

Konfigurieren des Status auf Catalyst 9800 WLC und ISE

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[AAA-Konfiguration auf dem 9800 WLC](#)

[WLAN-Konfiguration](#)

[Richtlinienprofilkonfiguration](#)

[Richtlinien-Tag-Konfiguration](#)

[Richtlinien-Tag-Zuweisung](#)

[Umleiten der ACL-Konfiguration](#)

[Richtlinien-ACL-Konfiguration](#)

[AAA-Konfiguration und Statureinstellung auf der ISE](#)

[Beispiele](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Checkliste](#)

[Debuggen sammeln](#)

[Referenzen](#)

Einleitung

Dieses Dokument beschreibt die Konfiguration eines Status-WLAN auf einem Catalyst 9800 WLC und der ISE über die grafische Benutzeroberfläche (Graphic User Interface, GUI).

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- 9800 WLC - allgemeine Konfiguration
- ISE-Richtlinien- und Profilkonfiguration

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

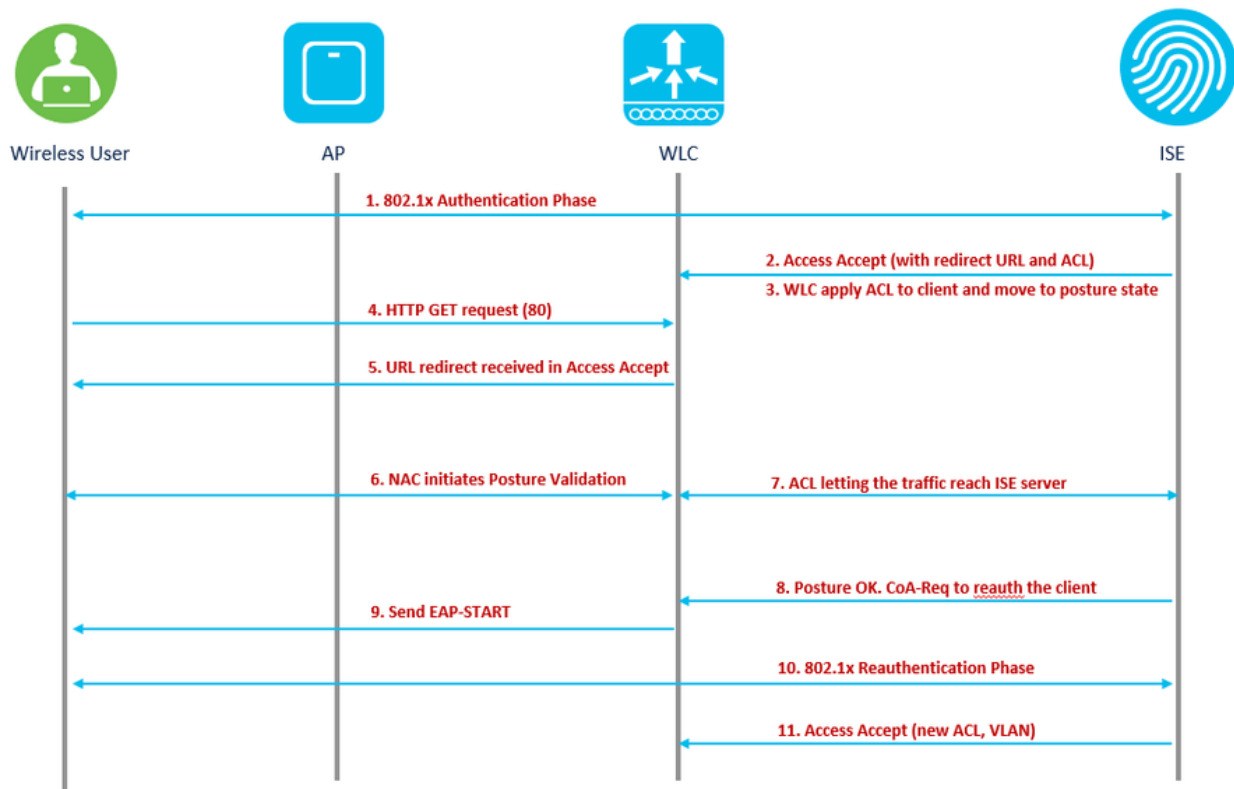
Wireless LAN Controller - RADIUS NAC- und CoA-Funktionsablauf

1. Der Client authentifiziert sich mithilfe der 802.1x-Authentifizierung.
2. RADIUS Access Accept beinhaltet die umgeleitete URL für Port 80 und vorab erstellte ACLs, die das Zulassen von IP-Adressen und Ports oder das Quarantäne-VLAN umfasst.
3. Der Client wird auf die unter "access accept" angegebene URL umgeleitet und in einen neuen Zustand versetzt, bis die Statusüberprüfung abgeschlossen ist. Der Client kommuniziert in diesem Zustand mit dem ISE-Server und überprüft sich anhand der auf dem ISE NAC-Server konfigurierten Richtlinien.
4. NAC-Agent auf Client initiiert Statusüberprüfung (Datenverkehr zu Port 80): Der Agent sendet eine HTTP-Erkennungsanforderung an Port 80, die der Controller an die im Zugriffs-Accept angegebene URL umleitet. Die ISE weiß, dass der Client die Verbindung herstellen will und direkt auf den Client reagiert. Auf diese Weise erfährt der Client die IP-Adresse des ISE-Servers und kommuniziert von nun an direkt mit dem ISE-Server.
5. WLC lässt diesen Datenverkehr zu, da die ACL so konfiguriert ist, dass dieser Datenverkehr zugelassen wird. Bei einer VLAN-Übersteuerung wird der Datenverkehr überbrückt, sodass er den ISE-Server erreicht.
6. Nach Abschluss der Bewertung durch den ISE-Client wird ein RADIUS-CoA-Req. mit Büroth-Service an den WLC gesendet. Dadurch wird eine erneute Authentifizierung des Clients (durch Senden von EAP-START) initiiert. Sobald die erneute Authentifizierung erfolgreich ist, sendet die ISE eine Zugriffsbestätigung mit einer neuen ACL (falls vorhanden), ohne URL-Umleitung oder Zugriffs-VLAN.
7. WLC unterstützt CoA-Req und Disconnect-Req gemäß RFC 3576. Der WLC muss die CoA-Anforderung für den Authentifizierungsdienst gemäß RFC 5176 unterstützen.
8. Statt herunterladbarer ACLs werden auf dem WLC vorkonfigurierte ACLs verwendet. Der ISE-

Server sendet nur den ACL-Namen, der bereits im Controller konfiguriert ist.

9. Dieses Design eignet sich sowohl für VLAN- als auch für ACL-Gehäuse. Im Fall einer VLAN-Übersteuerung leiten wir nur Port 80 um, der umgeleitet wird und den restlichen Verkehr (Bridge) auf das Quarantäne-VLAN überträgt. Auf die ACL wird die im Accept-Modus vor der Authentifizierung empfangene ACL angewendet.

Diese Abbildung zeigt den Funktionsablauf in visueller Darstellung:



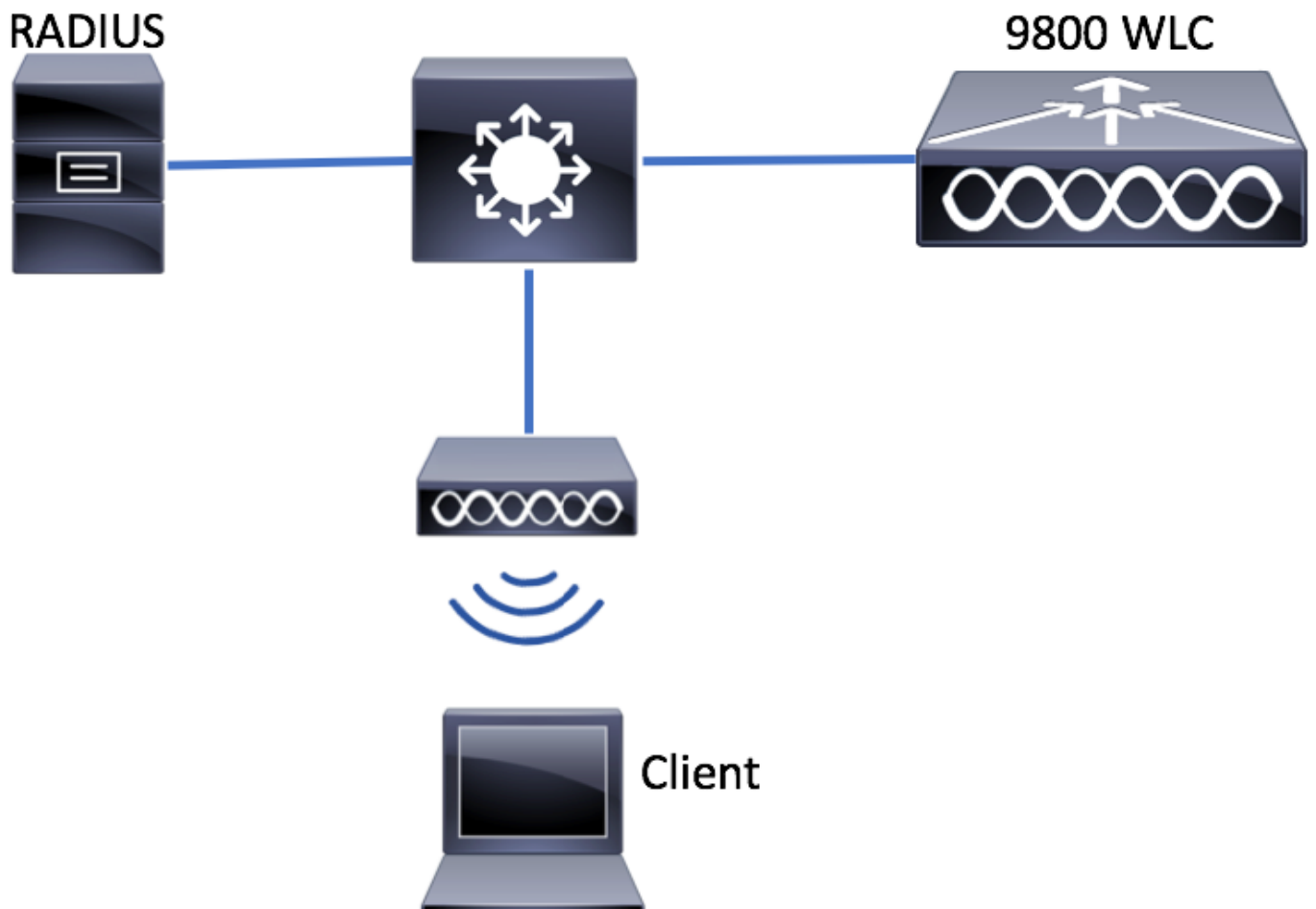
Feature-Workflow

In diesem Anwendungsfall wird eine SSID, die nur für Unternehmensbenutzer verwendet wird, für den Status aktiviert. Andere Anwendungsfälle wie BYOD, Guest oder andere sind für diese SSID nicht verfügbar.

Wenn ein Wireless-Client zum ersten Mal eine Verbindung mit der Posture-SSID herstellt, muss er das Posture-Modul auf das umgeleitete Portal der ISE herunterladen und installieren und schließlich mit den relevanten ACLs basierend auf dem Ergebnis der Statusprüfung (konform/nicht konform) anwenden.

Konfigurieren

Netzwerkdiagramm



Netzwerkdiagramm

AAA-Konfiguration auf dem 9800 WLC

Schritt 1: Fügen Sie den ISE-Server der 9800 WLC-Konfiguration hinzu. Navigieren Sie zu Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add, und geben Sie die RADIUS-Serverinformationen wie in den Bildern dargestellt ein. Stellen Sie sicher, dass die Unterstützung für CoA für den Status-NAC aktiviert ist.

Search Menu Items

- 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 Radius-Server erstellen

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 ☒ ENABLED

CoA Server Key Type Clear Text

CoA Server Key

Confirm CoA Server Key

Automate Tester ☐

Cancel Apply to Device

9800 Radius-Details erstellen

Schritt 2: Erstellen Sie eine Liste der Authentifizierungsmethoden. Navigieren Sie zu Configuration > Security > AAA > AAA Method List > Authentication > + Add, wie im Bild dargestellt:

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 - Authentifizierungsliste hinzufügen

Quick Setup: AAA Authentication

Method List Name*

Type* ⓘ

Group Type ⓘ

Fallback to local ☐

Available Server Groups

ldap
tacacs+

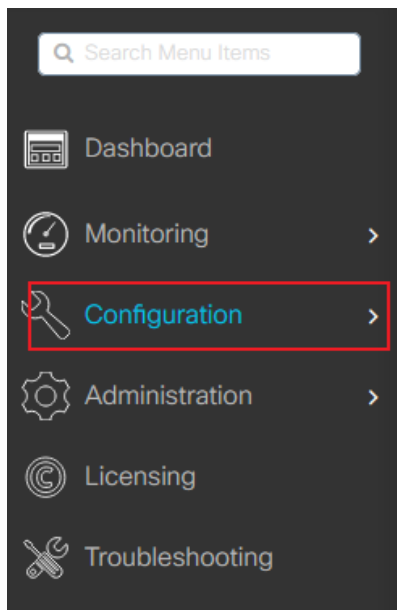
Assigned Server Groups

radius

Cancel Apply to Device

9800 - Authentifizierungslistendetails erstellen

Schritt 3. (Optional) Erstellen Sie eine Abrechnungsmethodenliste, wie in der Abbildung dargestellt:



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 Kundenliste hinzufügen

Quick Setup: AAA Accounting

Method List Name*

POSTUREacct

Type*

identity

Available Server Groups

Assigned Server Groups

ldap
tacacs+

radius

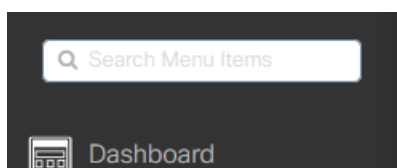
Cancel

Apply to Device

9800 Kundenlistendetails erstellen

WLAN-Konfiguration

Schritt 1: Erstellen Sie das WLAN. Navigieren Sie zu Configuration > Tags & Profiles > WLANs > + Add, und konfigurieren Sie das Netzwerk nach Bedarf:



Configuration > Tags & Profiles > WLANs

+ Add

× Delete

Clone

Enable WLAN

Disable WLAN

9800 WLAN hinzufügen

Schritt 2: Geben Sie die allgemeinen WLAN-Informationen ein.

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 WLAN erstellen allgemein

Schritt 3: Navigieren Sie zur Registerkarte Sicherheit, und wählen Sie die gewünschte Sicherheitsmethode aus. Wählen Sie in diesem Fall "802.1x" aus, und die AAA-Authentifizierungsliste (die Sie in Schritt 2 im Abschnitt zur AAA-Konfiguration erstellt haben) wird benötigt:

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 erstellen WLAN-Sicherheit 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 erstellt WLAN-Sicherheit AAA

Richtlinienprofilkonfiguration

In einem Richtlinienprofil können Sie den Clients neben anderen Einstellungen (wie Zugriffskontrolllisten (ACLs), Quality of Service (QoS), Mobility Anchor, Timer usw.) festlegen, welchem VLAN sie zugewiesen werden sollen. Sie können entweder Ihr Standardrichtlinienprofil verwenden oder ein neues erstellen.

Schritt 1: Erstellen eines neuen Richtlinienprofils. Navigieren Sie zu Configuration > Tags & Profiles > Policy, und erstellen Sie eine neue:

Q Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Configuration > Tags & Profiles > Policy

+ Add

× Delete

Clone

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

1

10

9800 Richtlinienprofil hinzufügen

Stellen Sie sicher, dass das Profil aktiviert ist.

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

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

2-65519

WLAN Switching Policy

Central Switching

ENABLED

Central Authentication

ENABLED

Central DHCP

ENABLED

Flex NAT/PAT

DISABLED

9800 Richtlinienprofil erstellen (allgemein)

Schritt 2: Wählen Sie das VLAN aus. Navigieren Sie zur Registerkarte Access Policies (Zugriffsrichtlinien), und wählen Sie den VLAN-Namen aus dem Dropdown-Menü aus, oder geben Sie die VLAN-ID manuell ein. Konfigurieren Sie keine ACL im Richtlinienprofil:

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 erstellt Richtlinienprofil-VLAN

Schritt 3: Konfigurieren Sie das Richtlinienprofil so, dass ISE-Außerkraftsetzungen (AAA-Außerkraftsetzung zulassen) und Autorisierungsänderung (CoA) (NAC-Status) akzeptiert werden. Sie können optional auch eine Abrechnungsmethode angeben:

⚠ 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

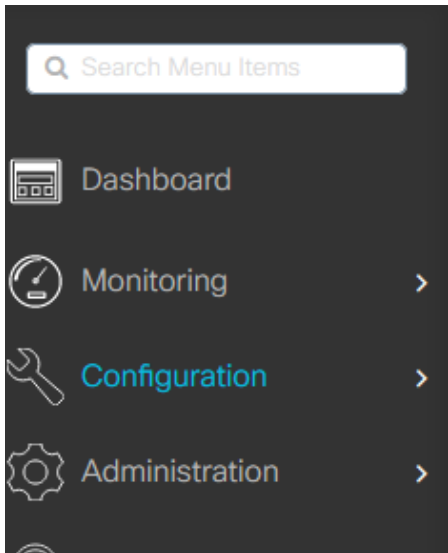
Advanced**WLAN Timeout**Session Timeout (sec) ⓘIdle Timeout (sec) Idle Threshold (bytes) Client Exclusion Timeout (sec) ☐ Guest LAN Session Timeout ☐**DHCP**IPv4 DHCP Required ☒DHCP Server IP Address [Show more >>>](#)**AAA Policy**Allow AAA Override ☒NAC State ☒Policy Name ⓘAccounting List ⓘ**WGB Parameters**Fabric 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 Richtlinienprofil erstellen Erweitert

Richtlinien-Tag-Konfiguration

Sie verbinden Ihre SSID innerhalb des Richtlinien-Tags mit Ihrem Richtlinienprofil. Sie können entweder ein neues Richtlinien-Tag erstellen oder das Standard-Richtlinien-Tag verwenden.

Navigieren Sie zu Configuration > Tags & Profiles > Tags > Policy, und fügen Sie bei Bedarf eine neue hinzu, wie im Bild gezeigt:



Configuration > Tags & Profiles > Tags

Policy

Site

RF

AP

+ Add

× Delete

Clone

Policy Tag Name

default-policy-tag

1

10

9800 policy tag add

Verknüpfen Sie Ihr WLAN-Profil mit dem gewünschten Richtlinienprofil:

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

Details zu 9800-Richtlinien-Tags

Richtlinien-Tag-Zuweisung

Weisen Sie den erforderlichen APs das Richtlinien-Tag zu. Navigieren Sie zu Configuration > Wireless > Access Points > AP Name > General Tags, nehmen Sie die erforderliche Zuweisung vor, und klicken Sie dann auf Update & Apply to Device .

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

Umleiten der ACL-Konfiguration

Die für die Posture Portal Redirect verwendete ACL erfüllt dieselben Anforderungen wie die CWA (Central Web Authentication).

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

ACL-Details für 9800-Umleitung

Richtlinien-ACL-Konfiguration

In diesem Fall müssen Sie separate ACLs für den 9800 WLC für die ISE definieren, um die konformen und nicht konformen Szenarien basierend auf dem Ergebnis der Port-Prüfung zu autorisieren.

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 allgemein

Verwenden Sie in diesem Fall einfach permit all (Alle zulassen). Eine weitere gängige Konfiguration besteht darin, dass die ISE keine ACL im konformen Ergebnis autorisiert. Dies entspricht der Erlaubnis aller ACLs auf der 9800-Seite:

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

X 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-konform

Bei einem nicht konformen Szenario erlaubt der Client nur Zugriff auf bestimmte Netzwerke, in der Regel den Behebungsserver (in diesem Fall die ISE selbst):

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

X 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 - nicht konform

AAA-Konfiguration und Statuseinstellung auf der ISE

Statusanforderung: In diesem Beispiel besteht die Anforderung zum Ermitteln der Konformität darin, zu ermitteln, ob auf dem Desktop, auf dem Windows-PC getestet wird, eine bestimmte Testdatei vorhanden ist.

Schritt 1: Hinzufügen des WLC 9800 als NAD auf der ISE Navigieren Sie zu Administration > Network Resources > Network Devices > Add:

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Cisco ISE' and 'Administration - Network Resources'. The main menu on the left has 'Network Devices' selected. The breadcrumb trail is 'Network Devices List > WLC9800'. The 'Network Devices' form is displayed with the following fields:

- Name: WLC9800
- Description: (empty)
- IP Address: 10.124.60.41 / 32
- Device Profile: Cisco
- Model Name: (empty)
- Software Version: (empty)
- Network Device Group: (empty)
- Location: All Locations (Set To Default)
- IPSEC: No (Set To Default)
- Device Type: All Device Types (Set To Default)

Netzwerkgerät hinzufügen 01

The screenshot shows the Cisco ISE Administration console with the 'RADIUS Authentication Settings' form. The breadcrumb trail is 'Network Devices List > WLC9800 > RADIUS Authentication Settings'. The form is divided into two sections:

- RADIUS UDP Settings**
 - Protocol: RADIUS
 - Shared Secret: (masked with dots) (Show)
 - ☐ Use Second Shared Secret (Info)
 - Second Shared Secret: (empty) (Show)
 - CoA Port: 1700 (Set To Default)
- RADIUS DTLS Settings** (Info)
 - ☐ DTLS Required (Info)
 - Shared Secret: radius/dtls (Info)
 - CoA Port: 2083 (Set To Default)
 - Issuer CA of ISE Certificates for CoA: Select if required (optional) (Info)
 - DNS Name: (empty)

Netzwerkgerät hinzufügen 02

Schritt 2: Laden Sie das Cisco Secure Client Headend-Bereitstellungspaket und das Compliance-Modul auf die Cisco Software CCO-Website herunter.

Zugriff auf und Suche nach 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](#) 

Sicherer 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-Modul 4.3

Schritt 3: Laden Sie das Cisco Secure Client Headend-Bereitstellungspaket und das Compliance-Modulpaket in ISE Client Provisioning hoch. Navigieren Sie zu Work Centers> Status> Client Provisioning> Resources . Klicken Sie auf Add, wählen Sie Agent-Ressourcen von der lokalen Festplatte aus dem Dropdown-Feld:

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

Sicheren Client hochladen

Cisco ISE

Work Centers - Posture

OverviewNetwork DevicesClient ProvisioningPolicy ElementsPosture PolicyPolicy SetsTroubleshootReportsSettings

Client Provisioning Policy

Resources

Client Provisioning Portal

Selected 0Total 13

Quick Filter

☐	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 ...

Hochladen des sicheren Clients und des Compliance-Moduls erfolgreich

Schritt 4: Erstellen eines Agentenstatusprofils Navigieren Sie zu Work Centers> Posture> Client Provisioning> Resources> Add> Agent Posture Profile:

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.																														

Agentenstatusprofil

Schritt 5: Agentenkonfiguration erstellen Navigieren Sie zu Work Centers > Status > Client-Bereitstellung > Ressourcen > Hinzufügen > Agentenkonfiguration:

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

Agent-Konfiguration hinzufügen

Schritt 6. Bestätigen Sie das Client-Bereitstellungsportal, verwenden Sie das Standardportal für Tests ist OK. (Generieren Sie CSR und beantragen Sie ein SSL-Zertifikat vom CA-Server, und ersetzen Sie das Zertifikatgruppen-Tag in diesem Portal Einstellungen. Andernfalls tritt während des Testprozesses eine nicht vertrauenswürdige Warnung für das Zertifikat auf.)

Navigieren Sie zu Work Centers> Status> 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

Client-Bereitstellungsportal 01 auswählen

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](#)

Client-Bereitstellungsportal 02 auswählen

Schritt 7: Erstellen einer Client-Bereitstellungsrichtlinie Navigieren Sie zu Work Centers > Status > 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
WLC9800-Windows	If Any	and Windows All	and Condition(s)	then 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

Client-Bereitstellungsrichtlinie erstellen

Schritt 8: Erstellen von Dateibedingungen Navigieren Sie zu Work Centers> Status> 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

Dateibedingung erstellen

Schritt 9: Korrekturen erstellen Navigieren Sie zu Work Centers > Status > 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

Dateibereinigung erstellen

Schritt 10: Anforderung erstellen. Navigieren Sie zu Work Centers> Status> 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	Any_AM_Installation_Mac_temporal
Anti-Spyware	Anti-Virus	Default_AppVis_Requirement_Win_temporal
File	Firewall	Default_AppVis_Requirement_Mac_temporal
Launch Program	Link	Default_Hardware_Attributes_Requirement_Win_temporal
Patch Management	Script	Default_Hardware_Attributes_Requirement_Mac_temporal
USB	Windows Server Update Servi...	Default_Firewall_Requirement_Win_temporal
Windows Update		Default_Firewall_Requirement_Mac_temporal
		WLC9800-Posture-Demo

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.

Statusanforderung erstellen

Schritt 11: Erstellen einer Statusrichtlinie Navigieren Sie zu Work Centers > Posture > Insert new policy:

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.

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	WLC9800-Posture-Demo Edit

Statusrichtlinie erstellen

Schritt 12: Erstellen Sie drei Autorisierungsprofile: Der Status lautet "Unbekannt". Der Status "Status" ist "Nicht konform". Der Statusstatus ist "Konformität". Navigieren Sie zu Richtlinie > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofile> Hinzufügen:

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		
☐	WLC9800-Posture-Compliant	Cisco	
☐	WLC9800-Posture-NonCompliant	Cisco	
☐	WLC9800-Posure-Unknown	Cisco	

Autorisierungsprofile erstellen 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/Host name/FQDN

☐ Suppress Profiler CoA for endpoints in Logical Profile

Erstellen von Autorisierungsprofilen 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

Erstellen von Autorisierungsprofilen 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

Schritt 13: Erstellen von PolicySets Navigieren Sie zu Richtlinie > Richtlinie.

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

Policy Sets erstellen

Sets> Symbol hinzufügen:

Schritt 14: Erstellen einer Authentifizierungsrichtlinie Navigieren Sie zu Richtlinie> Richtliniensätze> Erweitern Sie "WLC9800-Posture-Demo"> Authentifizierungsrichtlinie> Hinzufügen:

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

Authentifizierungsrichtlinie erstellen

Schritt 15: Autorisierungsrichtlinie erstellen Navigieren Sie zu Richtlinie> Richtlinienansätze> Erweitern Sie "WLC9800-Posture-Demo"> Autorisierungsrichtlinie> Hinzufügen:

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		

Autorisierungsrichtlinie erstellen

Beispiele

1. Verbundener Test-SSID stature_demo mit korrekten 802.1X-Anmeldedaten.



posture_demo
Secured

Enter your user name and password

wlc9800-user

••••••••



OK

Cancel

Network & Internet settings

Change settings, such as making a connection metered.

- Stellen Sie sicher, dass der WLC die richtige Umleitungs-URL und ACL von der ISE erhält. Sie können es über die GUI überprüfen:

Monitoring > **Wireless** > **Clients**

Clients Sleeping Clients Excluded Clients

< Delete Refresh

Selected 0 out of 1 Clients

☐	Client MAC Address	IPV4 Address	IPV6 Address	AP Name	SSID
☒	1826.49b1.c718	10.124.60.36	fe80::8194ed90:2ca8:3f8	AP_WALL_20	postu...

« ‹ 1 › » 10 ▾

Client

360 View **General** QOS Statistics ATF Statistics Mobility History Call Statistics

Client Properties AP Properties **Security Information** Client Statistics QOS Properties EoGRE

Common Session ID	00000000000000B15A140E0D
Acct Session ID	0x00000001
Auth Method Status List	
Method	Dot1x
SM State	AUTHENTICATED
SM Bend State	IDLE

Local Policies

Service Template	wlan_svc_posture_demo_gp_local (priority 254)
VLAN	VLAN1072
Absolute Timer	1800

Server Policies

URL Redirect ACL	POSTURE_REDIRECT_ACL
URL Redirect	https://demo-isr.local.bn:8443/portal/gateway?sessionid=0000000000000000B15A140ED&portal=e2b33062-b8d1-467b-b26f-8bd22bba10e7&action=cpp&token=797ecfa139e01bab3a4bb4f9eccf61a7

Resultant Policies

URL Redirect ACL	POSTURE_REDIRECT_ACL
URL Redirect	https://demo-isr.local.bn:8443/portal/gateway?sessionid=0000000000000000B15A140ED&portal=e2b33062-b8d1-467b-b26f-8bd22bba10e7&action=cpp&token=797ecfa139e01bab3a4bb4f9eccf61a7
VLAN Name	VLAN1072
VLAN	1072
Absolute Timer	1800
DNS Snooped IPv4 Addresses	None
DNS Snooped IPv6 Addresses	None

- Wenn die Umleitung nicht automatisch erfolgt, öffnen Sie einen Browser, und versuchen Sie eine zufällige IP-Adresse. Beispiel: 10.0.0.1. Wenn die Umleitung funktioniert, liegt möglicherweise ein DNS-Auflösungsproblem vor. Stellen Sie sicher, dass Sie über DHCP einen gültigen DNS-Server bereitgestellt haben und dass dieser Hostnamen auflösen kann.
- Wenn der Browser zur ISE-Portal-URL umgeleitet wurde, die Seite jedoch nicht geladen werden kann, überprüfen Sie, ob der ISE-Domänenname nicht zum DNS-Server hinzugefügt wurde. Der Client kann die Portal-URL daher nicht auflösen. Um dieses Problem schnell zu beheben, markieren Sie die Option Static IP/Host name/FQDN (Statischer IP-/Hostname/FQDN) unter dem Autorisierungsprofil, um die IP-Adresse in der Umleitungs-URL anzugeben. Dies kann jedoch ein Sicherheitsrisiko darstellen, da die IP-Adresse der ISE offen gelegt wird.

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

Debuggen sammeln

Aktivieren von Debuggen auf C9800

[Debuggen auf ISE aktivieren](#)

Referenzen

- [Konfigurieren von CWA auf Catalyst 9800 WLC und ISE - Cisco](#)
- [Wireless BYOD mit Identity Services Engine](#)
- [ISE-Status bereitstellen](#)
- [Fehlerbehebung bei ISE-Sitzungsmanagement und Status](#)
- [ISE-Statusumleitungsfluss mit ISE-Statusumleitungslosem Fluss vergleichen](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.