

在Catalyst 9800 WLC和ISE上配置终端安全评估

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[网络图](#)

[9800 WLC 上的 AAA 配置](#)

[WLAN 配置](#)

[策略配置文件配置](#)

[策略标签配置](#)

[策略标签分配](#)

[重定向 ACL 配置](#)

[策略ACL配置](#)

[ISE上的AAA配置和状态设置](#)

[Examples](#)

[验证](#)

[故障排除](#)

[核对清单](#)

[收集调试](#)

[参考](#)

简介

本文档介绍如何通过图形用户界面(GUI)在Catalyst 9800 WLC和ISE上配置终端安全评估WLAN。

先决条件

要求

Cisco 建议您了解以下主题：

- 9800 WLC常规配置
- ISE策略和配置文件配置

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 9800 WLC Cisco IOS® XE Cupertino v17.9.5
- 身份服务引擎(ISE)v3.2
- 笔记本电脑Windows 10企业版

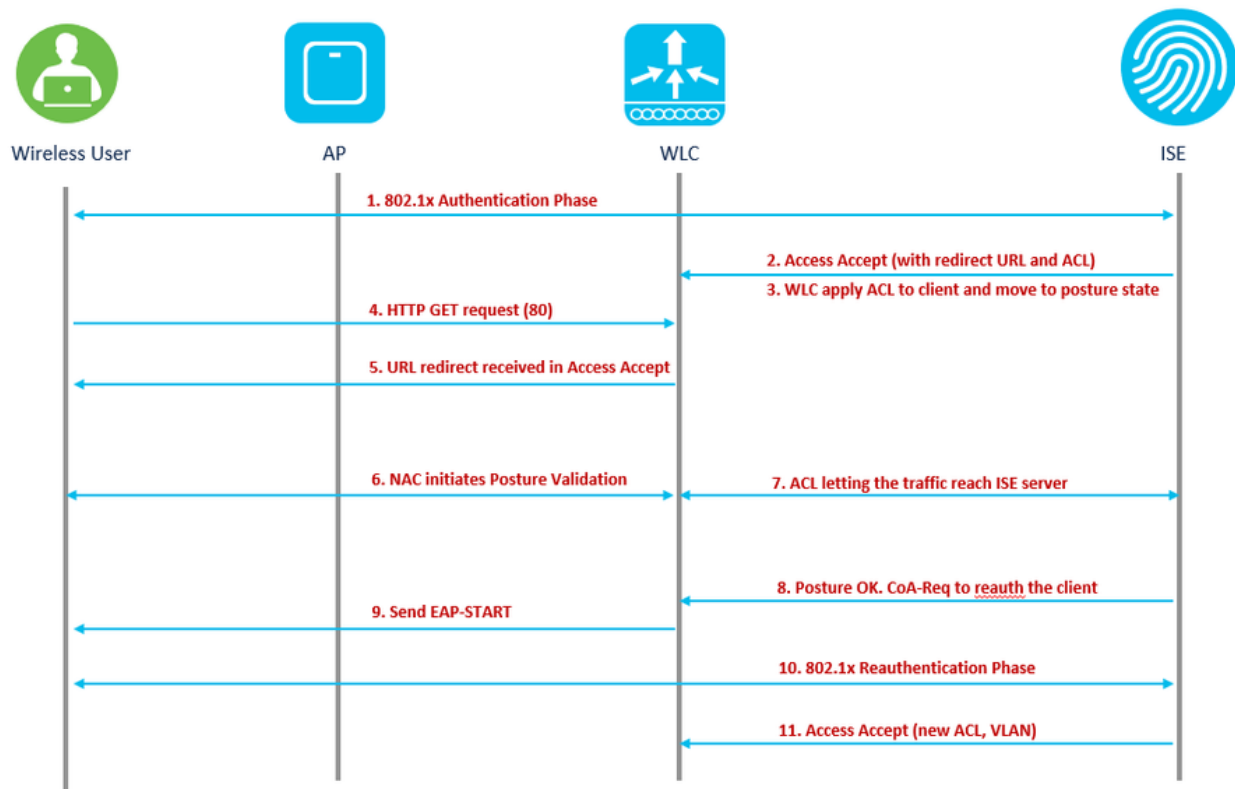
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

无线LAN控制器RADIUS NAC和CoA功能流

- 1.客户端使用dot1x身份验证进行身份验证。
2. RADIUS Access Accept传输端口80的重定向URL和包括允许IP地址和端口或隔离VLAN的预身份验证ACL。
- 3.客户端被重定向到access accept中提供的URL，并进入新状态，直到完成状态验证。处于此状态的客户端与ISE服务器通信，并根据ISE NAC服务器上配置的策略验证自身。
- 4.客户端上的NAC代理启动状态验证（流向端口80的流量）：代理将HTTP发现请求发送到端口80，控制器会重定向到访问接受中提供的URL。ISE知道客户端尝试访问并直接响应客户端。这样，客户端即可了解ISE服务器IP，从现在起，客户端将直接与ISE服务器进行通信。
5. WLC允许此流量，因为ACL配置为允许此流量。如果发生VLAN覆盖，流量会桥接以便到达ISE服务器。
- 6.当ISE客户端完成评估后，RADIUS CoA-Req with reauth service将发送到WLC。这将启动客户端的重新身份验证（通过发送EAP-START）。重新身份验证成功后，ISE会发送包含新ACL（如果有）和无URL重定向或访问VLAN的访问接受。
- 7.根据RFC 3576,WLC支持CoA-Req和Disconnect-Req。根据RFC 5176,WLC需要支持重新身份验证服务的CoA-Req。
- 8.在WLC上使用预配置的ACL，而不是可下载的ACL。ISE服务器仅发送ACL名称，该名称已在控制器中配置。
- 9.此设计适用于VLAN和ACL两种情况。如果发生VLAN覆盖，我们只需重定向端口80，并允许（桥接）隔离VLAN上的其余流量。对于ACL，应用访问接受中收到的预身份验证ACL。

此图直观地显示了此功能流：



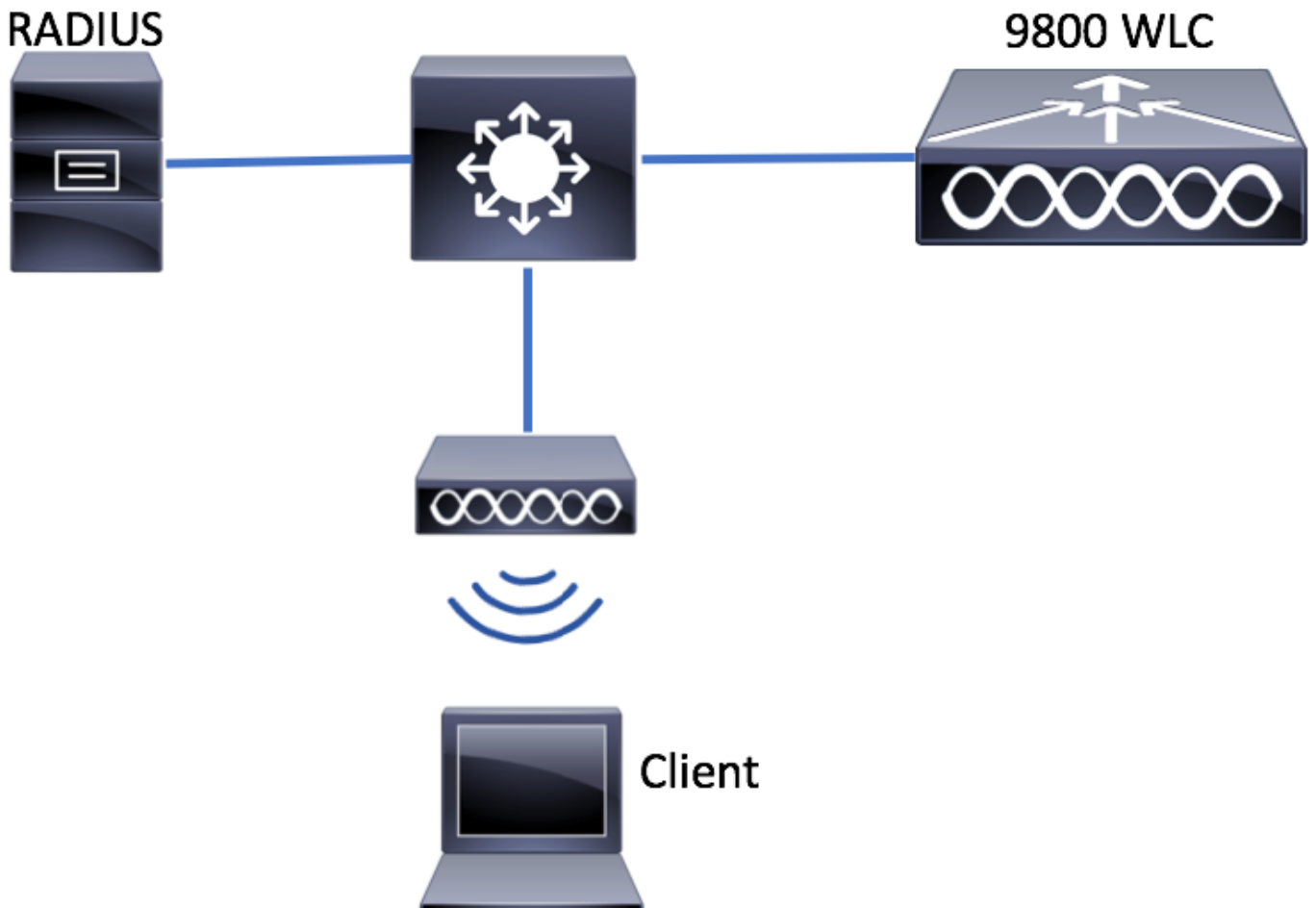
功能工作流程

对于此使用案例，仅用于企业用户的SSID将启用安全评估。此SSID上不存在其他使用案例，例如BYOD、访客或任何其他使用案例。

当无线客户端首次连接到终端安全评估SSID时，它必须下载终端安全评估模块并将其安装在ISE的重定向门户上，最后根据终端安全评估检查结果（兼容/不兼容）应用相关ACL。

配置

网络图



网络图

9800 WLC 上的 AAA 配置

步骤1.将ISE服务器添加到9800 WLC配置。导航到Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add并输入RADIUS服务器信息，如图所示。确保为状态NAC启用对CoA的支持。

The screenshot shows the Cisco ISE configuration interface. The left sidebar contains a search bar and a menu with the following items: Dashboard, Monitoring, Configuration (highlighted), Administration, Licensing, and Troubleshooting. The main content area shows the navigation path: Configuration > Security > AAA. Below this, there are tabs for Servers / Groups (highlighted), AAA Method List, and AAA Advanced. Under the Servers / Groups tab, there are buttons for + Add and × Delete. Below these buttons, there are two tabs: RADIUS (highlighted) and TACACS+. Under the RADIUS tab, there are two sub-tabs: Servers (highlighted) and Server Groups. The Servers sub-tab shows a table with columns for Name and Address. The table is currently empty, and there is a pagination bar at the bottom showing 0 items per page.

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创建radius详细信息

步骤2.创建身份验证方法列表。导航到Configuration > Security > AAA > AAA Method List > Authentication > + Add，如图所示：

Cisco Catalyst 9800-CL Wireless Controller

17.9.5

Welcome sis/

Last login 04/09/2024

Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Licensing

Troubleshooting

Walk Me Through

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

9800添加身份验证列表

Quick Setup: AAA Authentication



Method List Name*

posture-authn-list

Type*

dot1x



Group Type

group



Fallback to local

☐

Available Server Groups

ldap
tacacs+



Assigned Server Groups

radius



Cancel

Apply to Device

9800创建身份验证列表详细信息

步骤3. (可选) 创建记账方法列表，如图所示：

The screenshot shows the AAA Configuration interface. On the left is a sidebar with a search bar and menu items: Dashboard, Monitoring, Configuration (highlighted with a red box), Administration, Licensing, and Troubleshooting. The main area has a breadcrumb trail: Configuration > Security > AAA, followed by a 'Show Me How' button. Below this is a '+ AAA Wizard' button. A tab bar at the top of the main area contains 'Servers / Groups', 'AAA Method List' (highlighted with a red box), and 'AAA Advanced'. Under the 'AAA Method List' tab, there are sections for 'Authentication' and 'Authorization'. Under 'Authorization', the 'Accounting' section is highlighted with a red box. A modal window is open over the 'Accounting' section, showing '+ Add' and '× Delete' buttons. Below these buttons is a table with columns 'Name' and 'Type'. The table has one row with the value '0' in the 'Name' column. At the bottom of the modal, there are navigation arrows and a page number '0' out of '10'.

9800添加帐户列表

Quick Setup: AAA Accounting



Method List Name*

POSTUREacct

Type*

identity



Available Server Groups

Assigned Server Groups

ldap
tacacs+



radius



Cancel

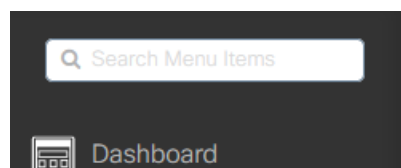


Apply to Device

9800创建客户列表详细信息

WLAN 配置

第 1 步：创建 WLAN.导航到Configuration > Tags & Profiles > WLANs > + Add并根据需要配置网络：



Configuration > Tags & Profiles > **WLANs**



Add



Delete



Clone

Enable WLAN

Disable WLAN

9800 WLAN添加

步骤2.输入WLAN一般信息。

Add WLAN

GeneralSecurityAdvanced

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创建WLAN常规

步骤3.导航到安全选项卡并选择所需的安全方法。在这种情况下，请选择“802.1x”，并且需要AAA身份验证列表(在AAA配置部分中的步骤2中创建):

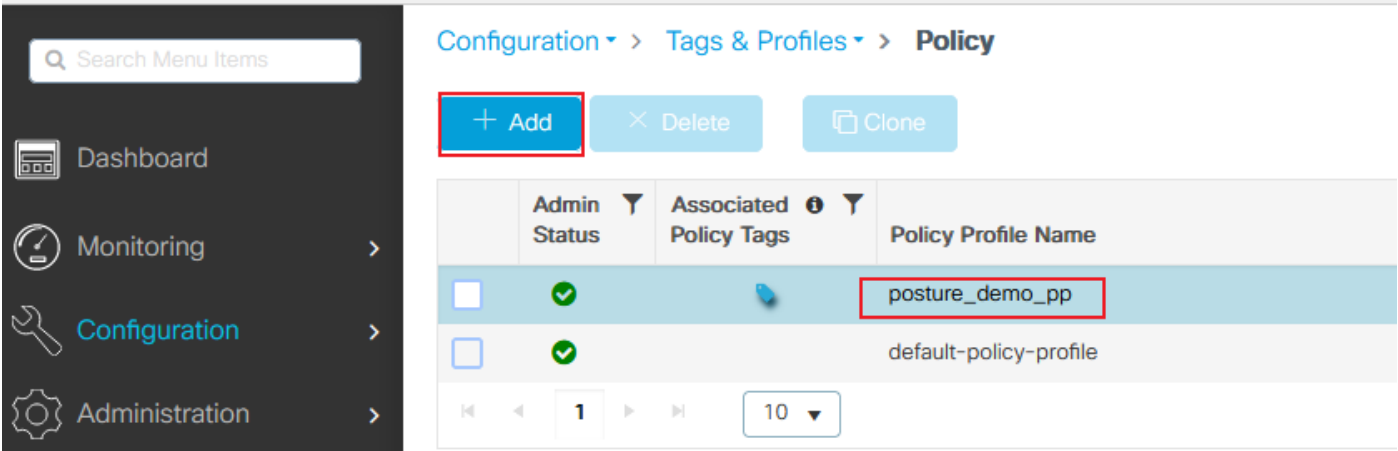
 Apply to Device

Edit WLAN

策略配置文件配置

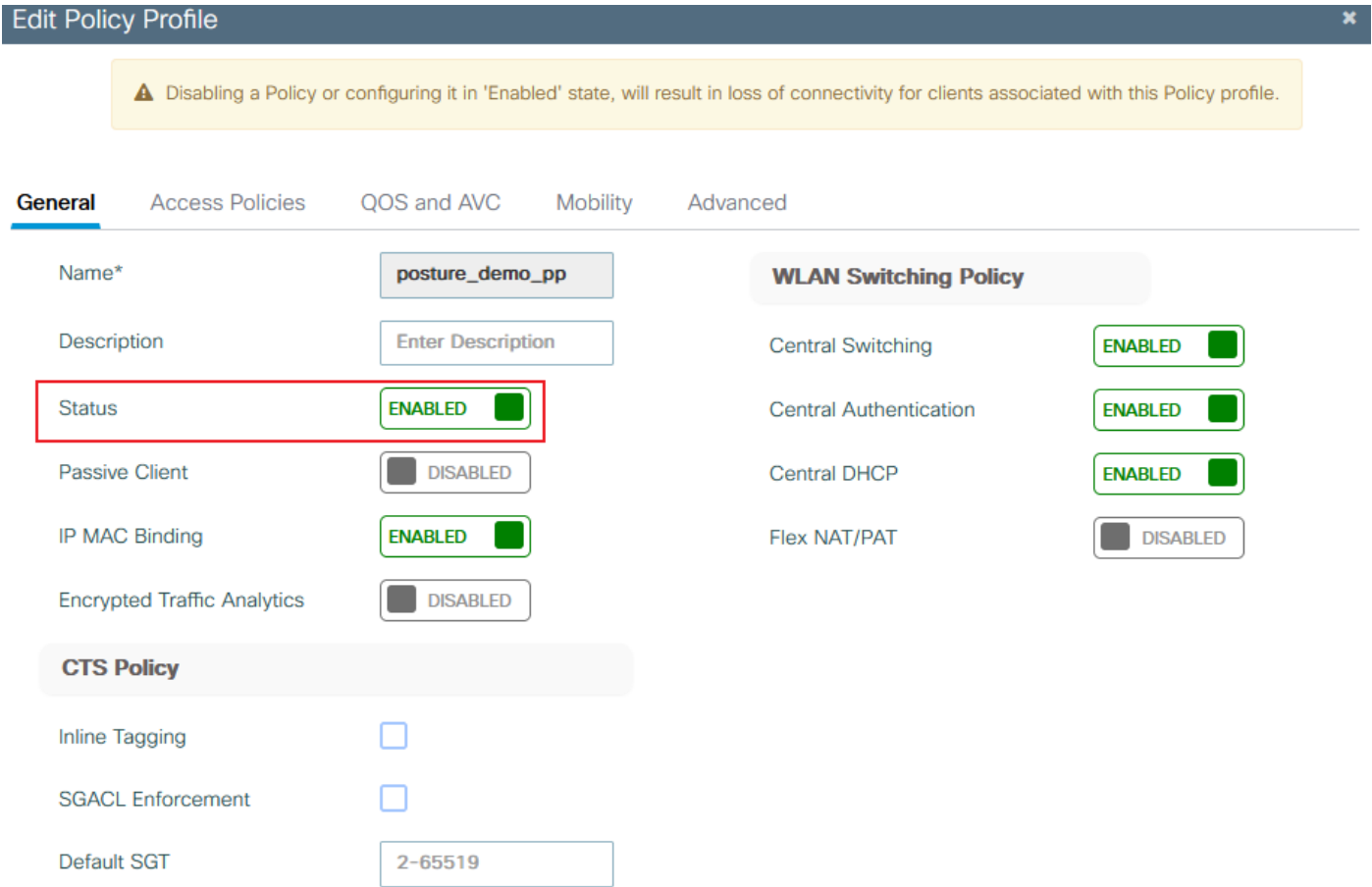
在策略配置文件中，您可以决定分配客户端到哪个VLAN，以及其他设置(如访问控制列表(ACL)、服务质量(QoS)、移动锚点、计时器等)。 您可以使用默认策略配置文件，也可以新建策略配置文件。

第 1 步：新建策略配置文件。导航到Configuration > Tags & Profiles > Policy并创建一个新的：



9800添加策略配置文件

确保已启用配置文件。



9800 create policy profile general

步骤2.选择VLAN。导航到访问策略选项卡，然后从下拉列表中选择VLAN名称或手动键入VLAN-ID。请勿在策略配置文件中配置ACL:

⚠ 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创建策略配置文件VLAN

第 3 步：配置策略配置文件，接受 ISE 覆盖（“允许 AAA 覆盖”）和授权更改 (CoA)（“NAC 状态”）。您也可以选择指定会计方法：

⚠ 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

ⓘ

Idle Timeout (sec)

300

Idle Threshold (bytes)

0

Client Exclusion Timeout (sec)

☐

60

Guest LAN Session Timeout

☐

DHCP

IPv4 DHCP Required

☒

DHCP Server IP Address

10.10.10.1

Show more >>>

AAA Policy

Allow AAA Override

☒

NAC State

☒

Policy Name

default-aaa-policy ✕ ▼

🔗

Accounting List

POSTUREacct ✕ ▼

🔗

WGB Parameters

Fabric Profile

☐

Search or Select ▼

🔗

Link-Local Bridging

☐

mDNS Service Policy

default-mdns-ser ... ▼

🔗

Clear

Hotspot Server

Search or Select ▼

🔗

User Defined (Private) Network

Status

☐

Drop Unicast

☐

DNS Layer Security

DNS Layer Security Parameter Map

Not Configured ▼

🔗

Clear

Flex DHCP Option for DNS

ENABLED

🟢

Flex DNS Traffic Redirect

☒

IGNORE

WLAN Flex Policy

VLAN Central Switching

☐

Split MAC ACL

Search or Select ▼

🔗

Air Time Fairness Policies

↶ Cancel

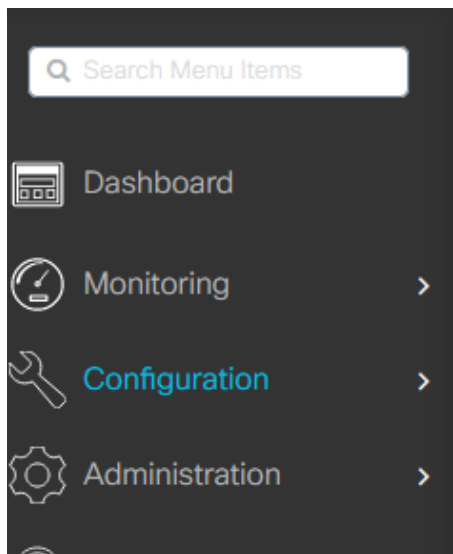
🔄 Update & Apply to Device

9800创建策略配置文件高级

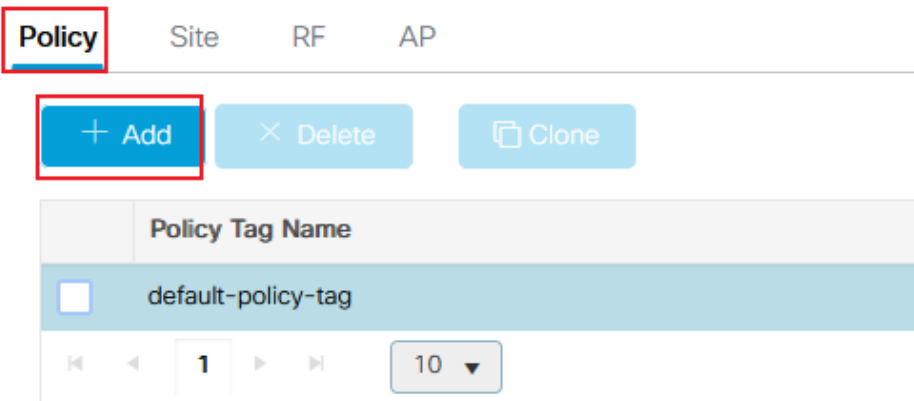
策略标签配置

在策略标签中，您可以将 SSID 与策略配置文件相关联。您可以新建策略标签，也可以使用 default-policy 标签。

导航到Configuration > Tags & Profiles > Tags > Policy，并根据需要添加新标签，如图所示：

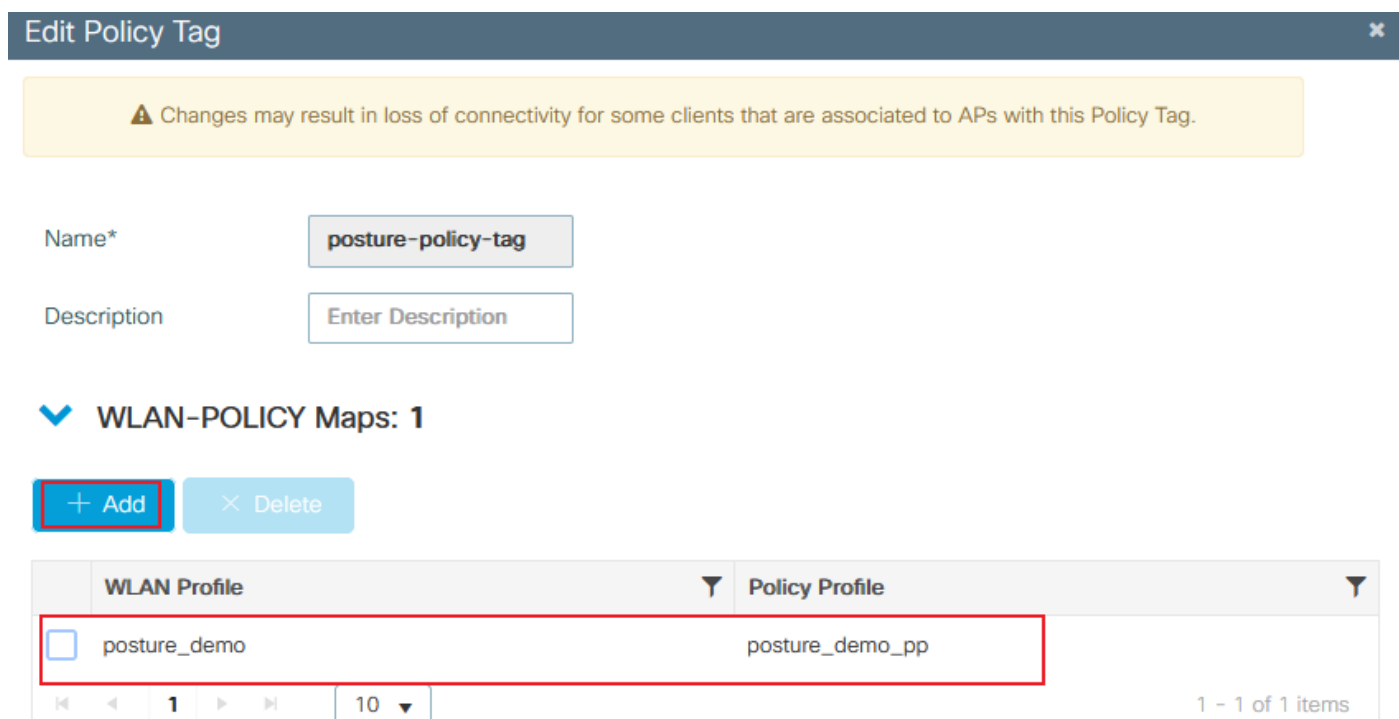


Configuration > Tags & Profiles > Tags



9800策略标记添加

将您的WLAN配置文件链接到所需的策略配置文件：



9800策略标记详细信息

策略标签分配

将策略标签分配给所需的 AP。导航到Configuration > Wireless > Access Points > AP Name > General Tags，进行所需的分配，然后单击Update & Apply to Device。

Edit AP

General

Interfaces

High Availability

Inventory

ICap

Advanced

Support Bundle

General

Tags

AP Name*

Location*

default location

Base Radio MAC

Ethernet MAC

Admin Status

ENABLED

AP Mode

Local

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

Policy

posture-policy-tag

Site

default-site-tag

RF

default-rf-tag

9800策略标记分配

重定向 ACL 配置

导航到Configuration > Security > ACL > + Add以创建新的ACL。

用于安全评估门户重定向的ACL与CWA（集中式Web身份验证）的要求相同。

您需要拒绝流向 ISE PSN 节点的流量以及 DNS，同时允许所有其余流量。此重定向ACL不是安全ACL，而是弃用ACL，它定义哪些流量进入CPU（在允许的情况下）进行进一步处理（如重定向）以及哪些流量停留在数据平面上（在拒绝时）并避免重定向。ACL必须如下所示（在本例中用您的ISE IP地址替换10.124.57.141）：

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重定向ACL详细信息

策略ACL配置

在这种情况下，您需要在9800 WLC上为ISE定义单独的ACL，以根据状态检查结果授权合规和不合规方案。

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一般信息

对于兼容方案，在本例中只需使用permit all。作为另一种常见配置，您还可以让ISE不授权合规结果中的任何ACL，这相当于permit all在9800端：

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 — 兼容

对于不合规情况，客户端仅允许访问特定网络，通常访问补救服务器（本例中为ISE自身）：

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 — 不合规

ISE上的AAA配置和状态设置

状态要求：在本示例中，确定合规性的要求是检测用于测试Windows PC的桌面上是否存在特定测

试文件。

步骤1.将WLC 9800添加为ISE上的NAD。导航到管理>网络资源>网络设备>添加:

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

Default Device

Device Security Settings

Network Devices List > WLC9800

Network Devices

Name

WLC9800

Description

IP Address

* IP :

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

添加网络设备01

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

Default Device

Device Security Settings

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

添加网络设备02

步骤2.在思科软件CCO网站上下载思科安全客户端前端部署包和合规性模块。

访问和搜索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		

安全客户端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合规性模块4.3

步骤3.将Cisco安全客户端头端部署包和合规性模块包上传到ISE客户端调配。导航到工作中心>状态>客户端调配>资源。单击添加，从下拉框中选择从本地磁盘选择代理资源：

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

上传安全客户端

Cisco ISE

Work Centers - Posture

OverviewNetwork DevicesClient ProvisioningPolicy ElementsPosture PolicyPolicy SetsTroubleshootReportsSettings

Client Provisioning PolicyResourcesClient Provisioning Portal

Selected 0 Total 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 ...

成功上传安全客户端和合规性模块

第4步：创建座席状态配置文件导航到工作中心>状态>客户端调配>资源>添加>座席状态配置文件：

Cisco ISE

Work Centers - Posture

OverviewNetwork DevicesClient ProvisioningPolicy ElementsPosture PolicyPolicy SetsTroubleshootReportsSettings

Client Provisioning PolicyResourcesClient 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.

座席状态配置文件

第5步：创建代理配置导航到工作中心>状态>客户端调配>资源>添加>代理配置：

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

☐

Dagnostic and Reporting Tool

☒

Profile Selection

* ISE Posture

bloomtest-Posture for Windows

添加代理配置

步骤6.确认客户端调配门户，使用默认门户进行测试。（请从CA服务器生成CSR并申请SSL证书，并替换此门户设置上的证书组标记。否则，在测试过程中会出现证书不受信任警告。）

导航至工作中心>状态>客户端调配>客户端调配门户：

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

选择Client Provisioning Portal 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

☒ 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

选择Client Provisioning Portal 02

步骤7.创建客户端调配策略。导航到Work Centers> Posture> Client Provisioning> Client Provisioning Policy > Edit>插入上述新策略。

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)	then WLC9800-windows
IOS	If Any	and Apple IOS All	and Condition(s)	then Cisco-ISE-NSP
Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP
Windows	If Any	and Windows All	and Condition(s)	then CiscoTemporalAgentWindows 4.10.02051 And WinSPWizard 3.0.0.3 And Cisco-ISE-NSP
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
Chromebook	If Any	and Chrome OS All	and Condition(s)	then Cisco-ISE-Chrome-NSP

创建客户端调配策略

步骤8.创建文件条件。导航至工作中心>状态>策略元素>条件>文件>文件条件>添加:

OverviewNetwork DevicesClient ProvisioningPolicy ElementsPosture PolicyPolicy SetsTroubleshootReportsSettings

Conditions

Anti-MalwareAnti-SpywareAnti-VirusApplicationCompoundDictionary CompoundDictionary SimpleDisk EncryptionExternal DataSourceFileFirewallHardware AttributesPatch ManagementRegistryScriptServiceUSB

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

创建文件条件

第9步：创建补救(Create Remediations)导航到工作中心(Work Centers)>状态(Posture)>策略元素(Policy Elements)>补救(Remediations)>文件(File)>添加(Add):

Cisco ISE

Work Centers · Posture

OverviewNetwork DevicesClient ProvisioningPolicy ElementsPosture PolicyPolicy SetsTroubleshootReportsSettings

Conditions

Remediations

ApplicationAnti-MalwareAnti-SpywareAnti-VirusFileFirewallLaunch ProgramLinkPatch ManagementScriptUSBWindows Server Update Servi...Windows UpdateRequirementsAllowed ProtocolsAuthorization ProfilesDownloadable ACLs

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

创建文件补救

步骤10.创建需求。导航至工作中心>状态>策略元素>要求>插入新要求:

Overview

Network Devices

Client Provisioning

Policy Elements

Posture Policy

Policy Sets

Troubleshoot

Reports

Settings

Conditions

Remediations

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>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 <a>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 <a>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 <a>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 <a>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 <a>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 <a>Edit
WLC9800-Posture-Demo	for Windows All	using Any version	using Agent	met if WLC9800-Posture-demo then	WLC9800-Posture-Demo <a>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.

创建状况要求

步骤11.创建状态策略。导航到工作中心>状态>插入新策略:

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 <a>Edit

创建状态策略

步骤12.创建三个授权配置文件：状态未知；安全评估状态为“不兼容”；安全评估状态是合规的。导航到Policy > Policy Elements> Results> Authorization> Authorization Profiles> Add:

Dictionaries

Conditions

Results

Authentication

Authorization

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

创建授权配置文件01

Dictionary

Conditions

Results

Authentication

Allowed Protocols

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > WLC9800-Posture-Unknown

Authorization Profile

* NameWLC9800-Posture-Unknown

Description

* Access TypeACCESS_ACCEPT

Network Device ProfileCisco

Service Template

Track Movement

Agentless Posture

Passive Identity Tracking

Common Tasks

Web Redirection (CWA, MDM, NSP, CPP)

Client Provisioning (Posture)ACLPoSTURE_REDIRECT_ACLValueClient Provisioning Portal (def:)

Static IP/Host name/FQDN

Suppress Profiler CoA for endpoints in Logical Profile

创建授权配置文件02

Dictionary

Conditions

Results

Authentication

Allowed Protocols

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > WLC9800-Posture-Compliant

Authorization Profile

* NameWLC9800-Posture-Compliant

Description

* Access TypeACCESS_ACCEPT

Network Device ProfileCisco

Service Template

Track Movement

Agentless Posture

Passive Identity Tracking

Common Tasks

Interface Template

Web Authentication (Local Web Auth)

Airspace ACL NamePoSTURE_COMPLIANT_ACL

Airspace IPv6 ACL Name

创建授权配置文件03

Navigation: Dictionaries | 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

步骤13.创建策略集。导航到Policy> Policy

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

创建策略集

集>添加图标:

步骤14.创建身份验证策略导航到策略>策略集>展开"WLC9800-Posture-Demo">身份验证策略>添加:

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 Options	0	⚙️
●	Default		All_User_ID_Stores Options	0	⚙️

创建身份验证策略

第15步：创建授权策略导航到Policy> Policy Sets>展开“WLC9800-Posture-Demo”> Authorization Policy>添加:

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	⚙️

创建授权策略

Examples

1.使用正确的802.1X凭证连接测试SSID posture_demo。



posture_demo
Secured

Enter your user name and password

wlc9800-user

••••••••



OK

Cancel

Network & Internet settings

Change settings, such as making a connection metered.

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。