

ISEからActive Directoryへのグループマップに基づくWLCを使用したダイナミックVLAN割り当ての設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[RADIUS サーバによるダイナミック VLAN 割り当て](#)

[設定](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[ISE と AD の統合および ISE でのユーザー認証と認証ポリシーの設定](#)

[SSID「office_hq」のdot1x認証およびAAAオーバーライドをサポートするWLC設定](#)

[確認](#)

[トラブルシューティング](#)

はじめに

このドキュメントでは、ダイナミック VLAN 割り当ての概念について説明します。

前提条件

このドキュメントでは、ワイヤレスLAN(WLAN)クライアントを特定のVLANにダイナミックに割り当てるようにワイヤレスLANコントローラ(WLC)とIdentity Services Engine(ISE)サーバを設定する方法について説明します。

要件

次の項目に関する知識があることが推奨されます。

- ワイヤレスLANコントローラ(WLC)とLightweightアクセスポイント(LAP)に関する基礎知識
- ISEなどの認証、認可、アカウントリング(AAA)サーバの機能に関する知識
- ワイヤレス ネットワークとワイヤレスのセキュリティ問題に関する全般的な知識
- ダイナミックVLAN割り当てに関する実践的で構成可能な知識
- Microsoft Windows ADサービス、ドメインコントローラ、およびDNSの概念に関する基本的な知識

- アクセスポイントプロトコルのコントロールとプロビジョニング (CAPWAP) に関する基礎知識

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。

- ファームウェア リリース 8.8.111.0 が稼働する Cisco 5520 シリーズ WLC
- Cisco 4800 シリーズ AP
- ネイティブ Windows サプリカントおよび Anyconnect NAM
- Cisco Secure ISE バージョン 2.3.0.298
- ドメイン コントローラとして設定された Microsoft Windows 2016 Server
- Cisco 2950 シリーズ スイッチバージョン 15.2(4)E1

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。

表記法

表記法の詳細については、『[シスコテクニカルティップスの表記法](#)』を参照してください。

RADIUS サーバによるダイナミック VLAN 割り当て

一般的な WLAN システムでは、Service Set Identifier (SSID) (コントローラの用語では WLAN) に関連付けられたすべてのクライアントに適用されるスタティックなポリシーが各 WLAN に存在します。この方式は強力ですが、異なる QoS ポリシーやセキュリティ ポリシーを継承するために各クライアントを異なる SSID に関連付ける必要があるため、さまざまな制約があります。

シスコの WLAN ソリューションは、ID ネットワーキングのサポートによってこの制限に対処します。これにより、ネットワークは単一の SSID をアドバタイズできますが、ユーザ クレデンシャルに基づいて、特定のユーザが異なる QoS、VLAN 属性、セキュリティ ポリシーを継承できるようになります。

ダイナミック VLAN 割り当ては、ユーザが入力したクレデンシャルに基づいてワイヤレス ユーザを特定の VLAN に割り当てる機能です。ユーザを特定の VLAN に割り当てるタスクは、Cisco ISE などの RADIUS 認証サーバによって処理されます。たとえば、これを利用すると、キャンパス ネットワーク内を移動するワイヤレス ホストを同じ VLAN に割り当てることができます。

Cisco ISE サーバは、内部データベースを含む複数のデータベースの1つに対してワイヤレスユー

ザを認証します。例：

- 内部 DB
- Active Directory
- 汎用の Lightweight Directory Access Protocol (LDAP)
- Open Database Connectivity (ODBC) に準拠したリレーショナル データベース
- Rivest, Shamir, and Adelman (RSA) SecurID トークン サーバ
- RADIUS に準拠したトークン サーバ

[Cisco ISE 認証プロトコルとサポートされている外部 ID ソース](#)には、ISE 内部および外部データベースでサポートされるさまざまな認証プロトコルが記載されています。

このドキュメントでは、Windows Active Directory(AD)外部データベースを使用するワイヤレスユーザの認証について説明します。

認証に成功すると、ISEはWindowsデータベースからそのユーザのグループ情報を取得し、ユーザをそれぞれの認可プロファイルに関連付けます。

クライアントがコントローラに登録されているLAPとの関連付けを試みると、LAPからWLCに対して、それぞれのEAP方式を使用してユーザのクレデンシャルが渡されます。

WLCは (EAPをカプセル化して) RADIUSプロトコルを使用してこれらのクレデンシャルをISEに送信し、ISEはKERBEROSプロトコルを使用して検証のためにユーザのクレデンシャルをADに渡します。

AD では、そのユーザークレデンシャルを検証し、認証に成功した場合は ISE に通知します。

認証に成功すると、ISE サーバーから WLC に特定の Internet Engineering Task Force (IETF) 属性が渡されます。これらのRADIUS属性により、ワイヤレスクライアントに割り当てる必要があるVLAN IDが決まります。ユーザはこの事前設定済みの VLAN ID に常に割り当てられるので、クライアントの SSID (WLC の用語では WLAN) は無視されます。

VLAN ID の割り当てに使用される RADIUS ユーザ属性は次のとおりです。

- IETF 64 (トンネルタイプ) —これをVLANに設定します
- IETF 65 (トンネルメディアムタイプ) —これを802に設定
- IETF 81 (トンネルプライベートグループID) —これをVLAN IDに設定します

VLAN ID は 12 ビットで、1 ~ 4094 の値 (両端の値を含む) を取ります。RFC 2868 で定義されているように、IEEE 802.1X で使用される Tunnel-Private-Group-ID は文字列型であるため、VLAN ID の整数値は文字列としてエンコードされます。これらのトンネル属性が送信される際には、Tag フィールドの値を設定する必要があります。

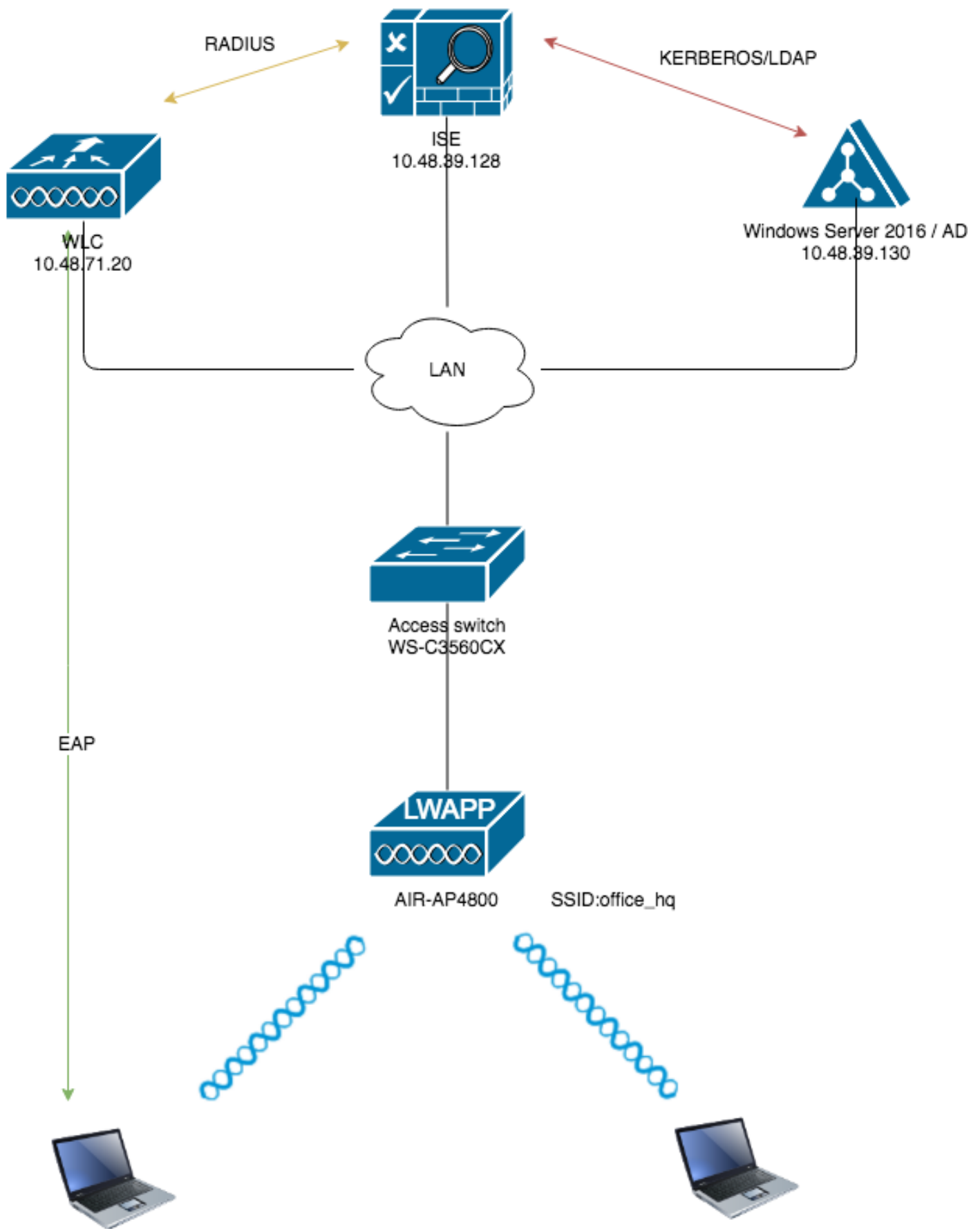
[RFC 2868](#)のセクション3.1で述べられているように、Tagフィールドは1オクテットの長さを持ち

、同じトンネルを参照する同じパケット内の属性をグループ化する手段を提供することを目的としています。このフィールドで有効な値は、0x01 ~ 0x1F (両端を含む) です。Tag フィールドを使用しない場合は、このフィールドをゼロ (0x00) に設定する必要があります。すべての RADIUS 属性の詳細は、[RFC 2868](#) を参照してください。

設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供します。

ネットワーク図



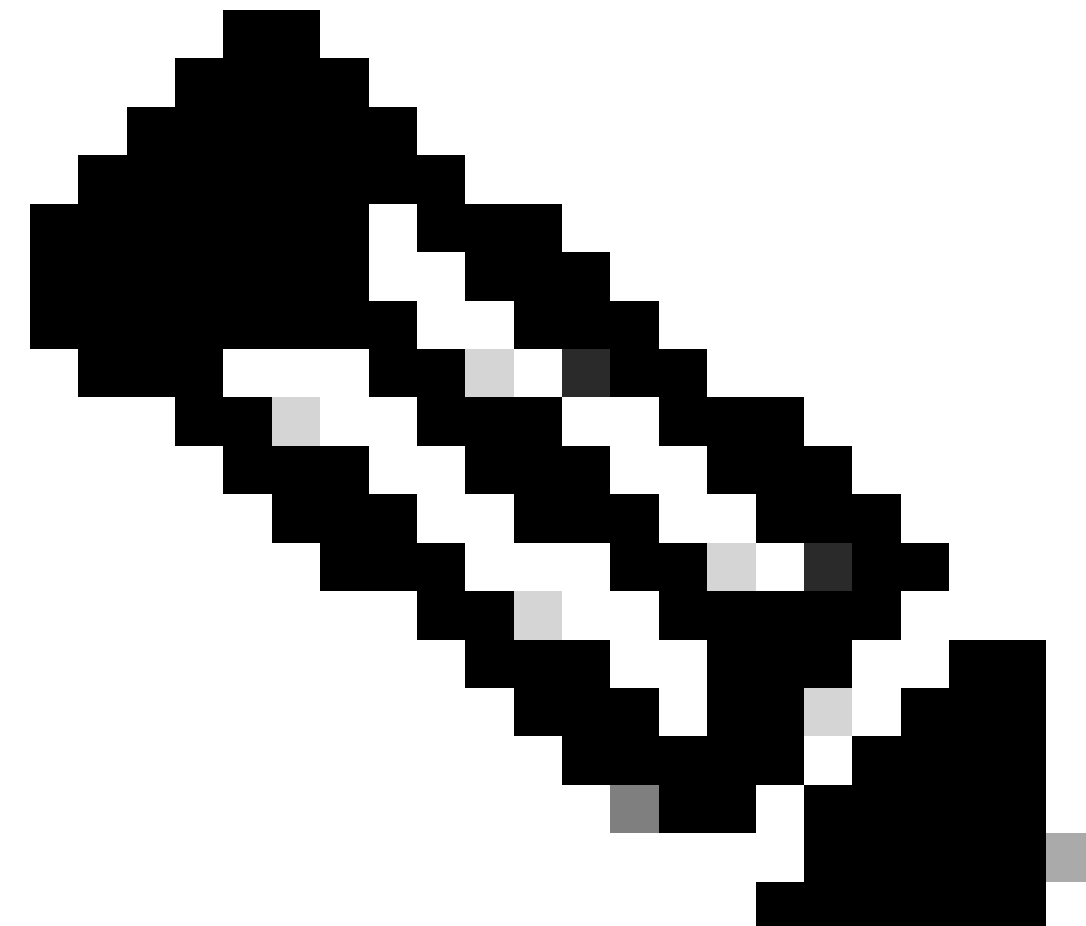
コンフィギュレーション

この図で使用されているコンポーネントの設定の詳細は、次のとおりです。

- ISE(RADIUS)サーバのIPアドレスは10.48.39.128です。
- WLC の管理インターフェイスおよび AP マネージャ インターフェイスのアドレスは 10.48.71.20 です。
- DHCPサーバはLANネットワークにあり、クライアントプールごとに設定されます。図には示されていません。
- VLAN1477 と VLAN1478 は、この設定全体で使用されます。マーケティング部門のユーザはVLAN1477に配置されるように設定され、人事部門のユーザはRADIUSサーバによってVLAN1478に配置されるように設定されます 両方のユーザが同じSSID(office_hq)に接続する場合.

VLAN1477:192.168.77.0/24。ゲートウェイ : 192.168.77.1 VLAN1478:192.168.78.0/24ゲートウェイ : 192.168.78.1

- このドキュメントでは、セキュリティメカニズムとしてPEAP-mschapv2 802.1xを使用します。
-



注 : シスコでは、WLANを保護するために、EAP-FAST認証やEAP-TLS認証などの高度な

認証方式を使用することを推奨しています。

これらの前提は、この設定を実行する前に実施済みです。

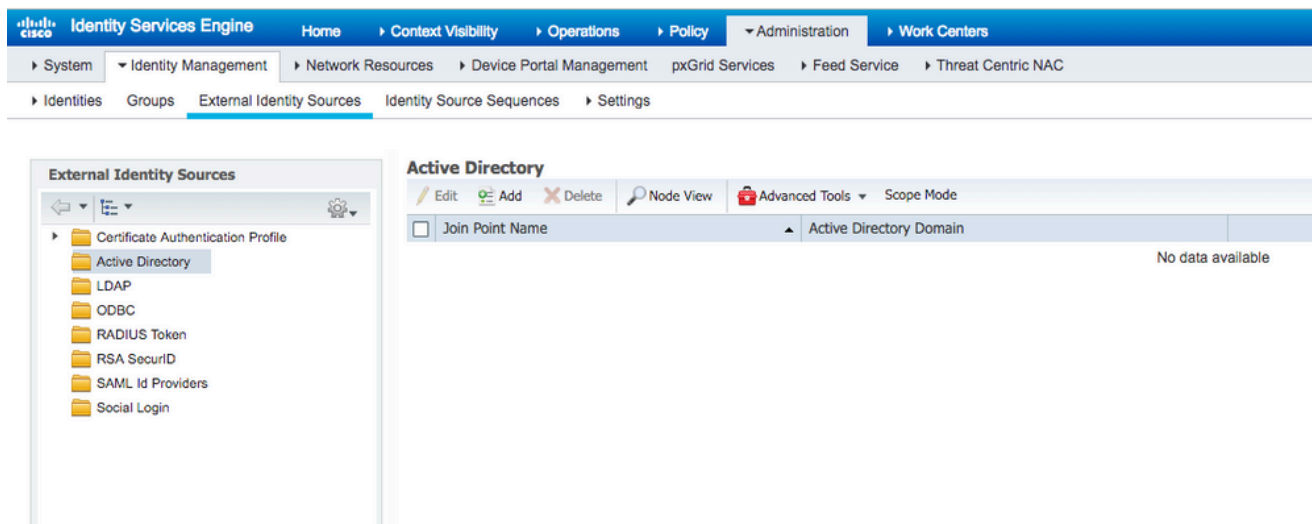
- LAPはすでにWLCに登録されています
- DHCPサーバにDHCPスコープが割り当てられている
- ネットワーク内のすべてのデバイス間にレイヤ3接続が存在する
- このドキュメントでは、ワイヤレス側で必要な設定について説明し、有線ネットワークが確立されていることを前提としています
- それぞれのユーザとグループはADで設定されます

ISE と AD のグループマッピングに基づいて、WLC でダイナミック VLAN 割り当てを行うには、次の手順を実行する必要があります。

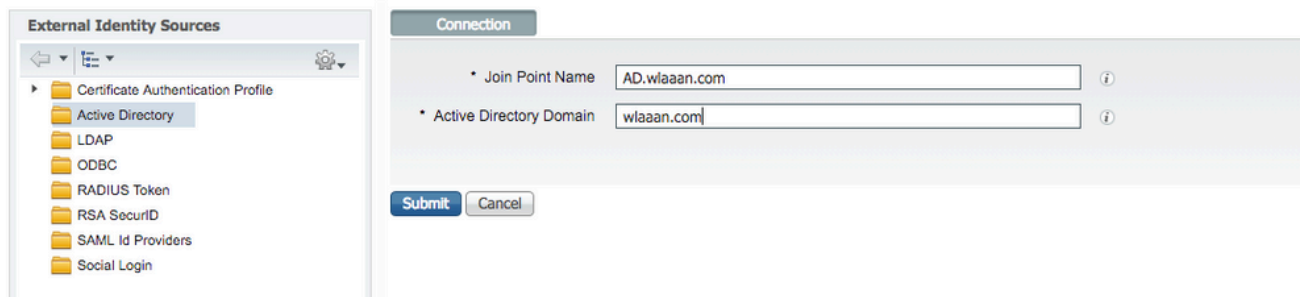
1. ISE と AD の統合および ISE でのユーザー認証と認証ポリシーの設定。
2. SSID 「office_hq」 のdot1x認証およびAAAオーバーライドをサポートするためのWLC設定。
3. エンドクライアントのサブリカントの設定。

ISE と AD の統合および ISE でのユーザー認証と認証ポリシーの設定

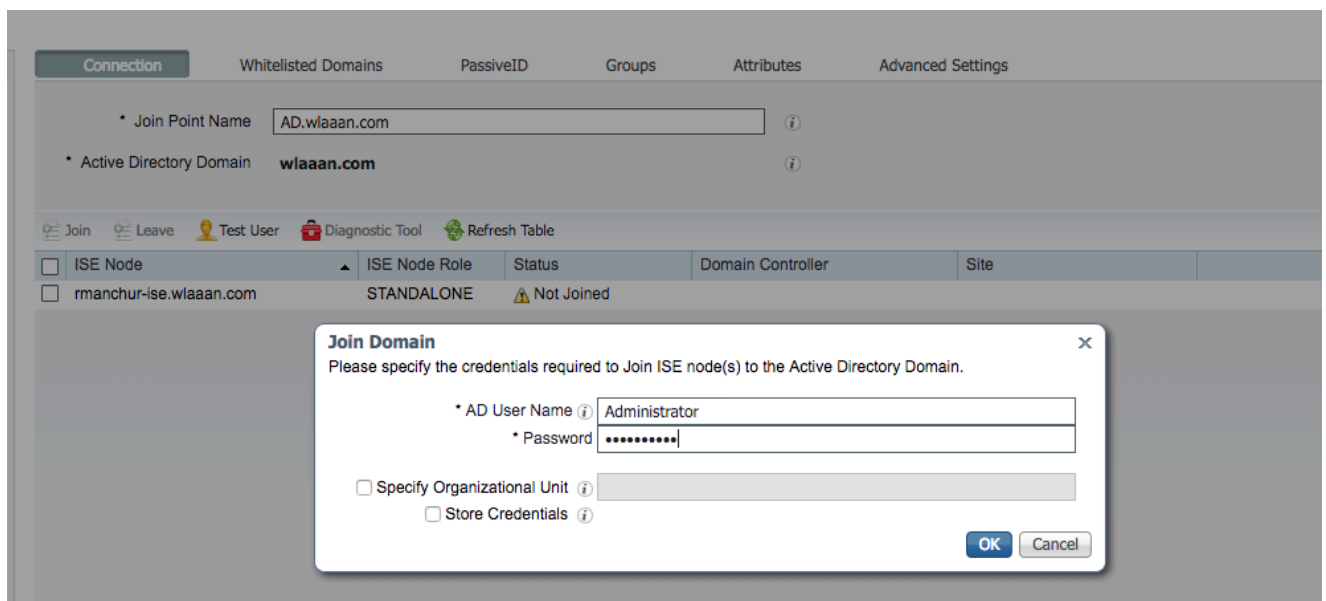
1. adminアカウントを使用してISE Web UIインターフェイスにログインします。
2. Administration > Identity management > External Identity Sources > Active directoryに移動します。



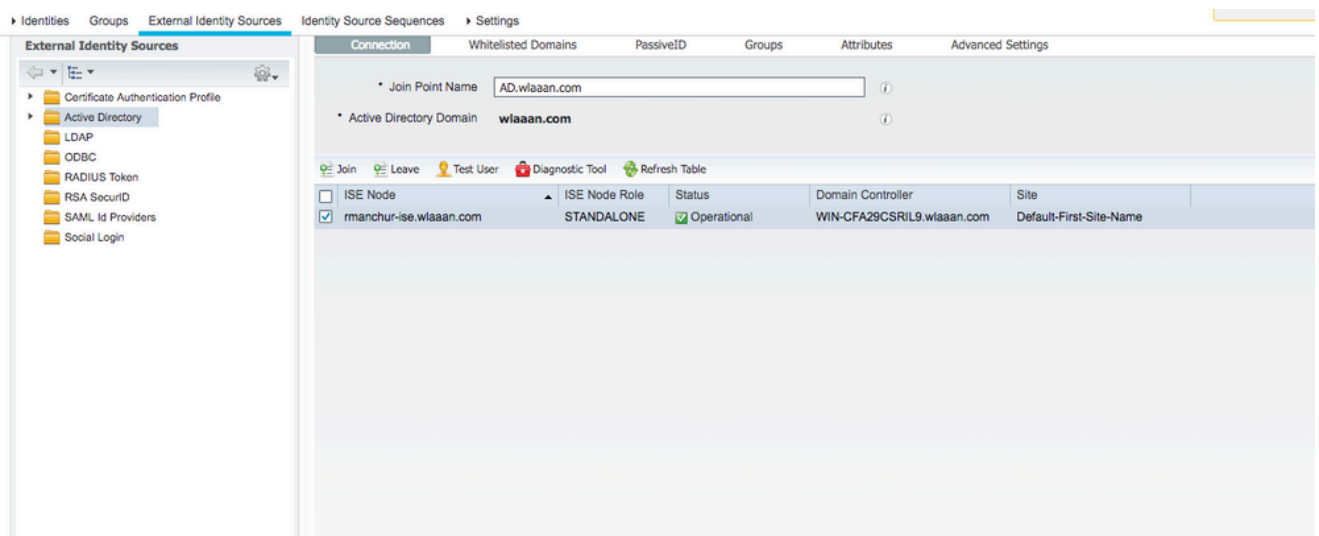
3. Addをクリックし、Active Directory Join Point Name設定でドメイン名とIDストア名を入力します。この例では、ISEがドメインに登録されwlaaan.com、ジョインポイントがAD.wlaaan.comとして指定されます。ローカルで有効なISE名です。



4. Submitのボタンを押すと、ポップアップウィンドウが開き、ISEをすぐにADに参加させるかどうかを尋ねられます。Yesを押し、Active Directoryユーザクレデンシャルと管理者権限を入力して、ドメインに新しいホストを追加します。



5. この時点を過ぎると、ISEがADに正常に登録されます。

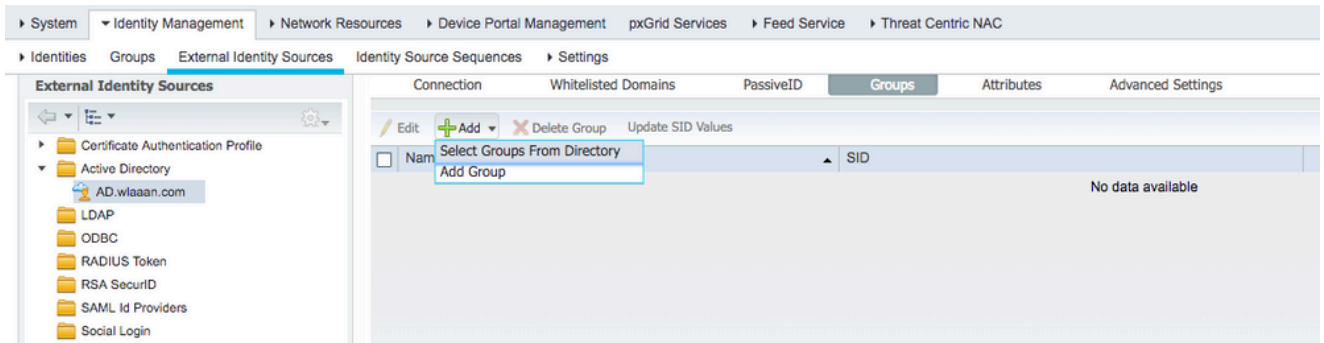


登録プロセスに問題がある場合は、Diagnostic Tool を使用して、AD接続に必要なテストを実行できます。

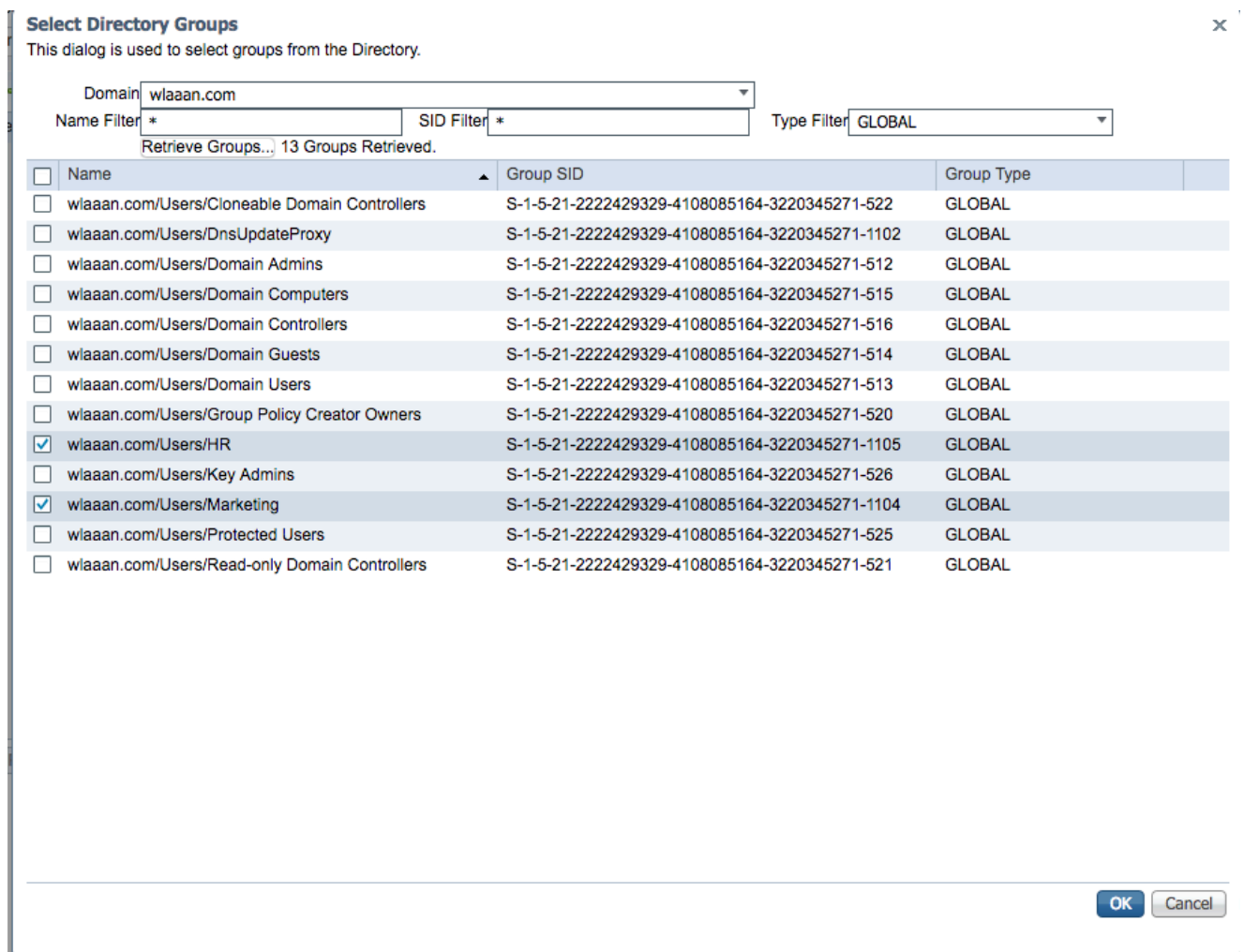
6. それぞれの認可プロファイルを割り当てるために使用されるアクティブなディレクトリのグループを取得する必要があります。Administration > Identity management > External Identity Sources > Active directory >

> Groups

に移動し、をクリックしてAddを選択Select Groups from Active Directoryします。



7. 新しいポップアップウィンドウが開き、特定のグループを取得するためのフィルタを指定するか、ADからすべてのグループを取得することができます。ADグループリストからそれぞれのグループを選択し、OKを押します。



8. それぞれのグループがISEに追加され、保存できます。と入力します。 Save

Connection	Whitelisted Domains	PassiveID	Groups	Attributes	Advanced Settings
Edit + Add x Delete Group Update SID Values					
<input type="checkbox"/>	Name	SID			
<input type="checkbox"/>	wlaaan.com/Users/HR	S-1-5-21-2222429329-4108085164-3220345271-1105			
<input type="checkbox"/>	wlaaan.com/Users/Marketing	S-1-5-21-2222429329-4108085164-3220345271-1104			

Save Reset

9. ISEネットワークデバイスリストへのWLCの追加：Administration > Network Resources > Network Devicesに移動し、Addを押します。
 WLCとISE間のWLC管理IPアドレスとRADIUS共有秘密を指定して、設定を完了します。

Cisco Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers
 System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC
 Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network Devices List > New Network Device

Network Devices

* Name: WLC5520
 Description:

IP Address: * IP: 10.48.71.20 / 32

IPv6 is supported only for TACACS. At least one IPv4 must be defined when RADIUS is selected

* Device Profile: Cisco
 Model Name:
 Software Version:

* Network Device Group

Location: LAB Set To Default
 IPSEC: Is IPSEC Device Set To Default
 Device Type: WLC-lab Set To Default

RADIUS Authentication Settings

RADIUS UDP Settings

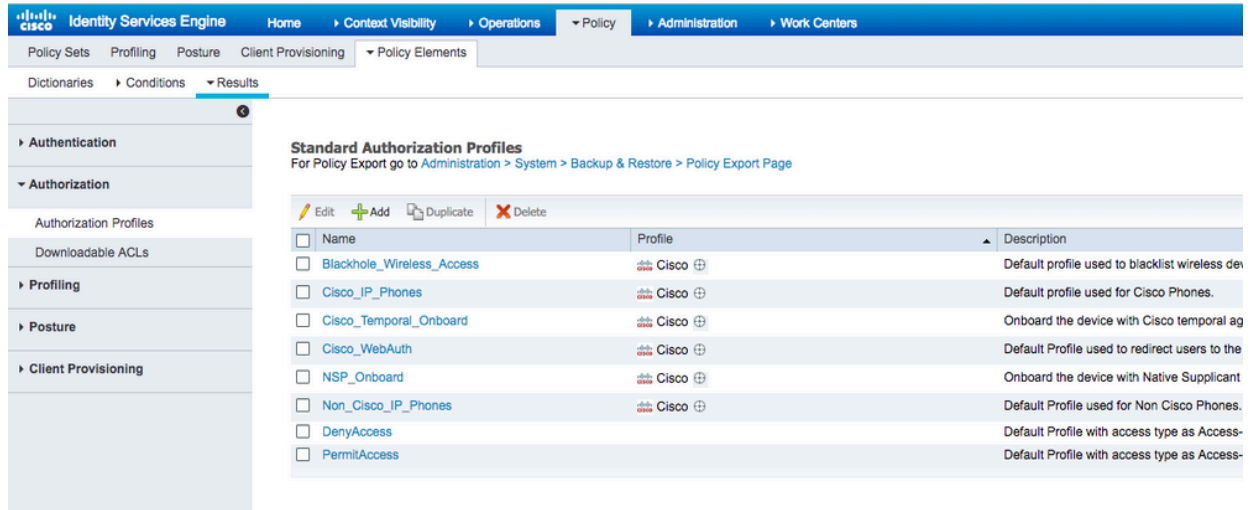
Protocol: RADIUS
 * Shared Secret: ***** Show
 CoA Port: 1700 Set To Default

RADIUS DTLS Settings [?](#)

10. ISEをADに参加させ、デバイスリストにWLCを追加した後、ユーザの認証ポリシーと認可ポリシーの設定を開始できます。

- MarketingからVLAN1477に、またHRグループからVLAN1478にユーザを割り当てるには、認可プロファイルを作成します。

新しいプロファイルを作成するには、 Policy > Policy Elements > Results > Authorization > Authorization profiles に移動し、 Add ボタンをクリックします。



The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The main content area is titled 'Standard Authorization Profiles' and includes a sub-header 'For Policy Export go to Administration > System > Backup & Restore > Policy Export Page'. Below this, there are action buttons for 'Edit', '+ Add', 'Duplicate', and 'Delete'. A table lists several authorization profiles:

Name	Profile	Description
<input type="checkbox"/> Blackhole_Wireless_Access	Cisco	Default profile used to blacklist wireless dev
<input type="checkbox"/> Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.
<input type="checkbox"/> Cisco_Temporal_Onboard	Cisco	Onboard the device with Cisco temporal ag
<input type="checkbox"/> Cisco_WebAuth	Cisco	Default Profile used to redirect users to the
<input type="checkbox"/> NSP_Onboard	Cisco	Onboard the device with Native Supplicant
<input type="checkbox"/> Non_Cisco_IP_Phones	Cisco	Default Profile used for Non Cisco Phones.
<input type="checkbox"/> DenyAccess		Default Profile with access type as Access-
<input type="checkbox"/> PermitAccess		Default Profile with access type as Access-

- 各グループのVLAN情報を使用して認可プロファイルの設定を完了します。この例ではMarketingグループの設定を示します。

Dictionarys > Conditions > Results

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name:

Description:

* Access Type:

Network Device Profile:

Service Template:

Track Movement:

Passive Identity Tracking:

Common Tasks

DACL Name

ACL (Filter-ID)

Security Group

VLAN Tag ID 1 ID/Name

Advanced Attributes Settings

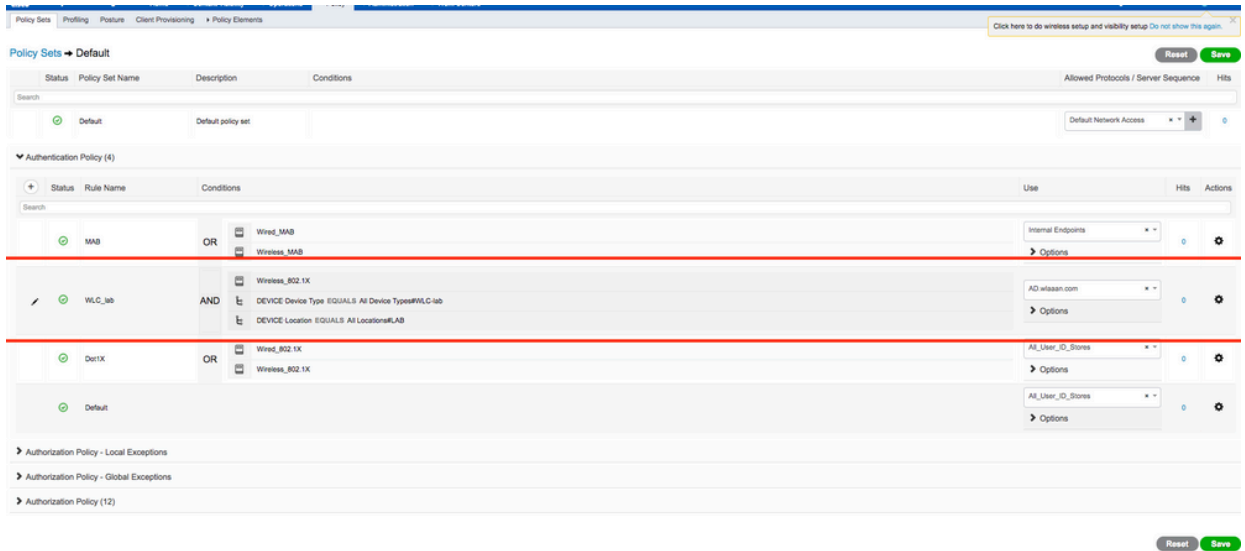
=

Attributes Details

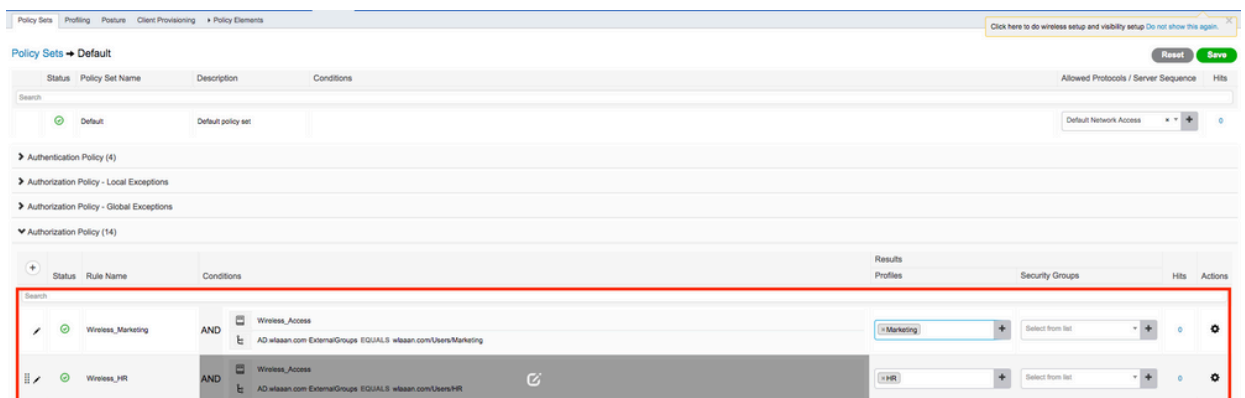
Access Type = ACCESS_ACCEPT
 Tunnel-Private-Group-ID = 1:1477
 Tunnel-Type = 1:13
 Tunnel-Medium-Type = 1:6

他のグループについても同様の設定を行い、それぞれのVLANタグ属性を設定する必要があります。

- 認可プロファイルを設定した後、ワイヤレスユーザの認証ポリシーを定義できます。この操作は、ポリシーセットを設定CustomDefault するか、変更することで実行できます。この例では、デフォルトポリシーセットを変更します。Policy > Policy Sets > Defaultに移動します。dot1x認証タイプのデフォルトではAll_User_ID_Storesが使用されますが、ADはAll_User_ID_StoresWLC_lab のアイデンティティソースリストの一部であるため、現在のデフォルト設定でも機能します。この例では、それぞれのLABコントローラに対してより具体的なルールを使用し、認証の唯一のソースとしてADを使用します。



- 次に、グループメンバーシップに基づいてそれぞれの認可プロファイルを割り当てるユーザの認可ポリシーを作成する必要があります。Authorization policyのセクションに移動し、この要件を満たすためにポリシーを作成します。



SSID「office_hq」のdot1x認証およびAAAオーバーライドをサポートするWLC設定

1. WLC上のRADIUS認証サーバとしてISEを設定します。Web UIインターフェイスのSecurity > AAA > RADIUS > Authenticationセクションに移動し、ISE IPアドレスと共有秘密情報を指定します

○

Security

- AAA
 - General
 - RADIUS
 - Authentication
 - Accounting
 - Auth Cached Users
 - Fallback
 - DNS
 - Downloaded AVP
 - TACACS+
 - LDAP
 - Local Net Users
 - MAC Filtering
 - Disabled Clients
 - User Login Policies
 - AP Policies
 - Password Policies
- Local EAP
- Advanced EAP
- Priority Order
- Certificate
- Access Control Lists
- Wireless Protection Policies
- Web Auth
- TrustSec
 - Local Policies
 - Umbrella
 - Advanced

RADIUS Authentication Servers > New

Server Index (Priority): 2

Server IP Address(Ipv4/Ipv6): 10.48.39.128

Shared Secret Format: ASCII

Shared Secret: [Redacted]

Confirm Shared Secret: [Redacted]

Apply Cisco ISE Default settings:

Apply Cisco ACA Default settings:

Key Wrap: (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Port Number: 1812

Server Status: Enabled

Support for CoA: Enabled

Server Timeout: 5 seconds

Network User: Enable

Management: Enable

Management Retransmit Timeout: 5 seconds

Tunnel Proxy: Enable

PAC Provisioning: Enable

IPSec: Enable

Cisco ACA: Enable

2. WLCのWLANsセクションでSSID`office_hq`を設定します。この例では、SSIDにWPA2/AES+dot1xおよびAAAの上書きを設定しています。適切なVLANはRADIUSを介して割り当てられるため、WLANには`interfaceDummy`が選択されます。このダミーインターフェイスをWLC上に作成し、IPアドレスを割り当てる必要がありますが、IPアドレスが有効である必要はなく、また配置するVLANをアップリンクスイッチ内に作成することもできないため、VLANが割り当てられていない場合は、クライアントはどこにも移動できません。

WLANs

Current Filter: None [\[Change Filter\]](#) [\[Clear Filter\]](#) Create New

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	test	test	Enabled	[WPA2][Auth(802.1X)]
2	WLAN	AndroidAP	AndroidAP	Enabled	[WPA2][Auth(PSK)]
253	WLAN	BTER-BTwifi-public	BTwifi-public	Enabled	[WPA2][Auth(PSK)]

WLANs > New

Type: WLAN

Profile Name: office_hq

SSID: office_hq

ID: 3

WLANS > Edit 'office_hq'

General | Security | QoS | Policy-Mapping | Advanced

Profile Name: office_hq
Type: WLAN
SSID: office_hq
Status: Enabled
Security Policies: [WPA2][Auth(802.1X)]
(Modifications done under security tab will appear after applying the changes.)
Radio Policy: All
Interface/Interface Group: dummy
Multicast Vlan Feature: Enabled
Broadcast SSID: Enabled
NAS-ID: none

WLANS > Edit 'office_hq'

General | Security | QoS | Policy-Mapping | Advanced

Layer 2 | Layer 3 | AAA Servers

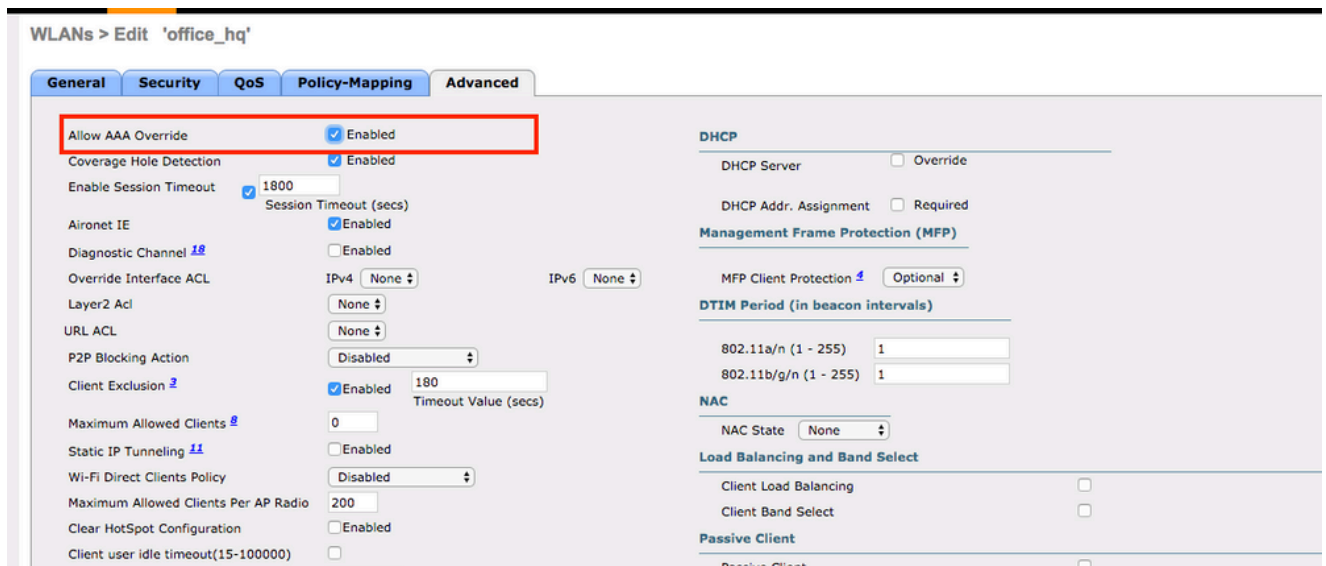
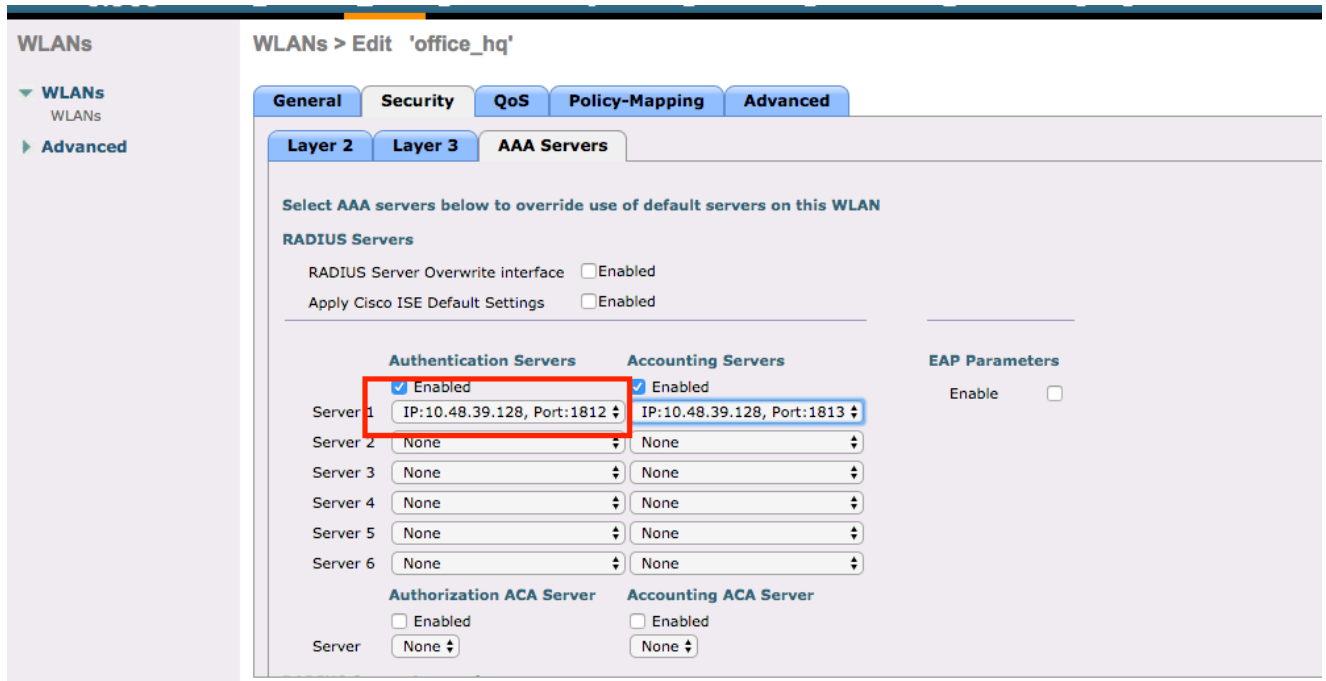
Layer 2 Security: WPA+WPA2
MAC Filtering:

Fast Transition
Fast Transition Over the DS: Adaptive
Reassociation Timeout: 20 Seconds

Protected Management Frame
PMF: Disabled

WPA+WPA2 Parameters
WPA Policy:
WPA2 Policy:
WPA2 Encryption: AES TKIP CCMP256 GCMP128 GCMP256
OSEN Policy:

Authentication Key Management
802.1X: Enable
CCKM: Enable



3. また、ユーザVLAN用のダイナミックインターフェイスをWLC上で作成する必要があります。Controller > Interfaces UIメニューに移動します。WLCは、そのVLANにダイナミックインターフェイスがある場合にのみ、AAA経由で受信したVLANの割り当てを受け入れます。

The screenshot shows the Cisco Controller configuration page for interface **vlan1477**. The interface name is highlighted in red. The configuration includes:

- General Information:** Interface Name: **vlan1477**, MAC Address: 00:a3:8e:e3:5a:1a
- Configuration:** Guest Lan, Quarantine, Quarantine Vlan Id (0), NAS-ID (none)
- Physical Information:** Port Number (1), Backup Port (0), Active Port (1), Enable Dynamic AP Management (unchecked)
- Interface Address:** VLAN Identifier (1477), IP Address (192.168.77.5), Netmask (255.255.255.0), Gateway (192.168.77.1), IPv6 Address (::), Prefix Length (128), IPv6 Gateway (::), Link Local IPv6 Address (fe80::2a3:8eff:fee3:5a1a/64)
- DHCP Information:** Primary DHCP Server (192.168.77.1), Secondary DHCP Server, DHCP Proxy Mode (Global)

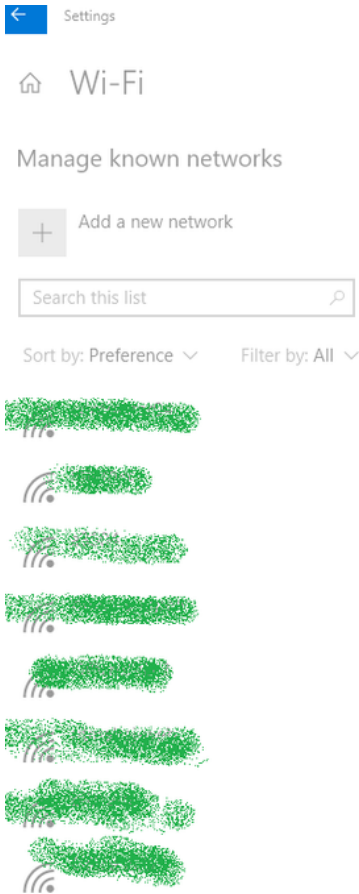
確認

接続をテストするには、Windows 10ネイティブサブリカントとAnyconnect NAMを使用します。

EAP-PEAP認証を使用しており、ISEが自己署名証明書(SSC)を使用しているため、証明書の警告に同意するか、証明書の検証を無効にする必要があります。企業環境では、ISEで署名済みの信頼できる証明書を使用し、エンドユーザデバイスに適切なルート証明書が信頼できるCAリストにインストールされていることを確認する必要があります。

Windows 10およびネイティブサブリカントとの接続をテストします。

1. Network & Internet settings > Wi-Fi > Manage known networksを開き、Add new networkボタンを押して新しいネットワークプロファイルを作成します。必要な情報を入力します。



Add a new network

Network name

Security type

EAP method

Authentication method

Connect automatically

Connect even if this network is not broadcasting

2. ISEの認証ログを確認し、ユーザに対して適切なプロファイルが選択されていることを確認します。

Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorization Policy	Authorizati...	IP Address	Network Device	Device Port	Identity Group	Posture St...	Server
Feb 15, 2019 02:16:43.300 PM	●		3	Bob	F4:8C:50:62:14:6B	Unknown	Default ==> W...	Default ==> Wireless_HR	HR						manchur-ise
Feb 15, 2019 02:09:56.389 PM	●			Bob	F4:8C:50:62:14:6B	Unknown	Default ==> W...	Default ==> Wireless_HR	HR		WLC5520		Unknown		manchur-ise

3. WLCでクライアントエントリをチェックし、エントリが正しいVLANに割り当てられ、RUN状態にあることを確認します。

Client MAC Addr	IP Address(Tx/Rx)	AP Name	WLAN Profile	WLAN SSID	User Name	Protocol	Status	Auth	Port	Slot Id	Tunnel	Fastlane
f4:8c:50:62:14:6b	192.168.78.36	AP4C77.609E.6162	office_hq	office_hq	Bob	802.11ac(5 GHz)	Associated	Yes	1	1	No	No

4. WLC CLIから、show client details
:

```
show client detail f4:8c:50:62:14:6b
Client MAC Address..... f4:8c:50:62:14:6b
Client Username ..... Bob
```

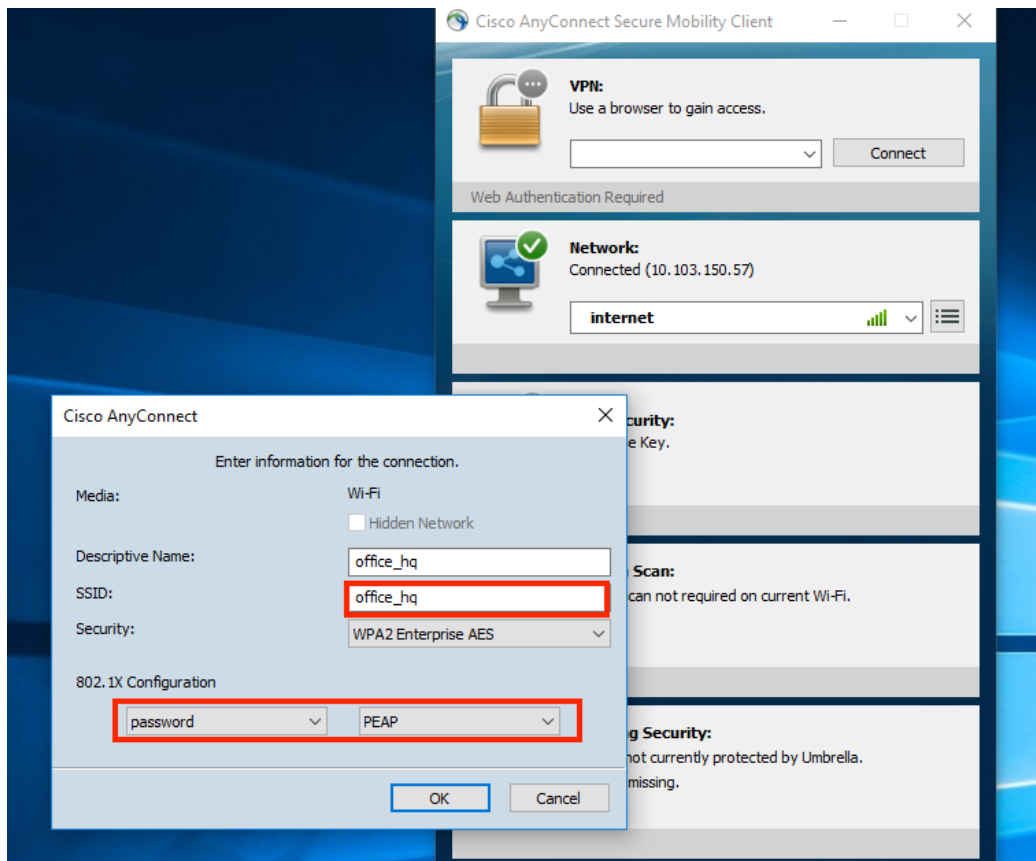
```

Client Webauth Username ..... N/A
Hostname: .....
Device Type: ..... Intel-Device
AP MAC Address..... 70:69:5a:51:4e:c0
AP Name..... AP4C77.6D9E.6162
AP radio slot Id..... 1
Client State..... Associated
User Authenticated by ..... RADIUS Server
Client User Group..... Bob
Client NAC OOB State..... Access
Wireless LAN Id..... 3
Wireless LAN Network Name (SSID)..... office_hq
Wireless LAN Profile Name..... office_hq
Hotspot (802.11u)..... Not Supported
Connected For ..... 242 secs
BSSID..... 70:69:5a:51:4e:cd
Channel..... 36
IP Address..... 192.168.78.36
Gateway Address..... 192.168.78.1
Netmask..... 255.255.255.0
...
Policy Manager State..... RUN
...
EAP Type..... PEAP
Interface..... vlan1478
VLAN..... 1478
Quarantine VLAN..... 0
Access VLAN..... 1478

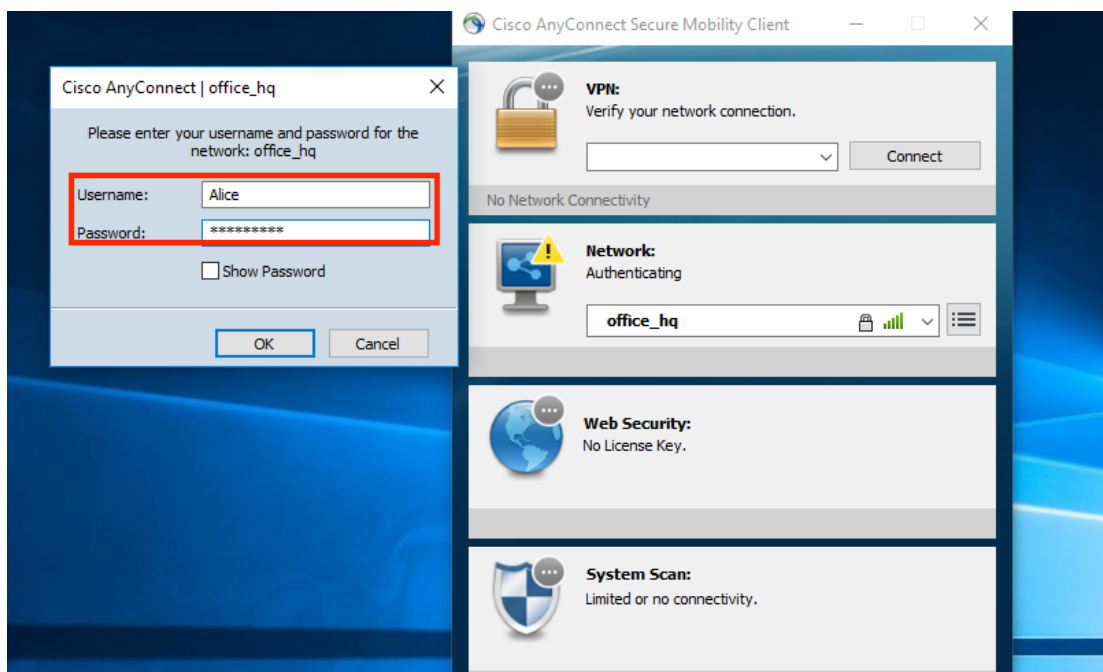
```

Windows 10およびAnyconnect NAMとの接続をテストします。

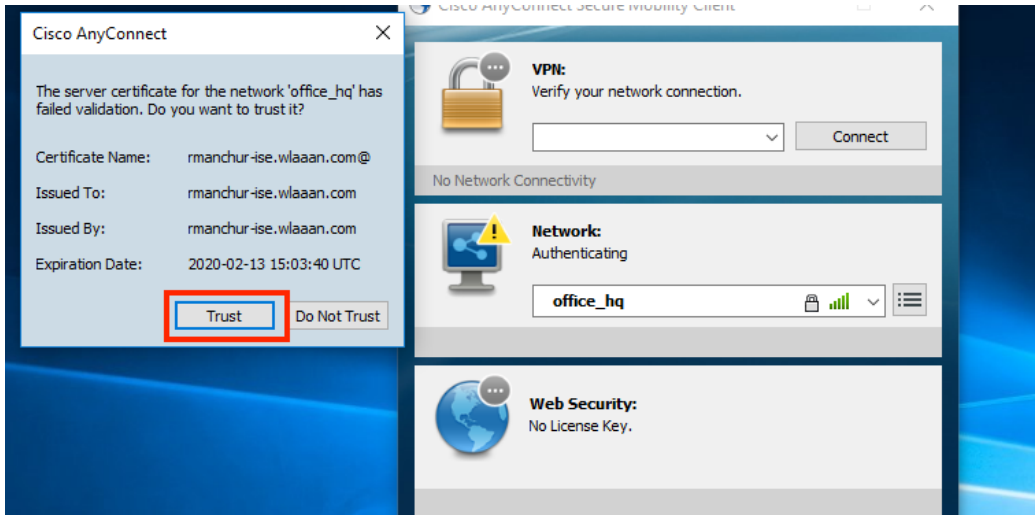
1. 使用可能なSSIDのリストからSSIDを選択し、それぞれのEAP認証タイプ (この例ではPEAP) と内部認証フォームを選択します。



2. ユーザー認証の対象となるユーザー名とパスワードを入力します。



3. ISEはSSCをクライアントに送信するため、証明書を信頼することを手動で選択する必要があります (実稼働環境では、信頼できる証明書をISEにインストールすることを強く推奨します)。



4. ISEの認証ログを確認し、ユーザに対して適切な認可プロファイルが選択されていることを確認します。

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorization Policy	Authorizati...	IP Address	Network Device	Device Port	Identity Group	Posture St...	Server	Mdm
Feb. 15, 2019 02:51:27.163 PM			0	Alice	F4:8C:50:62:14:6B	Monsoob-W...	Default >> ...	Default >> Wireless_Marketing	Marketing	192.168.77.32	Network Device	Device Port	Identity Group	Posture Status	Server	Mdm
Feb. 15, 2019 02:51:24.837 PM				Alice	F4:8C:50:62:14:6B	Monsoob-W...	Default >> ...	Default >> Wireless_Marketing	Marketing		WLC5520		Workstation			manchur-ise

5. WLCでクライアントエントリをチェックし、エントリが正しいVLANに割り当てられ、RUN状態にあることを確認します。

Client MAC Addr	IP Address(Ipv4/Ipv6)	AP Name	WLAN Profile	WLAN SSID	User Name	Protocol	Status	Auth	Port	Slot Id	Tunnel
f4:8c:50:62:14:6b	192.168.77.32	AP4C77.6D9E.6162	office_hq	office_hq	Alice	802.11ac(5 GHz)	Associated	Yes	1	1	No

6. WLC CLIから、show client details

:

```
Client MAC Address..... f4:8c:50:62:14:6b
Client Username ..... Alice
Client Webauth Username ..... N/A
Hostname: .....
Device Type: ..... Intel-Device
AP MAC Address..... 70:69:5a:51:4e:c0
AP Name..... AP4C77.6D9E.6162
AP radio slot Id..... 1
```

```

Client State..... Associated
User Authenticated by ..... RADIUS Server
Client User Group..... Alice
Client NAC OOB State..... Access
Wireless LAN Id..... 3
Wireless LAN Network Name (SSID)..... office_hq
Wireless LAN Profile Name..... office_hq
Hotspot (802.11u)..... Not Supported
Connected For ..... 765 secs
BSSID..... 70:69:5a:51:4e:cd
Channel..... 36
IP Address..... 192.168.77.32
Gateway Address..... 192.168.77.1
Netmask..... 255.255.255.0
...
Policy Manager State..... RUN
...
Policy Type..... WPA2
Authentication Key Management..... 802.1x
Encryption Cipher..... CCMP-128 (AES)
Protected Management Frame ..... No
Management Frame Protection..... No
EAP Type..... PEAP
Interface..... vlan1477
VLAN..... 1477

```

トラブルシューティング

1. WLCとISEの間のRADIUS接続をテストするには `test aaa radius username`

```
password
```

```
wlan-id
```

を使用し、結果を表示するには `test aaa show radius` を使用します。

```
test aaa radius username Alice password <removed> wlan-id 2
```

```
Radius Test Request
```

```
Wlan-id..... 2
ApGroup Name..... none
```

Attributes	Values
-----	-----
User-Name	Alice
Called-Station-Id	00-00-00-00-00-00:AndroidAP
Calling-Station-Id	00-11-22-33-44-55
Nas-Port	0x00000001 (1)
Nas-IP-Address	10.48.71.20

```
NAS-Identifier          0x6e6f (28271)
Airespace / WLAN-Identifier 0x00000002 (2)
User-Password           cisco!123
Service-Type            0x00000008 (8)
Framed-MTU              0x00000514 (1300)
Nas-Port-Type           0x00000013 (19)
Cisco / Audit-Session-Id 1447300a0000003041d5665c
Acct-Session-Id        5c66d541/00:11:22:33:44:55/743
```

test radius auth request successfully sent. Execute 'test aaa show radius' for response

(Cisco Controller) >test aaa show radius

Radius Test Request

```
Wlan-id..... 2
ApGroup Name..... none
```

Radius Test Response

Radius Server	Retry	Status
10.48.39.128	1	Success

Authentication Response:

Result Code: Success

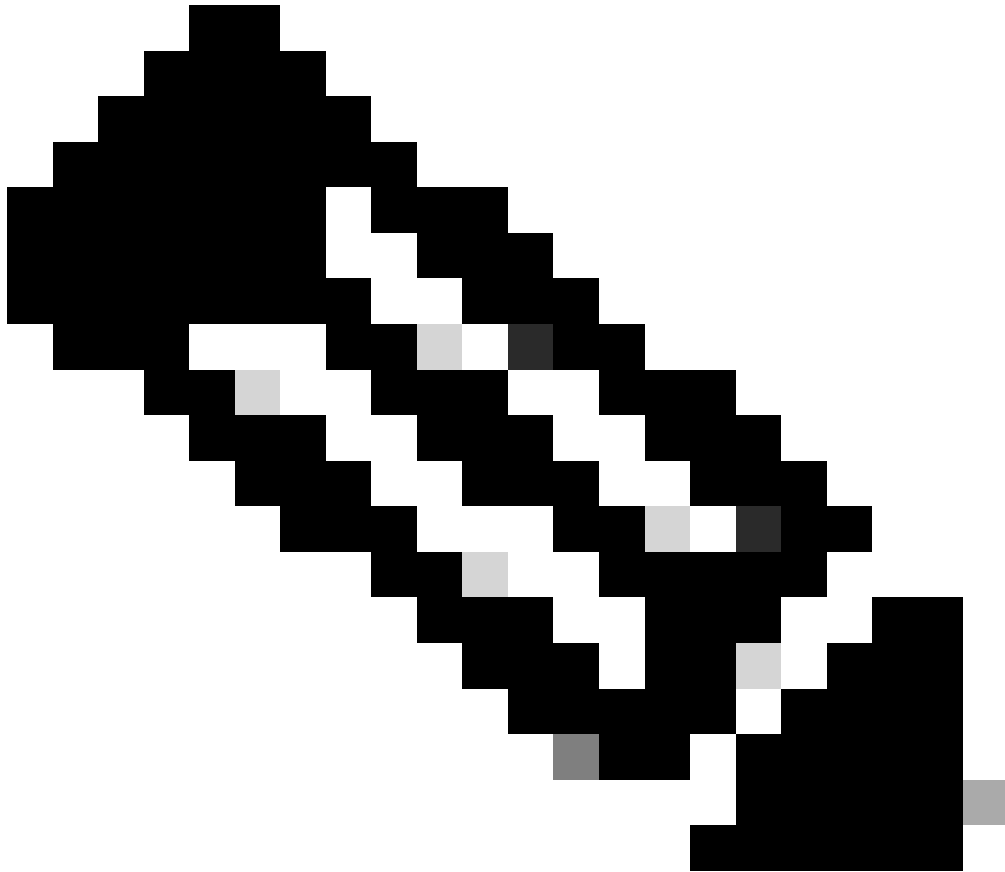
Attributes	Values
User-Name	Alice
State	ReauthSession:1447300a0000003041d5665c
Class	CACS:1447300a0000003041d5665c:rmanchur-ise/339603379/59
Tunnel-Type	0x0000000d (13)
Tunnel-Medium-Type	0x00000006 (6)
Tunnel-Group-Id	0x000005c5 (1477)

(Cisco Controller) >

2. debug client

を使用して、ワイヤレスクライアントの接続の問題をトラブルシューティングします。

3. WLCの認証と認可の問題をトラブルシューティングするには、 debug aaa all enableコマンドを使用します。



注:デバッグが行われるMACアドレスに基づいて出力を制限するには、このコマンドとのみ`debug mac addr`を使用します。

-
4. 認証の失敗の問題とAD通信の問題を特定するには、ISEライブログとセッションログを参照してください。

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。