSTURE_COMPLIANT_ACL

Airspace IPv6 ACL Name

Autorisatieprofielen maken 30

Dictionary

Conditions

Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

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

☐ Airespace IPv6 ACL Name

Advanced Attributes Settings

Stap 13. Maak beleidssets aan. Navigeren naar beleid> Beleid

Policy Sets

Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	WLC9800-Posture-Demo		AND Network Access-Device IP Address EQUALS 10.124.60.41 Normalised Radius-SSID CONTAINS posture_demo	Default Network Access	0	⚙️ ➡️	
●	Default	Default policy set		Default Network Access	0	⚙️ ➡️	

Reset Save

Beleidssets maken

Sets> Pictogram toevoegen:

Stap 14. Verificatiebeleid maken Navigeer naar beleid> Beleidssets> Uitvouwen "WLC9800-Posture-Demo"> Verificatiebeleid> Toevoegen:

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	0	⚙️ ➡️
---	----------------------	-----	---	------------------------	---	-------

Authentication Policy (2)

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

Verificatiebeleid maken

Stap 15. Autorisatiebeleid maken Navigeren naar beleid> Beleidssets> Uitvouwen "WLC9800-Posture-Demo"> Autorisatiebeleid> Toevoegen:

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	⚙️ ➡️
●	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	⚙️ ➡️

Autorisatiebeleid maken

Voorbeelden

1. Verbonden test SSID posture_demo met juiste 802.1X referenties.



posture_demo
Secured

Enter your user name and password

wlc9800-user

••••••••



OK

Cancel

Network & Internet settings

Change settings, such as making a connection metered.

- Als de browser is omgeleid naar de ISE portal URL maar de pagina niet kan worden geladen, controleer of de ISE domeinnaam niet is toegevoegd aan de DNS server, vandaar dat de client de portal URL niet kan oplossen. Om dit probleem snel op te lossen, controleert u de statische IP/hostnaam/FQDN onder het autorisatieprofiel om het IP-adres in een doorverwijzing naar URL op te geven. Dit kan echter een veiligheidsprobleem zijn, omdat het het IP-adres van de ISE aan het licht brengt.

▼ 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				

Debugs verzamelen

[Debugs inschakelen op C9800](#)

[Debugs inschakelen op ISE](#)

Referenties

- [CWA op Catalyst 9800 WLC en ISE configureren - Cisco](#)
- [Draadloze BYOD met Identity Services Engine](#)
- [ISE-houding implementeren](#)
- [Probleemoplossing voor ISE-sessiebeheer en -houding](#)
- [Vergelijken ISE-poortomleidingsstroom naar ISE-poortomleidingsloze stroom](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.