

# Catalyst 9800 WLCおよびISEでのポスチャの設定

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[9800 WLC での AAA 設定](#)

[WLAN 設定](#)

[ポリシープロファイルの設定](#)

[ポリシータグの設定](#)

[ポリシータグの割り当て](#)

[リダイレクト ACL 設定](#)

[ポリシーACLの設定](#)

[ISEでのAAA設定とポスチャ設定](#)

[例](#)

[確認](#)

[トラブルシュート](#)

[Checklist](#)

[デバッグの収集](#)

[参考資料](#)

---

## はじめに

このドキュメントでは、Graphic User Interface ( GUI ; グラフィックユーザインターフェイス ) を使用して、Catalyst 9800 WLCとISEでポスチャWLANを設定する方法について説明しています。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- 9800 WLCの一般設定
- ISEポリシーおよびプロファイルの設定

## 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

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

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

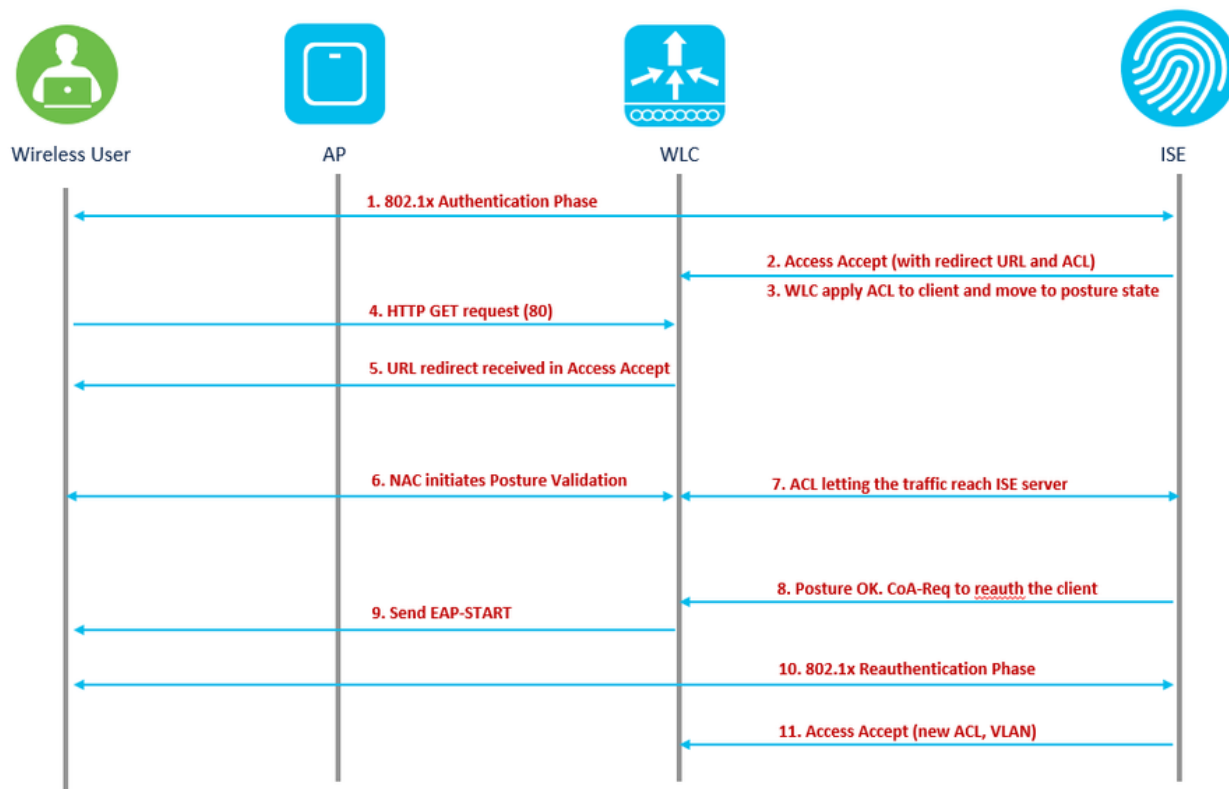
## 背景説明

ワイヤレス LAN コントローラの RADIUS NAC と CoA の機能フロー

1. クライアントはdot1x認証を使用して認証します。
2. RADIUS Access Acceptは、ポート80のリダイレクトされたURLと、許可するIPアドレスとポート、または検疫VLANを含む事前認証ACLを伝送します。
3. クライアントはAccess Acceptで提供されたURLにリダイレクトされ、ポスチャ検証が完了するまで新しい状態になります。この状態のクライアントが ISE サーバと通信し、ISE NAC サーバで設定されたポリシーに対して自身を検証します。
4. クライアント上のNACエージェントがポスチャ検証を開始（ポート80へのトラフィック）：エージェントがHTTPディスカバリ要求をポート80に送信し、コントローラがアクセスアクセプトで指定されたURLにリダイレクトします。ISE は、クライアントが到達しようと試みていることを認識し、クライアントに直接応答します。このようにして、クライアントは ISE サーバ IP について学習し、その後はクライアントが ISE サーバと直接通信します。
5. ACLがこのトラフィックを許可するように設定されているため、WLCはこのトラフィックを許可します。VLAN のオーバーライド時には、ISE サーバに到達できるようにトラフィックはブリッジされます。
6. ISEクライアントが評価を完了すると、再認証サービスを含むRADIUS CoA-ReqがWLCに送信されます。これによってクライアントの再認証が始まります（EAP-START を送信することにより）。再認証が成功すると、ISE は新しい ACL（あれば）を使用して Access Accept を送信し、URL リダイレクトまたはアクセス VLAN は行われません。
7. WLCは、RFC 3576に従ってCoA-ReqおよびDisconnect-Reqをサポートしています。WLC は RFC 5176 に従って再認証サービスの CoA-Req をサポートする必要があります。
8. ダウンロード可能ACLの代わりに、事前設定されたACLがWLCで使用されます。ISE サーバは、コントローラですでに設定されている ACL 名のみを送信します。
9. この設計は、VLANとACLの両方のケースに対応します。VLAN のオーバーライドの場合、ポー

ト 80 のみをリダイレクトし、隔離 VLAN の残りのトラフィックを許可 (ブリッジ) します。ACL では、Access Accept で受信したプレ認証 ACL が適用されます。

次の図は、この機能フローを視覚的に表したものです。



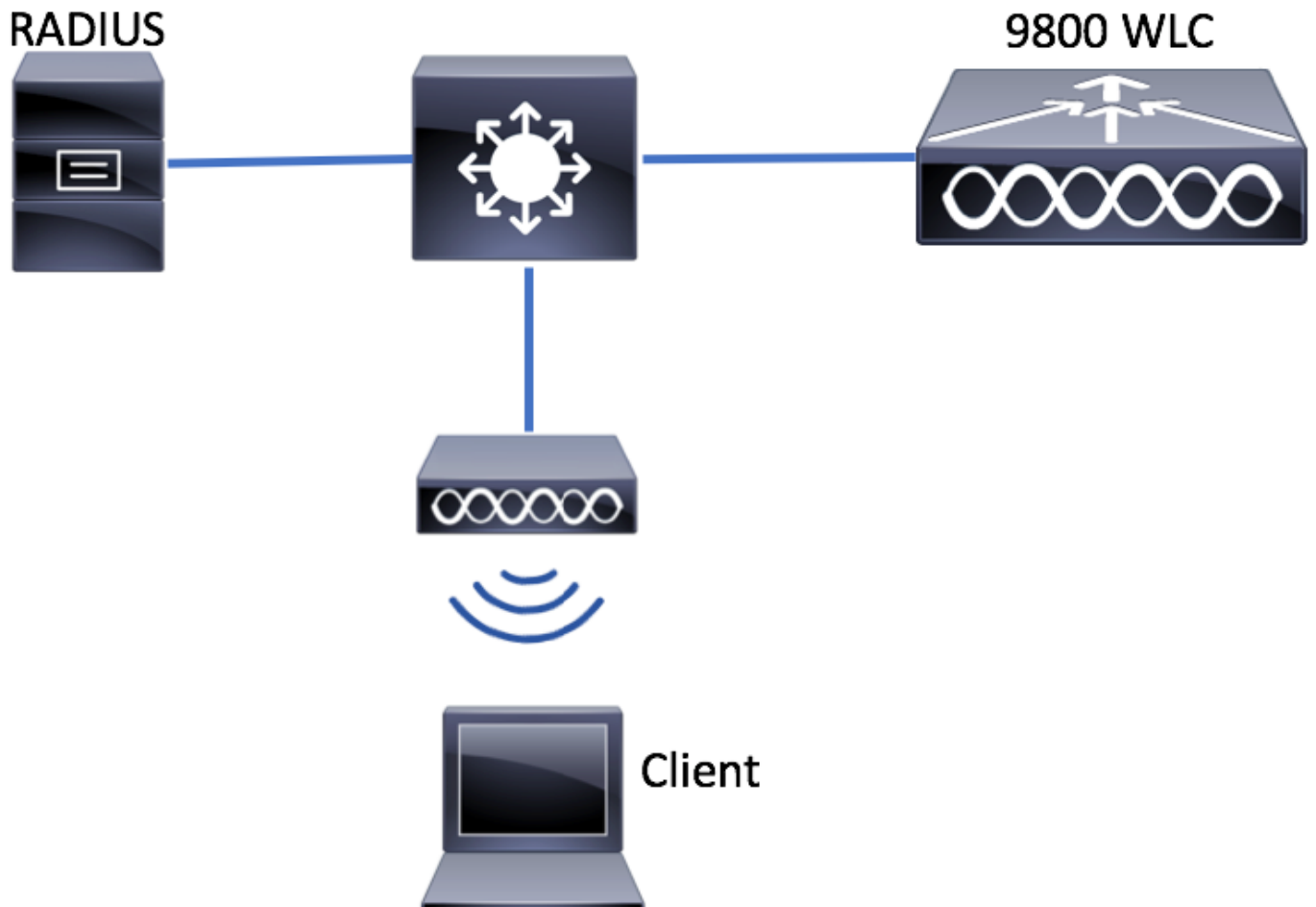
#### 機能ワークフロー

この使用例では、企業ユーザ専用のSSIDをポスチャに対して有効にします。このSSIDには、BYOD、ゲスト、その他のユースケースは存在しません。

ワイヤレスクライアントが初めてポスチャSSIDに接続するときには、ISEのリダイレクトされたポータルにポスチャモジュールをダウンロードしてインストールし、ポスチャチェック結果 ( 準拠/非準拠 ) に基づいて最終的に関連ACLに適用する必要があります。

## 設定

### ネットワーク図



ネットワーク図

## 9800 WLC での AAA 設定

ステップ 1 : ISEサーバを9800 WLC設定に追加します。Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Addの順に移動し、図に示すようにRADIUSサーバの情報を入力します。ポスチャNACでCoAのサポートが有効になっていることを確認します。

- 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 |
|-------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| <div> <div>◀</div> <div>◀</div> <div>0</div> <div>▶</div> <div>▶</div> </div> <div> <div>10</div> <div>▼</div> </div> <div>items per page</div> |         |

## 9800 radiusサーバの作成

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の詳細の作成

ステップ 2：認証方式リストを作成します。図に示すように、Configuration > Security > AAA > AAA Method List > Authentication > + Addの順に移動します。

← Cisco 17.9.5 Cisco Catalyst 9800-CL Wireless Controller

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 |
|----------------------------------|-------|------------|
| <input type="checkbox"/> default | login | local      |

1 10 ▼

## 9800認証一覧の追加

## 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認証リストの作成の詳細

ステップ3: ( オプション ) 図に示すように、アカウントリング方式リストを作成します。

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アカウントリストの追加

## Quick Setup: AAA Accounting



Method List Name\*

POSTUREacct

Type\*

identity



Available Server Groups

Assigned Server Groups

ldap  
tacacs+



radius



Cancel

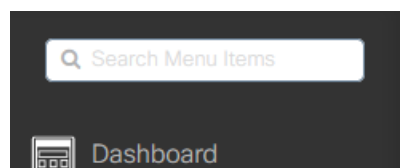


Apply to Device

9800アカウントリストの作成の詳細

## WLAN 設定

ステップ 1 : WLAN を作成します。Configuration > Tags & Profiles > WLANs > + Addの順に移動し、必要に応じてネットワークを設定します。



Configuration > Tags & Profiles > **WLANs**



Add



Delete



Clone

Enable WLAN

Disable WLAN

9800 WLAN追加

ステップ 2 : WLANの一般情報を入力します。

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 : 一般的なWLANの作成

ステップ 3 : Securityタブに移動し、必要なセキュリティ方式を選択します。この場合、「802.1x」を選択すると、AAA認証リスト(AAA Configurationセクションのステップ2で作成したもの)が必要になります。

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:WLANセキュリティL2の作成

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:WLANセキュリティAAAの作成

ポリシープロファイルの設定

ポリシープロファイル内では、他の設定(アクセスコントロールリスト(ACL)、Quality of Service(QoS)、モビリティアンカー、タイマーなど)の中から、VLANを割り当てるクライアントを決定できます。デフォルトのポリシープロファイルを使用することも、新規に作成することもできます。

ステップ 1：新しいポリシープロファイルを作成します。Configuration > Tags & Profiles > Policyの順に移動し、新しいポリシーを作成します。

Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Configuration > Tags & Profiles > Policy

+ Add

× Delete

Clone

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

1

10

9800ポリシープロファイルの追加

プロファイルを有効にします。

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ポリシープロファイルの作成 ( 全般 )

ステップ 2 : VLANを選択します。Access Policiesタブに移動し、ドロップダウンからVLAN名を選択するか、手動でVLAN IDを入力します。ポリシープロファイルではACLを設定しないでください。

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のポリシープロファイルVLANの作成

ステップ 3 : ISEオーバーライド ( AAAオーバーライドを許可 ) および認可変更(CoA) ( NAC状態 ) を受け入れるようにポリシープロファイルを設定します。必要に応じて、次の会計処理基準も指定できます。

⚠ 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

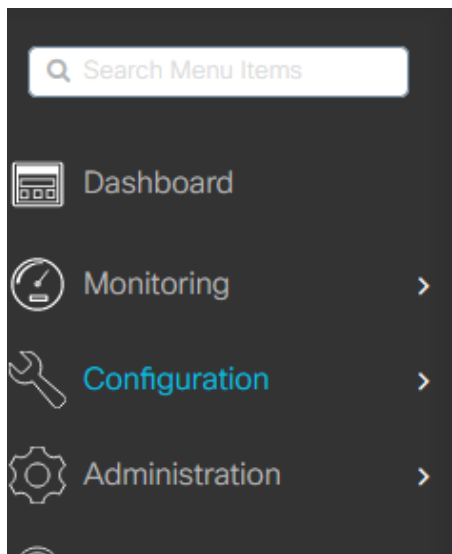
**Advanced****WLAN Timeout**Session Timeout (sec)  ⓘIdle Timeout (sec) Idle Threshold (bytes) Client Exclusion Timeout (sec) ☐ Guest LAN Session Timeout ☐**DHCP**IPv4 DHCP Required ☒DHCP Server IP Address [Show more >>>](#)**AAA Policy**Allow AAA Override ☒NAC State ☒Policy Name  ⓘAccounting List  ⓘ**WGB 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 : ポリシープロファイルの高度な作成

## ポリシータグの設定

ポリシータグで、SSID をポリシープロファイルにリンクします。新しいポリシータグを作成するか、default-policy タグを使用します。

Configuration > Tags & Profiles > Tags > Policyの順に移動し、図に示すように、必要に応じて新しいポリシーを追加します。



Configuration > Tags & Profiles > Tags

**Policy** Site RF AP

**+ Add** × Delete Clone

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

1 10 ▼

9800ポリシータグの追加

WLANプロファイルを目的のポリシープロファイルにリンクします。

Edit Policy Tag

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

Name\*

posture-policy-tag

Description

Enter Description

▼ WLAN-POLICY Maps: 1

+ Add

× Delete

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

1 10 ▼ 1 - 1 of 1 items

9800ポリシータグの詳細

## ポリシータグの割り当て

必要な AP にポリシータグを割り当てます。Configuration > Wireless > Access Points > AP Name > General Tagsの順に移動し、必要な割り当てを行ってから、Update & Apply to Deviceをクリックします。

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ポリシータグの割り当て

## リダイレクト ACL 設定

Configuration > Security > ACL > + Addの順に選択し、新しいACLを作成します。

ポスチャポータルリダイレクトに使用されるACL(ISE)の要件は、CWA ( 中央Web認証 ) と同じです。

ISE PSN ノードへのトラフィックと DNS を拒否し、他はすべて許可する必要があります。このリダイレクトACLは、セキュリティACLではなく、追加の処理 ( リダイレクションなど ) のために ( 許可時に ) CPUに送られるトラフィックと、データプレーンにとどまる ( deny時に ) トラフィックを定義し、リダイレクションを回避するパントACLです。ACLは次のようになります ( この例では10.124.57.141をISE IPアドレスに置き換えます ) 。

Edit ACL

ACL Name\*

POSTURE\_REDIRECT\_ACL

ACL Type

IPv4 Extended

Rules

Sequence\*

Action

permit

Source Type

any

Destination Type

any

Protocol

ahp

Log

☐

DSCP

None

+ Add

× Delete

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

9800リダイレクトACLの詳細

## ポリシーACLの設定

この場合、ポチュアチェックの結果に基づいて準拠シナリオと非準拠シナリオを認可するために、ISEの9800 WLCで個別のACLを定義する必要があります。

Configuration > Security > ACL

+ Add

× Delete

Associate Interfaces

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

◀

1

▶

10

9800 ACL全般

準拠するシナリオの場合、この場合は単にpermit allを使用します。もう1つの一般的な設定として、ISEで準拠した結果でどのACLも認可しないように設定することもできます。これは、9800側でpermit allに相当します。

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

1
10

1 - 1 of 1 items

## 9800 ACL – 準拠

非準拠シナリオでは、クライアントは特定のネットワーク(通常は修復サーバ (この場合はISE 自体))へのアクセスのみを許可します。

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

1
10

1 - 5 of 5 items

## 9800 ACL – 非準拠

## ISEでのAAA設定とポスチャ設定

ポスチャ要件：この例では、Windows PCのテストに使用されるデスクトップに特定のテストファイルが存在するかどうかを検出することが、コンプライアンスを判断するための要件です。

ステップ 1：ISEでNADとしてWLC 9800を追加します。Administration > Network Resources > Network Devices > Addの順に移動します。

The screenshot shows the Cisco ISE Administration console. The breadcrumb trail is Administration > Network Resources > Network Devices > Add. The left sidebar shows 'Network Devices' selected. The main form is titled 'Network Devices List > WLC9800'. The form fields are as follows:

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

ネットワークデバイスの追加01

The screenshot shows the 'RADIUS Authentication Settings' for the WLC9800. The breadcrumb trail is Administration > Network Resources > Network Devices > Add > RADIUS Authentication Settings. The left sidebar shows 'Network Devices' selected. The main form is titled 'RADIUS Authentication Settings'. The form fields are as follows:

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

ネットワークデバイスの追加02

ステップ 2：Cisco Software CCO Webサイトで、Cisco Secure Clientヘッドエンド導入パッケージとコンプライアンスモジュールをダウンロードします。

## Cisco Secure Clientへのアクセスと検索：

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](#) 

セキュアクライアント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コンプライアンスモジュール4.3

ステップ 3： Cisco Secure Clientヘッドエンド導入パッケージおよびコンプライアンスモジュールパッケージをISEクライアントプロビジョニングにアップロードします。Work Centers > Posture > Client Provisioning > Resources の順に移動します。Addをクリックし、ドロップダウンボックスからAgent resources from local diskを選択します。

| Overview                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Network Devices | Client Provisioning | Policy Elements |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|---------------------|-----------------|
| <div>Client Provisioning Policy</div> <div>Resources</div> <div>Client Provisioning Portal</div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                 |                     |                 |
| <div> Edit    Add    Duplicate    Delete</div> <div><div><input type="checkbox"/></div><div>Agent resources from Cisco site</div></div> <div><div><input type="checkbox"/></div><div>Agent resources from local disk</div></div> <div><div><input type="checkbox"/></div><div>Native Supplicant Profile</div></div> <div><div><input type="checkbox"/></div><div>Agent Configuration</div></div> <div><div><input type="checkbox"/></div><div>Agent Posture Profile</div></div> <div><div><input type="checkbox"/></div><div>AMP Enabler Profile</div></div> |                 |                     |                 |

セキュアクライアントのアップロード

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

Edit

+ Add

Duplicate

Delete

Selected 0

Total 13

Quick Filter

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

セキュアクライアントとコンプライアンスモジュールが正常にアップロードされました

ステップ 4 : エージェントポスチャプロファイルの作成 : Work Centers> Posture> Client Provisioning> Resources> Add> Agent Posture Profileの順に選択します。

| Cisco ISE                            |                 | Work Centers - Posture                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                 |                |             | <div> <div></div> <div></div> <div></div> <div></div> </div> |         |          |           |       |             |                  |    |                                    |                                |    |                                                               |                        |    |                                                         |               |      |                                 |                   |        |                                                                                        |              |          |                                                                                                                                     |                                      |          |                                                       |
|--------------------------------------|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|----------------|-------------|--------------------------------------------------------------|---------|----------|-----------|-------|-------------|------------------|----|------------------------------------|--------------------------------|----|---------------------------------------------------------------|------------------------|----|---------------------------------------------------------|---------------|------|---------------------------------|-------------------|--------|----------------------------------------------------------------------------------------|--------------|----------|-------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|----------|-------------------------------------------------------|
| Overview                             | Network Devices | Client Provisioning                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Policy Elements | Posture Policy | Policy Sets | Troubleshoot                                                 | Reports | Settings |           |       |             |                  |    |                                    |                                |    |                                                               |                        |    |                                                         |               |      |                                 |                   |        |                                                                                        |              |          |                                                                                                                                     |                                      |          |                                                       |
| Client Provisioning Policy           |                 | <div> <div>ISE Posture Agent Profile Settings &gt; bloomtest-Posture for Windows</div> </div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                 |                |             |                                                              |         |          |           |       |             |                  |    |                                    |                                |    |                                                               |                        |    |                                                         |               |      |                                 |                   |        |                                                                                        |              |          |                                                                                                                                     |                                      |          |                                                       |
| Resources                            |                 | <div>Agent Posture Profile</div> <div> <div>Name *</div> <div>bloomtest-Posture for Windows</div> </div> <div> <div>Description:</div> <div>test windows PC for connecting WLC9800</div> </div> <div> <div>Agent Behavior</div> <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> </div> |                 |                |             |                                                              |         |          | 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                 |                |             |                                                              |         |          |           |       |             |                  |    |                                    |                                |    |                                                               |                        |    |                                                         |               |      |                                 |                   |        |                                                                                        |              |          |                                                                                                                                     |                                      |          |                                                       |

エージェントポスチャプロファイル

ステップ 5 : エージェント設定の作成 : Work Centers> Posture> Client Provisioning> Resources> Add> Agent Configurationの順に移動します。

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

エージェント設定の追加

手順 6：クライアントプロビジョニングポータルを確認し、テストに既定のポータルを使用することを確認します。[OK]です（CSRを生成し、CAサーバーからSSL証明書を適用し、このポータル設定の証明書グループタグを置き換えてください。そうしないと、テストプロセス中に証明書の信頼できない警告が発生します。）

Work Centers > Posture > Client Provisioning > Client Provisioning Portalsの順に移動します。

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 Provisioning Portal 01を選択します

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

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

Client Provisioning Portal 02を選択します

手順 7 : クライアントプロビジョニングポリシーの作成上記で、Work Centers > Posture > Client Provisioning > Client Provisioning Policy > Edit > insert new policyの順に移動します。

Overview

Network Devices

Client Provisioning

Policy Elements

Posture Policy

Policy Sets

Troubleshoot

Reports

Settings

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                                                                                  |
|-----------------------------------------------------|-----------------|-------------------|------------------|------------------------------------------------------------------------------------------|
| <input checked="" type="checkbox"/> WLC9800-Windows | If Any          | and Windows All   | and Condition(s) | then WLC9800-windows Edit                                                                |
| <input checked="" type="checkbox"/> IOS             | If Any          | and Apple iOS All | and Condition(s) | then Cisco-ISE-NSP Edit                                                                  |
| <input checked="" type="checkbox"/> Android         | If Any          | and Android       | and Condition(s) | then Cisco-ISE-NSP Edit                                                                  |
| <input checked="" type="checkbox"/> Windows         | If Any          | and Windows All   | and Condition(s) | then CiscoTemporalAgentWindows 4.10.02051 And WinSPWizard 3.0.0.3 And Cisco-ISE-NSP Edit |
| <input checked="" type="checkbox"/> MAC OS          | If Any          | and Mac OSX       | and Condition(s) | then CiscoTemporalAgentOSX 4.10.02051 And MacOsXSPWizard 2.7.0.1 And Cisco-ISE-NSP Edit  |
| <input checked="" type="checkbox"/> Chromebook      | If Any          | and Chrome OS All | and Condition(s) | then Cisco-ISE-Chrome-NSP Edit                                                           |

クライアントプロビジョニングポリシーの作成

ステップ 8 : ファイル条件の作成Work Centers > Posture > Policy Elements > Conditions > File > File Conditions > Addの順に移動します。

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

ファイル条件の作成

ステップ 9：是正の作成「ワークセンター」>「ポスチャ」>「ポリシー要素」>「是正」>「ファイル」>「追加」に移動します。

≡ 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

ファイル修復の作成

ステップ 10：要件を作成します。Work Centers > Posture > Policy Elements > Requirements > Insert New Requirementの順に移動します。

|          |                 |                     |                 |                |             |              |         |          |
|----------|-----------------|---------------------|-----------------|----------------|-------------|--------------|---------|----------|
| 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 Services | 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 <a href="#">Edit</a>                |
| Default_AppVis_Requirement_Win_temporal              | for Windows All  | using 4.x or later | using Temporal Agent | met if Default_AppVis_Condition_Win then   | Select Remediations <a href="#">Edit</a>              |
| Default_AppVis_Requirement_Mac_temporal              | for Mac OSX      | using 4.x or later | using Temporal Agent | met if Default_AppVis_Condition_Mac then   | Select Remediations <a href="#">Edit</a>              |
| Default_Hardware_Attributes_Requirement_Win_temporal | for Windows All  | using 4.x or later | using Temporal Agent | met if Hardware_Attributes_Check then      | Select Remediations <a href="#">Edit</a>              |
| Default_Hardware_Attributes_Requirement_Mac_temporal | for Mac OSX      | using 4.x or later | using Temporal Agent | met if Hardware_Attributes_Check then      | Select Remediations <a href="#">Edit</a>              |
| Default_Firewall_Requirement_Win_temporal            | for Windows All  | using 4.x or later | using Temporal Agent | met if Default_Firewall_Condition_Win then | Default_Firewall_Remediation_Win <a href="#">Edit</a> |
| Default_Firewall_Requirement_Mac_temporal            | for Mac OSX      | using 4.x or later | using Temporal Agent | met if Default_Firewall_Condition_Mac then | Default_Firewall_Remediation_Mac <a href="#">Edit</a> |
| WLC9800-Posture-Demo                                 | for Windows All  | using Any version  | using Agent          | met if WLC9800-Posture-demo then           | WLC9800-Posture-Demo <a href="#">Edit</a>             |

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

ポスチャ要件の作成

ステップ 11ポスチャポリシーの作成Work Centers> Posture> Insert new policyの順に移動します

。

|           |                        |
|-----------|------------------------|
| Cisco ISE | Work Centers - Posture |
|-----------|------------------------|

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

|                |          |         |
|----------------|----------|---------|
| Posture Policy | Guide Me | WLC9800 |
|----------------|----------|---------|

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                                   |
|-------------------------------------|----------------|----------------------|-----------------|-------------------|-------------------|--------------|------------------|------------------------------------------------|
| <input checked="" type="checkbox"/> | Policy Options | WLC9800-Posture-Demo | if Any          | and Windows All   | and Any version   | and Agent    | and              | then WLC9800-Posture-Demo <a href="#">Edit</a> |

ポスチャポリシーの作成

ステップ 123つの認証プロファイルの作成：ポスチャステータスが不明、ポスチャステータスが非準拠、ポスチャステータスが準拠Policy> Policy Elements> Results> Authorization> Authorization Profiles> Addの順に移動します。

|              |            |         |
|--------------|------------|---------|
| 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](#)

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

## 認可プロファイルの作成01

Dictionaryes 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

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

## 認可プロファイルの作成02

Dictionaryes 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

## 認可プロファイルの作成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

ステップ 13 ポリシーセットを作成します。Policy> Policyの順に移動します。

Policy Sets

Reset Reset Policyset Hitcounts Save

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

Reset Save

ポリシーセットの作成

セット>追加アイコン:

ステップ 14 : 認証ポリシーの作成 Policy > Policy Setsに移動> "WLC9800-Posture-Demo"> Authentication Policy>追加:

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<br>Options<br>All_User_ID_Stores<br>Options | 0    |         |
| Default        |                 |            |                                                            | 0    |         |

認証ポリシーの作成

ステップ 15 : 認可ポリシーの作成Policy > Policy Setsに移動し、「WLC9800-Posture-Demo」>「Authorization Policy」>「Add」を展開します。

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               |      |         |

認証ポリシーの作成

## 例

1. 正しい802.1XクレデンシャルでテストSSID posture\_demo を接続しました。



posture\_demo  
Secured

Enter your user name and password

wlc9800-user

••••••••



OK

Cancel

## Network & Internet settings

Change settings, such as making a connection metered.

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。