

SDアクセスでの中央Web認証の設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[トポロジ](#)

[概要](#)

[Cisco Catalyst CenterでのCWAの設定](#)

[ネットワークプロファイルの作成](#)

[SSID の作成](#)

[ファブリックプロビジョニング](#)

[Cisco ISEにプロビジョニングされた設定の確認](#)

[許可プロファイル](#)

[ポリシーセット](#)

[ゲストポータルの設定](#)

[WLCにプロビジョニングされた設定の確認](#)

[SSID 設定](#)

[ワイヤレスポリシープロファイルの設定](#)

[ポリシータグの設定](#)

[リダイレクトACL 設定](#)

[アクセスポイントでのACLのリダイレクト](#)

はじめに

このドキュメントでは、中央Web認証(CWA)を設定するための手順を説明し、すべてのコンポーネントの確認手順の概要を示します。

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。

- Cisco Catalystセンター
- Cisco Identity Services Engine (ISE)
- Catalyst 9800ワイヤレスコントローラーアーキテクチャ
- 認証、許可、アカウントिंग (AAA)

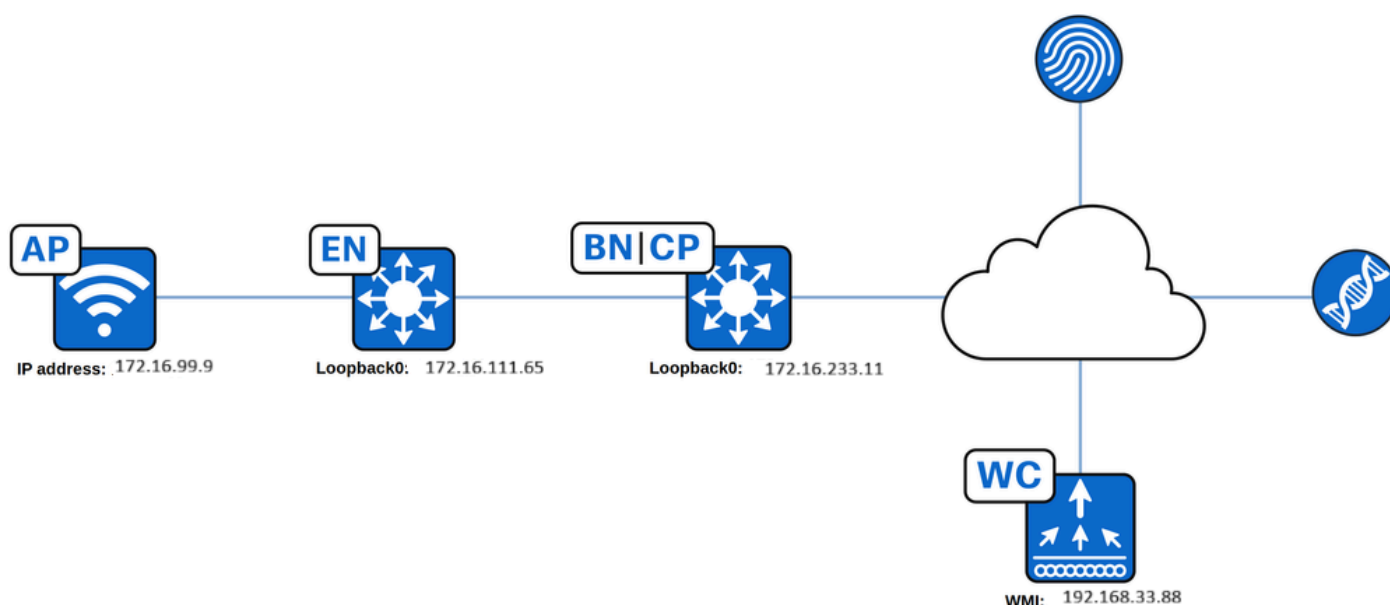
使用するコンポーネント

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。

- シスコワイヤレスLANコントローラ(WLC):C9800-CL、Cisco IOS® XE 17.12.04
- Cisco Catalyst Center – バージョン2.3.7.7
- Cisco Identity Services Engine(ISE) : バージョン3.0.0.458
- SDAエッジノード : C9300-48P、Cisco IOS® XE 17.12.05
- SDAボーダーノード/コントロールプレーン : C9500-48P、Cisco IOS® XE17.12.05
- Ciscoアクセスポイント – C9130AXI-A、バージョン17.9.5.47

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。

トポロジ



概要

中央Web認証(CWA)は、ゲストタイプSSIDを使用して、設定済みのリダイレクトACLを使用して、ユーザのWebブラウザをCisco ISEでホストされるキャプティブポータルにリダイレクトします。キャプティブポータルでは、ユーザが登録と認証を行うことができ、認証が成功すると、ワイヤレスLANコントローラ(WLC)が適切な認可を適用してフルネットワークアクセスを許可します。このガイドでは、Cisco Catalyst Centerを使用してCWAを設定する手順について説明します。

Cisco Catalyst CenterでのCWAの設定

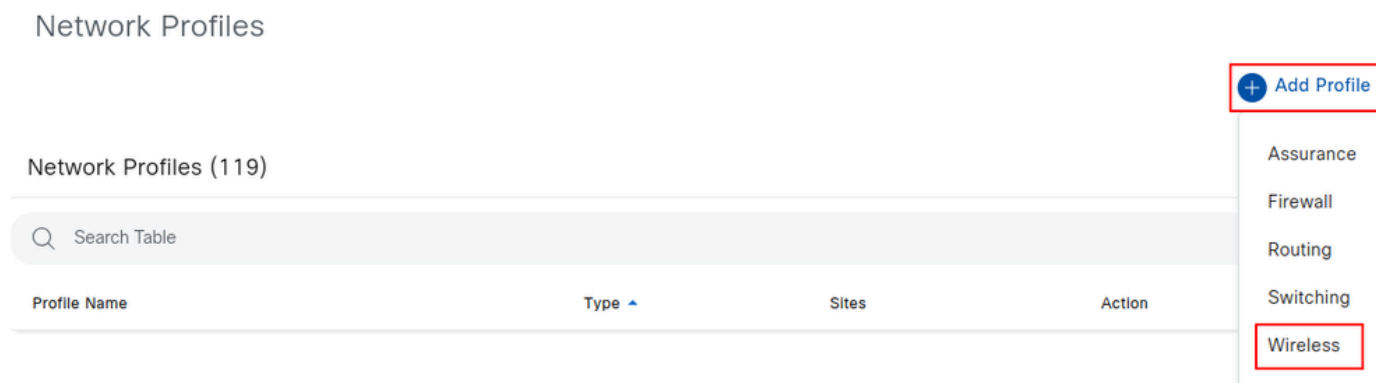
ネットワークプロファイルの作成

ネットワークプロファイルを使用すると、特定のサイトに適用できる設定を構成できます。ネットワークプロファイルは、Cisco Catalyst Centerのさまざまな要素に対して作成できます。

- 保証
- ファイアウォール
- ルーティング
- スイッチング
- テレメトリアプライアンス
- ワイヤレス

CWAでは、ワイヤレスプロファイルを設定する必要があります。

ワイヤレスプロファイルを設定するには、Design > Network Profilesの順に選択し、Add Profileをクリックして、Wirelessを選択します。



必要に応じてプロファイルに名前を付けます。この例では、ワイヤレスプロファイルの名前はCWA_Cisco_Wireless_Profileです。Add SSIDを選択することで、このプロファイルに既存のSSIDを追加できます。SSIDの作成については、次のセクションで説明します。

Add a Network Profile

Following tasks must be completed before creating a Wireless Network Profile.

1. Define SSIDs, Interface, RF Profiles and AP Profiles under [Network Settings > Wireless](#)
2. Define CLI Templates under [CLI Templates](#) (Optional)
3. Define Feature Templates under [Feature Templates](#) (Optional)

Note: Changes in SSIDs, AP Zones, Feature Templates, CLI Templates sections require Controller provisioning. Changes in Custom Tags/Groups require Access Point provisioning.

Profile Name*
CWA_Cisco_Wireless_Profile

Site: [Assign](#)

[SSIDs](#) [AP Zones](#) [Feature Templates](#) [CLI Templates](#) [Advanced Settings](#) ▾

[Add SSID](#)

Assignを選択してこのプロファイルを適用するサイトを選択し、目的のサイトを選択するサイトを選択したら、Saveをクリックします。

Profile Name*

CWA_Cisco_Wireless_Profile

Site: [Assign](#)

SSIDs

AP Zones

Feature Templates

CLI Templates

Advanced Settings ▾

Add SSID

SSID の作成

Design > Network Settings > Wireless > SSIDsの順に移動し、Addをクリックします。

SSIDs

Configure SSIDs for enterprise and guest wireless networks. You can assign them to sites via Wireless Network Profiles.

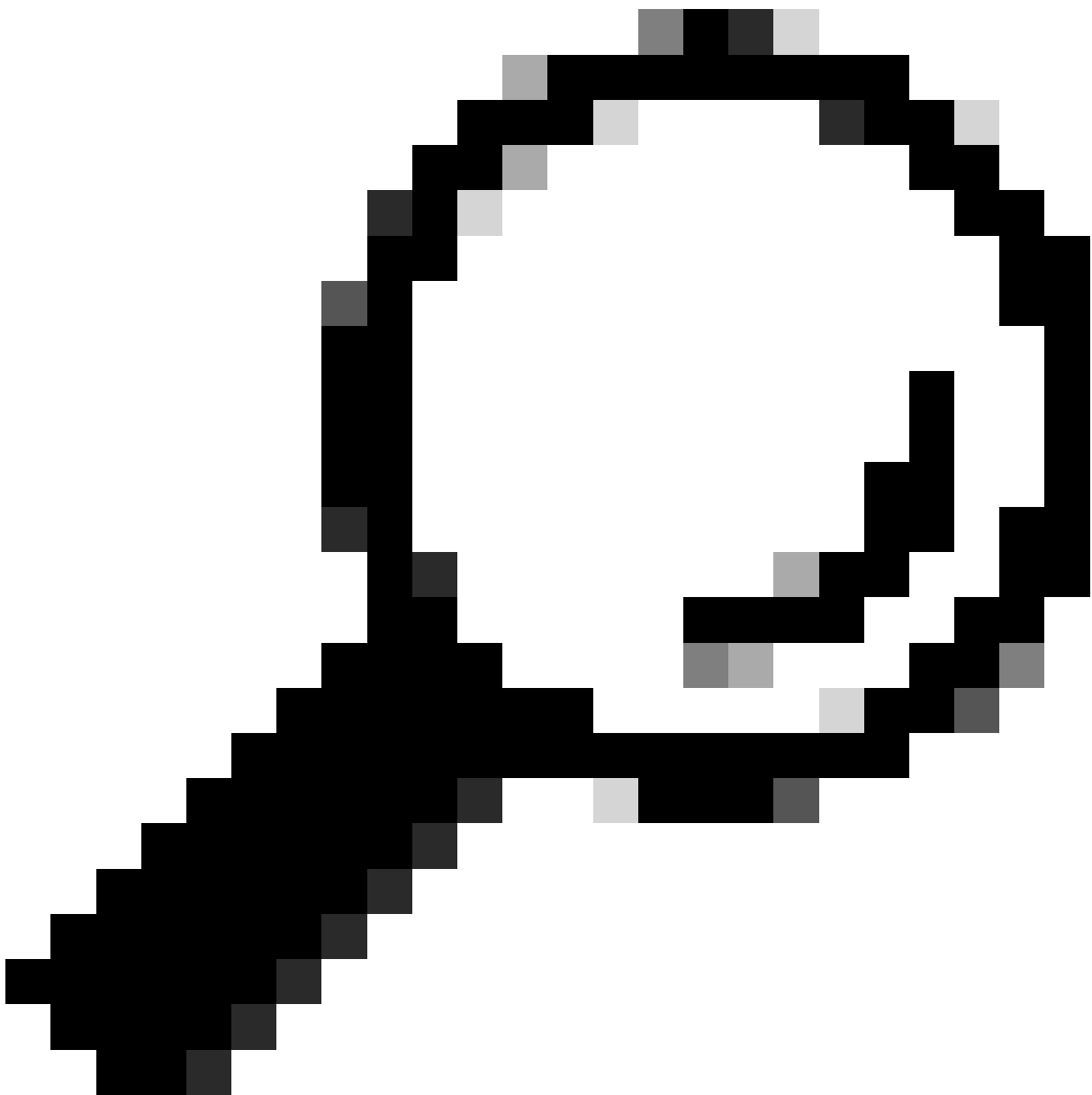
SSID (79)

[+ Add](#)

Search Table

[Edit](#) [Delete](#) [SSID Scheduler](#) ⓘ 0 Selected

☐	Network Name (SSID) ▾	WLAN Profile Name	Policy Profile Name	SSID Type	L2 Security	L3 Security	Wireless Profiles	Portal Name	AAA Servers
☐	1865test	1865test_... (2)	1865test_... (2)	Enterprise	wpa3_personal	open	fernaronom_wireless, J... See all	N/A	Configure AAA



ヒント:CWAのSSIDを作成するには、ゲストタイプを選択する必要があります。この選択により、WLC上のSSIDのワイヤレスポリシープロファイルにコマンドnacコマンドが追加されます。このコマンドを使用すると、ユーザがキャプティブポータルに登録した後、CoAを再認証に使用できます。この設定を行わないと、ユーザは登録とポータルへのリダイレクトを繰り返し繰り返す無限ループに陥る可能性があります。

Addを選択した後、SSID設定ワークフローに進みます。最初のページで、SSID nameを設定します。また、無線ポリシーbandを選択し、管理ステータスやブロードキャスト設定を含むSSID状態を定義できます。このコンフィギュレーションガイドでは、SSIDの名前はCWA_Ciscoです。

Wireless Network Name (SSID)* CWA_Cisco	WLAN Profile Name* CWA_Cisco_profile	Policy Profile Name CWA_Cisco_profile
--	---	--

Radio Policy

☒ 2.4GHz ☒ 5GHz ☒ 6GHz ⓘ

802.11b/g Policy
802.11bg ▼ ☐ Band Select ⓘ ☐ 6 GHz Client Steering

☐ Fast Lane ⓘ

Quality of Service(QoS) ⓘ

Egress
VoIP (Platinum) ⓘ ▼ Ingress
VoIP (Platinum) Up ⓘ ▼ ⓘ

SSID STATE

☒ Admin Status ☒ Broadcast SSID

SSID名を入力すると、WLANプロファイル名とポリシープロファイル名が自動的に生成されます。Nextを選択して次に進みます。

CWA SSIDには、少なくとも1つのAAA/PSNを設定する必要があります。何も設定されていない場合は、Configure AAAを選択し、ドロップダウンリストからPSN IPアドレスを選択します。

Authentication, Authorization, and Accounting Configuration

Atleast one AAA/PSN is required for CWA SSIDs. Configure AAA to add one.

 [Configure AAA](#)

☐ AAA Override

☒ MAC Filtering

☐ Deny RCM Clients ⓘ

Pre-Auth ACL List Name ▼

AAAサーバを選択した後、レイヤ3セキュリティパラメータを設定し、ポータルタイプ(自己登録またはホットスポット)を選択します。

ホットスポットゲストポータル：ホットスポットゲストポータルは、ユーザ名やパスワードを必要とせずにゲストにネットワークアクセスを提供します。ここで、ユーザはアクセプタブルユースポリシー(AUP)を受け入れてネットワークにアクセスし、その後のインターネットアクセスに

至る必要があります。 クレデンシャルゲストポータル：クレデンシャルゲストポータルを使用してアクセスするには、ゲストがユーザ名とパスワードを持っている必要があります。

L3 SECURITY

☒ Web Policy ☐ Open

Most secure

Guest users are redirected to a Web Portal for authentication

Authentication Server

What kind of portal are you creating today ?

Where will your guests redirect after successful authentication ?

Central Web Authentication Self Registered Original URL

Self Registered

Hotspot

ユーザが使用ポリシーを登録または承認した後に実行されるアクションも設定できます。Success Page、Original URL、およびCustom URLの3つのオプションを使用できます。

Authentication Server

Where will your guests redirect after successful authentication ?

What kind of portal are you creating today ?

Central Web Authentication Self Registered Original URL

Success Page

Original URL

Custom URL

各オプションの動作を次に説明します。

成功ページ：認証が成功したことを示す確認ページにユーザをリダイレクトします。

Original URL：キャプティブポータルによって代行受信される前に要求された元のURLにユーザをリダイレクトします。

カスタムURL：指定したカスタムURLにユーザをリダイレクトします。このオプションを選択すると、宛先URLを定義するための追加フィールドが有効になります

同じページのAuthentication, Authorization, and Accounting Configurationの下で、Pre-auth ACLも設定できます。このACLを使用すると、DHCP、DNS、またはPSNのIPアドレス以外のプロトコルに対するエントリを追加できます。これらのアドレスはネットワーク設定から取得され、プロビジョニング中にリダイレクトACLに追加されます。この機能は、Cisco Catalyst Centerバージョン2.3.3.x以降で使用できます。

Authentication, Authorization, and Accounting Configuration

AAA Configured (1)

☒ AAA Override

☒ MAC Filtering

☐ Deny RCM Clients 

Pre-Auth ACL List Name 

事前認証ACLを設定するには、Design > Network Settings > Wireless > Security Settingsの順に選択し、Addをクリックします。

Pre-Auth ACLs AP Authorization List AP Impersonation Configure DTLS Ciphersuites

Configure Pre-Auth Access Control Lists. You can assign them to SSIDs during SSID creation or modification.

Pre-Auth Access Control Lists (10)

 Add

最初の名前はCatalyst CenterのACLを識別し、2番目の名前はWLCのACL名に対応します。2番目の名前は、WLCで設定されている既存のリダイレクトACLと一致する可能性があります。参考として、Catalyst Centerは名前Cisco DNA_ACL_WEBAUTH_REDIRECTをWLCにプロビジョニングします。事前認証ACLからのエントリは、既存のエントリの後に追加されます。

New Pre-Auth ACL

Pre-Auth ACL List Name*
Name_on_Catalyst_Center 

Pre-Auth ACL Name*
DNAC_ACL_WEBAUTH_REDIRECT 

SSID作成ワークフローに戻り、Nextを選択すると、高速移行、セッションタイムアウト、クライアントユーザタイムアウト、レート制限などの詳細設定が表示されます。必要に応じてパラメータを調整し、Nextを選択して続行します。この構成ガイドでは、デフォルト設定を使用しています。

Advanced Settings

Configure the advanced fields to complete SSID setup.

SSID Name: CWA_Cisco (Guest)

MFP Client Protection ⓘ

☒ Optional ☐ Required ☐ Disabled

Protected Management Frame (802.11w)

☐ Optional ☐ Required ☒ Disabled

☒ 11k - Neighbor List

☐ Radius Client Profiling ⓘ

☒ Coverage Hole Detection

WLAN Timeouts

☒ Session Timeout ⓘ

In (secs)*

28800

Range is from 1 to 86400

☒ Client Exclusion

In (secs)*

180

Range is from 0 to 2147483647

☒ Client User Idle Timeout

In (secs)*

300

Range is from 15 to 100000

11v BSS Transition Support

☒ BSS Max Idle Service

☒ Directed Multicast Service

Nextを選択すると、機能テンプレートをSSIDに関連付けるよう求めるプロンプトが表示されます。必要に応じて、Addをクリックして必要なテンプレートを選択し、完了したらNextをクリックします。

Associate Feature Templates to SSID

Select a design instance from the table or add new design instance to associate the Feature Templates to SSID.

Design Instances

[Refresh](#)

[Export](#)

[Import](#)

[Add](#)

SSIDを、先ほど作成したワイヤレスプロファイルに関連付けます。詳細については、「ワイヤレスネットワークプロファイルの作成」の項を参照してください。このセクションでは、SSIDがファブリック対応かどうかを選択することもできます。完了したら、Associate profileをクリックします。

SSID Name: CWA_Cisco (Guest)

+ Add Profile

Search

100NG SOM RA

adortiz-test-profile

anarami-wireless

angel test

antvegaprofile

Cnicolet_Oeiras

CWA_Cisco_Wireless_P...

Associate Profile

Cancel

Profile Name

CWA_Cisco_Wireless_Profile

WLAN Profile Name

CWA_Cisco_profile

Policy Profile Name

CWA_Cisco_profile

Fabric

☒ Yes

☐ No

802.11be Profile Name

ワイヤレス管理トラストポイントの表示

プロファイルをSSIDに関連付けたら、Nextをクリックしてキャプティブポータルを作成および設計します。を起動するには、Create Portalをクリックします。

SSID Name: CWA_Cisco (Guest)

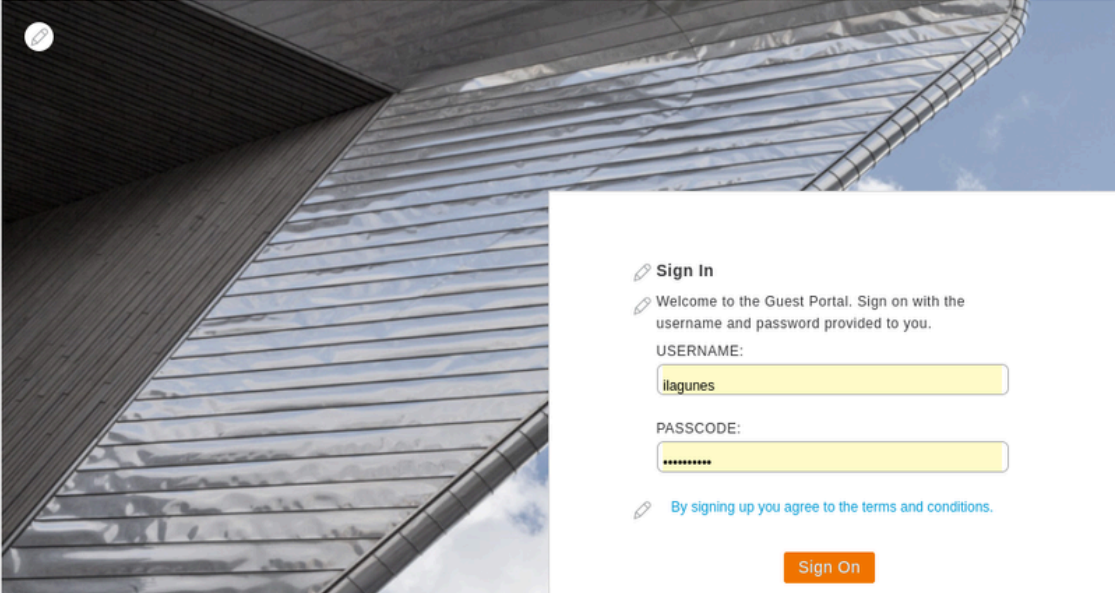
No Self Registration Portal Available

Use the create portal button to create a new portal

Create Portal

ポータル名は、FQDN内のドメイン名とISE上のポリシーセット名を定義します。完了したら、[Save] をクリックします。ポータルは編集可能なままであり、必要に応じて削除できます。

Portal

CWA_Cisco_Portal		Login Page	▼
> Page Content			
Access Code			
Header Text			

 **Sign In**

 Welcome to the Guest Portal. Sign on with the username and password provided to you.

USERNAME:

PASSCODE:

 [By signing up you agree to the terms and conditions.](#)

Sign On

Nextを選択すると、前のステップで定義されたすべての設定パラメータの要約が表示されます。

Summary

Review all changes

SSID Name: CWA_Cisco (Guest)

> Basic Settings [Edit](#)

> Security Settings [Edit](#)

> Advanced Settings [Edit](#)

∨ Associate Feature Templates to SSID [Edit](#)

Design Instance	N/A
-----------------	-----

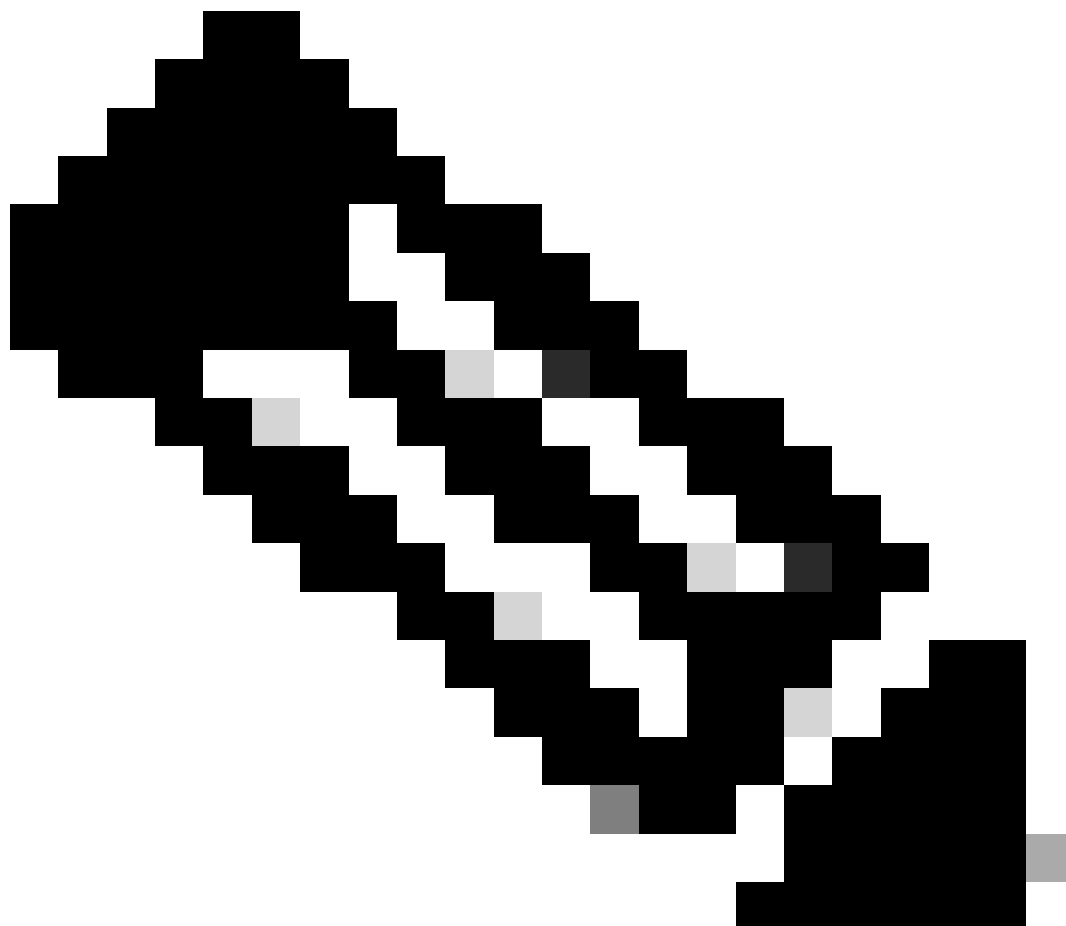
∨ Network Profile Settings [Edit](#)

CWA_Cisco_Wireless_Profile	Fabric (Associated)
----------------------------	-------------------------------------

設定の詳細を確認し、Saveを選択して変更を適用します。

ファブリックプロビジョニング

ワイヤレスネットワークプロファイルをファブリックサイトに関連付けると、SSIDがProvision > Fabric Sites > (Your site) > Wireless SSIDsの下に表示されます。



注：サイトのワイヤレスLANコントローラで、ワイヤレスSSIDの下にSSIDを表示するように設定する必要があります

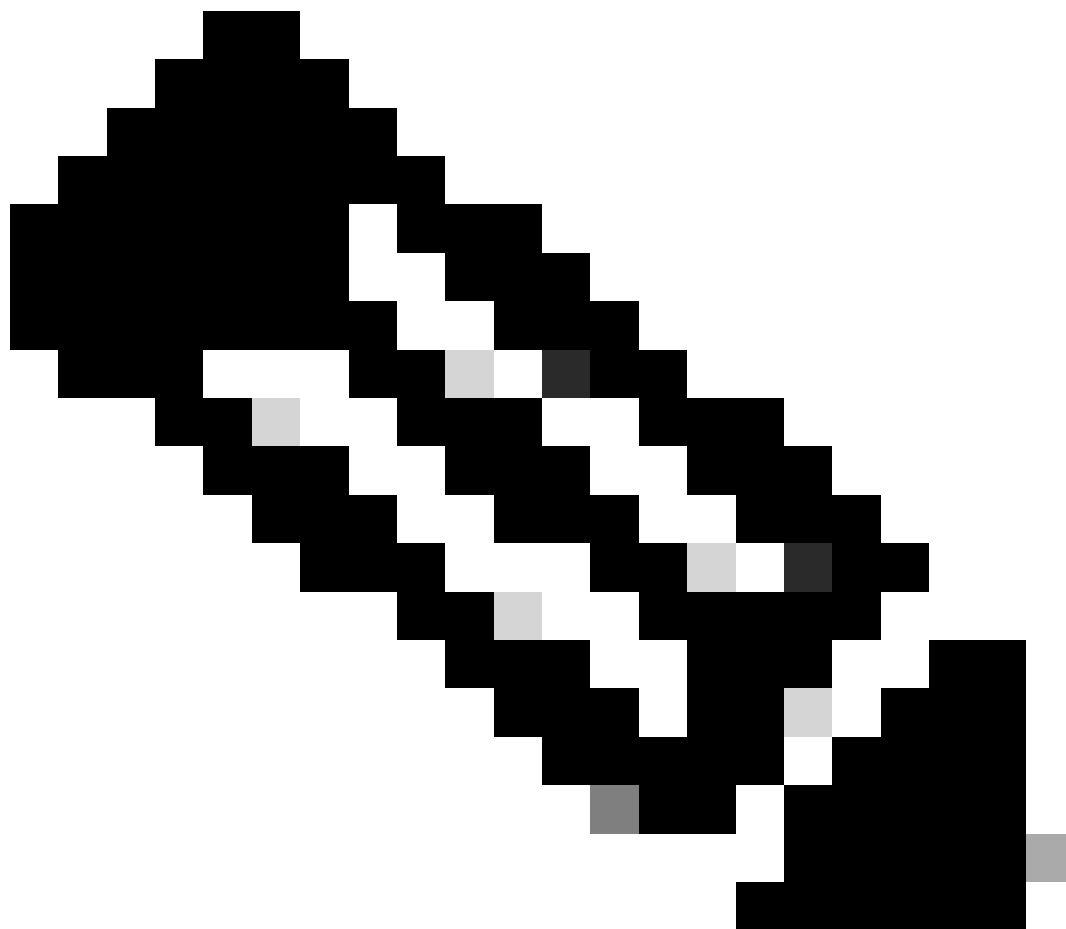
SSIDプールを選択し、オプションでセキュリティグループタグを関連付けて、Deployをクリックします。SSIDは、プールが割り当てられている場合にのみ、アクセスポイントによってブロードキャストされます。

☒ Enable Wireless Multicast ⓘ

SSID Name	Type	Security	Traffic Type	Address Pool	Security Group
CWA_Cisco	Guest	Open	Voice + Data	Choose Pool test ⓘ	Assign SGT

1 Record(s) Show Records: 25 1 - 1 ⓘ

AireOSおよびCatalyst 9800コントローラでは、ネットワーク設定でSSID設定を変更した後に、ワイヤレスLANコントローラを再プロビジョニングします。



注:SSIDにプールが割り当てられていない場合、APはSSIDをブロードキャストしないものと想定されます。SSIDは、プールが割り当てられた後にのみブロードキャストされます。プールが割り当てられると、コントローラを再プロビジョニングする必要がなくなります。

Cisco ISEにプロビジョニングされた設定の確認

このセクションでは、Catalyst CenterによってCisco ISEにプロビジョニングされる設定を検証します。

許可プロファイル

Catalyst CenterがCisco ISEでプロビジョニングする設定の一部は、認証プロファイルです。このプロファイルは、パラメータに基づいてクライアントに割り当てられる結果を定義し、VLAN割り当て、ACL、またはURLリダイレクトなどの特定の設定を含めることができます。

ISEで認可プロファイルを表示するには、Policy > Policy Elements > Resultsに移動します。ポータル名がCWA_Cisco_Portalの場合、プロファイル名はCWA_Cisco_Portal_Profileです。説明フィ

ールドには、テキスト「DNA generated Authorization Profile for portal - CWA_Cisco_Portal」が表示されます。

Standard Authorization Profiles

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

Selected 0 Total 18

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

All [v](#) [f](#)

☐	Name	Profile	Description
☐	AuthProfile-DNAC	Cisco	SGT Authentication Profile para DNACtl
☐	Block_Wireless_Access	Cisco	Default profile used to block wireless devices. Ensure that you configure a NULL RC
☐	CWA_Cisco_Portal_Profile	Cisco	DNA generated Authorization Profile for portal - CWA_Cisco_Portal

この認可プロファイルによってワイヤレスLANコントローラ(WLC)に送信された属性を表示するには、認可プロファイル名をクリックして、「一般的なタスク」セクションを参照してください。

この認可プロファイルは、リダイレクトACLとリダイレクトURLを配信します。

Web Redirection属性には、次の2つのパラメータがあります。

1. ACL Name:Cisco DNA_ACL_WEBAUTH_REDIRECTを設定
2. 値：キャプティブポータルの名前を参照します(この例ではCWA_Cisco_Portal)。

[証明書更新メッセージの表示]オプションを使用すると、エンドポイントが現在使用している証明書を更新するためにポータルを使用できます。

追加オプションのStatic IP/Host Name/FQDNは、Display Certificates Renewal Messageの下にあります。この機能を使用すると、ポータルのFQDNではなくIPアドレスを配信できます。これは、キャプティブポータルがDNSサーバに到達できないためにロードに失敗した場合に役立ちます。

Common Tasks

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

Centralized Web Auth

ACL

DNAC_ACL_WEBAUTH_RE...

Value CWA_Cisco_Portal

☒ Display Certificates Renewal Message

☐ Static IP/Host name/FQDN

☐ Suppress Profiler CoA for endpoints in Logical Profile

ポリシーセット

Policy > Policy Sets > Default > Authorization Policyの順に移動し、CWA_Cisco_Portalという名前のポータル用に作成された2つのポリシーセットを表示します。これらのポリシーセットは次のとおりです。

- CWA_Cisco_Portal_GuestAccessポリシー
- CWA_Cisco_Portal_Redirectポリシー

✓	CWA_Cisco_Portal_GuestAccessPolicy	AND	Wireless_MAB Guest_Flow Radius-Called-Station-ID ENDS_WITH :CWA_Cisco	PermitAccess x	Guests
✓	CWA_Cisco_Portal_RedirectPolicy	AND	Wireless_MAB Radius-Called-Station-ID ENDS_WITH :CWA_Cisco	CWA_Cisco_Portal_Pr... x	Select from list

CWA_Cisco_Portal_GuestAccessPolicyポリシーは、クライアントが自己登録またはホットスポットポータルを通じてWeb認証プロセスをすでに完了しているときに適用されます。

✓	CWA_Cisco_Portal_GuestAccessPolicy	AND	Wireless_MAB Guest_Flow Radius-Called-Station-ID ENDS_WITH :CWA_Cisco	PermitAccess x	Guests
---	------------------------------------	-----	---	----------------	--------

このポリシーセットは、次の3つの基準に一致します。

- Wireless_MAB: Cisco ISEがワイヤレスLANコントローラからMAC認証バイパス(MAB)認証要求を受信するときに使用されます。
- Guest_Flow: GuestEndpoints IDグループに対してエンドポイントのMACアドレスをチェックするISEを参照します。エンドポイントのMACアドレスがこのグループに存在しない場合、ポリシーは適用されません。
- RADIUS Called-Station-ID ENDS_WITH :CWA_Cisco: Called-Station-IDは、ブリッジまたはアクセスポイント(AP)のMACアドレスをASCII形式で保存するISEのRADIUS属性で、アクセスされるSSIDをセミコロン(:)で区切って追加します。この例では、CWA_CiscoがSSID名を表しています。

列プロファイルの下に「PermitAccess」という名前が表示されています。これは、編集できない予約済み認可プロファイルです。これにより、ネットワークへのフルアクセスが提供され、また、列「Security Groups」の下でSGTを割り当てることもできます。この場合、この列は「Guests」です。

PermitAccessプロファイルが使用されます。これは、編集できず、ネットワークへのフルアクセスを許可する予約された認可プロファイルです。SGTはSecurity Groups列で割り当てることもできます。この場合、SGTはGuestsに設定されます。

次に確認するポリシーはCWA_Cisco_Portal_RedirectPolicyです。

✓	CWA_Cisco_Portal_RedirectPolicy	AND	Wireless_MAB Radius-Called-Station-ID ENDS_WITH :CWA_Cisco	CWA_Cisco_Portal_Pr... x	Select from list
---	---------------------------------	-----	---	--------------------------	------------------

このポリシーセットは、次の2つの基準に一致します。

- Wireless_MAB: Cisco ISEがワイヤレスLANコントローラからMAB認証要求を受信するときに使用されます。
- RADIUS Called-Station-ID ENDS_WITH :CWA_Cisco: Called-Station-IDは、ブリッジまたはアクセスポイント(AP)のMACアドレスをASCII形式で保存するISEのRADIUS属性で、アクセスされるSSIDをセミコロン(:)で区切って追加します。この例では、:CWA_CiscoがSSID名を表しています。

これらのポリシーの順序は重要です。CWA_Cisco_Portal_RedirectPolicyがリストの先頭にある場合、MAB認証と、RADIUS属性Called-Station-ID ENDS_WITH :CWA_Trainingを使用するSSID名のみが照合されます。この設定では、エンドポイントがすでにポータルを介して認証されている

場合でも、このポリシーは無期限に照合され続けます。その結果、PermitAccessプロファイルを紹介したフルアクセスは許可されず、クライアントは認証とポータルへのリダイレクトの連続ループに留まります。

ゲストポータルの設定

ポータルを表示するには、Work Centers > Guest Access > Portals & Componentsの順に移動します。

ここで作成したゲストポータルは、Catalyst Center CWA_Cisco_Portalと同じ名前を使用します。追加の詳細を表示する場合は、ポータル名を選択します。

Guest Portals

Choose one of the three pre-defined portal types, which you can edit, customize, and authorize for guest access.

Create Edit Duplicate Delete

CWA_Cisco_Portal
Wireless Setup Self-Registration Guest Portal
✔ Used in 1 rules in the Authorization policy

Deadpool_Site
Wireless Setup Self-Registration Guest Portal
✔ Used in 1 rules in the Authorization policy

Hotspot Guest Portal (default)
Guests do not require username and password credentials to access the network, but you can optionally require an access code
⚠ Authorization setup required

WLCにプロビジョニングされる設定の確認

このセクションでは、Catalyst CenterによってワイヤレスLANコントローラにプロビジョニングされる設定を検証します。

SSID 設定

WLCのGUIで、Configuration > Tags & Profiles > WLANsの順に選択して、SSIDの設定を表示します。

Selected WLANs : 0					
☐	Status	Name	ID	SSID	2.4/5 GHz Security
☐	✔	CWA_Cisco_profile	21	CWA_Cisco	[open], MAC Filtering

SSID CWA_CiscoのWLC上での名前はCWA_Cisco_profileで、IDは21で、MACフィルタリングを使用するセキュリティタイプはOpenです。SSIDをダブルクリックして、その設定を表示します。

Profile Name*	CWA_Cisco_profile	Radio Policy ⓘ
SSID*	CWA_Cisco	Show slot configuration
WLAN ID*	21	
Status	ENABLED ☒	6 GHz Status ☐ DISABLED
Broadcast SSID	ENABLED ☒	5 GHz Status ☒ ENABLED
		2.4 GHz Status ☒ ENABLED
		802.11b/g Policy 802.11b/g

SSIDは5 GHzと2.4 GHzの両方のチャンネルでUP状態でブロードキャストしており、ポリシープロファイルCWA_Cisco_Profileに添付されています。Securityタブをクリックして設定を表示します。

☐ WPA + WPA2	☐ WPA2 + WPA3	☐ WPA3	☐ Static WEP	☒ None
MAC Filtering ☒	Authorization List*	Cisco-0044d514 ⓘ default dnac-cts- CWA_Cisco- 0044d514		
OWE Transition Mode ☐				
Lobby Admin Access ☐				
Fast Transition Status Disabled Over the DS ☐ Reassociation Timeout * 20				

キー設定には、レイヤ2セキュリティ方式 (MACフィルタリング) とAAA許可リスト(Cisco DNA-cts-CWA_Cisco-0044d514)が含まれます。 この設定を確認するには、Configuration > Security > AAA > AAA Method List > Authorizationの順に移動します。

Authentication

Authorization

Accounting

+ Add

x Delete

	Name	Type	Group Type	Group1	Group2	Group3	Group4
☐	default	exec	local	N/A	N/A	N/A	N/A
☐	default	network	local	N/A	N/A	N/A	N/A
☐	dnac-cts-CWA_Traini-6a20f88c	network	group	dnac-rGrp-CWA_Traini-6a20f88c	N/A	N/A	N/A
☐	dnac-cts-Guest_pers-6fc56a40	network	group	dnac-rGrp-Guest_pers-6fc56a40	N/A	N/A	N/A
☐	dnac-cts-CWA_Cisco-0044d514	network	group	dnac-rGrp-CWA_Cisco-0044d514	N/A	N/A	N/A

方式リストは、Group1列のRADIUSグループCisco DNA-rGrp-CWA_Cisco-0044d514を指しています。この設定を表示するには、Configuration > Security > AAA > Server/Groups > Server Groupsの順に移動します。

Servers	Server Groups			
	Name	Server 1	Server 2	Server 3
☐	dnac-rGrp-CWA_Cisco-0044d514	dnac-radius_10.88.244.180	N/A	N/A

サーバグループCisco DNA-rGrp-CWA_Cisco-0044d514は、Server 1列のCisco DNA-radius_10.88.244.180を指しています。Serversタブで設定を確認します。

Servers	Server Groups			
	Name	Address	Auth Port	Acct Port
☐	dnac-radius_10.88.244.180	10.88.244.180	1812	1813

サーバCisco DNA-radius_10.88.244.180のIPアドレスは10.88.244.180です。その名前をクリックすると、設定が表示されます

Name*	dnac-radius_10.88.244.	Support for CoA ⓘ	ENABLED ☒
Server Address*	10.88.244.180	CoA Server Key Type	Hidden ▼
Set New Key	☐	CoA Server Key ⓘ	
Auth Port	1812	Automate Tester	☐
Acct Port	1813		
Server Timeout (seconds)	4		
Retry Count	3		

重要な設定は認可変更(CoA)です。これは、キャプティブポータルで認証された後に、認証、認可、およびアカウントing(AAA)セッションの属性を変更するメカニズムを提供します。この機能がない場合、エンドポイントは、ポータルでの登録が完了した後もweb-auth pending状態のままになります。

ワイヤレス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、クライアントにVLAN、ACL、QoS、モビリティアンカー、タイマーなどの設定を割り当てることができます。ポリシープロファイルの設定を表示するには、Configuration > Tags & Profiles > Policyの順に移動します。

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

ポリシー名をクリックすると、設定が表示されます。

General

Access Policies

QOS and AVC

Mobility

Advanced

Name*

CWA_Cisco_profile

Description

CWA_Cisco_profile

Status

ENABLED ☒

Passive Client

☐ DISABLED

IP MAC Binding

ENABLED ☒

Encrypted Traffic Analytics

☐ DISABLED

CTS Policy

Inline Tagging

☐

SGACL Enforcement

☐

Default SGT

2-65519

WLAN Switching Policy

Central Switching

☐ DISABLED

Central Authentication

ENABLED ☒

Central DHCP

☐ DISABLED

Flex NAT/PAT

☐ DISABLED

ポリシーステータスはEnabledで、他のファブリックSSIDと同様、中央スイッチングと中央DHCPは無効です。Advancedタブをクリックし、AAA Policyセクションに移動して、追加の設定の詳細を表示します。

AAA Policy

Allow AAA Override



NAC State



Policy Name

default-aaa-policy ✕ ▼



Accounting List

Search or Select ▼



Interim Accounting

ENABLED



AAA OverrideとNetwork Access Control (NAC ; ネットワークアクセスコントロール) の両方をイネーブルにできます。AAA Overrideを使用すると、コントローラはRADIUSサーバから返されたACLやURLなどの属性を受け入れて、これらの属性をクライアントに適用できます。NACでは、クライアントがポータルに登録された後、認可変更(CoA)を有効にします。

この設定は、WLC上のCLIを使用して表示することもできます。

ポリシープロファイルを確認するには、SSIDを接続してコマンドを実行します。

```
<#root>
```

```
WLC#show fabric wlan summary
```

```
Number of Fabric wlan : 1
```

```
WLAN  Profile Name      SSID      Status
```

```
-----
```

```
21
```

```
CWA_Cisco_profile
```

```
CWA_Cisco  UP
```

ポリシープロファイルCWA_Cisco_profileの設定を表示するには、次のコマンドを実行します。

```
<#root>
```

```
WLC#show running-config | section policy CWA_Cisco_profile
```

```
wireless profile policy CWA_Cisco_profile
```

```
aaa-override
```

```
no central dhcp
```

```
no central switching
```

```
description CWA_Cisco_profile
dhcp-tlv-caching
exclusionlist timeout 180
fabric CWA_Cisco_profile
http-tlv-caching
```

```
nac
```

```
service-policy input platinum-up
service-policy output platinum
no shutdown
```

ポリシータグの設定

ポリシータグは、WLANをポリシープロファイルにリンクする方法です。Configuration > Tags & Profiles > WLANsの順に選択し、WLAN名をクリックしてAdd to Policy Tagsの順に移動すると、SSIDに割り当てられているポリシータグが識別されます。

General Security Advanced Add To Policy Tags

+ Add × Delete

☐	Policy Tag	Policy Profile
☐	PT_ilagu_TOYOT_Foor6_a5548	CWA_Cisco_profile

◀ ▶ 1 10 ▼ 1 - 1 of 1 items

SSID CWA_Cisco_profileの場合、この設定を確認するためにポリシータグPT_ilagu_TOOT_Foor6_a5548が使用されます。これを確認するには、Configuration > Tags & Profiles > Tags > Policyの順に選択します。

Policy Tag Name	Description
☐ default-policy-tag	default policy-tag
☐ PT_ilagu_TOYOT_Foor6_a5548	PolicyTagName PT_ilagu_TOYOT_Foor6_a55

名前をクリックすると、詳細が表示されます。ポリシータグPT_ilagu_TOOT_Foor6_a5548は、WLC上の名前CWA_Cisco_profileに関連付けられたWLAN CWA_Cisco (WLANのページを参照) をポリシープロファイルCWA_Cisco_profileにリンクします。

WLAN-POLICY Maps: 1

+ Add × Delete

WLAN Profile	Policy Profile
☐ CWA_Cisco_profile	CWA_Cisco_profile

1 10 1 - 1 of 1 items

WLAN名CWA_Cisco_profileは、WLAN CWA_Ciscoを参照します。

Status	Name	ID	SSID
☐	CWA_Cisco_profile	21	CWA_Cisco

リダイレクト ACL 設定

CWAでは、リダイレクトアクセスコントロールリスト(ACL)によって、WLCにリダイレクトしてさらに処理するトラフィックと、リダイレクションをバイパスするトラフィックが定義されます。この設定は、SSIDを作成し、インベントリからWLCをプロビジョニングした後で、WLCにプッシュされます。これを表示するには、Configuration > Security > ACLの順に移動します。Catalyst CenterがリダイレクトACLに使用するACLの名前は、Cisco DNA_ACL_WEBAUTH_REDIRECTです。

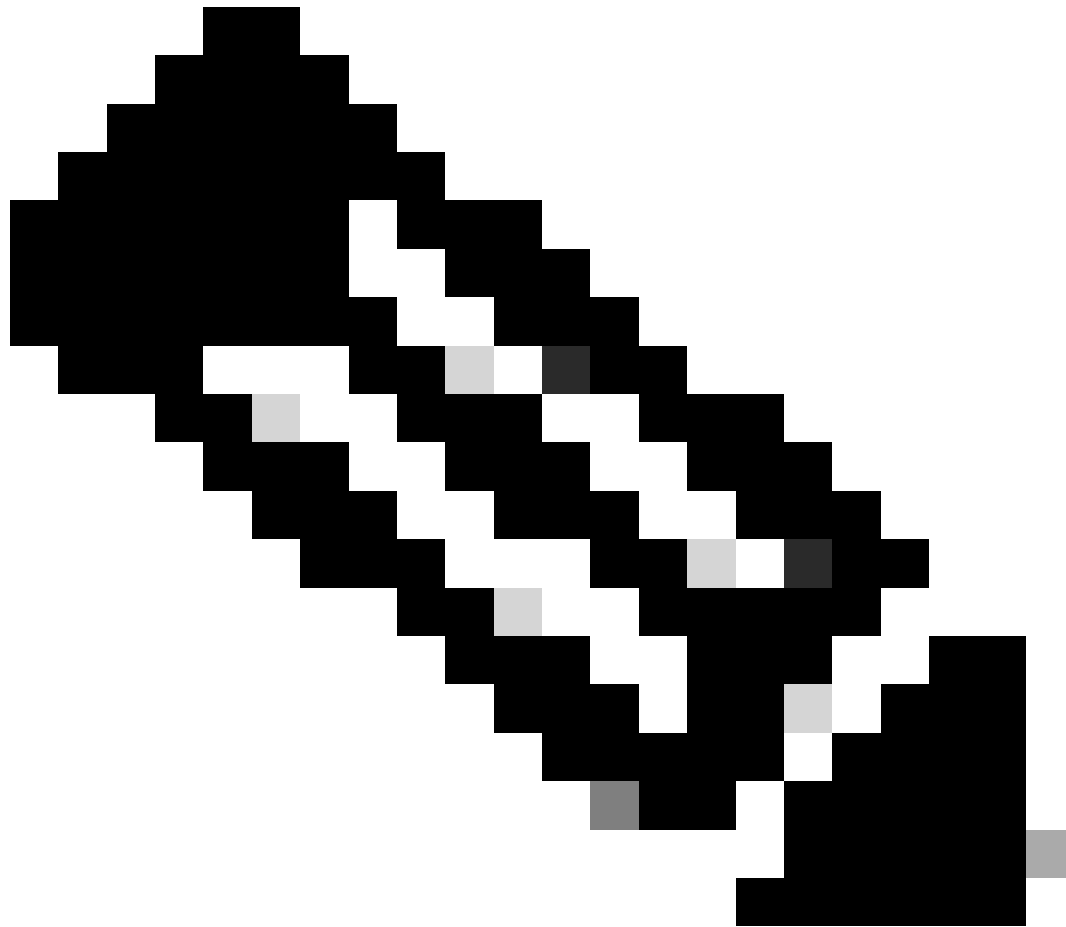
ACL Name	ACL Type	ACE Count	Downloaded ACL
☐ DNAC_ACL_WEBAUTH_REDIRECT	IPv4 Extended	9	No

1 10

名前をクリックすると、設定が表示されます。値は、Catalyst Centerのサイトのネットワーク設定のネットワーク設定から取得されます。

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
☐ 1	deny	8.8.8.8		any		udp	eq bootps	eq bootpc	None	Disable
☐ 2	deny	any		8.8.8.8		udp	eq bootpc	eq bootps	None	Disable
☐ 3	deny	1.1.1.1		any		udp	eq bootps	eq bootpc	None	Disable
☐ 4	deny	any		1.1.1.1		udp	eq bootpc	eq bootps	None	Disable
☐ 5	deny	9.9.9.9		any		udp	eq bootps	eq bootpc	None	Disable
☐ 6	deny	any		9.9.9.9		udp	eq bootpc	eq bootps	None	Disable
☐ 7	deny	10.88.244.180		any		ip	None	None	None	Disable
☐ 8	deny	any		10.88.244.180		ip	None	None	None	Disable
☐ 9	permit	any		any		tcp	0 - 65535	eq www	None	Disable

1 10 1 - 9 of 9 items



注：これらの値は、Catalyst Centerで設定されているサイトのネットワーク設定から取得され、DHCP/DNS値はWLANで設定されているプールから取得されます。ISE PSN IPアドレスは、SSIDワークフロー内のAAA設定で参照されます。

WLC CLIでリダイレクションACLを表示するには、次のコマンドを実行します。

<#root>

WLC#show ip access-lists Cisco DNA_ACL_WEBAUTH_REDIRECT

```
Extended IP access list Cisco DNA_ACL_WEBAUTH_REDIRECT
1 deny udp host 8.8.8.8 eq bootps any eq bootpc
2 deny udp any eq bootpc host 8.8.8.8 eq bootps
3 deny udp host 1.1.1.1 eq bootps any eq bootpc
4 deny udp any eq bootpc host 1.1.1.1 eq bootps
5 deny udp host 9.9.9.9 eq bootps any eq bootpc
6 deny udp any eq bootpc host 9.9.9.9 eq bootps
7 deny ip host 10.88.244.180 any
8 deny ip any host 10.88.244.180
9 permit tcp any range 0 65535 any eq www
```


リダイレクトACLをFlex Profileに適用して、アクセスポイントに送信できます。このコマンドを実行して、この設定を確認します

```
<#root>
```

```
WLC#show running-config | section flex
```

```
wireless profile flex default-flex-profile
```

```
  acl-policy Cisco DNA_ACL_WEBAUTH_REDIRECT
```

```
central-webauth
```

```
urlfilter list Cisco DNA_ACL_WEBAUTH_REDIRECT
```

アクセスポイントでのACLのリダイレクト

アクセスポイントでは、permitとdenyの値が逆になっています。permitはトラフィックの転送を示し、denyはリダイレクトを示しています。AP上のリダイレクトACLの設定を確認するには、次のコマンドを実行します。

```
<#root>
```

```
AP#sh ip access-lists
```

```
Extended IP access list Cisco DNA_ACL_WEBAUTH_REDIRECT
```

```
1 permit udp 8.8.8.8 0.0.0.0 dhcp_server any eq 68
```

```
2 permit udp any dhcp_client 8.8.8.8 0.0.0.0 eq 67
```

```
3 permit udp 1.1.1.1 0.0.0.0 dhcp_server any eq 68
```

```
4 permit udp any dhcp_client 1.1.1.1 0.0.0.0 eq 67
```

```
5 permit udp 9.9.9.9 0.0.0.0 dhcp_server any eq 68
```

```
6 permit udp any dhcp_client 9.9.9.9 0.0.0.0 eq 67
```

```
7 permit ip 10.88.244.180 0.0.0.0 any
```

```
8 permit ip any 10.88.244.180 0.0.0.0
```

```
9 deny tcp any range 0 65535 any eq 80
```

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。