

Configurazione dell'assegnazione dinamica della VLAN con i WLC basati su ISE per la mappa del gruppo di Active Directory

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Assegnazione dinamica di VLAN con server RADIUS](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Integrazione da ISE ad AD e configurazione dei criteri di autenticazione e autorizzazione per gli utenti su ISE](#)

[Configurazione WLC per supporto autenticazione dot1x e override AAA per SSID 'office_hq'](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

Questo documento descrive il concetto di assegnazione dinamica delle VLAN.

Prerequisiti

Nel documento viene descritto come configurare il controller WLC (Wireless LAN Controller) e il server Identity Services Engine (ISE) in modo da assegnare dinamicamente i client WLAN (Wireless LAN) a una VLAN specifica.

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di Wireless LAN Controller (WLC) e Lightweight Access Point (LAP)
- Conoscenza funzionale di un server di autenticazione, autorizzazione e accounting (AAA), ad esempio ISE
- Conoscenza approfondita delle reti wireless e dei problemi di sicurezza wireless
- Conoscenza funzionale e configurabile dell'assegnazione dinamica delle VLAN

- Conoscenza di base dei servizi Microsoft Windows AD, nonché di un controller di dominio e dei concetti relativi al DNS
- Conoscenze base di controllo e provisioning del protocollo CAPWAP (Access Point Protocol)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco serie 5520 WLC con firmware versione 8.8.11.0
- Cisco serie 4800 AP
- Supplicant Windows nativo e Anyconnect NAM
- Cisco Secure ISE versione 2.3.0.298
- Microsoft Windows 2016 Server configurato come controller di dominio
- Cisco serie 3560-CX Switch con versione 15.2(4)E1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

Assegnazione dinamica di VLAN con server RADIUS

Nella maggior parte dei sistemi WLAN, ogni WLAN dispone di un criterio statico che viene applicato a tutti i client associati a un SSID (Service Set Identifier) o a una WLAN nella terminologia del controller. Sebbene potente, questo metodo presenta delle limitazioni in quanto richiede ai client di associarsi a SSID diversi per ereditare criteri QoS e di sicurezza diversi.

La soluzione WLAN di Cisco risolve questo limite con il supporto delle reti di identità. In questo modo, la rete può annunciare un singolo SSID, ma determinati utenti possono ereditare diversi attributi QoS e VLAN e/o criteri di sicurezza in base alle credenziali dell'utente.

L'assegnazione dinamica della VLAN è una di queste funzionalità che permette a un utente wireless di accedere a una VLAN specifica in base alle credenziali fornite dall'utente. L'attività di assegnazione degli utenti a una VLAN specifica viene gestita da un server di autenticazione RADIUS, ad esempio Cisco ISE. Questa funzionalità può essere utilizzata, ad esempio, per fare in

modo che l'host wireless rimanga sulla stessa VLAN su cui si sposta all'interno della rete di un campus.

Il server Cisco ISE esegue l'autenticazione degli utenti wireless su uno dei diversi database possibili, incluso il database interno. Ad esempio:

- DB interno
- Active Directory
- Protocollo LDAP (Generic Lightweight Directory Access Protocol)
- Database relazionali compatibili con ODBC (Open Database Connectivity)
- Server token Rivest, Shamir e Adelman (RSA) SecurID
- Server token conformi a RADIUS

[I protocolli di autenticazione Cisco ISE e le origini di identità esterne supportate](#) elencano i vari protocolli di autenticazione supportati dai database interni ed esterni di ISE.

In questo documento viene illustrata l'autenticazione degli utenti wireless che utilizzano il database esterno di Windows Active Directory.

Una volta completata l'autenticazione, ISE recupera le informazioni sul gruppo dell'utente dal database di Windows e lo associa al rispettivo profilo di autorizzazione.

Quando un client tenta di associarsi a un LAP registrato con un controller, il LAP passa le credenziali dell'utente al WLC con l'aiuto del rispettivo metodo EAP.

WLC invia queste credenziali ad ISE con l'uso del protocollo RADIUS (incapsulamento dell'EAP) e ISE passa le credenziali degli utenti ad AD per la convalida con l'aiuto del protocollo KERBEROS.

AD convalida le credenziali dell'utente e, se l'autenticazione ha esito positivo, informa ISE.

Una volta completata l'autenticazione, il server ISE passa alcuni attributi IETF (Internet Engineering Task Force) al WLC. Questi attributi RADIUS determinano l>ID VLAN che deve essere assegnato al client wireless. L'SSID (WLAN, in termini di WLC) del client non conta perché l'utente è sempre assegnato a questo ID VLAN predeterminato.

Gli attributi utente RADIUS utilizzati per l'assegnazione dell>ID VLAN sono:

- IETF 64 (tipo tunnel)—Impostare su VLAN
- IETF 65 (tipo tunnel medio)—Impostare su 802
- IETF 81 (ID gruppo privato tunnel)—Impostare su ID VLAN

L>ID VLAN è 12 bit e assume un valore compreso tra 1 e 4094 inclusi. Poiché Tunnel-Private-Group-ID è di tipo stringa, come definito nella RFC2868 per l'utilizzo con IEEE 802.1X, il valore intero dell>ID VLAN viene codificato come stringa. Quando vengono inviati questi attributi del

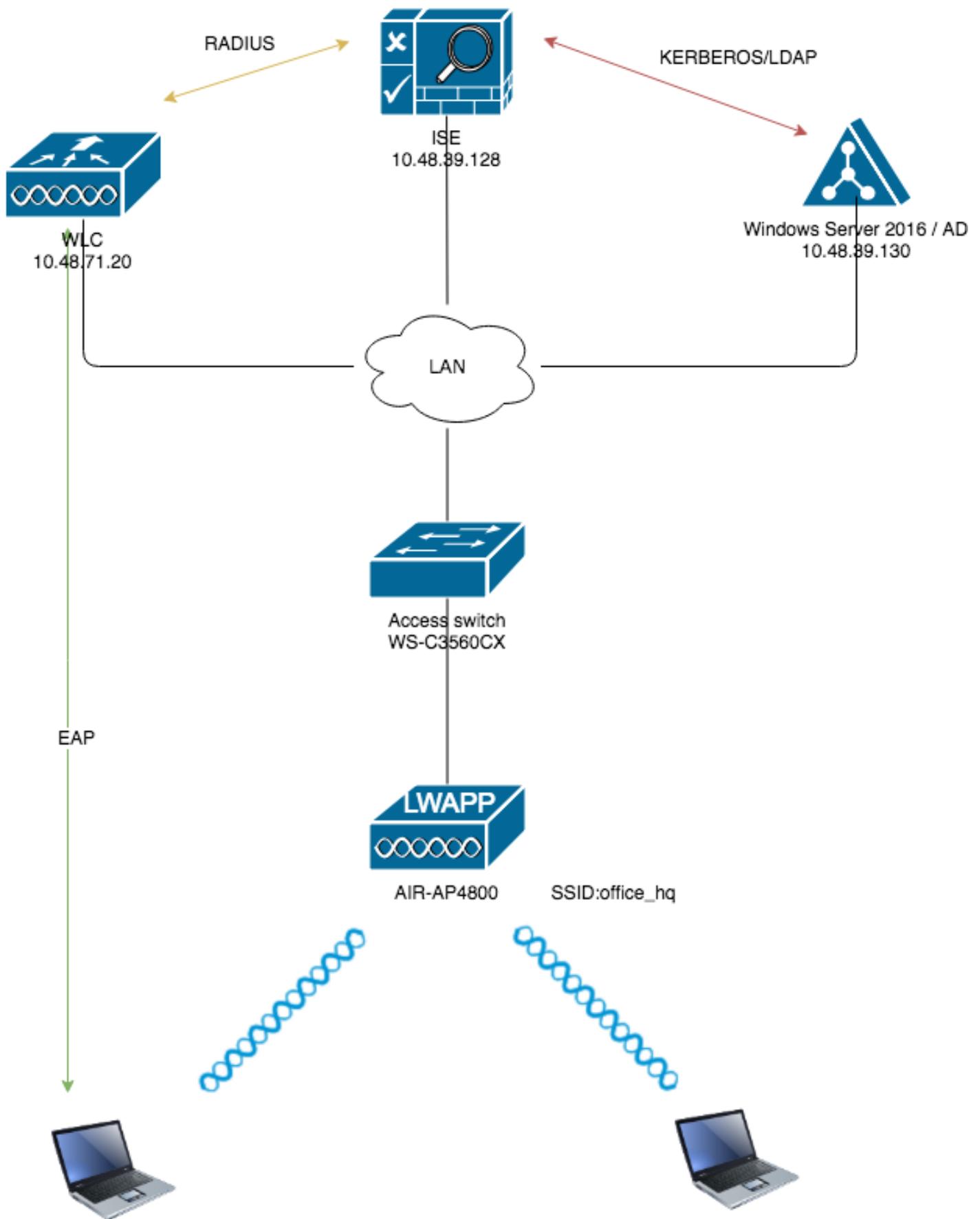
tunnel, è necessario compilare il campo Tag.

Come indicato nella [RFC 2868](#), sezione 3.1: il campo Tag è lungo un ottetto e serve a raggruppare gli attributi nello stesso pacchetto e fa riferimento allo stesso tunnel. I valori validi per questo campo sono compresi tra 0x01 e 0x1F inclusi. Se il campo Tag non è utilizzato, deve essere zero (0x00). Per ulteriori informazioni su tutti gli attributi RADIUS, consultare la [RFC 2868](#).

Configurazione

In questa sezione vengono fornite le informazioni necessarie per configurare le funzionalità descritte nel documento.

Esempio di rete



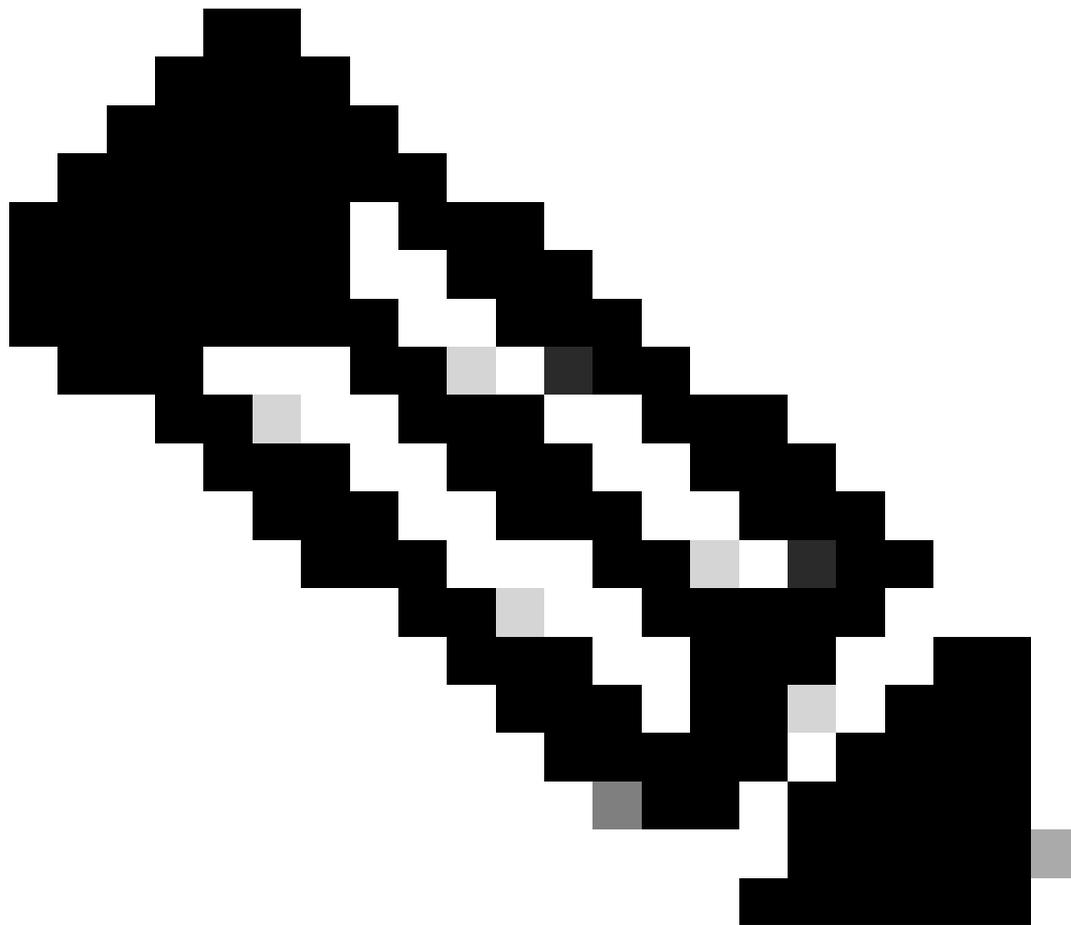
Configurazioni

Di seguito sono riportati i dettagli di configurazione dei componenti utilizzati nel diagramma:

- L'indirizzo IP del server ISE (RADIUS) è 10.48.39.128.
- L'indirizzo dell'interfaccia di gestione e AP-manager del WLC è 10.48.71.20.
- Il server DHCP risiede nella rete LAN ed è configurato per i rispettivi pool di client; non viene visualizzato nel diagramma.
- In questa configurazione vengono usate le VLAN1477 e VLAN1478. Gli utenti del reparto Marketing sono configurati in modo da essere inseriti nella VLAN1477 e gli utenti del reparto HR sono configurati in modo da essere inseriti nella VLAN1478 dal server RADIUS quando entrambi gli utenti si connettono allo stesso SSID — office_hq.

VLAN147: 192.168.77.0/24. Gateway: 192.168.77.1 VLAN1478: 192.168.78.0/24. Gateway: 192.168.78.1

- Per la sicurezza, questo documento usa PEAP-mschapv2 802.1x con.



Nota: Cisco consiglia di utilizzare metodi di autenticazione avanzati, come l'autenticazione EAP-FAST e EAP-TLS, per proteggere la WLAN.

Prima di eseguire la configurazione, vengono fatti i seguenti presupposti:

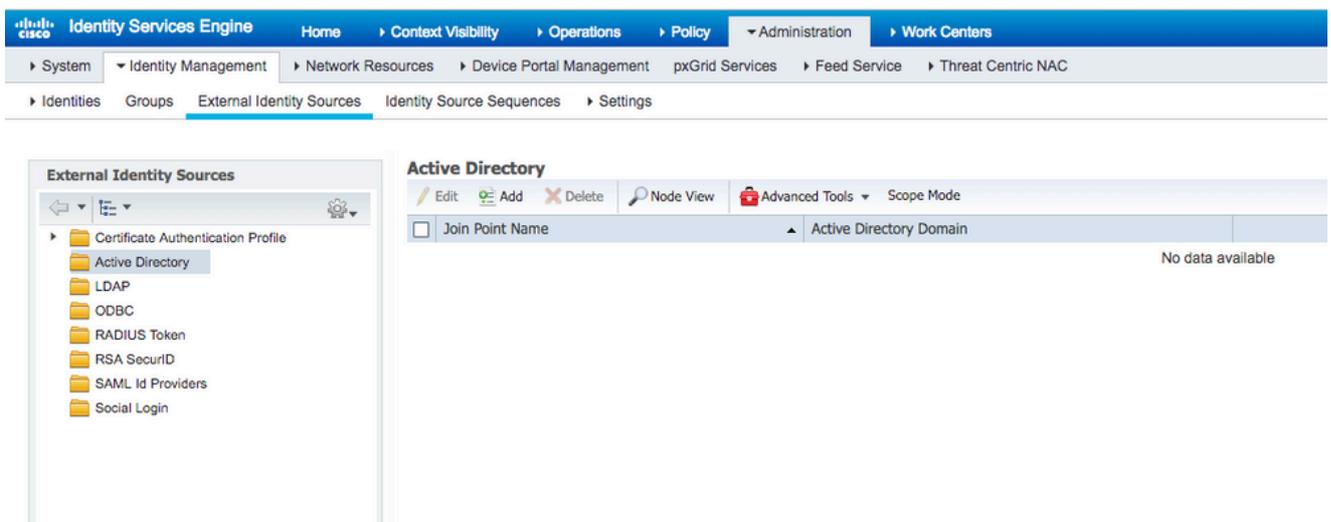
- Il LAP è già registrato nel WLC
- Al server DHCP è assegnato un ambito DHCP
- Connettività di livello 3 esistente tra tutti i dispositivi della rete
- Nel documento viene descritta la configurazione richiesta sul lato wireless e si presume che la rete cablata sia installata
- I rispettivi utenti e gruppi sono configurati in Active Directory

Per eseguire l'assegnazione dinamica della VLAN con i WLC basati sulla mappatura ISE al gruppo AD, è necessario eseguire i seguenti passaggi:

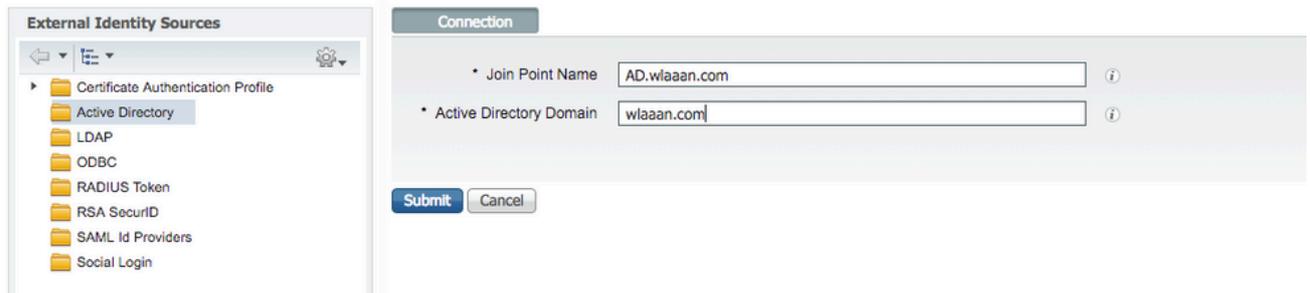
1. Integrazione da ISE ad AD e configurazione dei criteri di autenticazione e autorizzazione per gli utenti su ISE.
2. Configurazione WLC per supportare l'autenticazione dot1x e l'override AAA per SSID 'office_hq'.
3. Fine configurazione del supplicant client.

Integrazione da ISE ad AD e configurazione dei criteri di autenticazione e autorizzazione per gli utenti su ISE

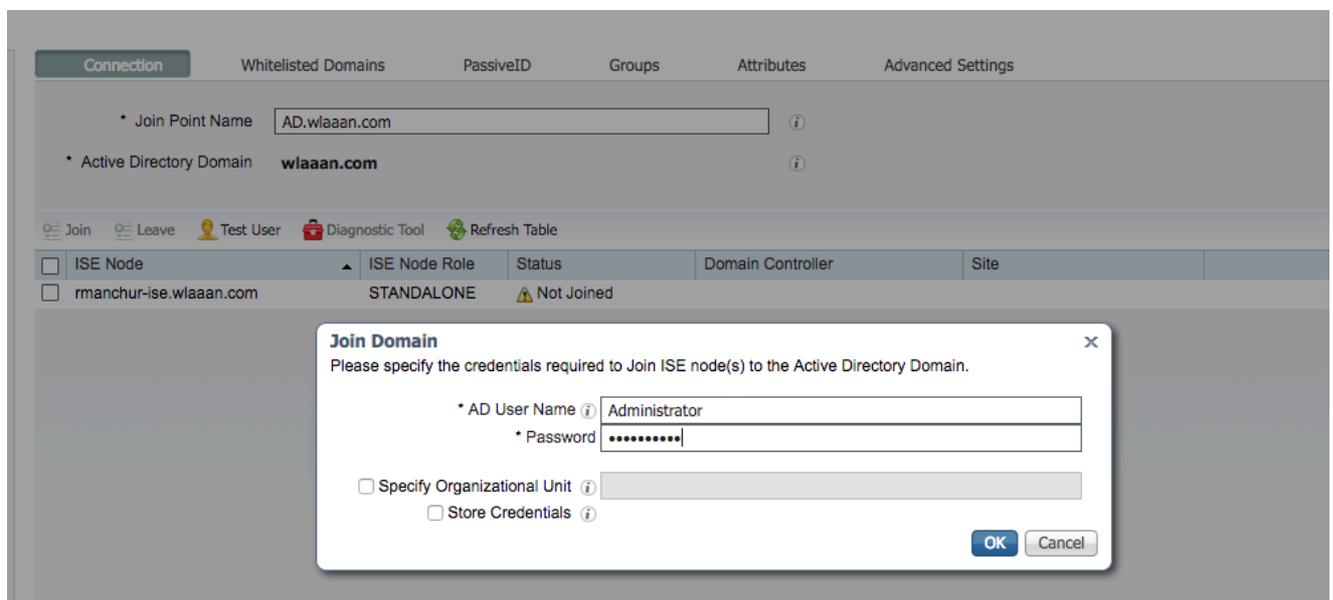
1. Accedere all'interfaccia utente Web ISE utilizzando un account admin.
2. Passare a Administration > Identity management > External Identity Sources > Active directory.



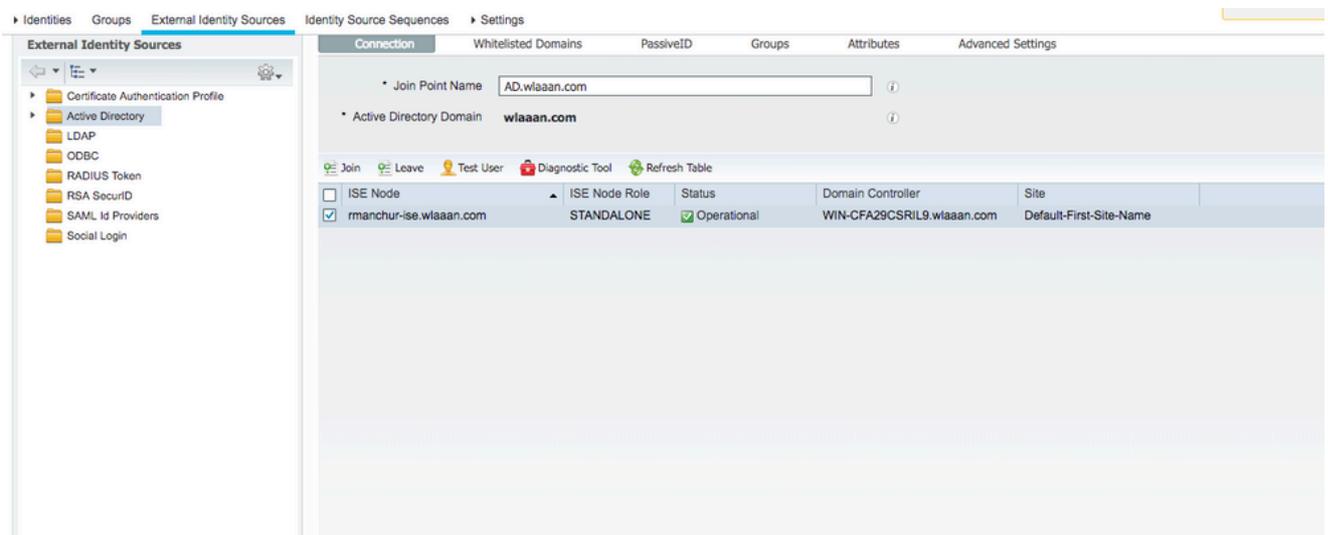
3. Fare clic su Aggiungi e immettere il nome del dominio e il nome dell'archivio identità dalle impostazioni di Nome punto di accesso Active Directory. Nell'esempio, l'ISE è registrato sul dominio wlaaan.com e il nome joinpoint è AD.wlaaan.com- localmente significativo per ISE.



4. Una finestra popup si apre dopo che **Submit** è stato premuto il pulsante che chiede se si desidera partecipare immediatamente ad ISE to AD. Premere **Yes** e fornire le credenziali utente di Active Directory con diritti di amministratore per aggiungere un nuovo host al dominio.



5. A questo punto, è necessario che ISE sia stata correttamente registrata in Active Directory.



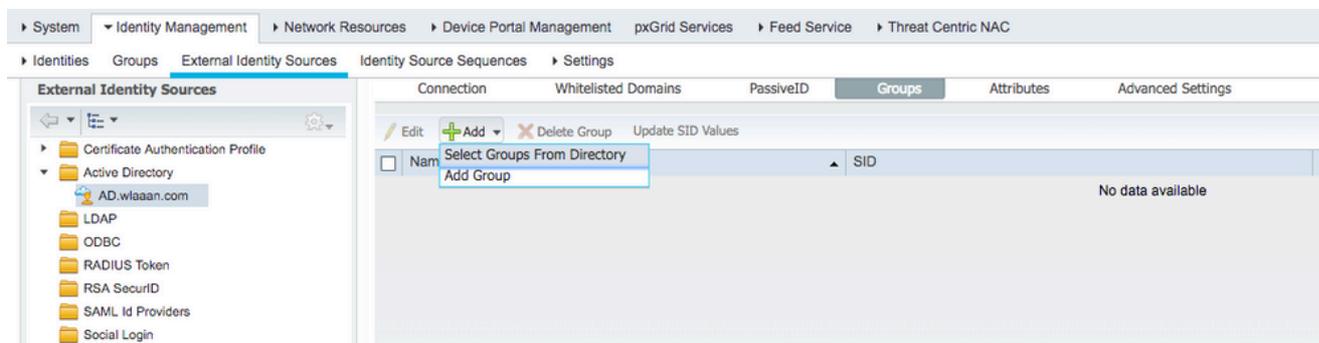
In caso di problemi con il processo di registrazione, è possibile utilizzare **Diagnostic Tool** per

eseguire i test richiesti per la connettività AD.

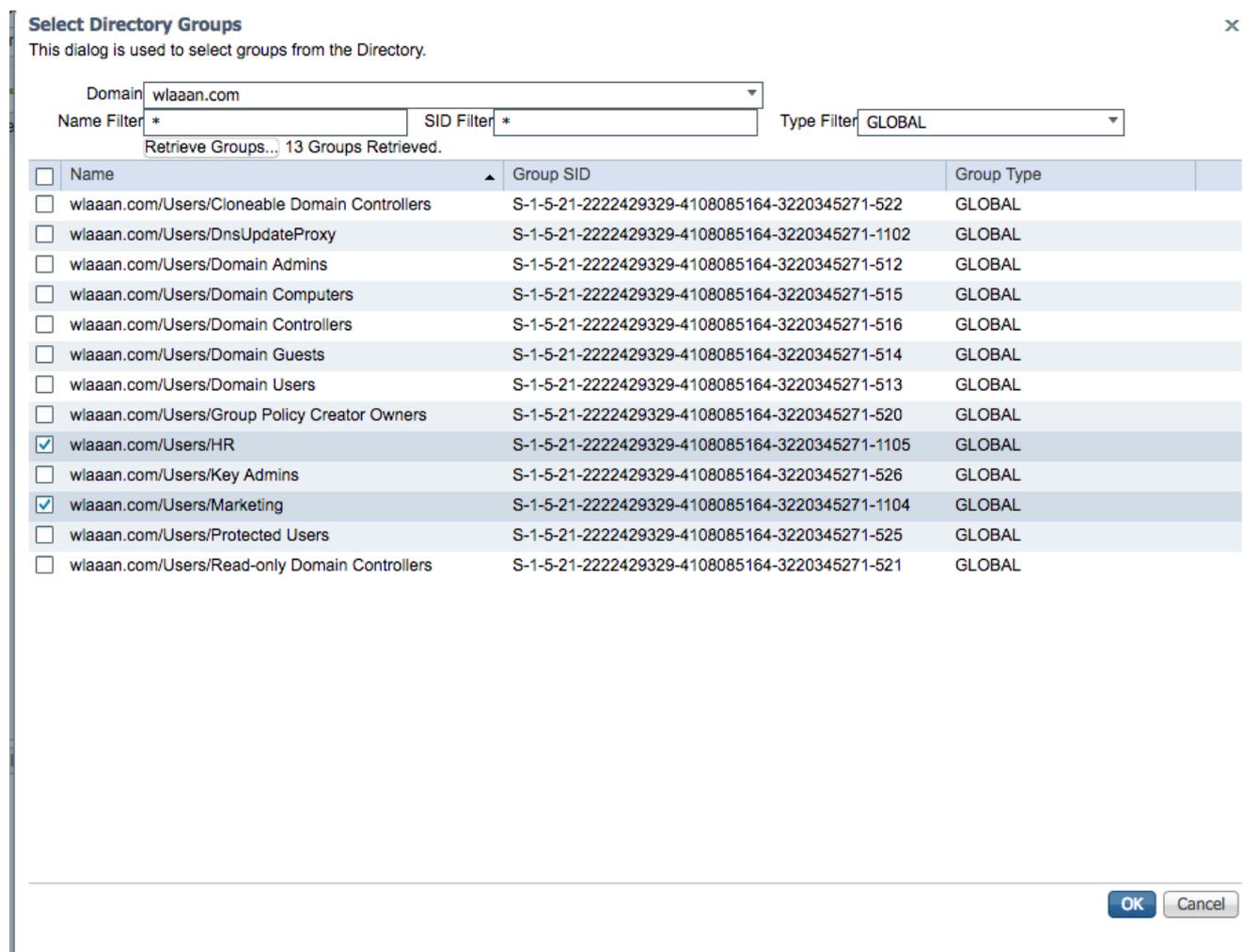
6. È necessario recuperare i gruppi per le directory attive utilizzate per assegnare i rispettivi profili di autorizzazione. Passare a Administration > Identity management > External Identity Sources > Active directory >

> Groups

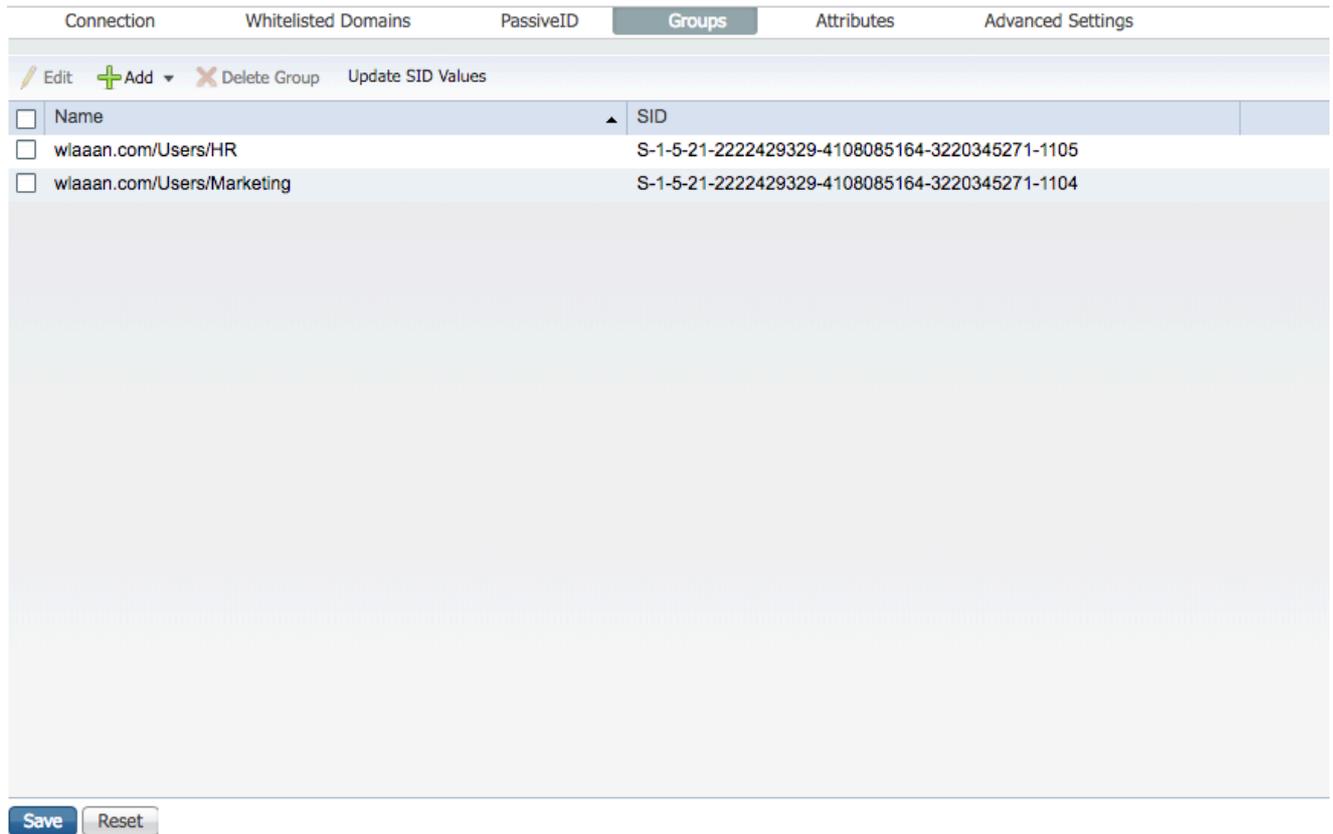
, quindi fare clic su **Add** scegliere **Select Groups from Active Directory**.



7. Viene visualizzata una nuova finestra popup in cui è possibile specificare un filtro per recuperare gruppi specifici o recuperare tutti i gruppi da Active Directory. Scegliere i rispettivi gruppi dall'elenco dei gruppi AD e premere **OK**.



8. I rispettivi gruppi vengono aggiunti ad ISE e possono essere salvati. Premere **Save**.



9. Add WLC to the ISE Network device list: passare a **Administration > Network Resources > Network Devices** e premere **Add**.

Configurazione completa, fornendo l'indirizzo IP di gestione WLC e il segreto condiviso RADIUS tra WLC e ISE.

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. Ora, dopo aver aggiunto ISE ad AD e il WLC all'elenco dei dispositivi, è possibile avviare la configurazione dei criteri di autenticazione e autorizzazione per gli utenti.

- Creare un profilo di autorizzazione per assegnare gli utenti da Marketing a VLAN1477 e dal gruppo HR a VLAN1478.

Per creare un nuovo profilo, individuare Policy > Policy Elements > Results > Authorization > Authorization profiles e fare clic sul **Add** pulsante.

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

Standard Authorization Profiles
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Edit Add Duplicate Delete

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-

- Completare la configurazione del profilo di autorizzazione con le informazioni sulla VLAN per il gruppo corrispondente. Nell'esempio vengono mostrate le impostazioni di configurazione del Marketing gruppo.

Dictionaries ▸ Conditions ▾ Results

▸ Authentication
 ▾ Authorization
 Authorization Profiles
 Downloadable ACLs
 ▸ Profiling
 ▸ Posture
 ▸ Client Provisioning

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 ID/Name

Advanced Attributes Settings

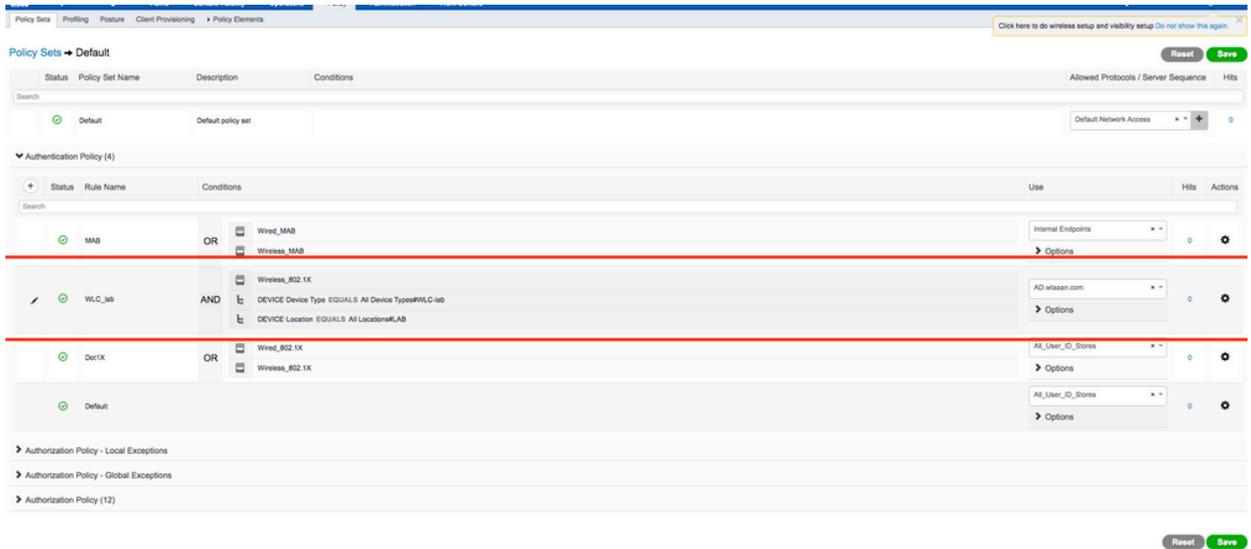
=

Attributes Details

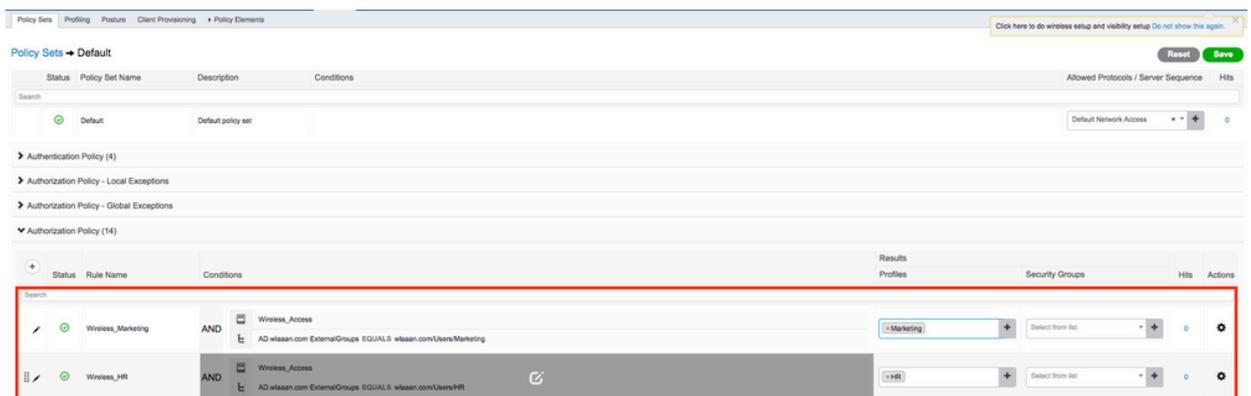
Access Type = ACCESS_ACCEPT
 Tunnel-Private-Group-ID = 1:1477
 Tunnel-Type = 1:13
 Tunnel-Medium-Type = 1:6

Una configurazione simile deve essere eseguita per altri gruppi e devono essere configurati i rispettivi attributi del tag VLAN.

- Dopo aver configurato i profili di autorizzazione, è possibile definire i criteri di autenticazione per gli utenti wireless. A tale scopo, è possibile configurare Customo modificare il set di criteri Default. In questo esempio viene modificato il set di criteri Predefinito. Passare a Policy > Policy Sets > Default. Per impostazione predefinita per dot1x il tipo di autenticazione, ISE verrà utilizzato All_User_ID_Stores, anche se funziona anche con le impostazioni predefinite correnti poiché AD fa parte dell'elenco delle origini di identità di All_User_ID_Stores, in questo esempio viene utilizzata una regola WLC_lab più specifica per il rispettivo controller LAB e AD viene utilizzata come unica origine per l'autenticazione.



- È ora necessario creare criteri di autorizzazione per gli utenti che assegnano i rispettivi profili di autorizzazione in base all'appartenenza ai gruppi. Per soddisfare questo requisito, passare Authorization policy alla sezione e creare i criteri.



Configurazione WLC per il supporto dell'autenticazione dot1x e sostituzione AAA per SSID 'office_hq'

1. Configurare ISE come server di autenticazione RADIUS su WLC. Andare alla Security > AAA > RADIUS > Authentication sezione nell'interfaccia utente Web e fornire l'indirizzo IP ISE e le informazioni segrete condivise.

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. Configurare SSIDoffice_hqnella sezioneWLANsdel WLC; nell'esempio seguente viene configurato SSID conWPA2/AES+dot1xe AAA override. L'interfacciaDummyviene scelta per la WLAN, in quanto la VLAN corretta viene assegnata comunque tramite RADIUS. Questa interfaccia fittizia deve essere creata sul WLC e deve essere specificato un indirizzo IP, ma l'indirizzo IP non deve essere valido e la VLAN in cui viene inserita non può essere creata nello switch uplink in modo che se non viene assegnata alcuna VLAN, il client non possa andare da nessuna parte.

WLANs

WLANs

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

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

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

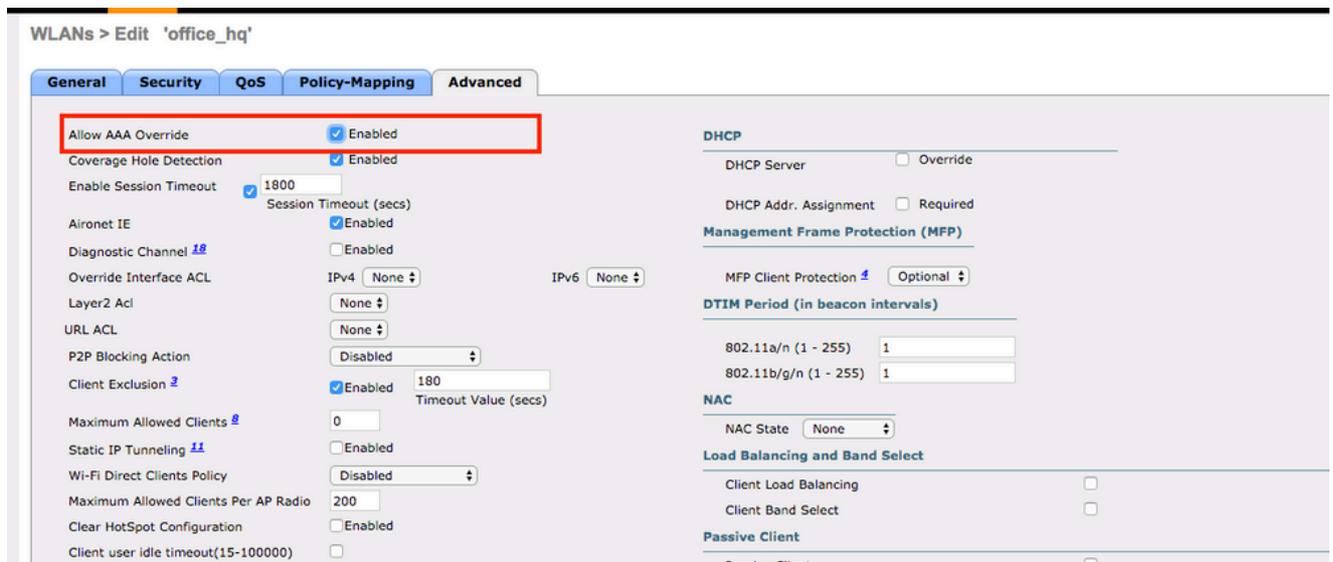
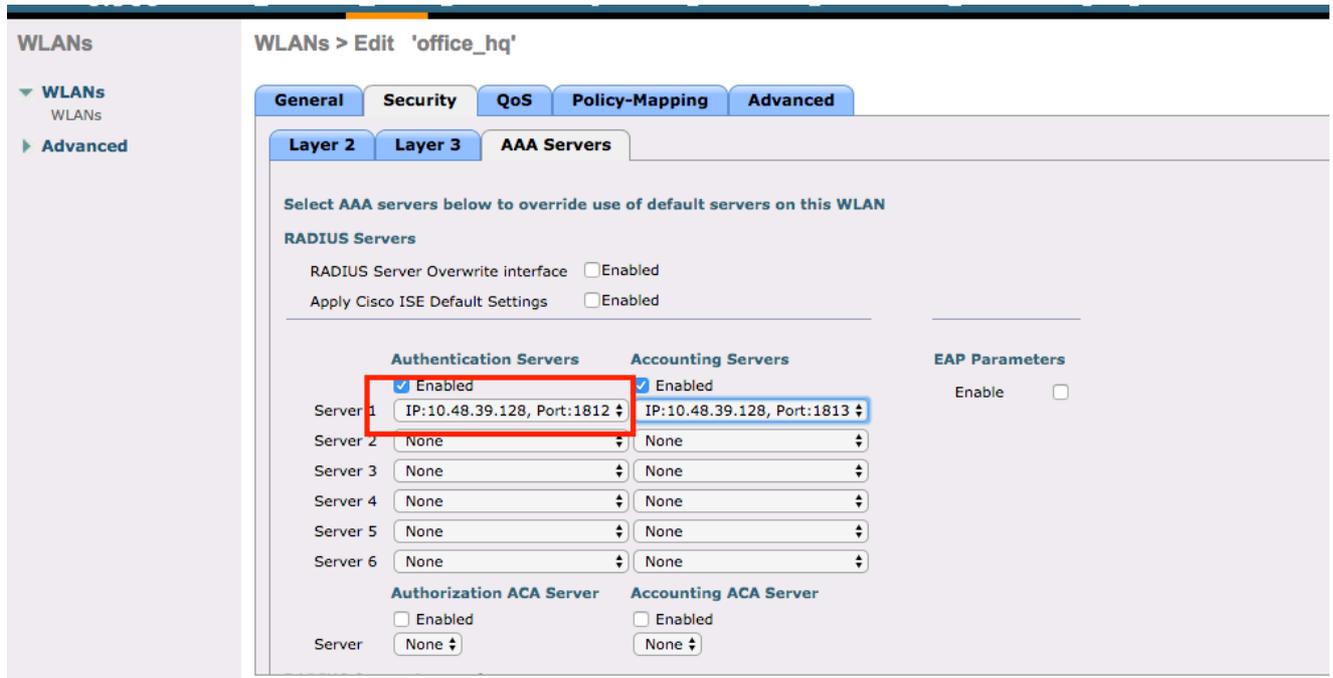
Layer 2 Security: WPA+WPA2
MAC Filtering:

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. Inoltre, è necessario creare interfacce dinamiche sul WLC per le VLAN utente. Passare al menu dell'Controller > Interfaces 'interfaccia utente'. Il WLC può onorare l'assegnazione VLAN ricevuta tramite AAA solo se ha un'interfaccia dinamica in quella VLAN.

Controller

- General
- Icons
- Inventory
- Interfaces
- Interface Groups
- Multicast
- Network Routes
- Fabric Configuration
- Redundancy
- Mobility Management
- Ports
- NTP
- CDP
- PMIPv6
- Tunneling
- IPv6
- mDNS
- Advanced
- Lawful Interception

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:

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

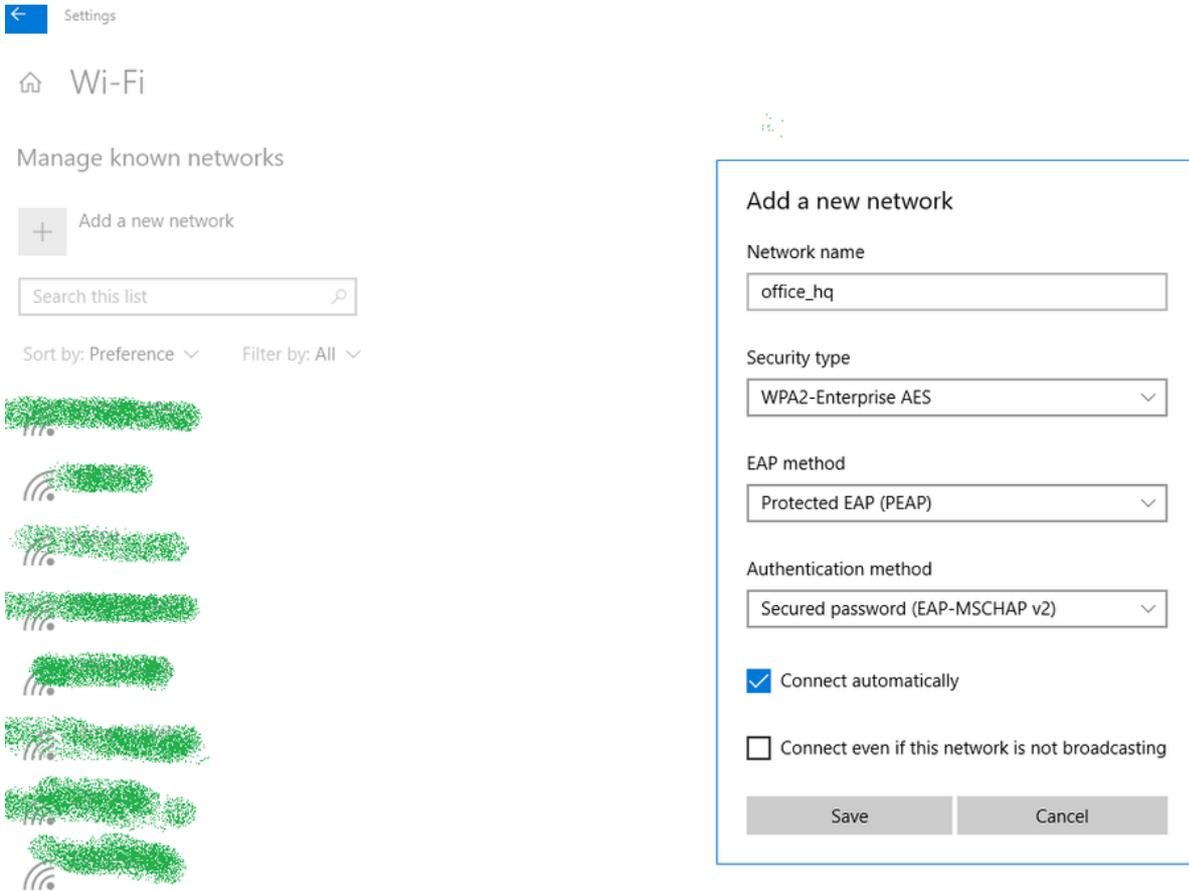
Verifica

Per verificare le connessioni, usare il supplicant nativo Windows 10 e Anyconnect NAM.

Poiché si utilizza l'autenticazione EAP-PEAP e ISE utilizza un certificato autofirmato (SSC), è necessario accettare un avviso di certificato o disabilitare la convalida del certificato. In un ambiente aziendale, è necessario utilizzare un certificato firmato e attendibile su ISE e verificare che i dispositivi dell'utente finale dispongano del certificato radice appropriato installato nell'elenco delle CA attendibili.

Test connessione con Windows 10 e supplicant nativo:

1. Aprire Network & Internet settings > Wi-Fi > Manage known networks e creare un nuovo profilo di rete premendo il Add new network pulsante; immettere le informazioni richieste.



2. Verificare che l'utente abbia selezionato il profilo corretto per l'accesso con autenticazione ISE.

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. Verificare che la voce del client sul WLC sia stata assegnata alla VLAN corretta e che si trovi nello stato RUN.

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. Dalla CLI del WLC, lo stato del client può essere verificato con `show client details` :

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

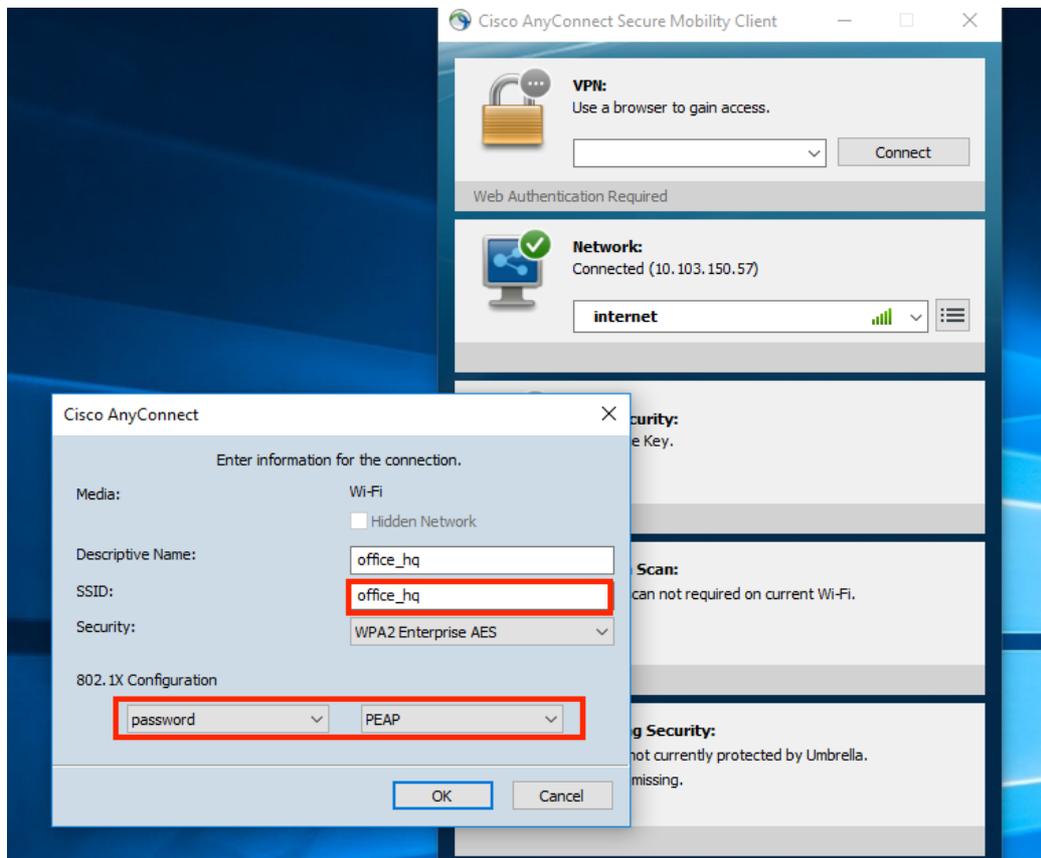
```

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..... v1an1478
VLAN..... 1478
Quarantine VLAN..... 0
Access VLAN..... 1478

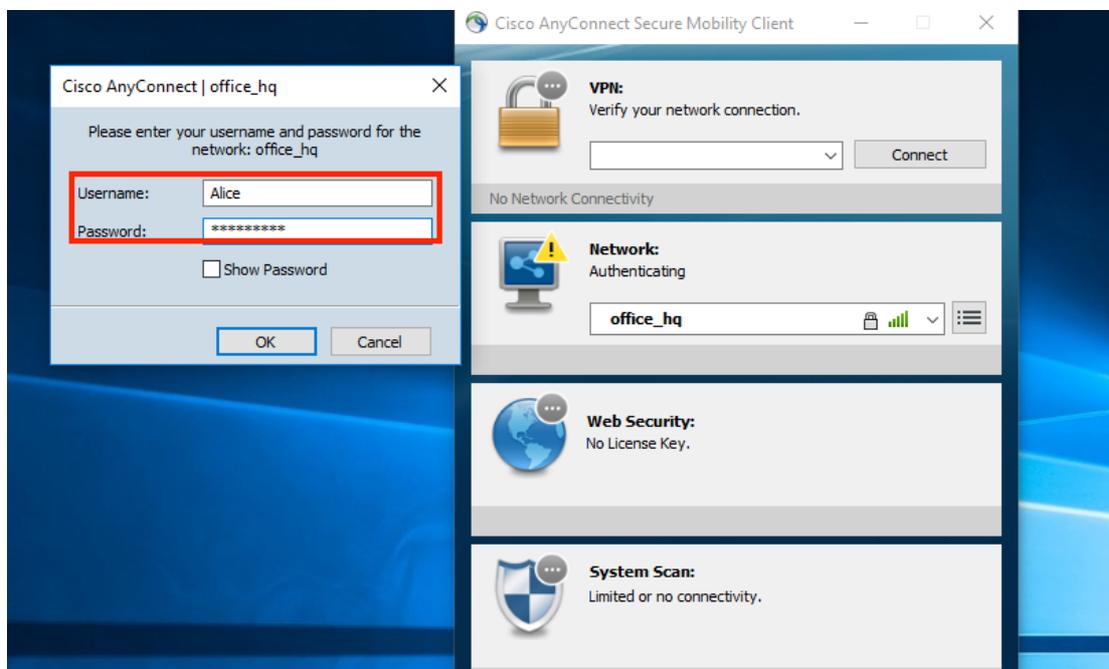
```

Test della connessione a Windows 10 e Anyconnect NAM:

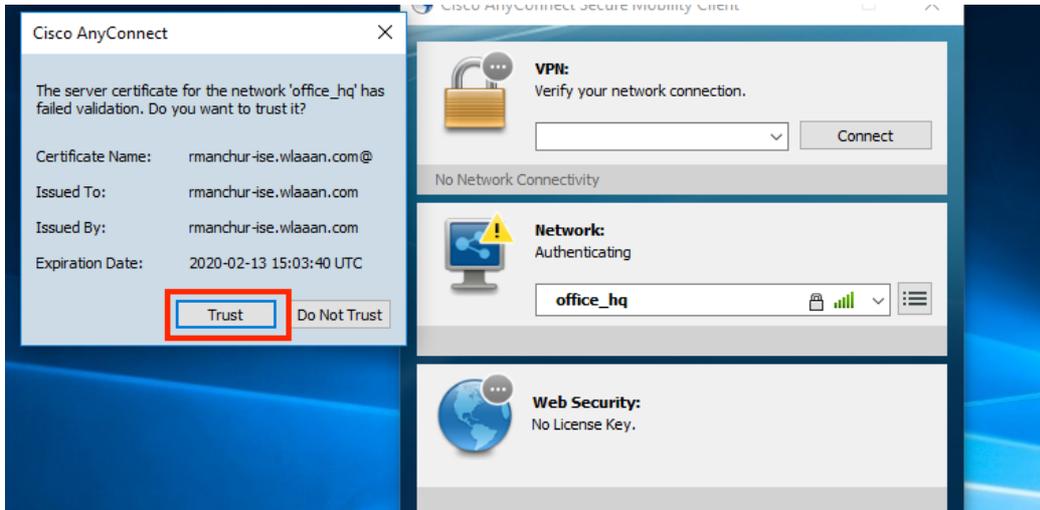
1. Scegliere il SSID dall'elenco SSID disponibili e il rispettivo tipo di autenticazione EAP (in questo esempio PEAP) e il modulo di autenticazione interna.



2. Specificare nome utente e password per l'autenticazione utente.



3. Poiché ISE sta inviando un certificato SSC al client, è necessario scegliere manualmente di considerare attendibile il certificato (nell'ambiente di produzione si consiglia di installare il certificato attendibile su ISE).



4. Verificare i log di autenticazione su ISE e accertarsi che sia selezionato il profilo di autorizzazione corretto per l'utente.

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	192.168.77.32	WLC5520		Workstation			manchur-ise

5. Verificare che la voce del client sul WLC sia stata assegnata alla VLAN corretta e che si trovi nello stato RUN.

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. Dalla CLI del WLC, lo stato del client può essere verificato con `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

```

Risoluzione dei problemi

1. Per visualizzare i risultati, usare il comando `test aaa radius username`

```
password
```

```
wlan-id
```

in modo da verificare la connessione RADIUS tra WLC, `test aaa show radius` ISE e.

```
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

```

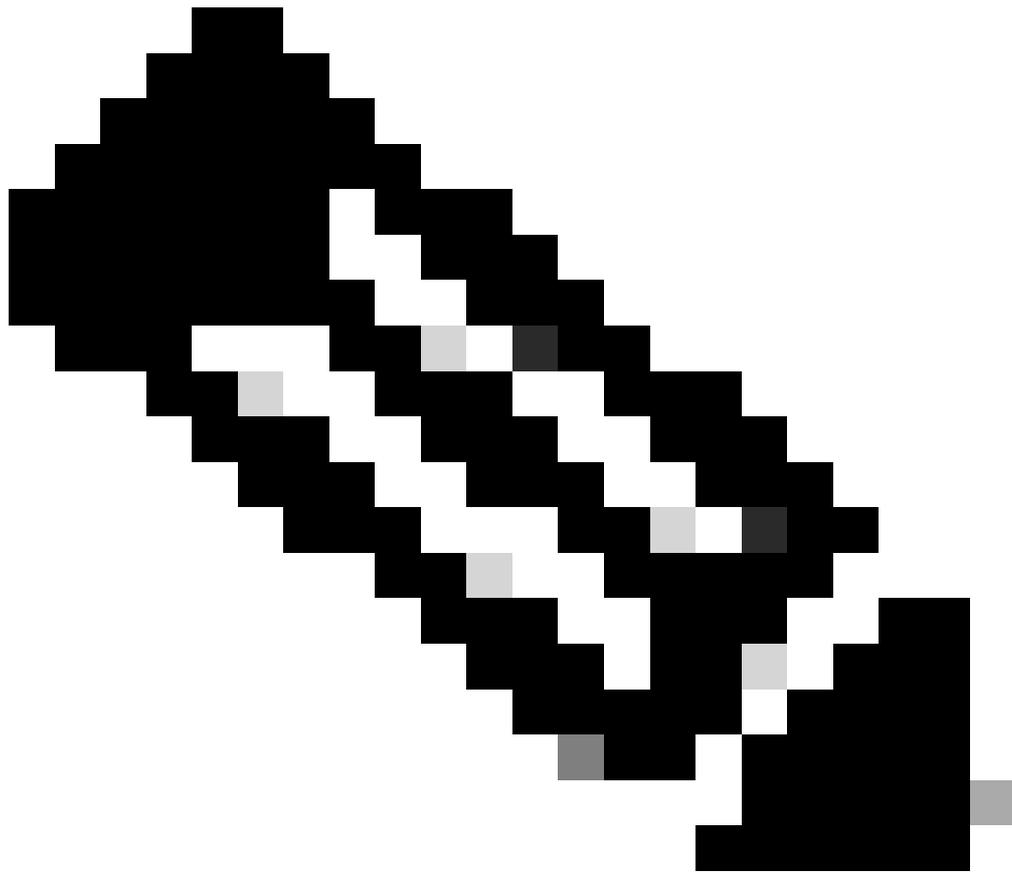
Radius Server	Retry	Status
10.48.39.128	1	Success

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. Per risolvere i problemi di connettività dei client wireless, debug client utilizzare.
3. Usare il comando debug aaa all enable per risolvere i problemi di autenticazione e autorizzazione sul WLC.



Nota: utilizzare questo comando solo con `debug mac addr` per limitare l'output in base all'indirizzo MAC per il quale viene eseguito il debug.

-
4. Per identificare i problemi relativi agli errori di autenticazione e ai problemi di comunicazione di Active Directory, consultare i log di ISE in tempo reale e i log delle sessioni.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).