Configurazione di PEAP e EAP-FAST con ACS 5.2 e WLC

Sommario

Introduzione

In questo documento viene spiegato come configurare il controller WLC (Wireless LAN Controller) per l'autenticazione EAP (Extensible Authentication Protocol) con l'utilizzo di un server RADIUS esterno, ad esempio Access Control Server (ACS) 5.2.

Prerequisiti

Requisiti

Prima di provare la configurazione, verificare che siano soddisfatti i seguenti requisiti:

- Conoscere a fondo i WLC e i Lightweight Access Point (LAP)
- Conoscenza funzionale del server AAA
- Conoscere a fondo le reti wireless e i problemi di sicurezza wireless

Componenti usati

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

- Cisco 5508 WLC con firmware versione 7.0.20.0
- Cisco serie 3502 LAP
- Supplicant nativo di Microsoft Windows 7 con driver Intel 6300-N versione 14.3
- Cisco Secure ACS con versione 5.2
- Cisco serie 3560 Switch

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

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

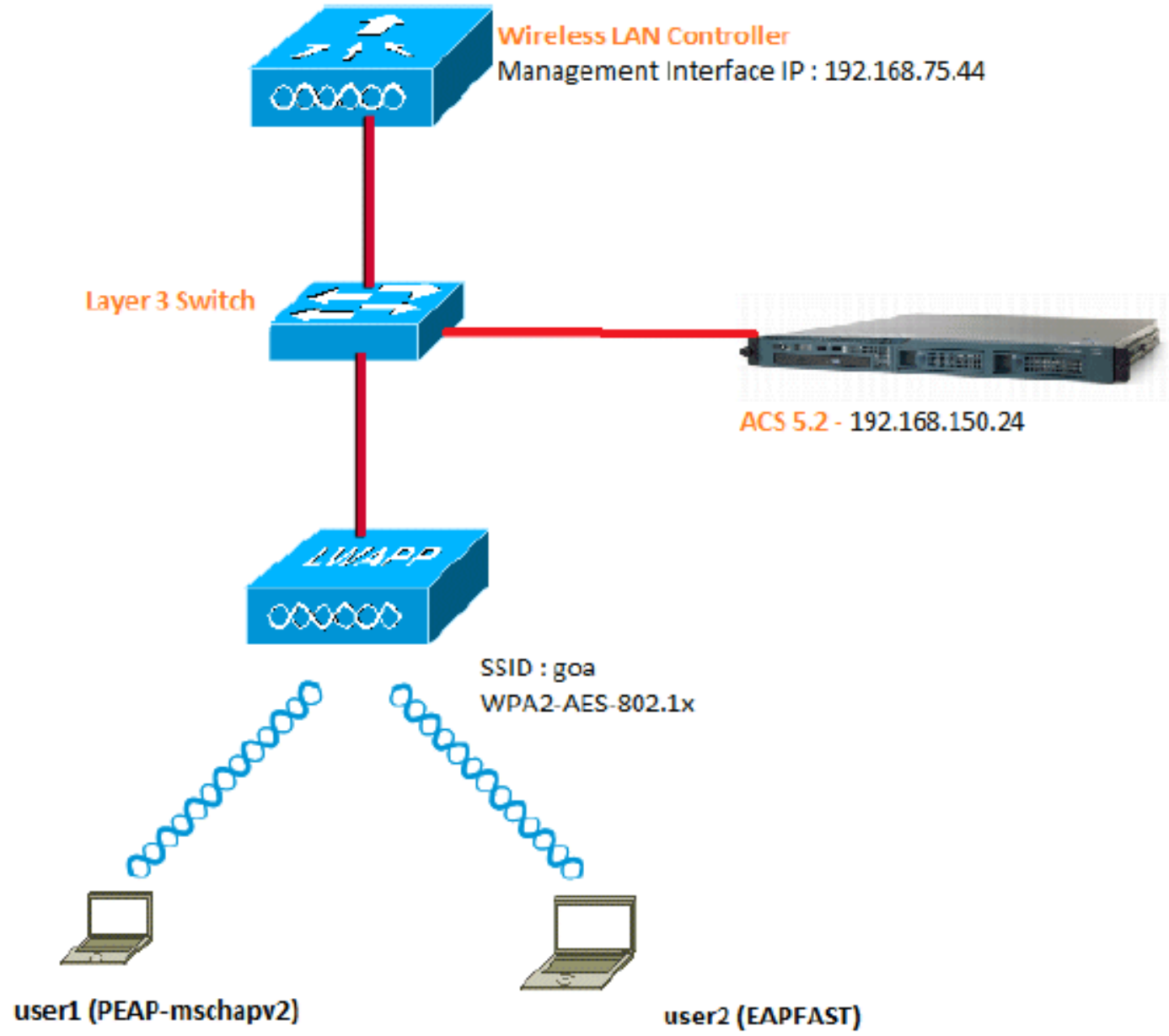
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



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

- L'indirizzo IP del server ACS (RADIUS) è 192.168.150.24.
- L'indirizzo dell'interfaccia di gestione e AP-manager del WLC è 192.168.75.44.
- L'indirizzo dei server DHCP è 192.168.150.25.
- In questa configurazione, viene usata la VLAN 253. Entrambi gli utenti si connettono allo stesso SSID "goa". Tuttavia, l'utente 1 è configurato per l'autenticazione tramite PEAP-MSCHAPv2 e l'utente 2 tramite EAP-FAST.
- Gli utenti verranno assegnati alla VLAN 253:VLAN 253: 192.168.153.x/24. Gateway: 192.168.153.1VLAN 75: 192.168.75.x/24. Gateway: 192.168.75.1

Presupposti

- Gli switch sono configurati per tutte le VLAN di layer 3.
- Al server DHCP viene assegnato un ambito DHCP.
- Esiste una connettività di livello 3 tra tutti i dispositivi della rete.
- Il LAP è già unito al WLC.
- Ogni VLAN ha una maschera /24.

- In ACS 5.2 è installato un certificato autofirmato.

Procedura di configurazione

Questa configurazione è suddivisa in tre fasi principali:

1. Configurare il server RADIUS.
2. Configurare il WLC.
3. Configurare Wireless Client Utility.

Configurazione del server RADIUS

La configurazione del server RADIUS è suddivisa in quattro passaggi:

1. Configurare le risorse di rete.
2. Configurare gli utenti.
3. Definire gli elementi dei criteri.
4. Applicare i criteri di accesso.

ACS 5.x è un sistema di controllo degli accessi basato su regole. ovvero ACS 5.x utilizza un modello di criteri basato su regole anziché il modello basato su gruppi utilizzato nelle versioni 4.x.

Il modello di policy basato su regole ACS 5.x offre un controllo dell'accesso più potente e flessibile rispetto al precedente approccio basato su gruppi.

Nel modello basato su gruppi meno recente, un gruppo definisce i criteri in quanto contiene e associa tre tipi di informazioni:

- Informazioni sull'identità: queste informazioni possono essere basate sull'appartenenza a gruppi AD o LDAP oppure su un'assegnazione statica per gli utenti ACS interni.
- Altre restrizioni o condizioni: restrizioni temporali, restrizioni per i dispositivi e così via.
- Autorizzazioni: livelli di privilegio per VLAN o Cisco IOS®.

Il modello di policy di ACS 5.x si basa sulle seguenti regole:

- If condition then result

Ad esempio, vengono utilizzate le informazioni descritte per il modello basato su gruppi:

- If identity-condition, restricted-condition e authorization-profile.

Di conseguenza, questo ci offre la flessibilità di limitare a quali condizioni l'utente può accedere alla rete e quale livello di autorizzazione è consentito quando vengono soddisfatte condizioni specifiche.

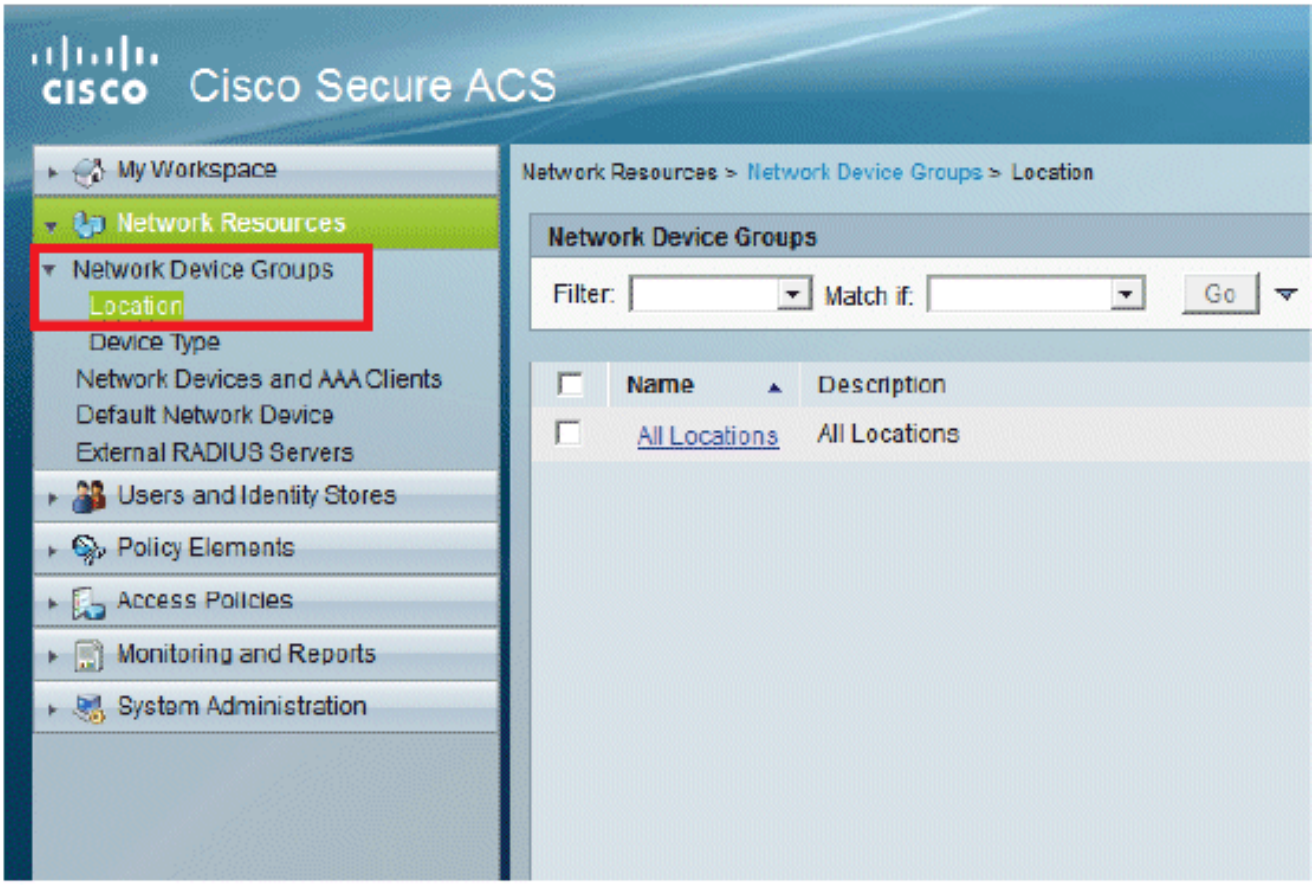
Configura risorse di rete

In questa sezione viene configurato il client AAA per il WLC sul server RADIUS.

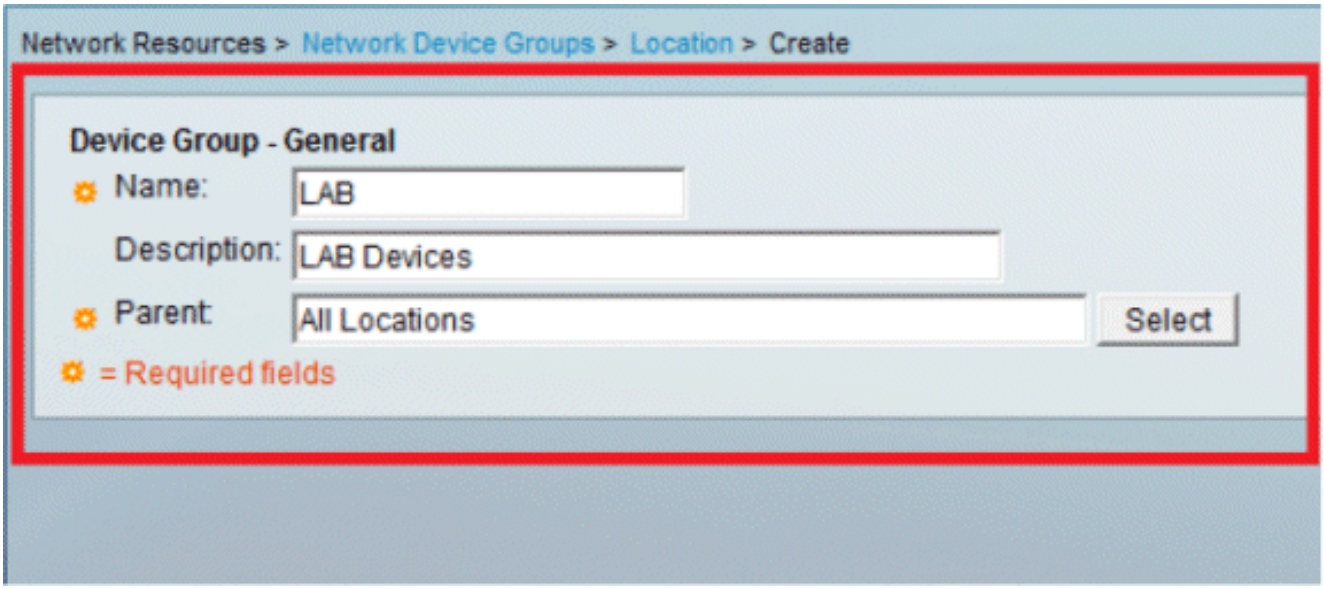
In questa procedura viene illustrato come aggiungere il WLC come client AAA sul server RADIUS in modo che il WLC possa passare le credenziali dell'utente al server RADIUS.

Attenersi alla seguente procedura:

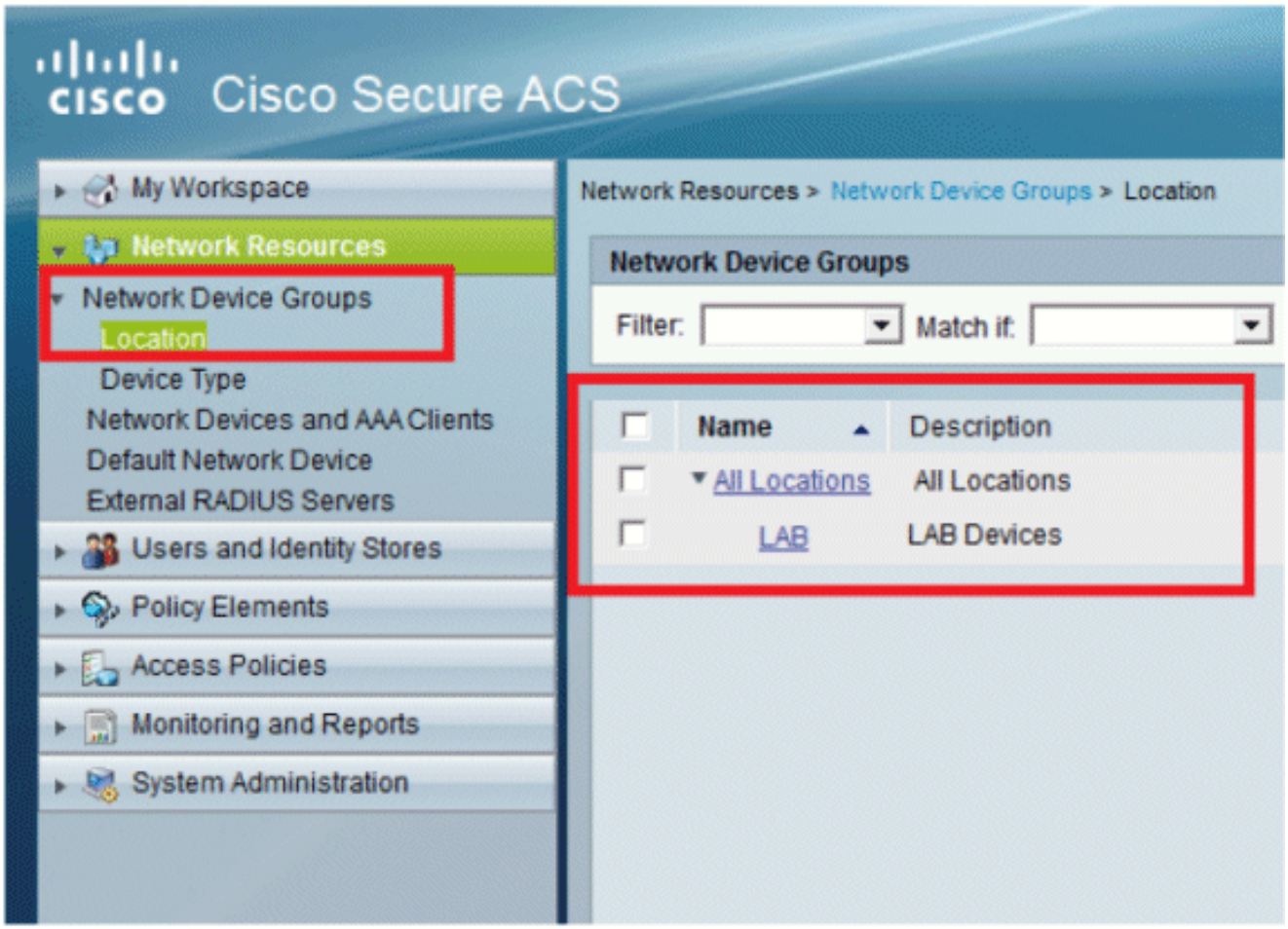
1. Dalla GUI di ACS, selezionare **Risorse di rete > Gruppi di dispositivi di rete > Posizione**, quindi fare clic su **Crea** (in basso).



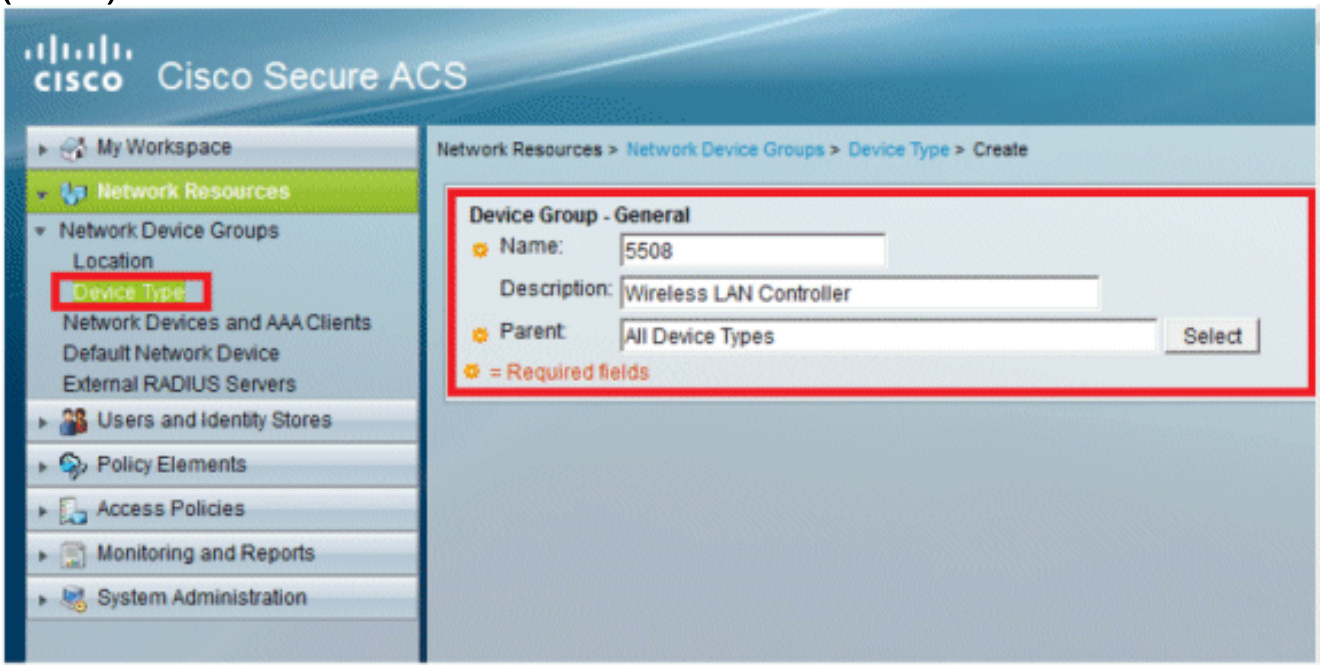
2. Aggiungere i campi obbligatori e fare clic su **Invia**.



Viene visualizzata la seguente schermata:

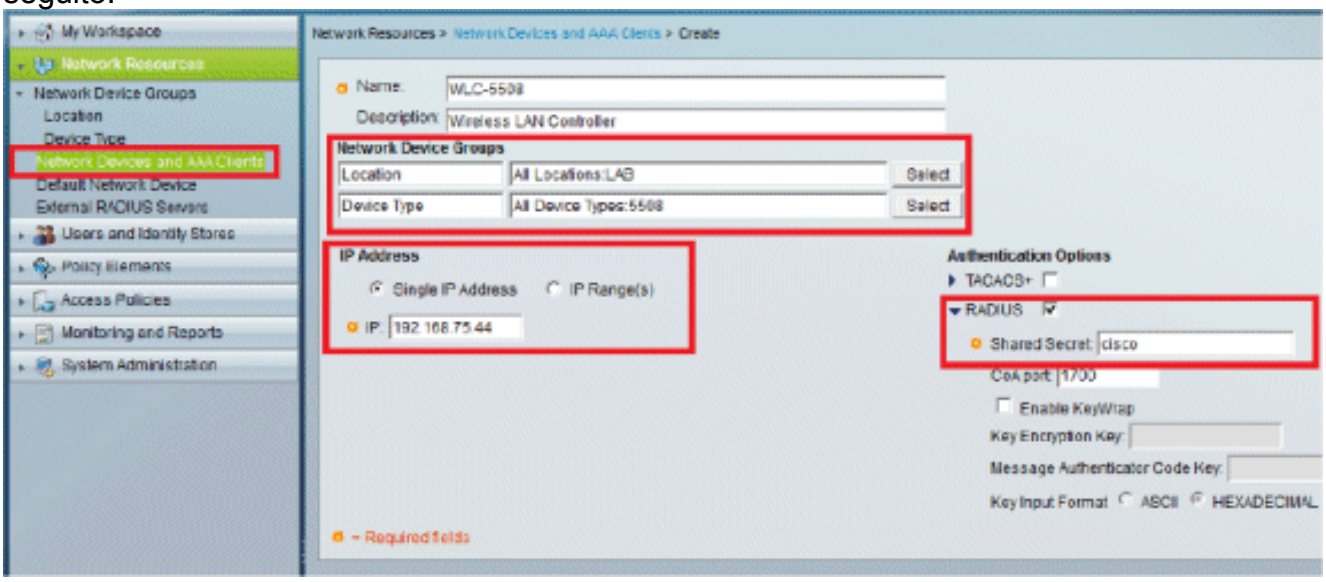


3. Selezionate **Tipo periferica (Device Type) > Crea (Create)**.

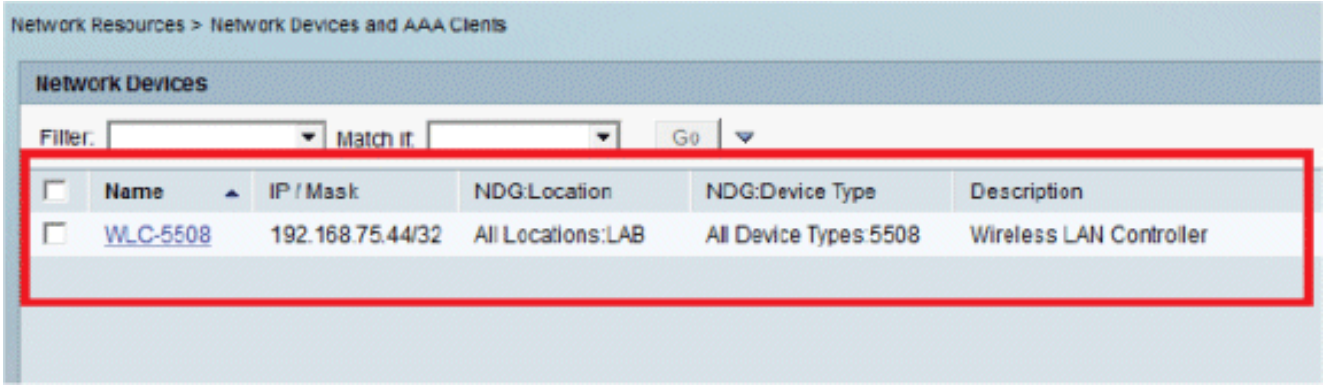


4. Fare clic su **Invia**. Viene visualizzata la seguente schermata:

5. Selezionare **Risorse di rete > Dispositivi di rete e client AAA**.
6. Fare clic su **Create** (Crea) e immettere i dettagli come illustrato di seguito:



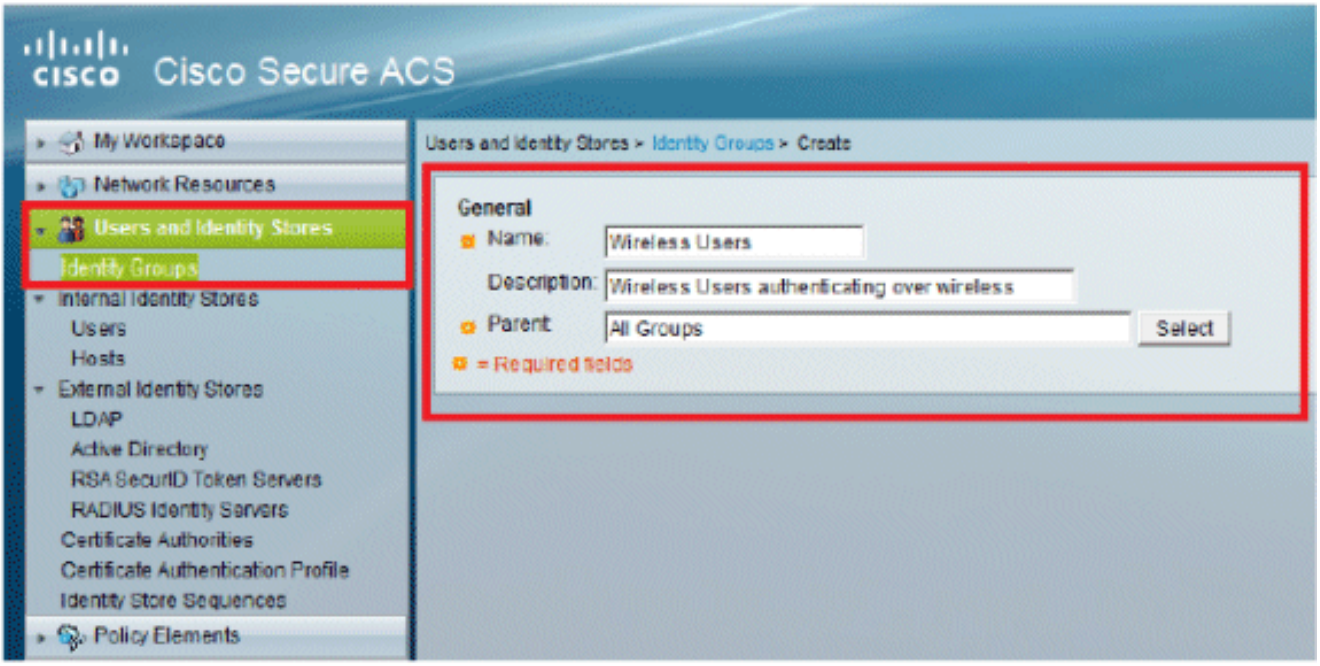
7. Fare clic su **Invia**. Viene visualizzata la seguente schermata:



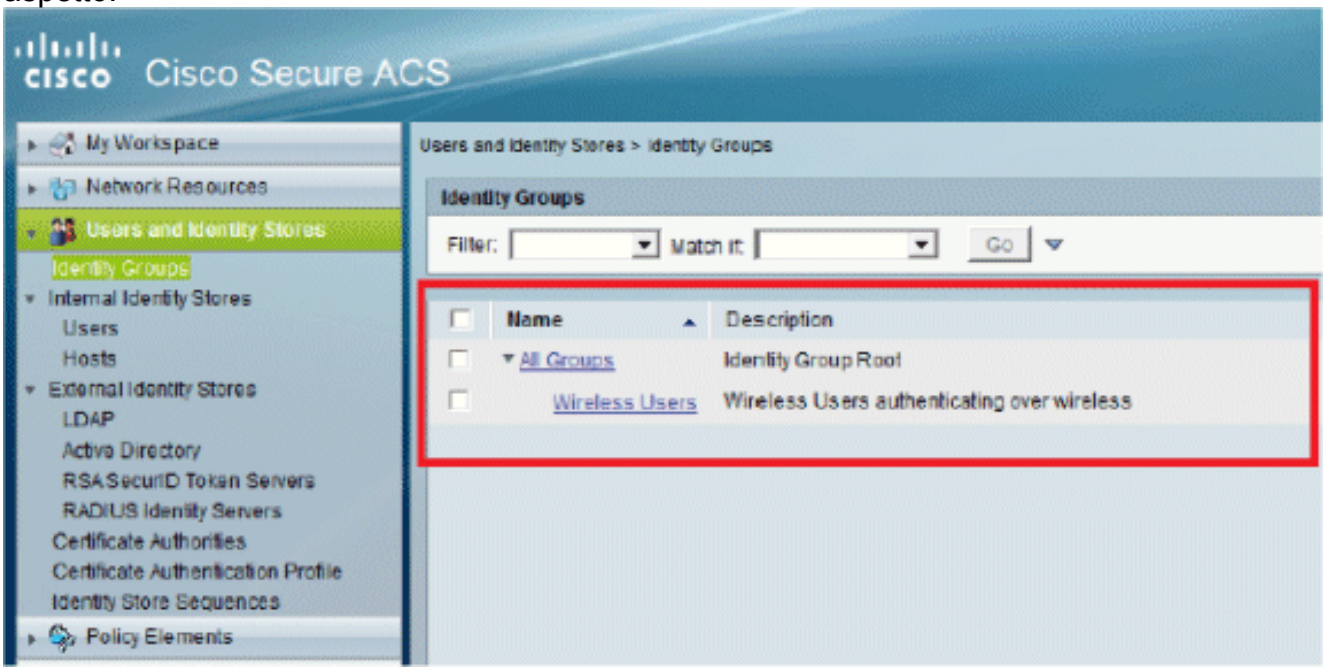
Configura utenti

In questa sezione verranno creati utenti locali su ACS. Entrambi gli utenti (utente1 e utente2) vengono assegnati nel gruppo denominato "Utenti wireless".

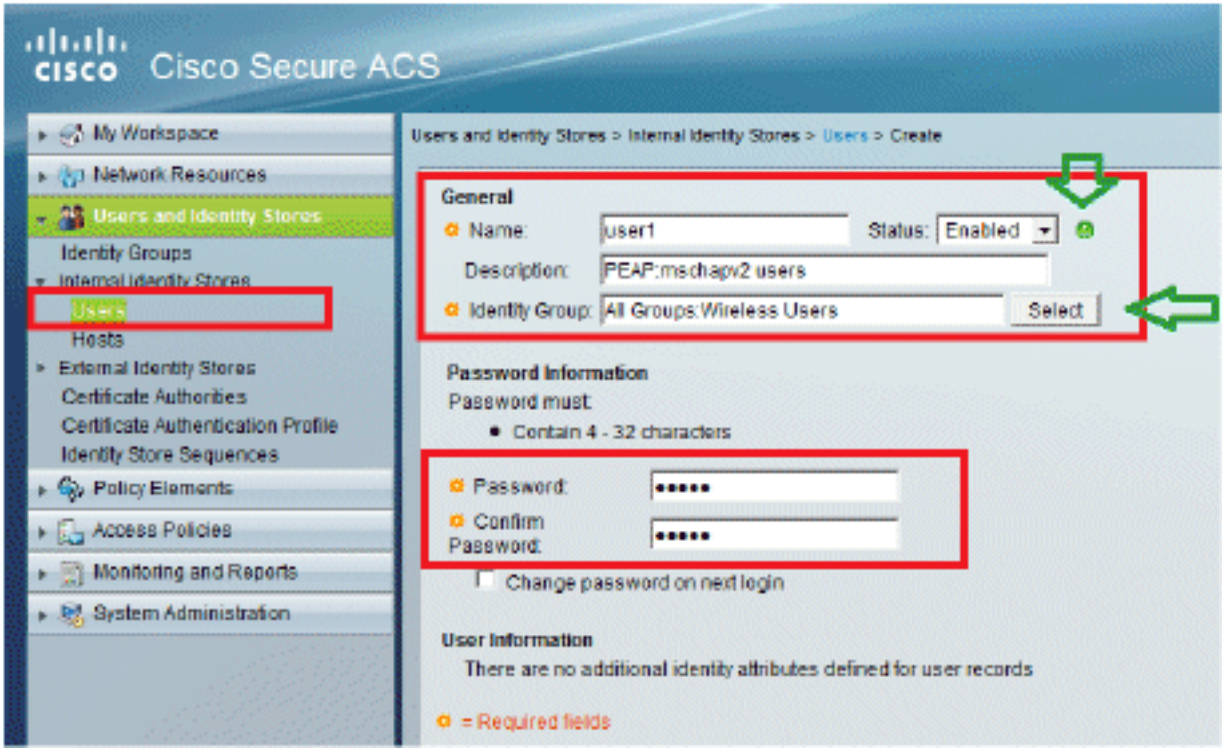
1. Andare a **Utenti e archivi identità > Gruppi di identità > Crea**.



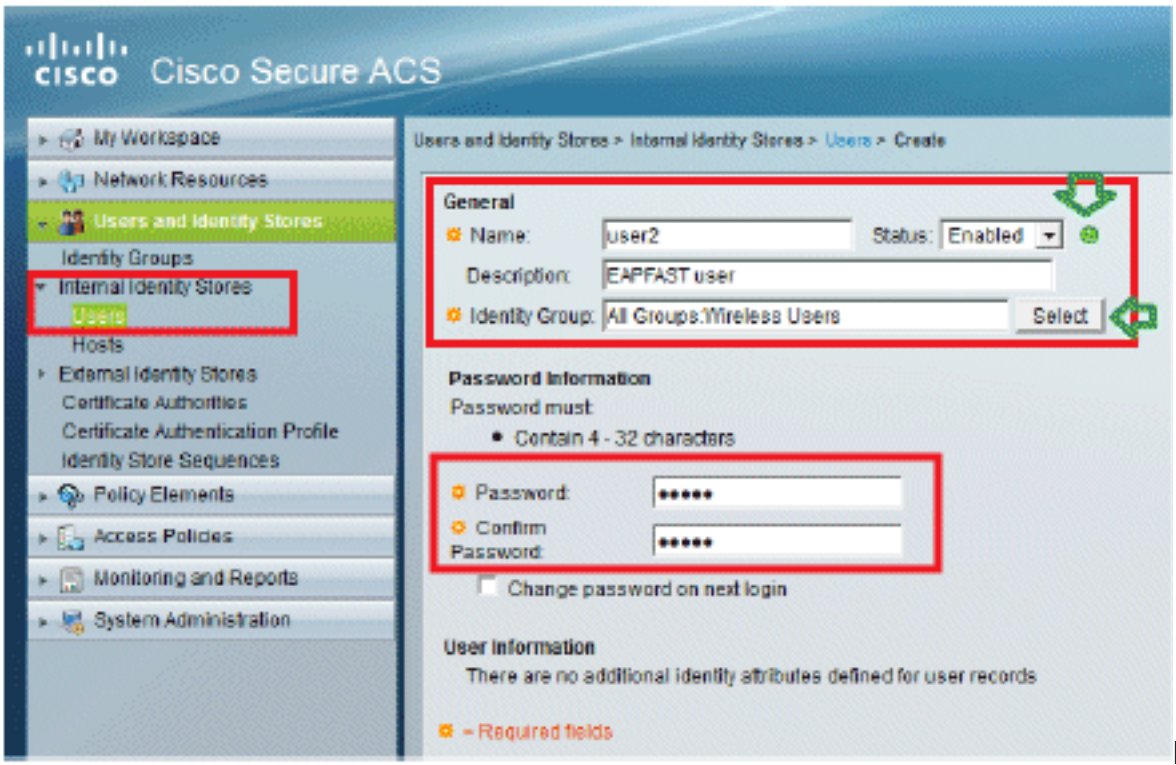
2. Dopo aver fatto clic su **Invia**, la pagina avrà il seguente aspetto:

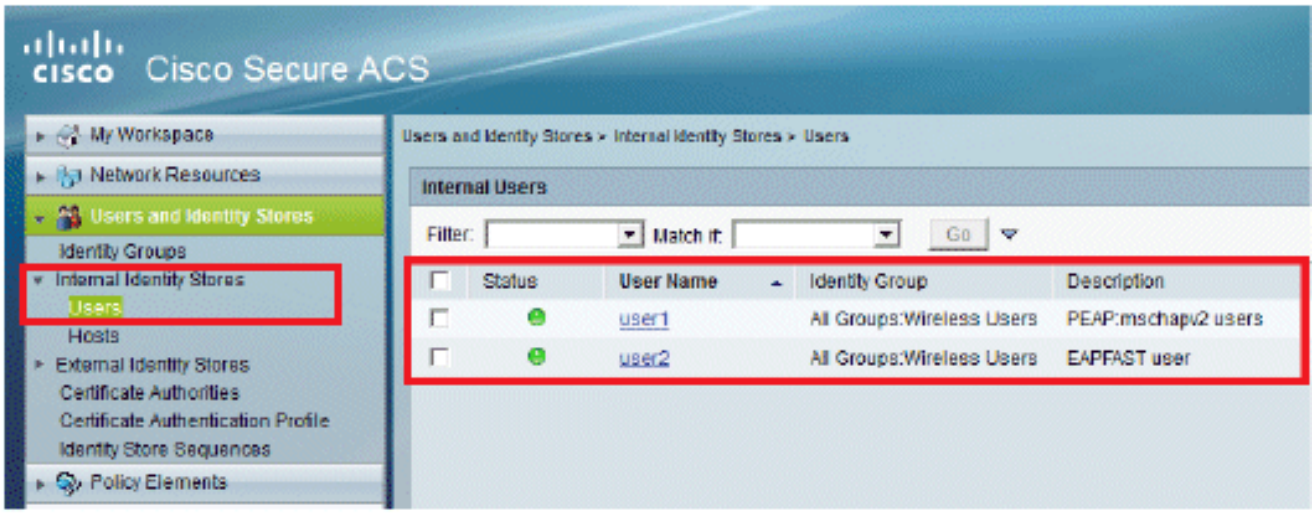


3. Creare gli utenti **user1** e **user2**, quindi assegnarli al gruppo "Wireless Users".Fare clic su **Utenti e archivi identità > Gruppi di identità > Utenti >**



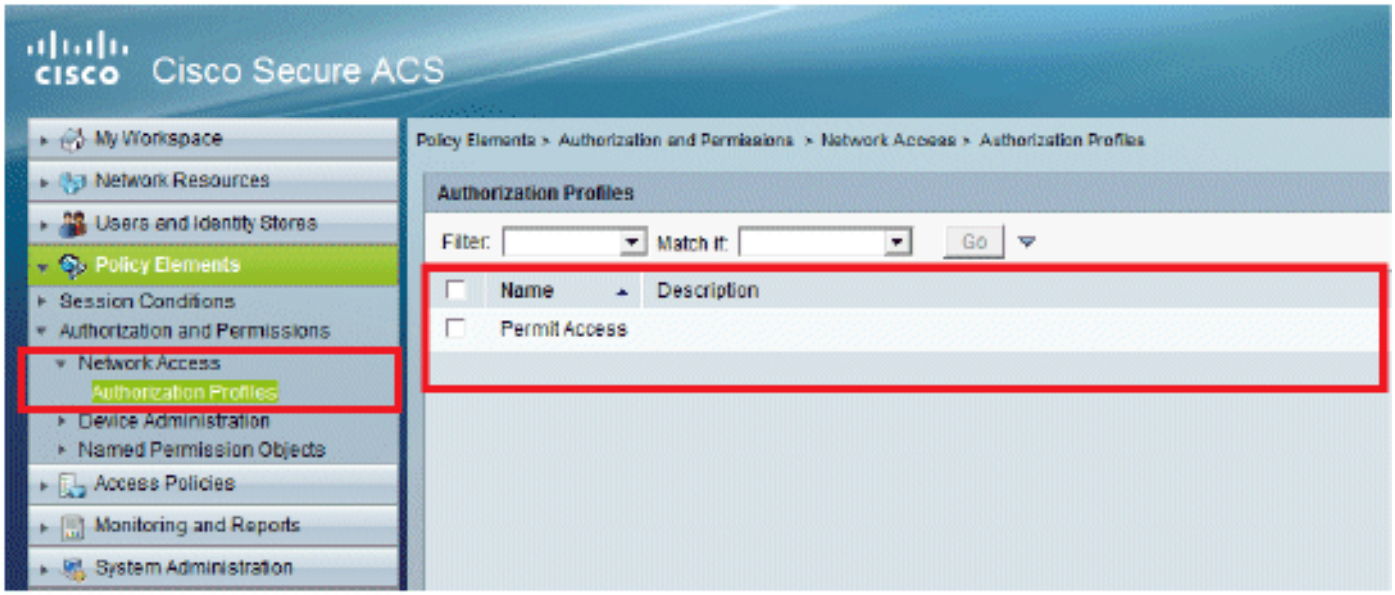
Crea. Analogamente, create user2. Lo schermo avrà il seguente aspetto:





Definizione degli elementi dei criteri

Verificare che l'opzione **Permit Access** sia impostata.

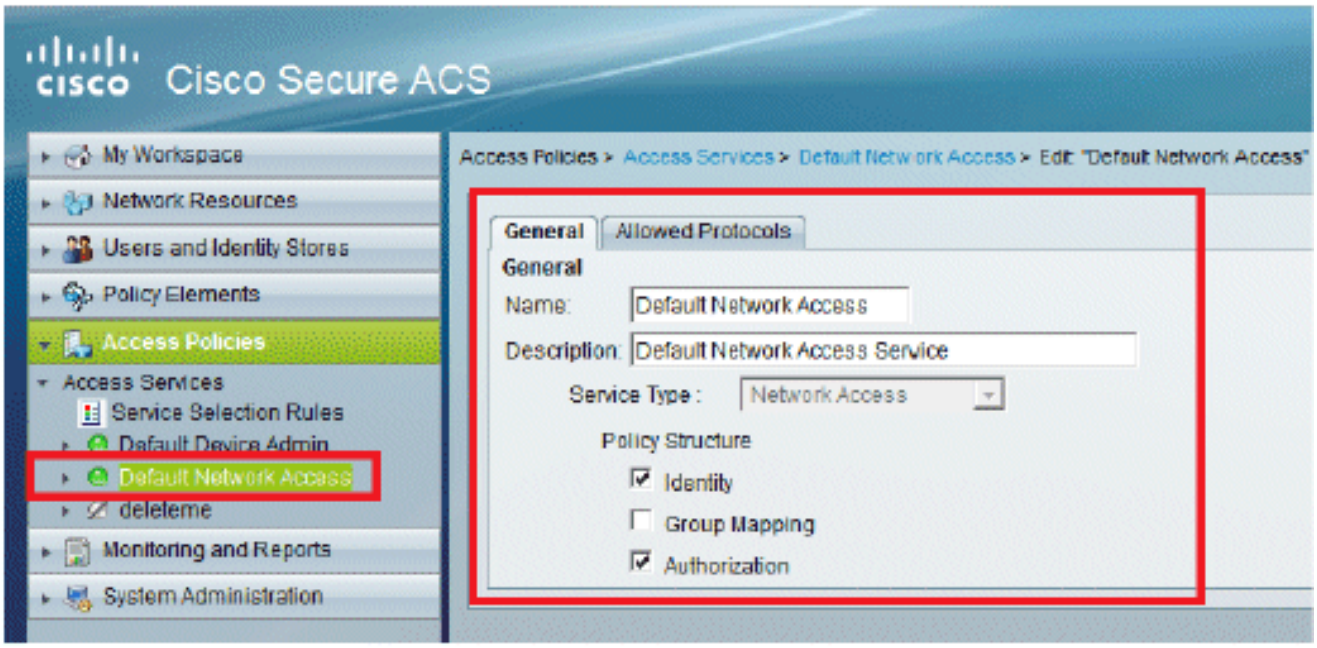


Applica criteri di accesso

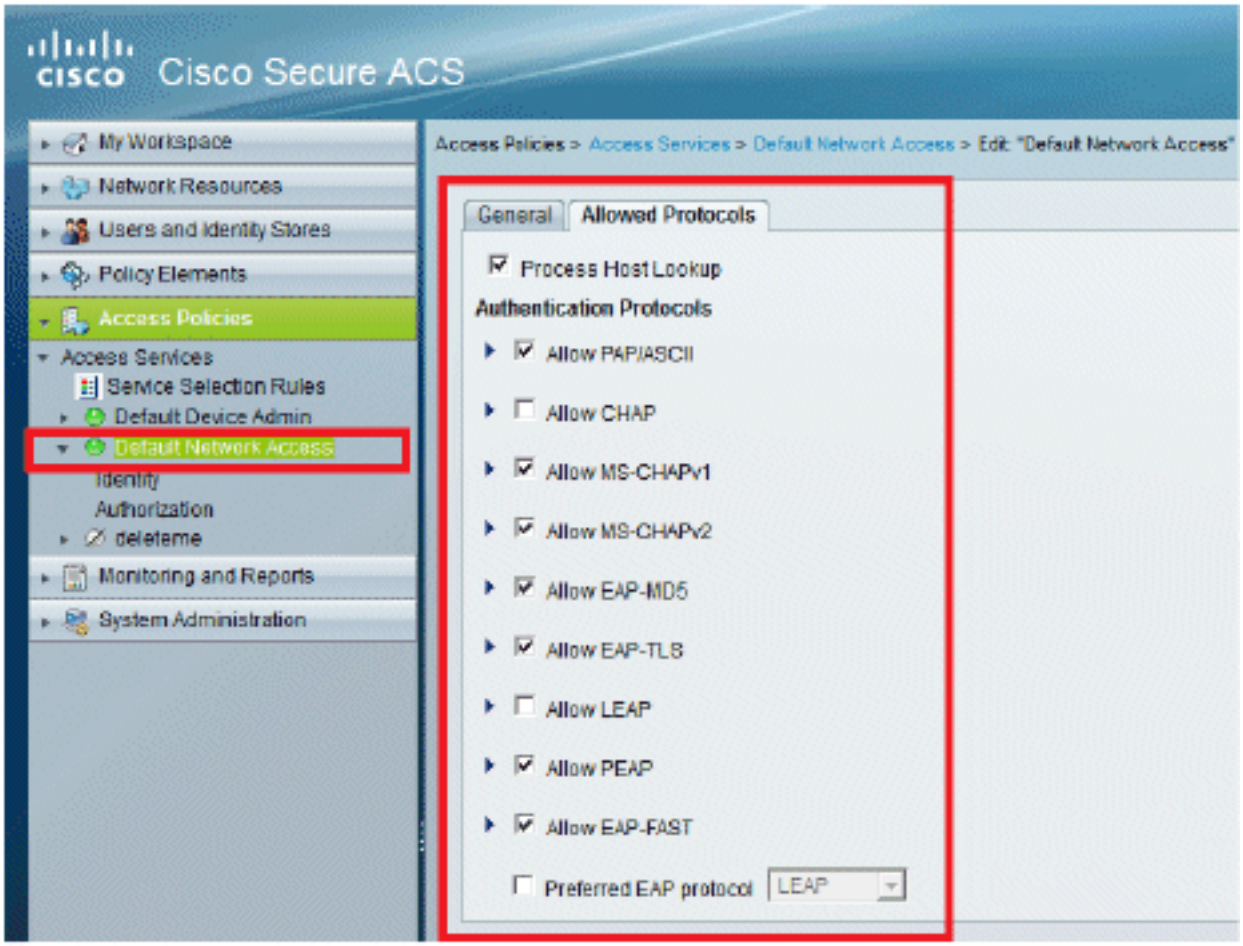
In questa sezione verranno selezionati i metodi di autenticazione da utilizzare e la modalità di configurazione delle regole. Le regole verranno create in base ai passaggi precedenti.

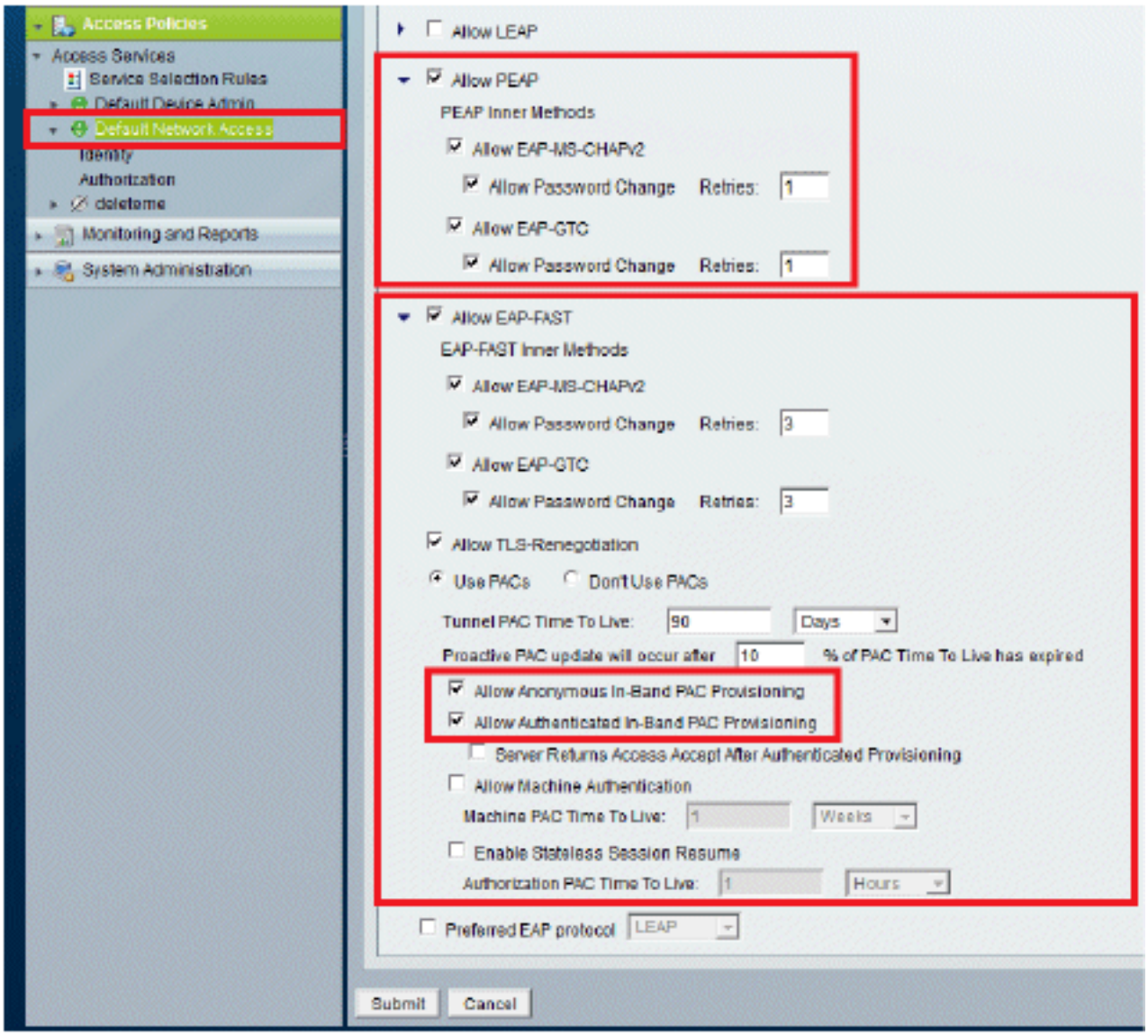
Attenersi alla seguente procedura:

1. Selezionare **Access Policies > Access Services > Default Network Access > Edit: "Default Network Access"**.

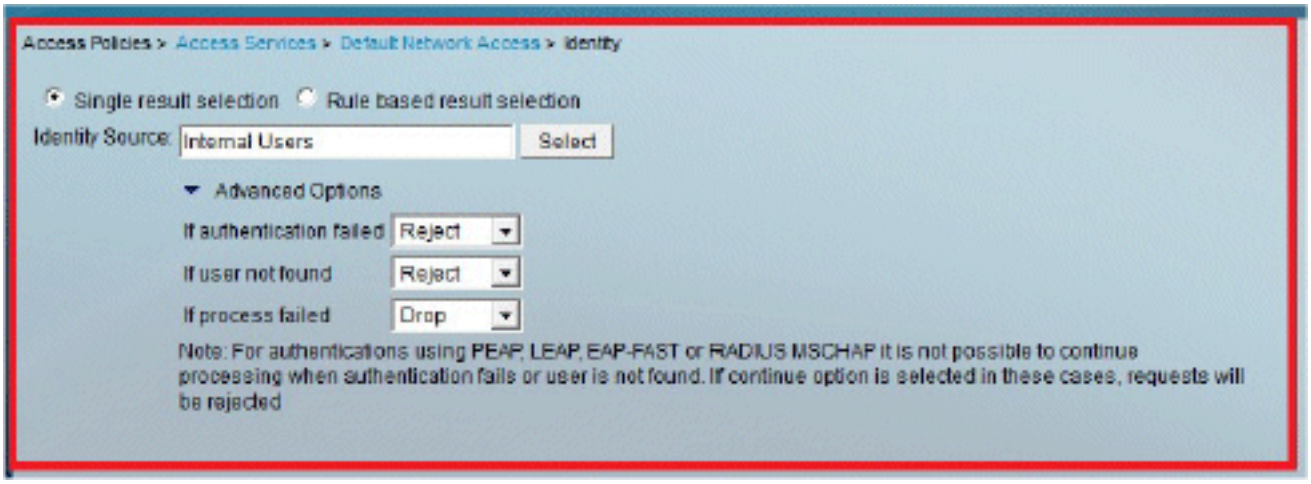


2. Selezionare il metodo EAP che si desidera venga autenticato dai client wireless. Nell'esempio vengono utilizzati **PEAP- MSCHAPv2** e **EAP-FAST**.



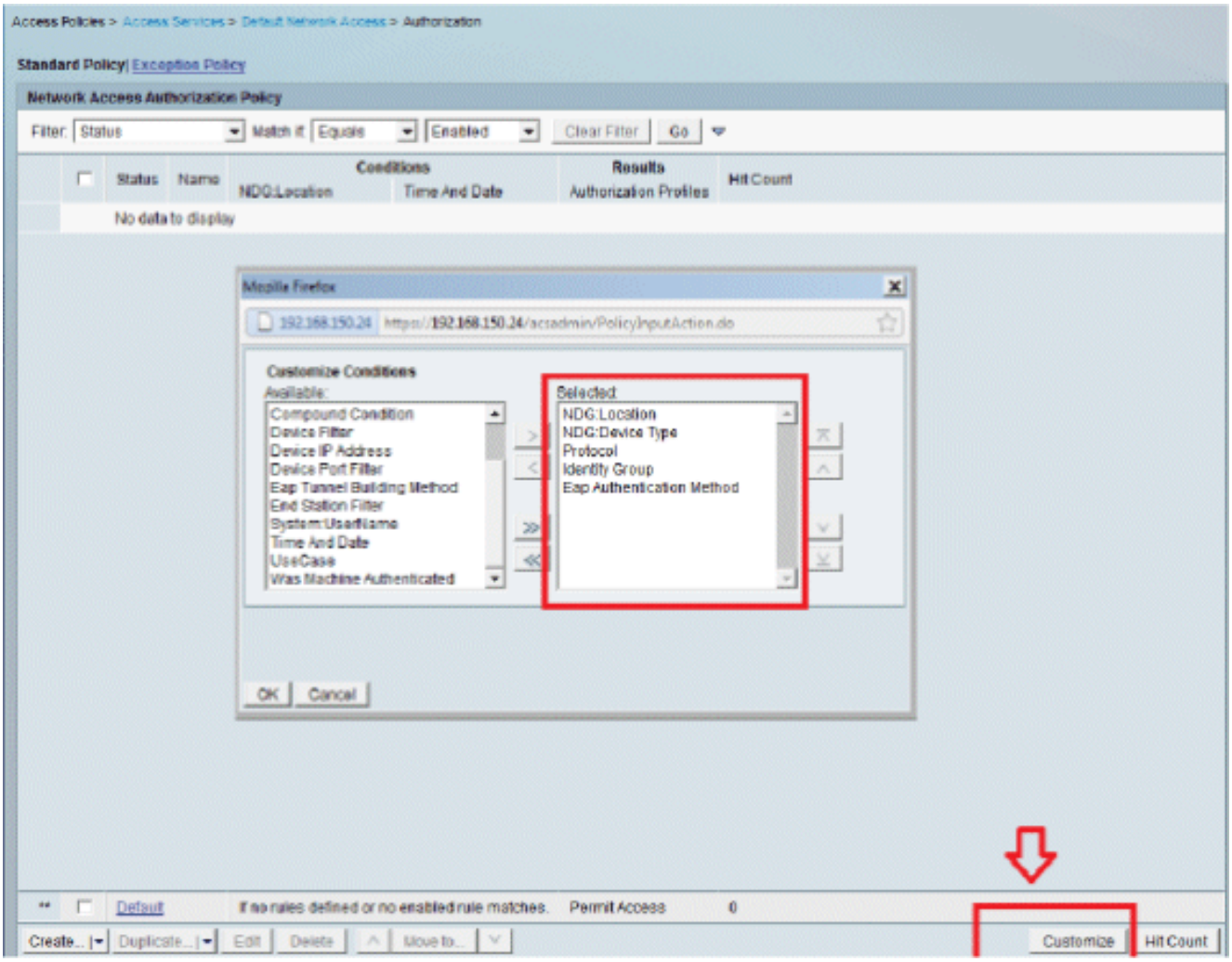


3. Fare clic su **Invia**.
4. Verificare il gruppo di identità selezionato. In questo esempio, viene utilizzato **Internal Users**, creato su ACS. **Salvare** le modifiche.

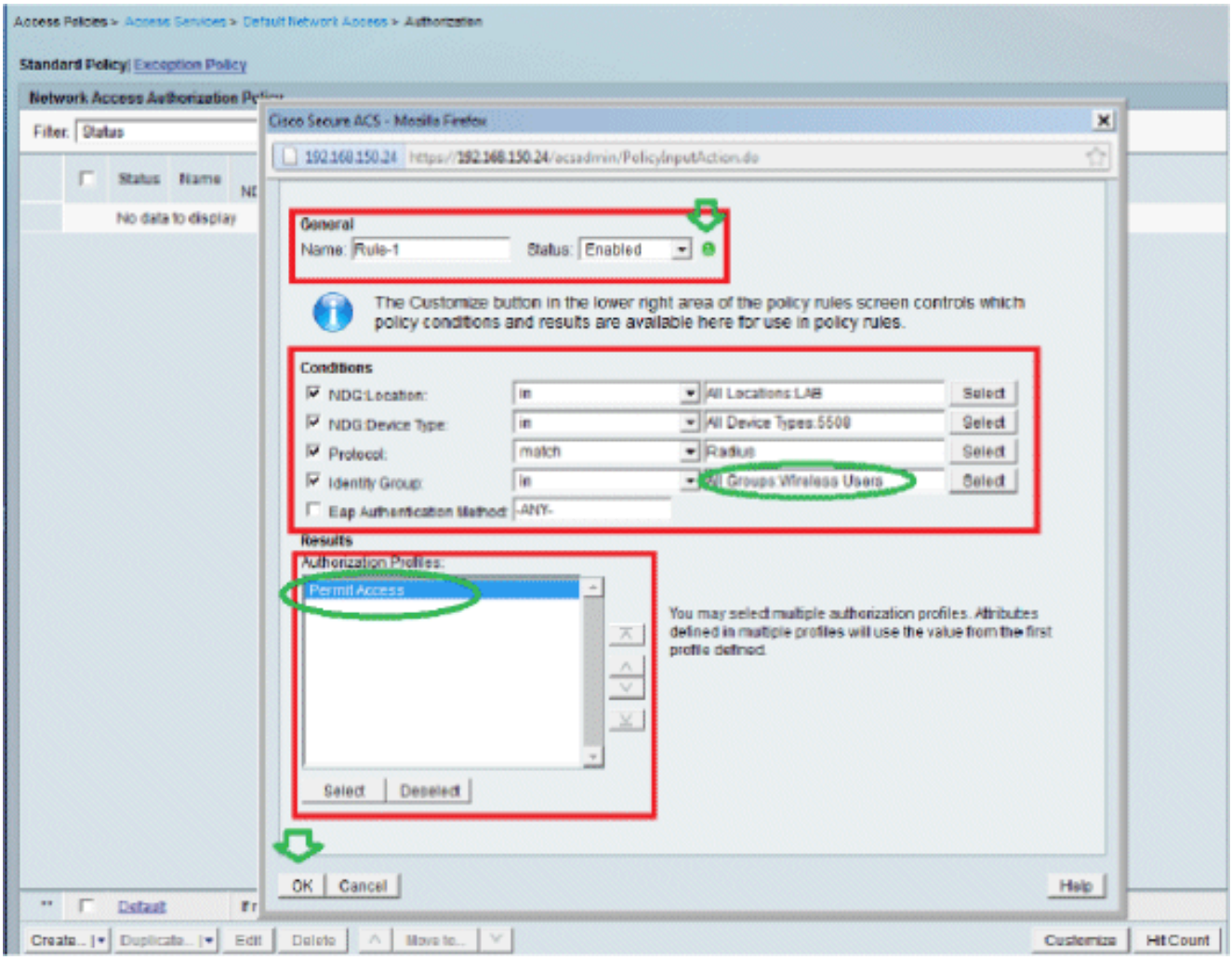


5. Per verificare il profilo di autorizzazione, selezionare **Access Policies > Access Services > Default Network Access > Authorization** (Policy di accesso **> Servizi di accesso > Accesso di rete predefinito**).Èpossibile personalizzare in base a quali condizioni sarà consentito l'accesso degli utenti alla rete e in quali profili di autorizzazione (attributi) sarà possibile passare dopo l'autenticazione. Questa granularità è disponibile solo in ACS 5.x. In questo

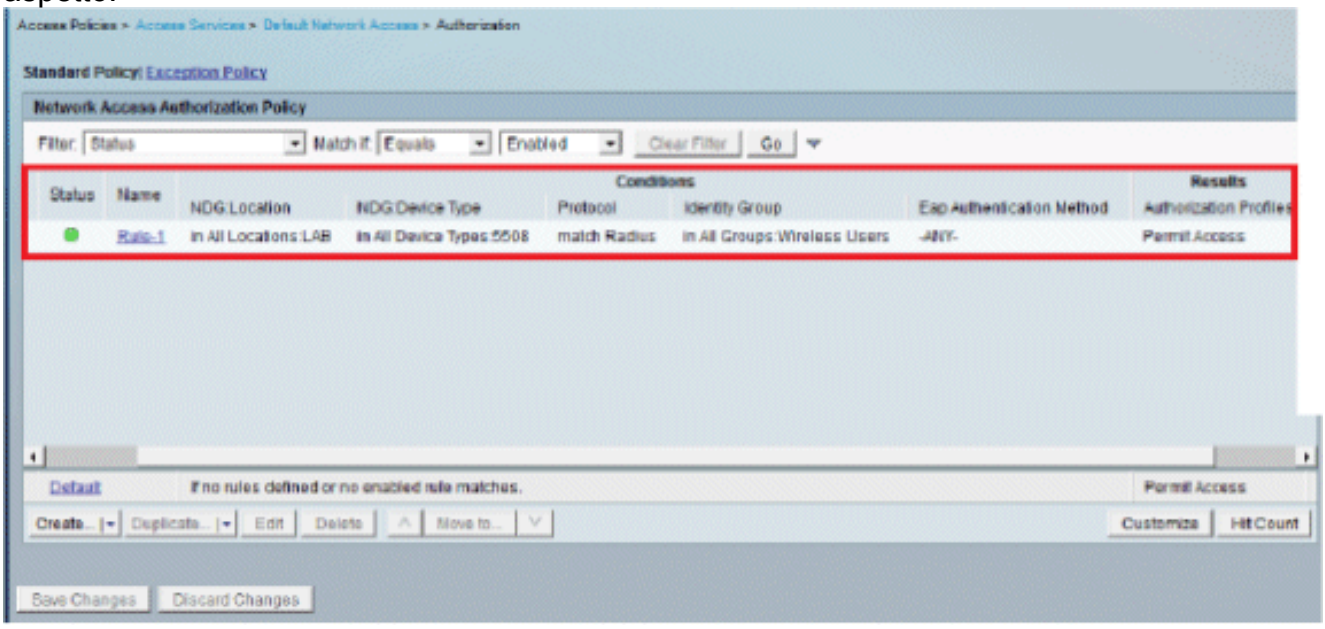
esempio sono stati selezionati Location, **Device Type**, **Protocol**, **Identity Group** e **EAP Authentication Method**.



6. Fare clic su **OK**, quindi su **Salva modifiche**.
7. Il passaggio successivo consiste nella creazione di una regola. Se non viene definita alcuna regola, al client viene consentito l'accesso senza condizioni.Selezionate **Crea (Create) > Regola-1 (Rule-1)**. Questa regola è destinata agli utenti del gruppo "Utenti wireless".

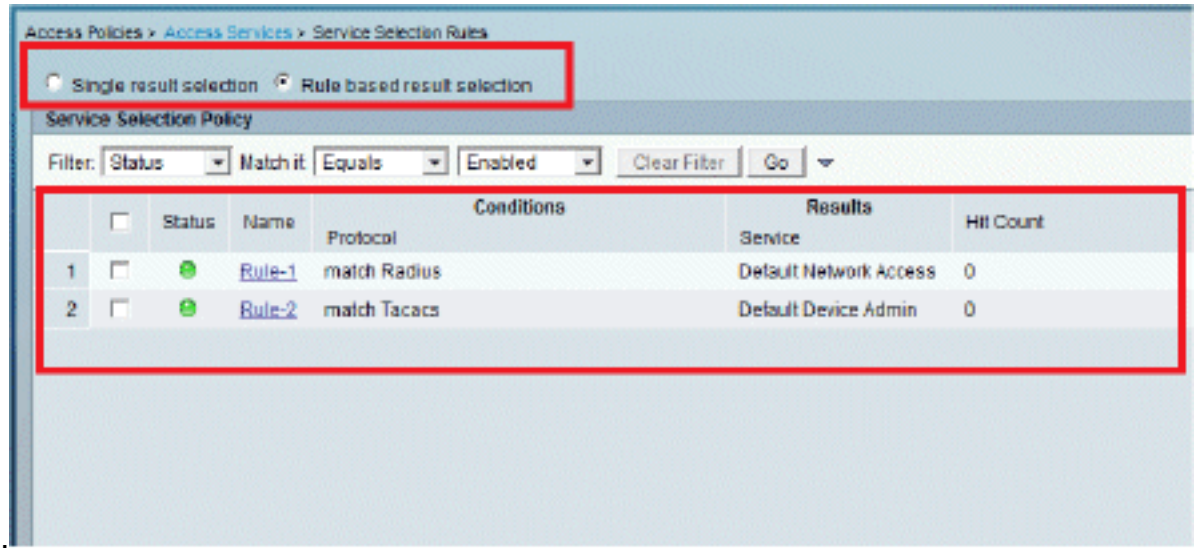


8. Salvare le modifiche. Lo schermo avrà il seguente aspetto:



Se si desidera negare agli utenti che non soddisfano le condizioni, modificare la regola predefinita in "nega accesso".

9. Verranno ora definite **le regole di selezione del servizio**. Utilizzare questa pagina per configurare un criterio semplice o basato su regole per determinare il servizio da applicare alle richieste in ingresso. In questo esempio viene utilizzato un criterio basato su

regole. 

Configurare il WLC

Questa configurazione richiede i seguenti passaggi:

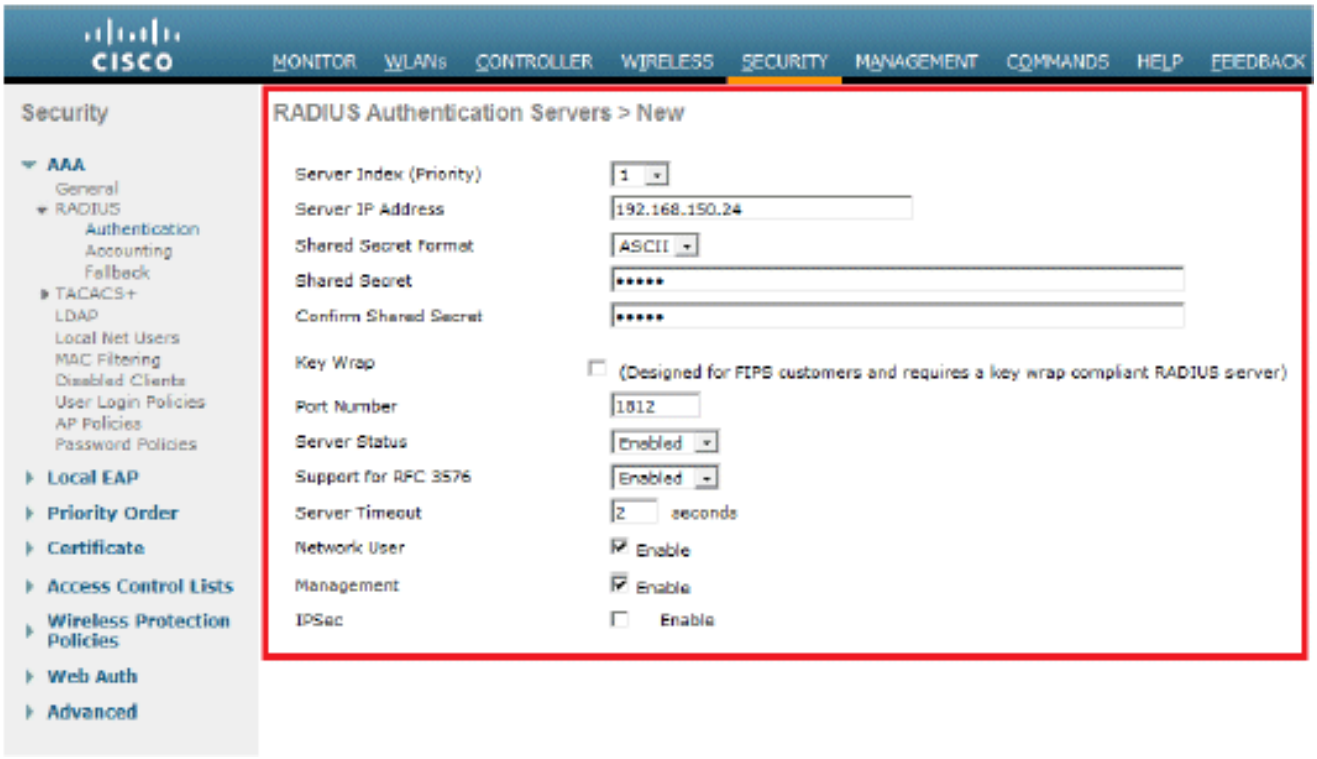
1. Configurare il WLC con i dettagli del server di autenticazione.
2. Configurare le interfacce dinamiche (VLAN).
3. Configurare le WLAN (SSID).

Configurare il WLC con i dettagli del server di autenticazione

Ènecessario configurare il WLC in modo che possa comunicare con il server RADIUS per autenticare i client e per qualsiasi altra transazione.

Attenersi alla seguente procedura:

1. Dalla GUI del controller, fare clic su **Security** (Sicurezza).
2. Immettere l'indirizzo IP del server RADIUS e la chiave privata condivisa utilizzata tra il server RADIUS e il WLC.La chiave privata condivisa deve essere uguale a quella configurata nel server
RADIUS.

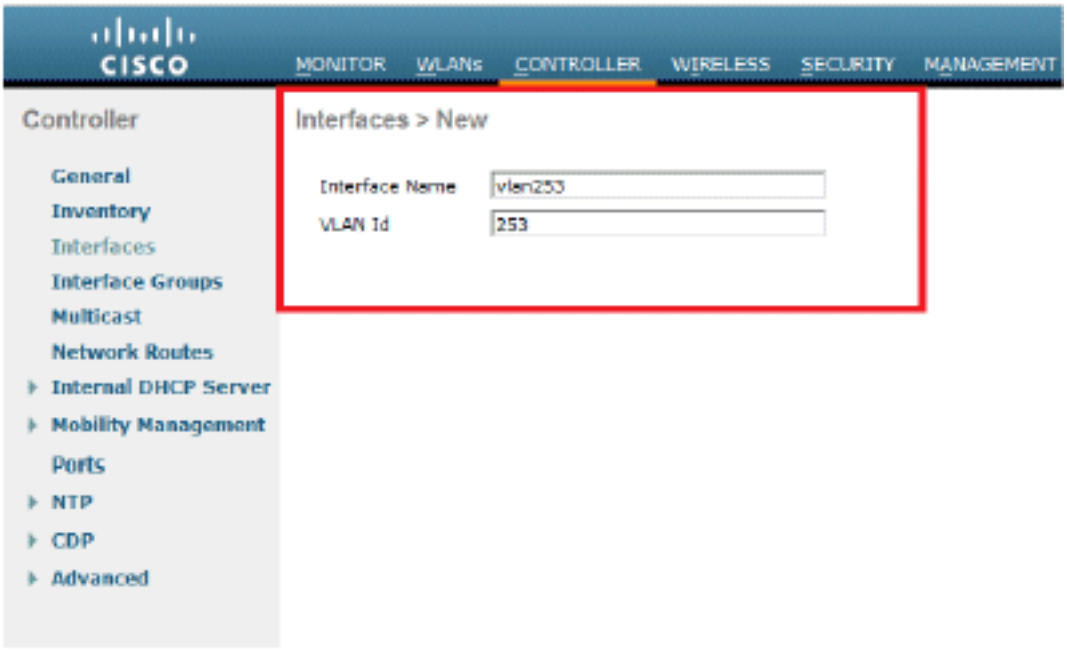


Configurazione delle interfacce dinamiche (VLAN)

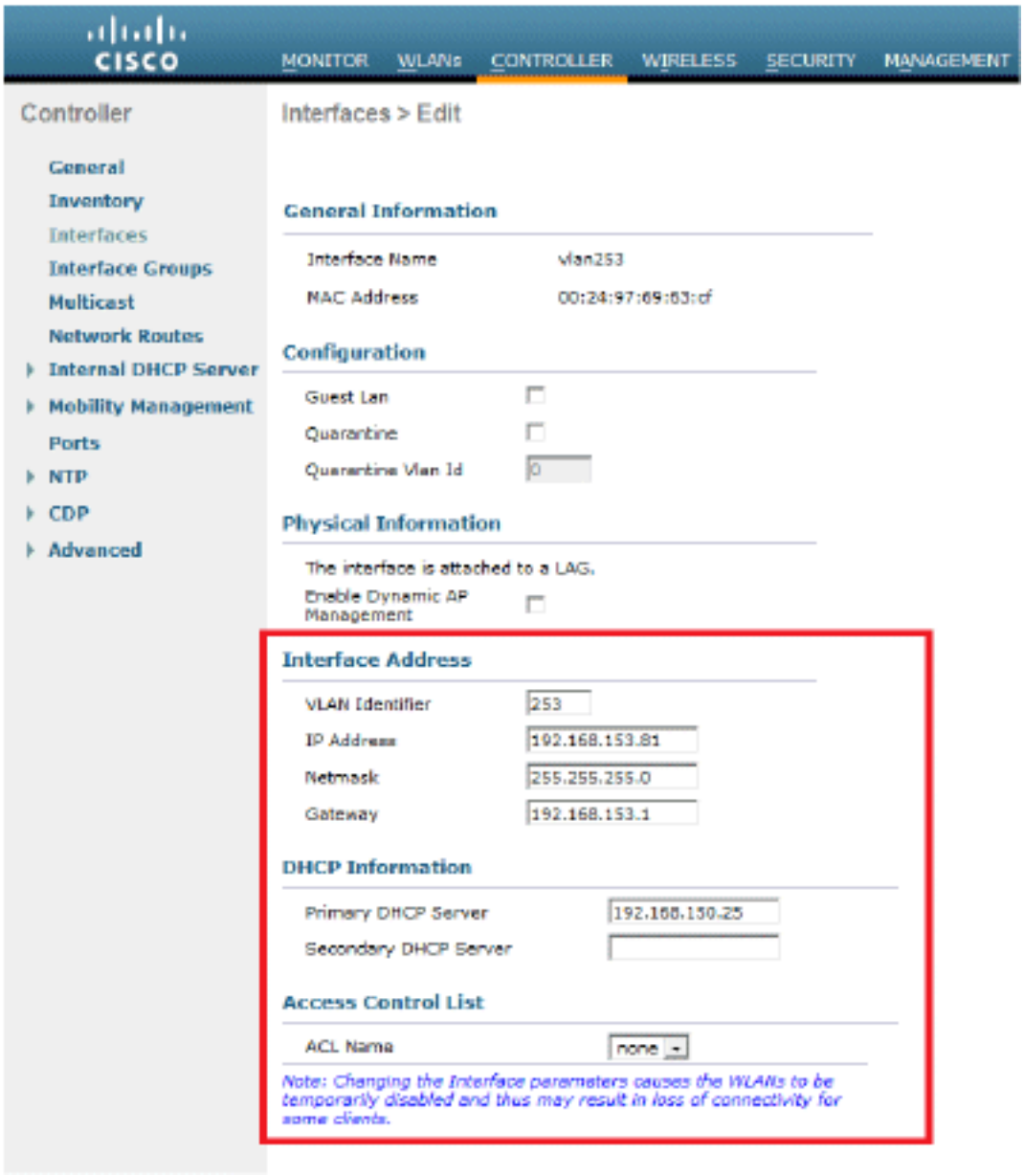
In questa procedura viene descritto come configurare le interfacce dinamiche sul WLC.

Attenersi alla seguente procedura:

1. L'interfaccia dinamica viene configurata dalla GUI del controller nella finestra **Controller >**

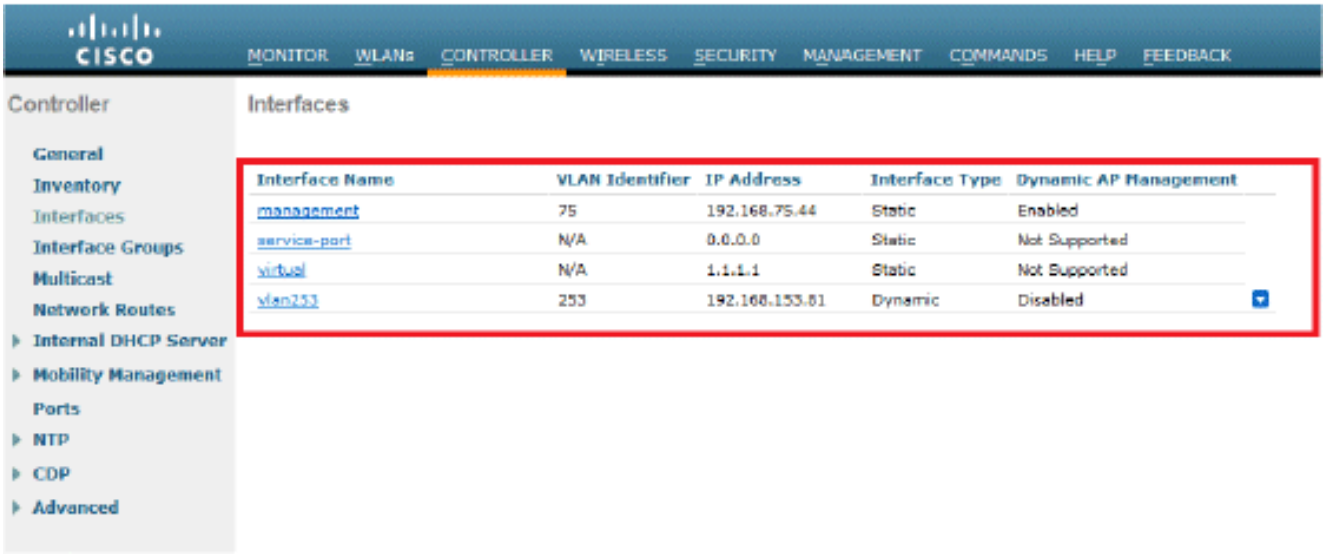


Interfacce.
2. Fare clic su **Apply** (Applica).Viene visualizzata la finestra Edit (Modifica) di questa interfaccia dinamica (qui VLAN 253).
3. Immettere l'indirizzo IP e il gateway predefinito dell'interfaccia



dinamica.

4. Fare clic su **Apply** (Applica).
5. Le interfacce configurate avranno il seguente aspetto:

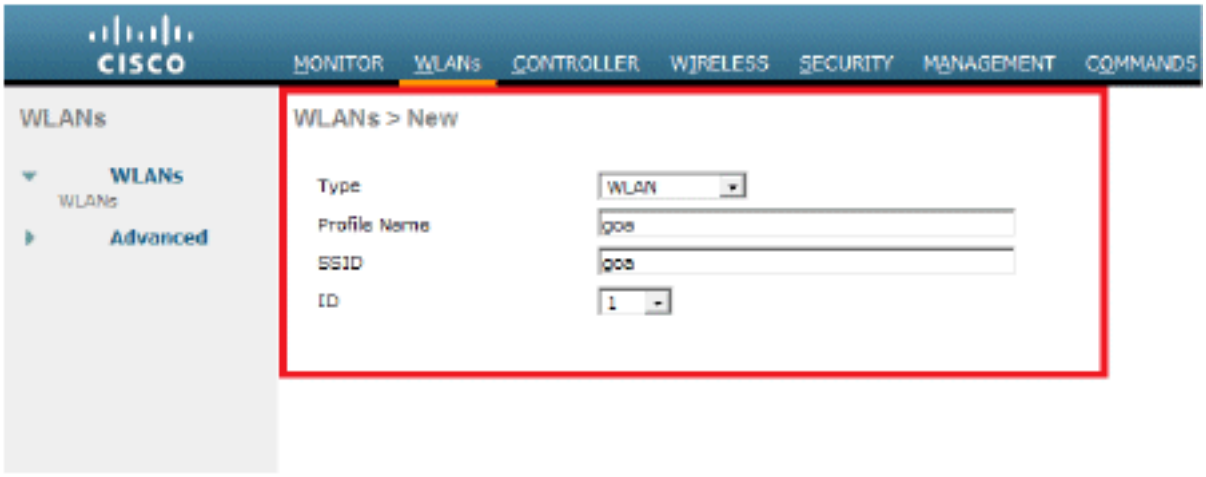


Configurazione delle WLAN (SSID)

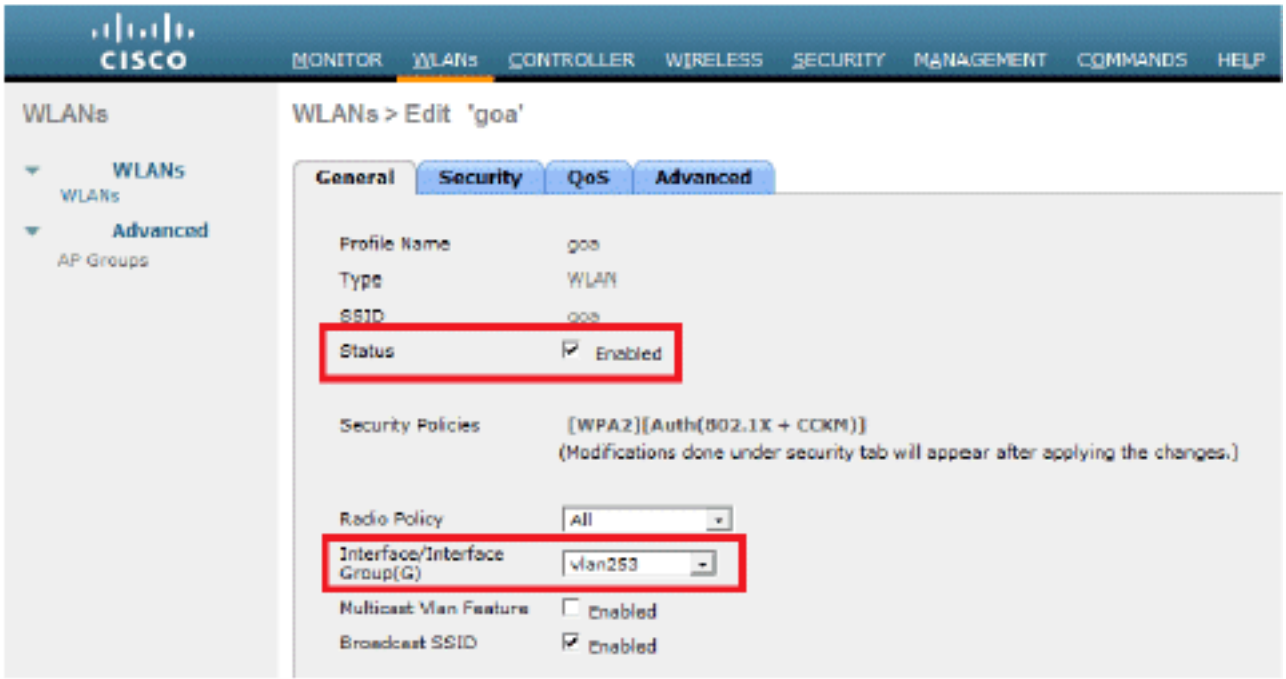
In questa procedura viene spiegato come configurare le WLAN nel WLC.

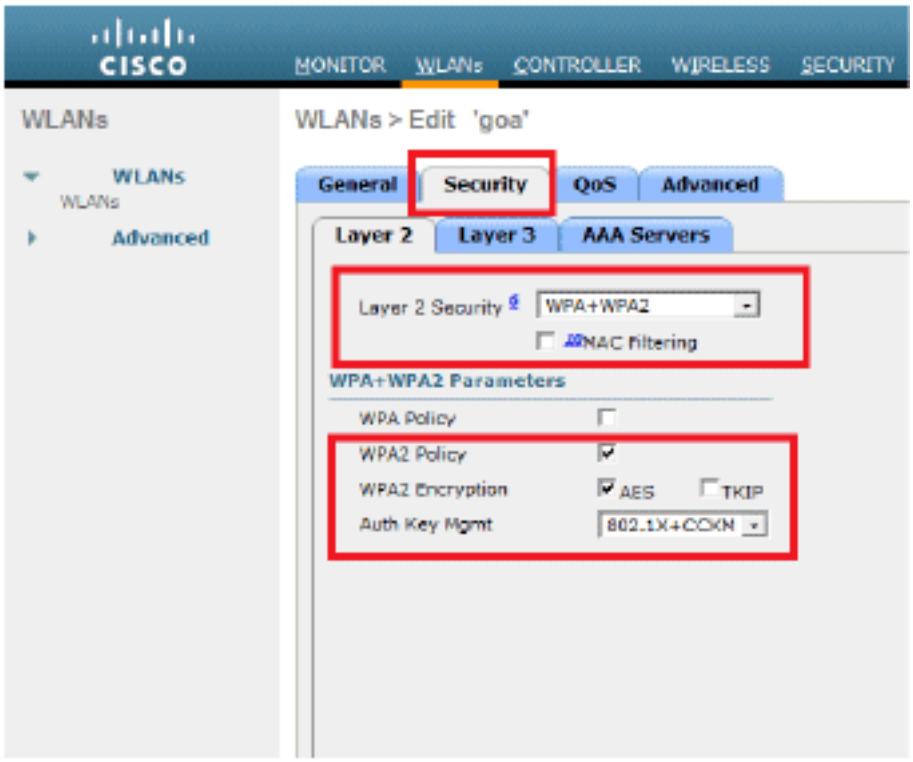
Attenersi alla seguente procedura:

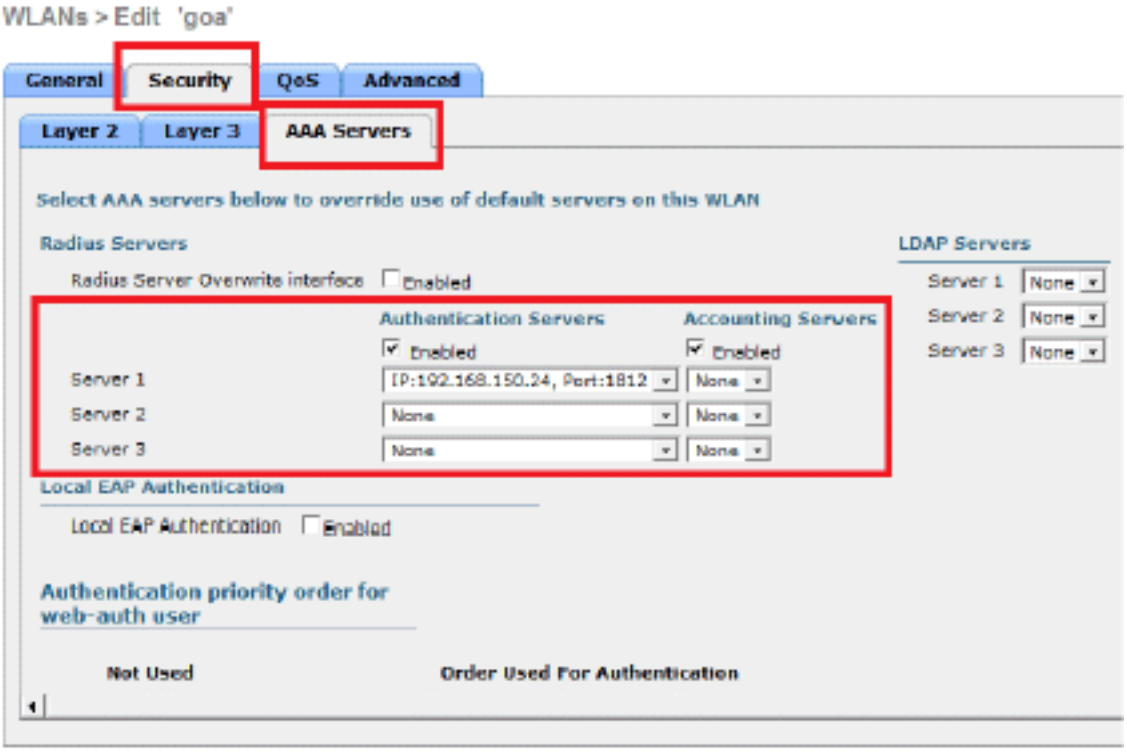
1. Dalla GUI del controller, selezionare **WLAN > Create New** (Crea nuova) per creare una nuova WLAN. Viene visualizzata la finestra Nuove WLAN.
2. Immettere l'ID WLAN e le informazioni sull'SSID WLAN.Èpossibile immettere qualsiasi nome come SSID WLAN. In questo esempio viene usato **goa** come SSID della WLAN.

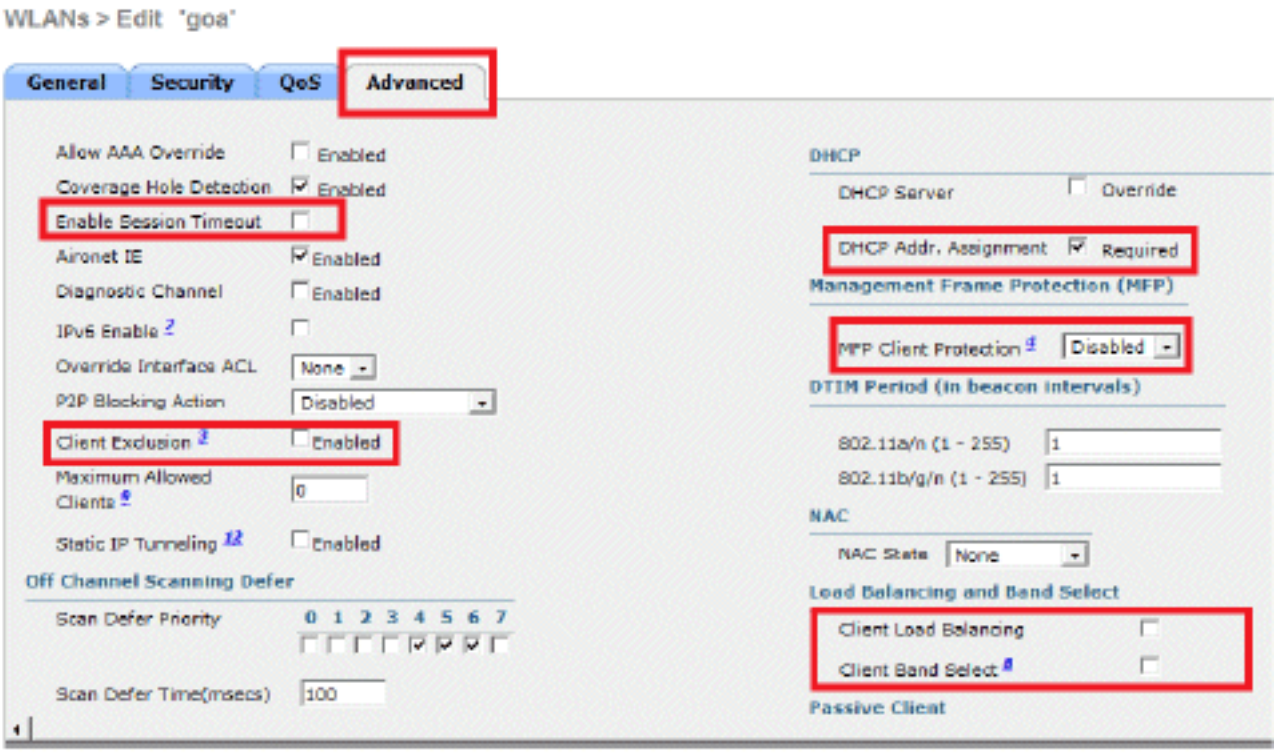


3. Per accedere alla finestra Edit (Modifica) dell'obiettivo WLAN, fare clic su **Apply** (Applica).




MONITOR
WLANs
CONTROLLER
WIRELESS
SECURITY
WLANs
WLANs > Edit 'goa'
WLANs
WLANs
Advanced
General
Security
QoS
Advanced
Layer 2
Layer 3
AAA Servers
Layer 2 Security
WPA+WPA2
MAC Filtering
WPA+WPA2 Parameters
WPA Policy
WPA2 Policy
WPA2 Encryption
AES
TKIP
Auth Key Mgmt
802.1X+CCKM


WLANs > Edit 'goa'
General
Security
QoS
Advanced
Layer 2
Layer 3
AAA Servers
Select AAA servers below to override use of default servers on this WLAN
Radius Servers
Radius Server Overwrite interface
Enabled
Authentication Servers
Accounting Servers
Enabled
Enabled
Server 1
IP:192.168.150.24, Port:1812
None
Server 2
None
None
Server 3
None
None
LDAP Servers
Server 1
None
Server 2
None
Server 3
None
Local EAP Authentication
Local EAP Authentication
Enabled
Authentication priority order for web-auth user
Not Used
Order Used For Authentication



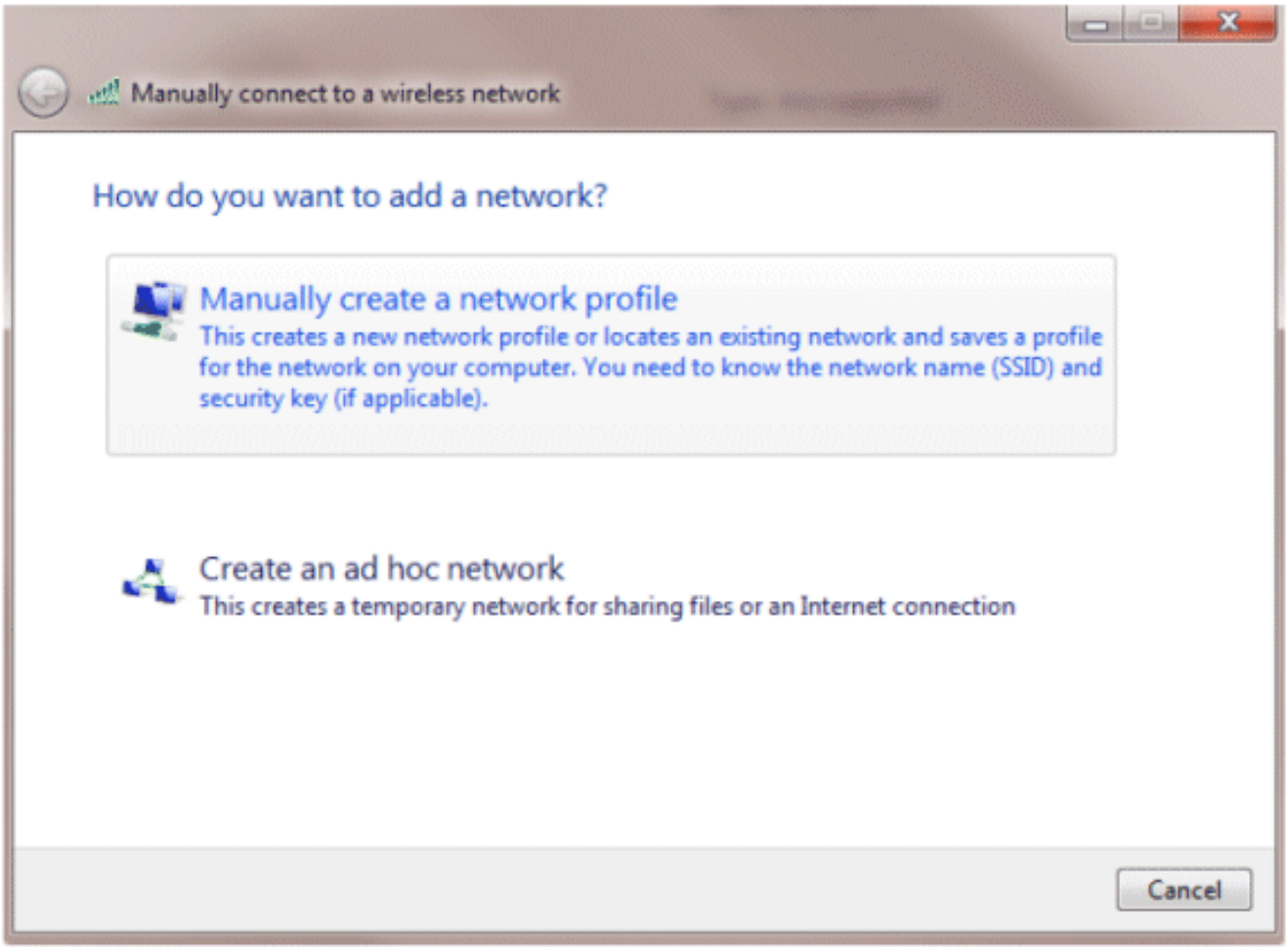
Configurare Wireless Client Utility

PEAP-MSCHAPv2 (utente1)

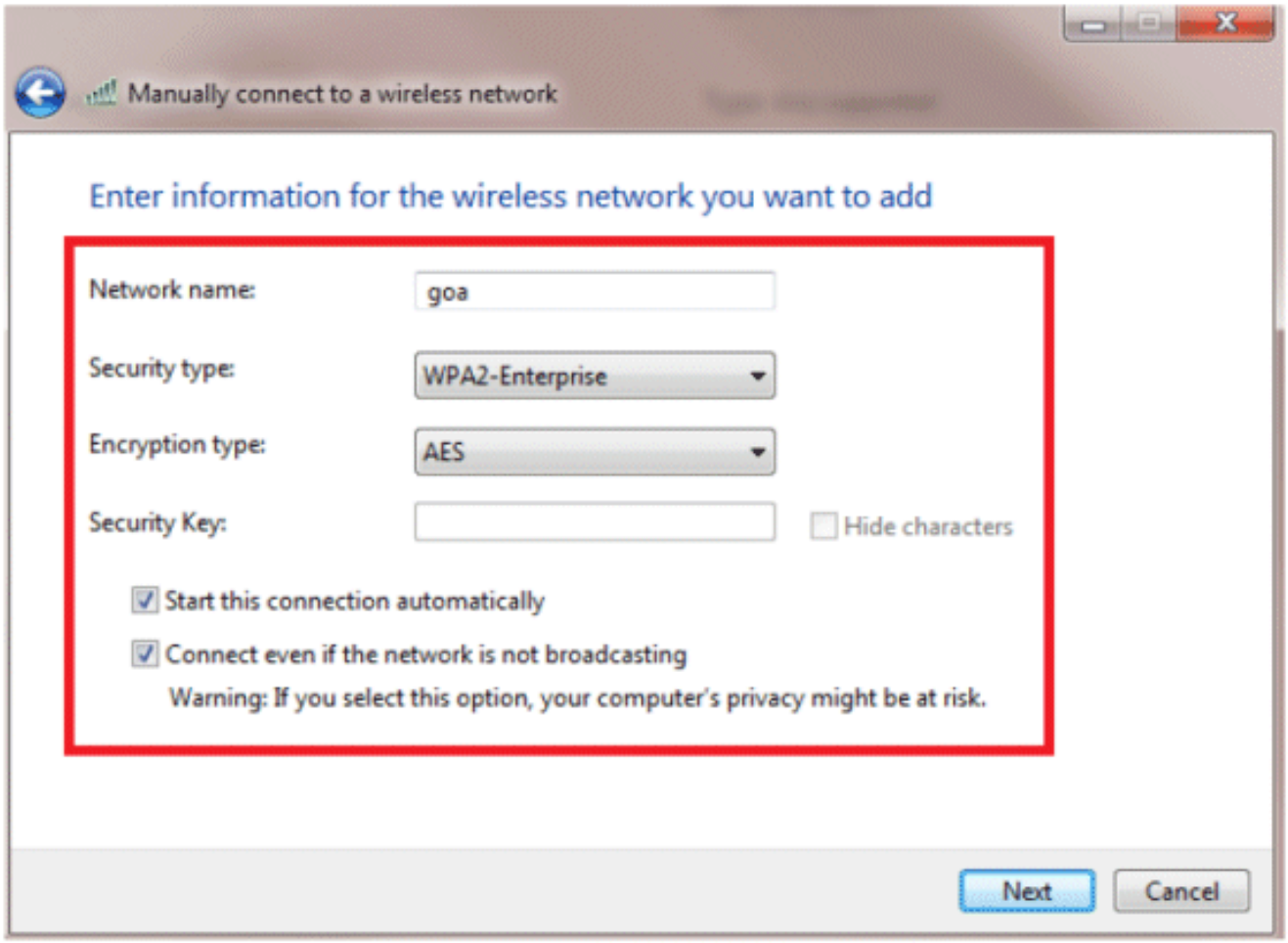
Nel nostro client di test, utilizziamo Windows 7 Native Supplicant con una scheda Intel 6300-N con versione del driver 14.3. È consigliabile eseguire il test utilizzando i driver più recenti dei fornitori.

Completare questa procedura per creare un profilo in Windows Zero Config (WZC):

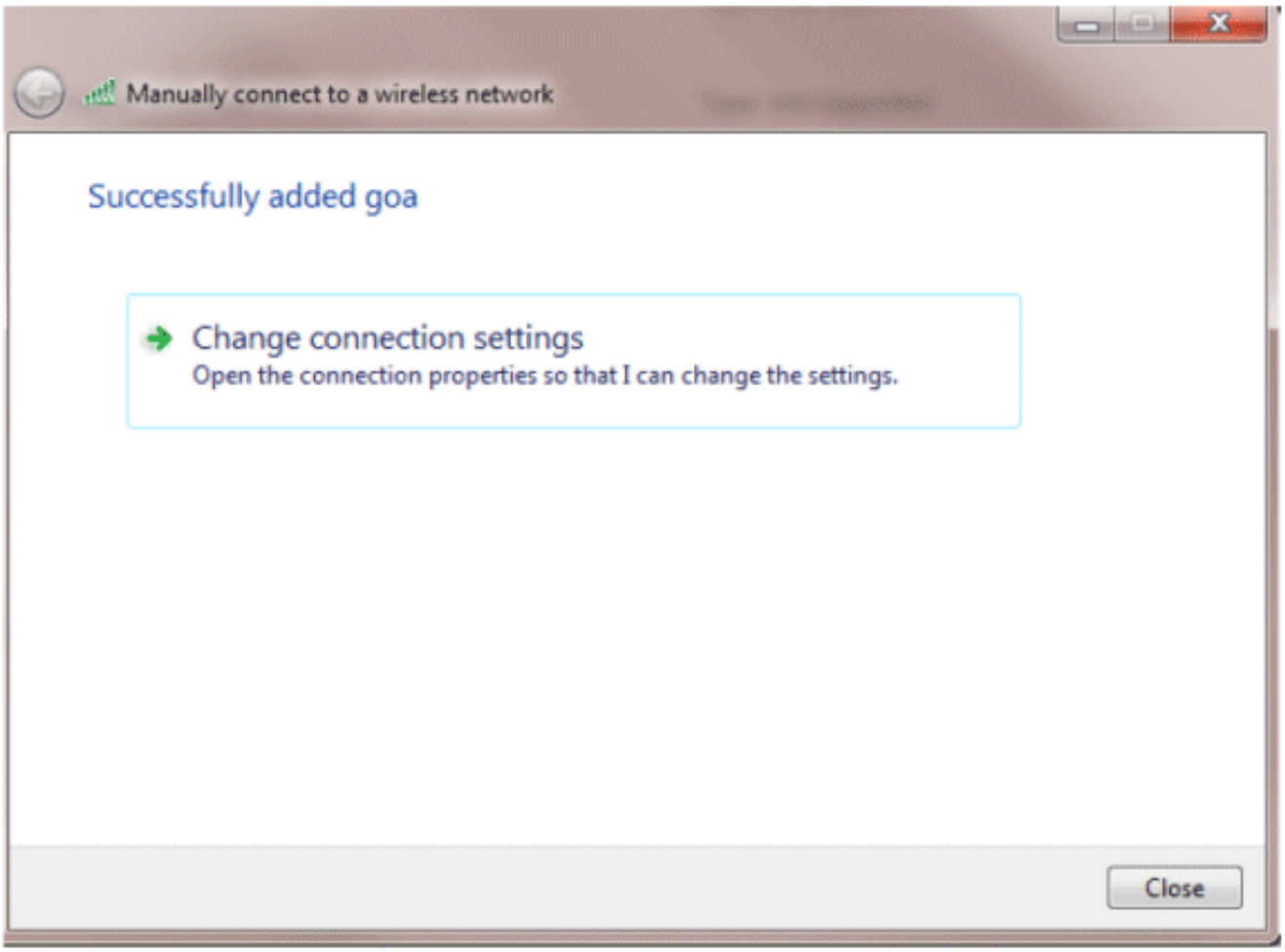
1. Selezionare **Pannello di controllo > Rete e Internet > Gestisci reti wireless**.
2. Fare clic sulla scheda **Aggiungi**.
3. Fare clic su **Crea manualmente un profilo di rete**.



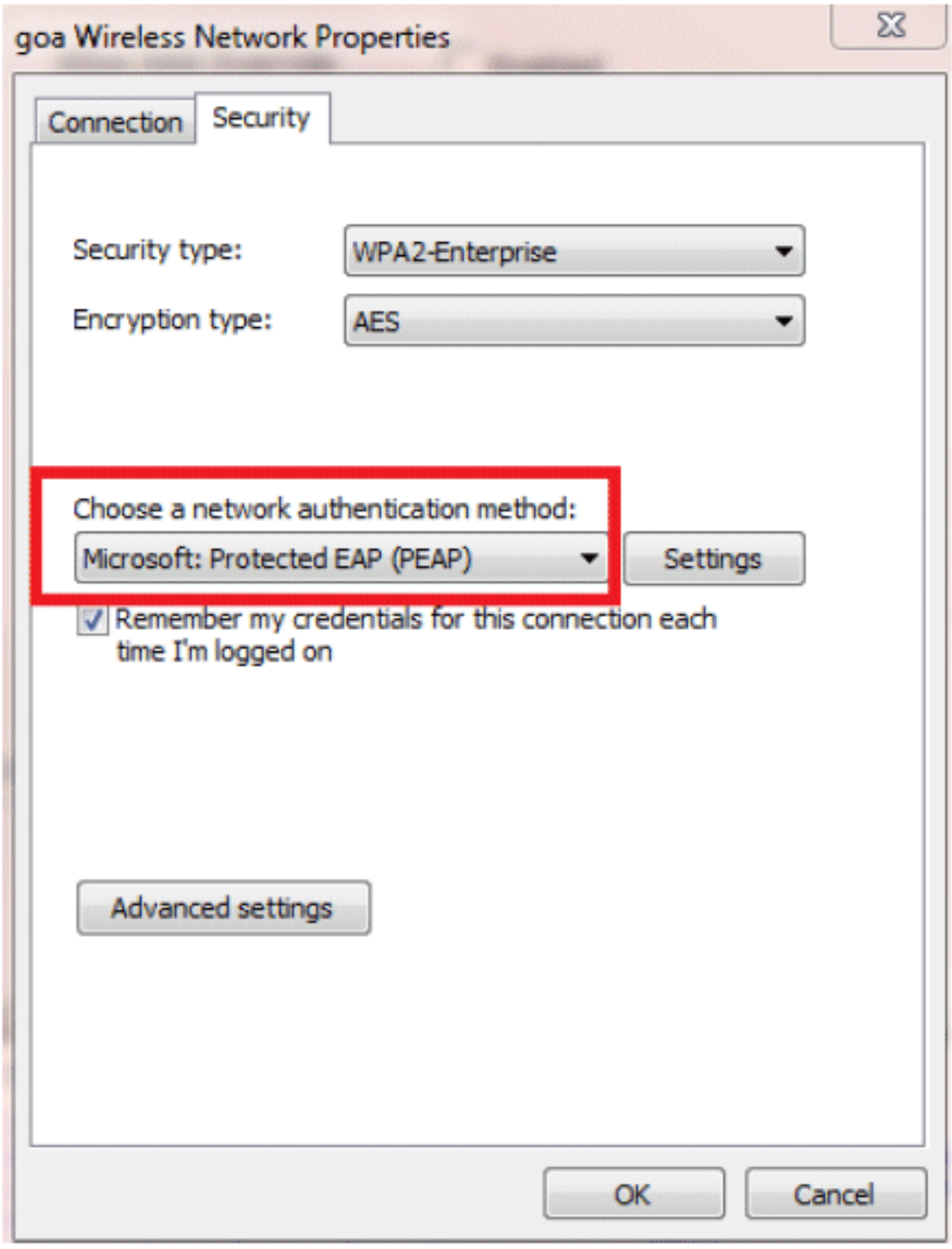
4. Aggiungere i dettagli come configurato sul WLC.**Nota:** per SSID viene fatta distinzione tra maiuscole e minuscole.
5. Fare clic su **Next**
   (Avanti).

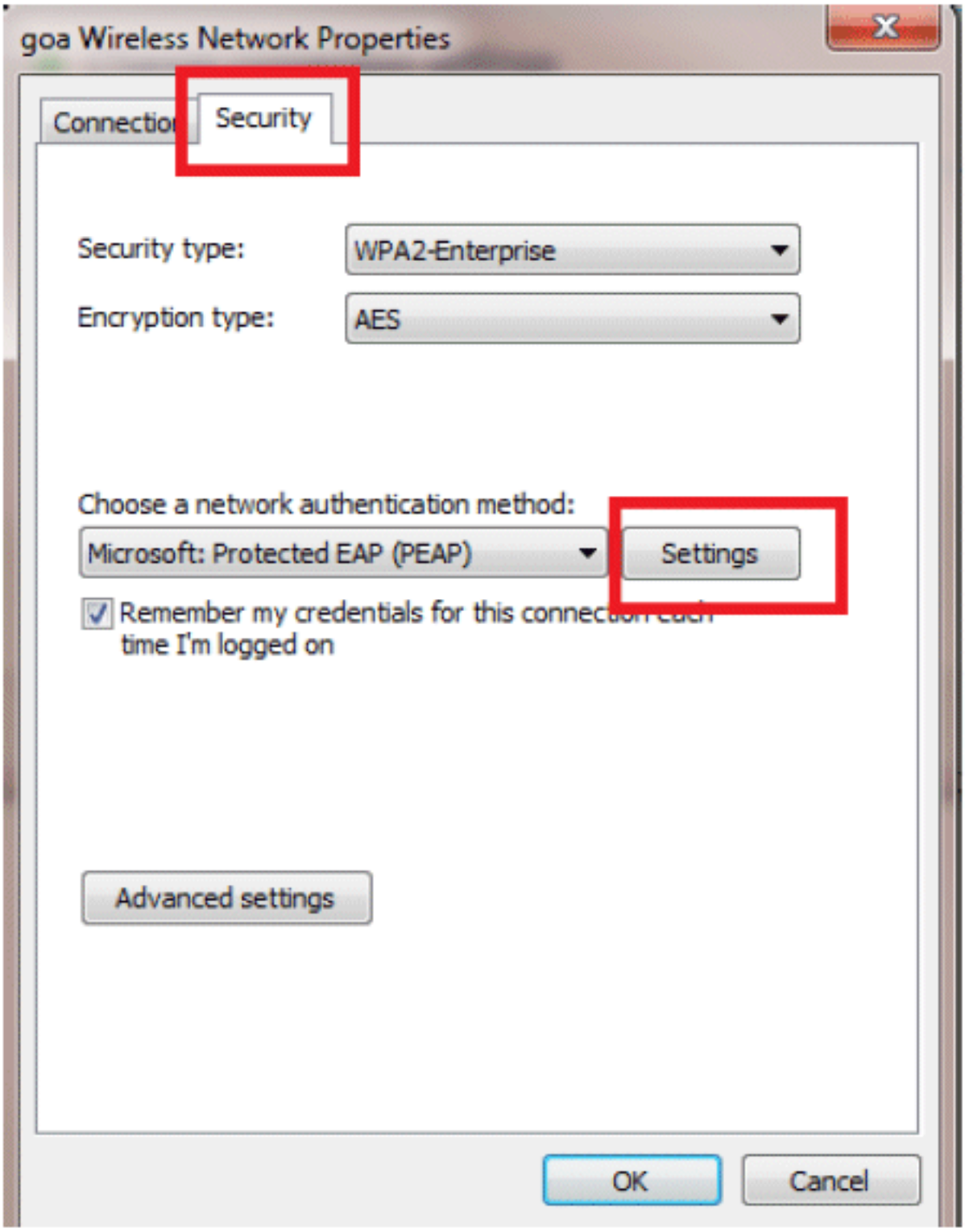


6. Fare clic su **Cambia impostazioni di connessione** per ricontrollare le impostazioni.

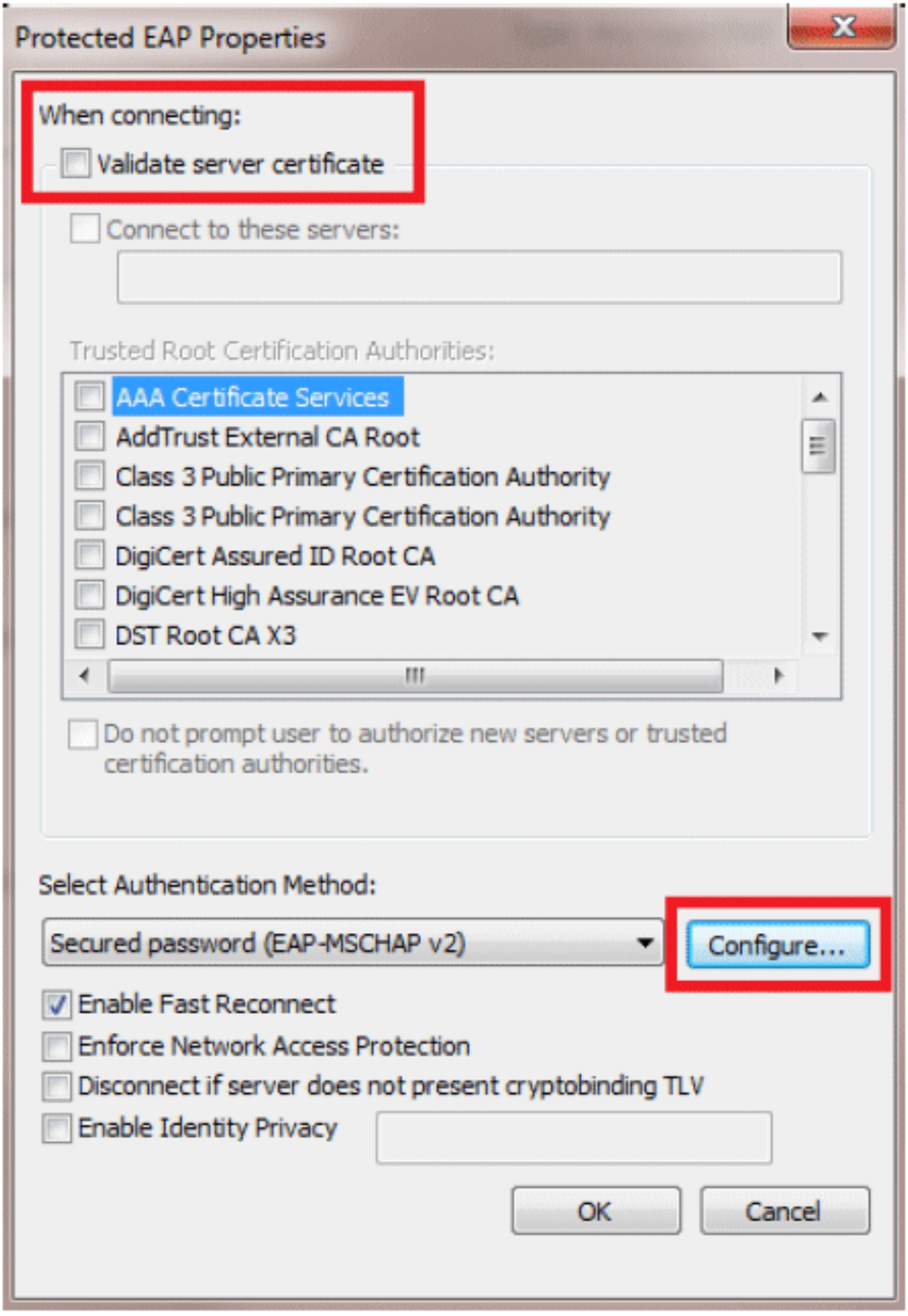


7. Assicurarsi che **PEAP** sia abilitato.



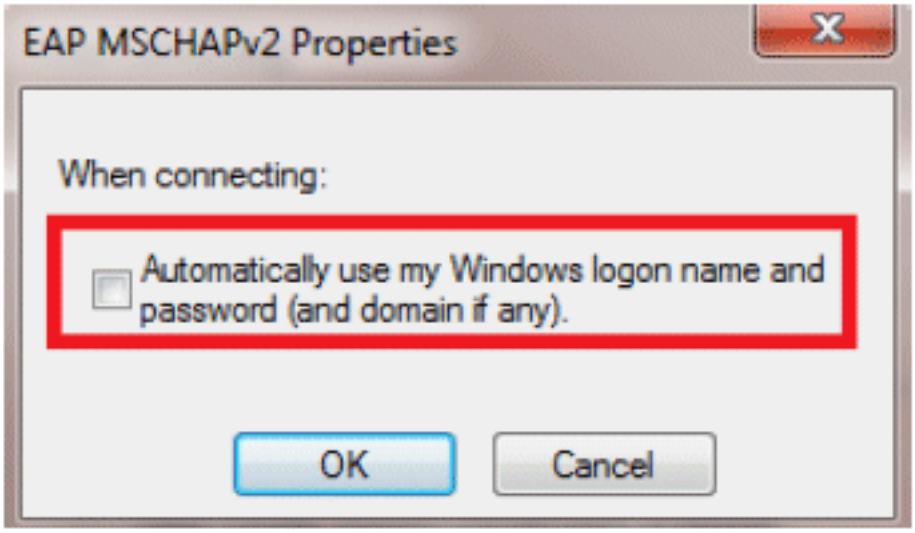


8. In questo esempio il certificato server non viene convalidato. Se si seleziona questa casella e non è possibile connettersi, provare a disabilitare la funzionalità e ripetere il



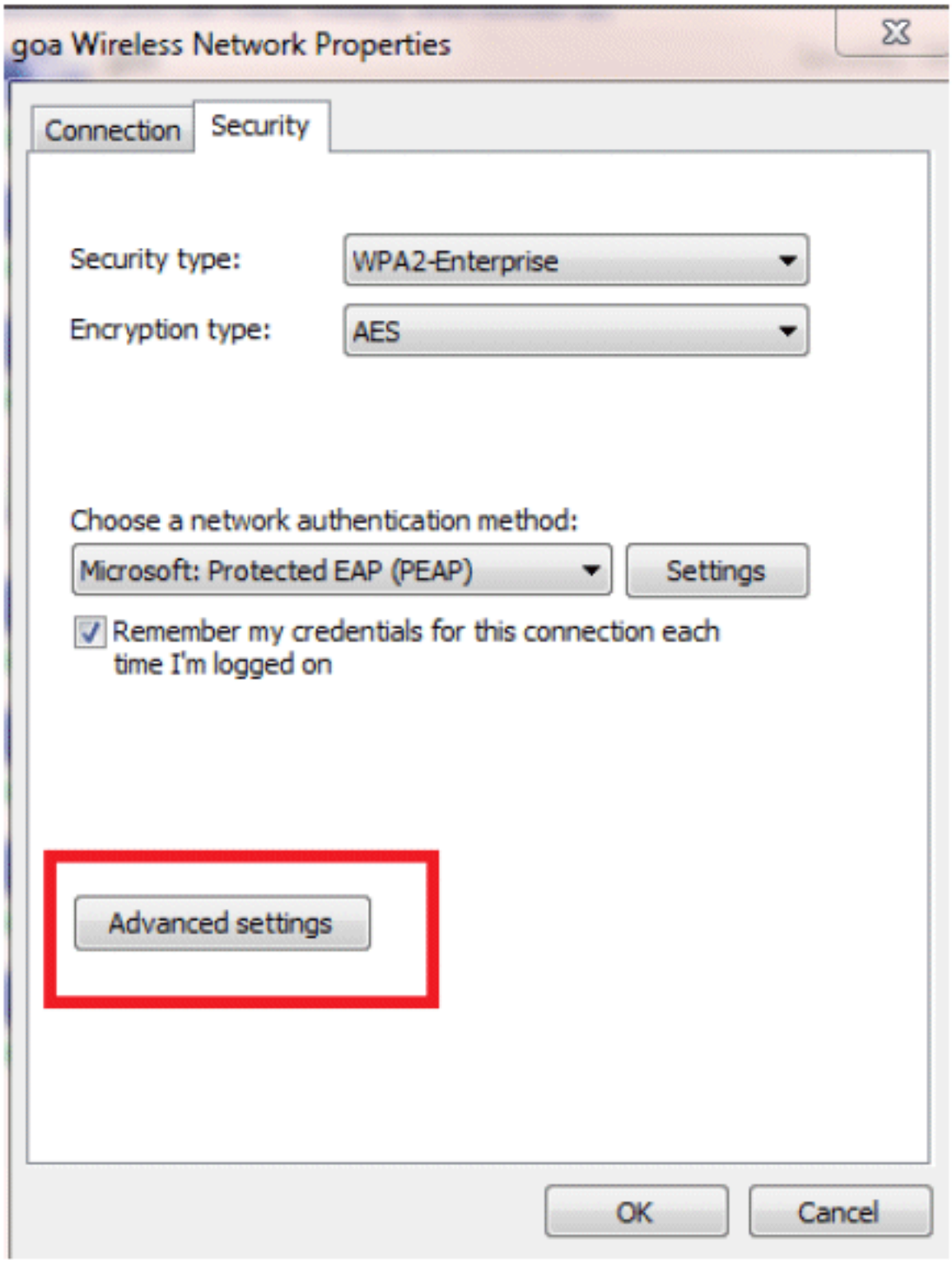
test.

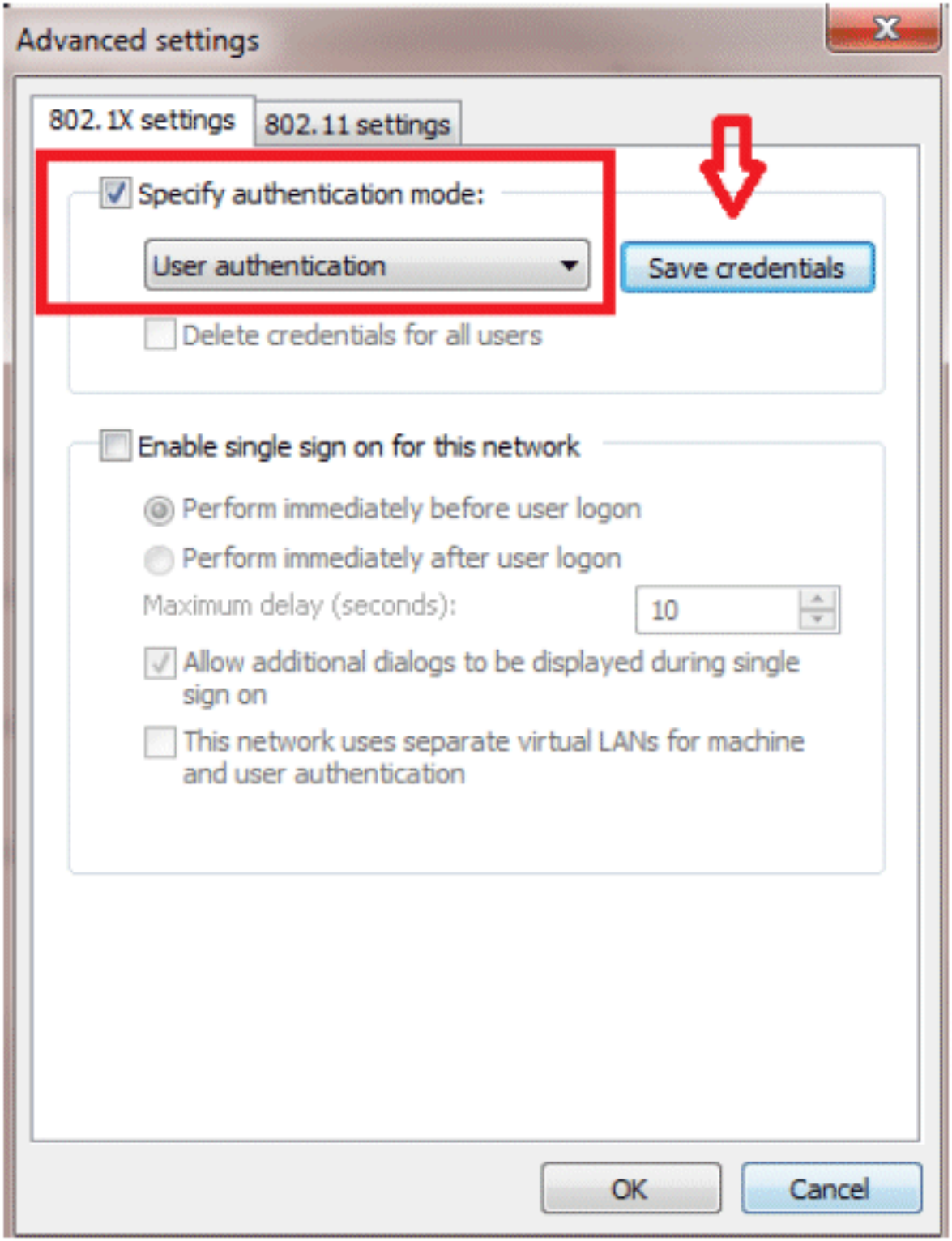
9. In alternativa, è possibile utilizzare le credenziali di Windows per eseguire l'accesso. Tuttavia, in questo esempio non useremo questo metodo. Fare clic su

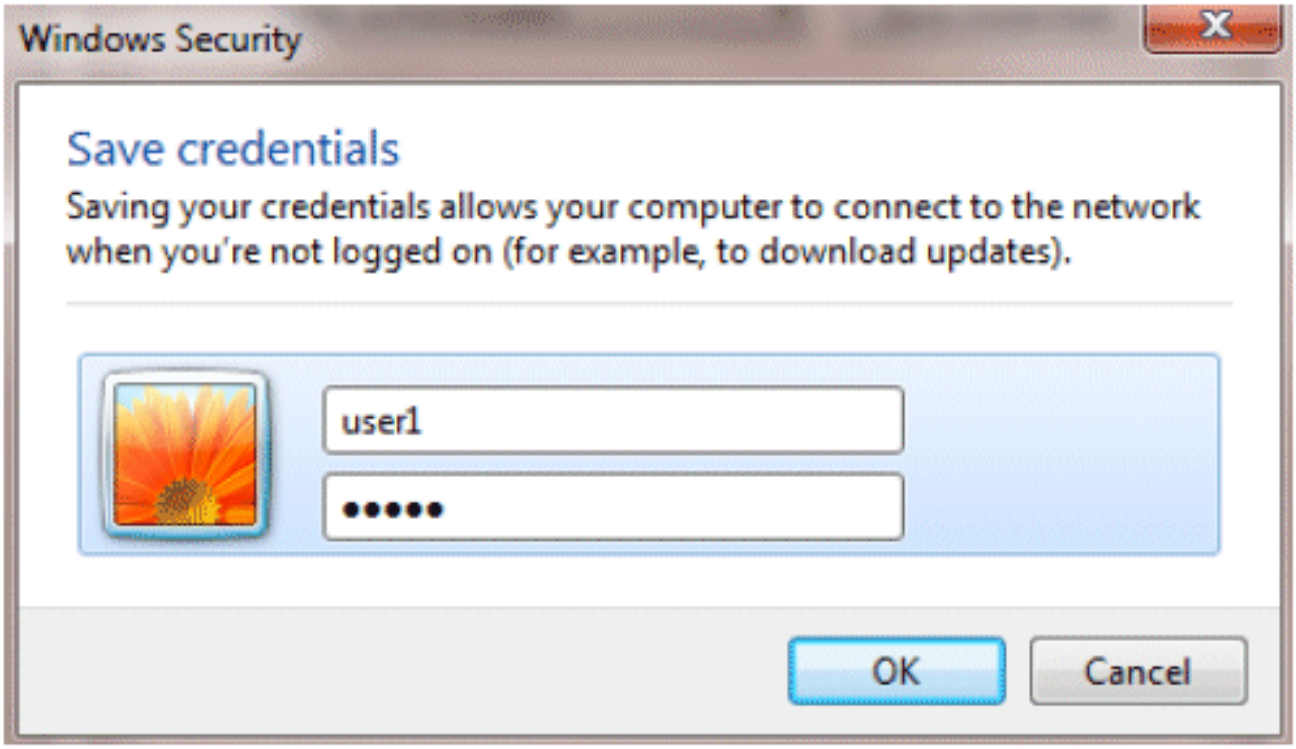


OK.

10. Per configurare il nome utente e la password, fare clic su **Advanced settings** (Impostazioni avanzate).


goa Wireless Network Properties
Connection
Security
Security type:
WPA2-Enterprise
Encryption type:
AES
Choose a network authentication method:
Microsoft: Protected EAP (PEAP)
Settings
Remember my credentials for this connection each time I'm logged on
Advanced settings
OK
Cancel


Advanced settings
802.1X settings
802.11 settings
Specify authentication mode:
User authentication
Save credentials
Delete credentials for all users
Enable single sign on for this network
Perform immediately before user logon
Perform immediately after user logon
Maximum delay (seconds):
10
Allow additional dialogs to be displayed during single sign on
This network uses separate virtual LANs for machine and user authentication
OK
Cancel



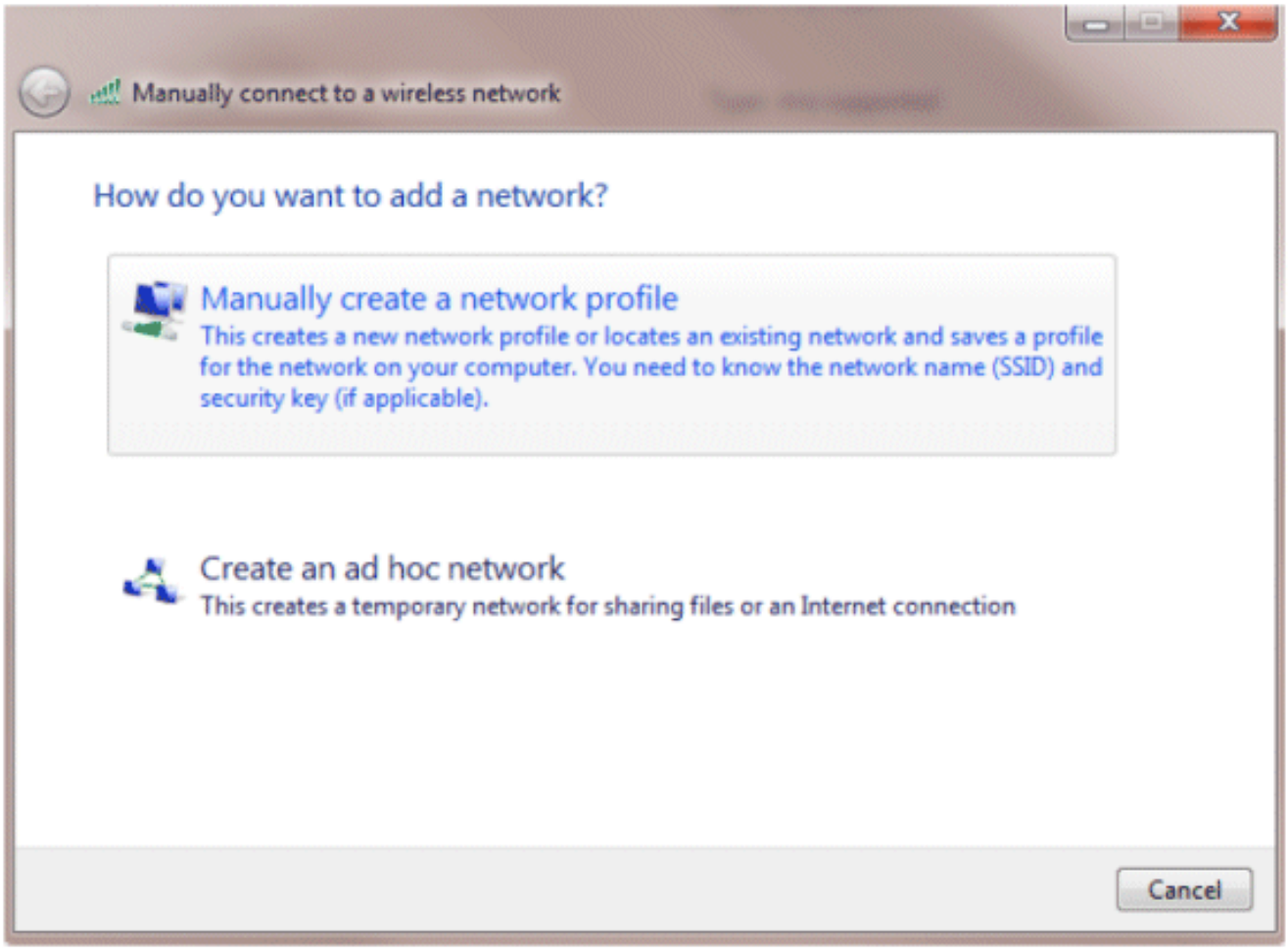
L'utilità Client è pronta per la connessione.

EAP-FAST (utente 2)

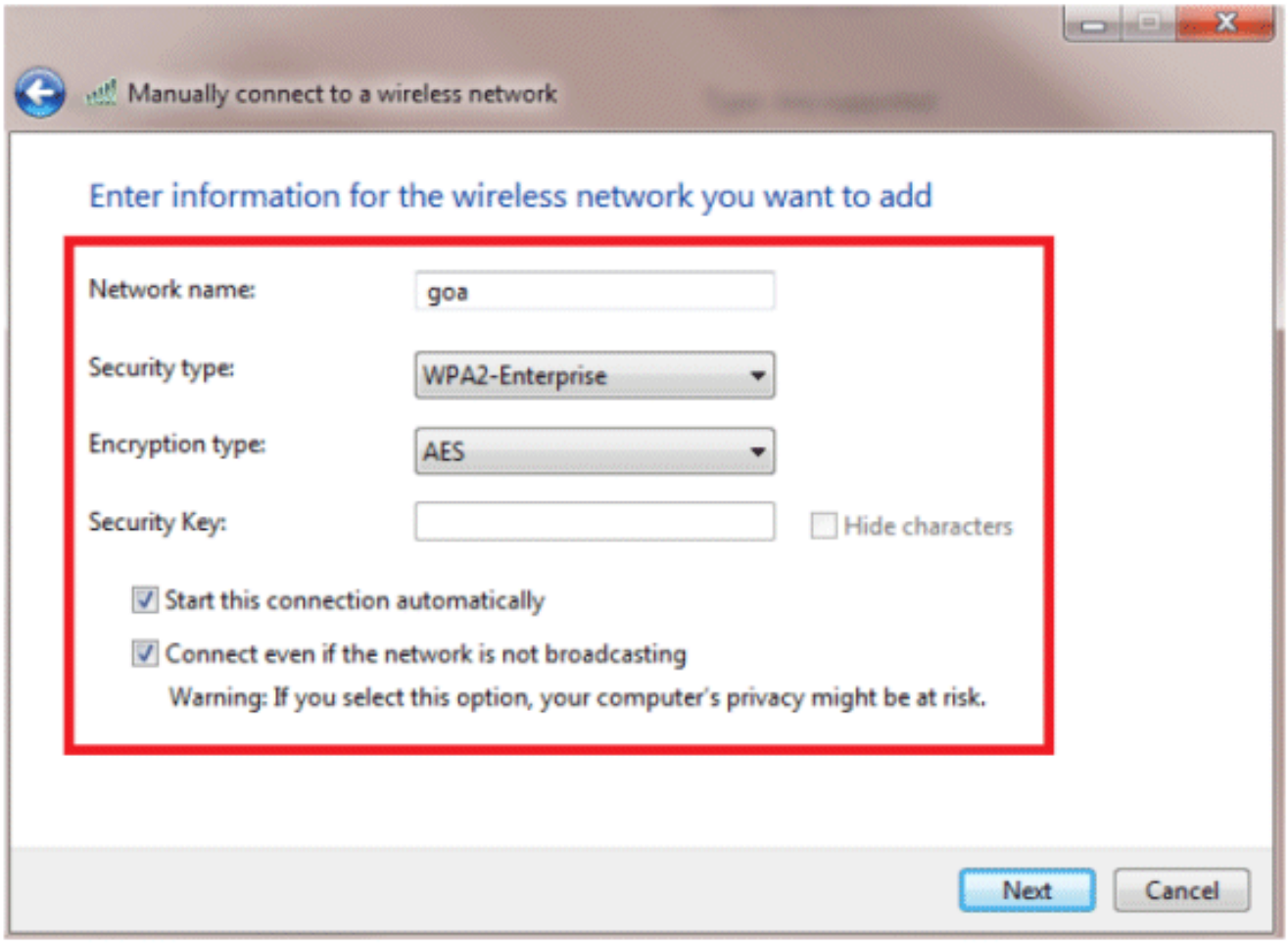
Nel nostro client di test, utilizziamo Windows 7 Native Supplicant con una scheda Intel 6300-N con versione del driver 14.3. È consigliabile eseguire il test utilizzando i driver più recenti dei fornitori.

Per creare un profilo in WZC, completare i seguenti passaggi:

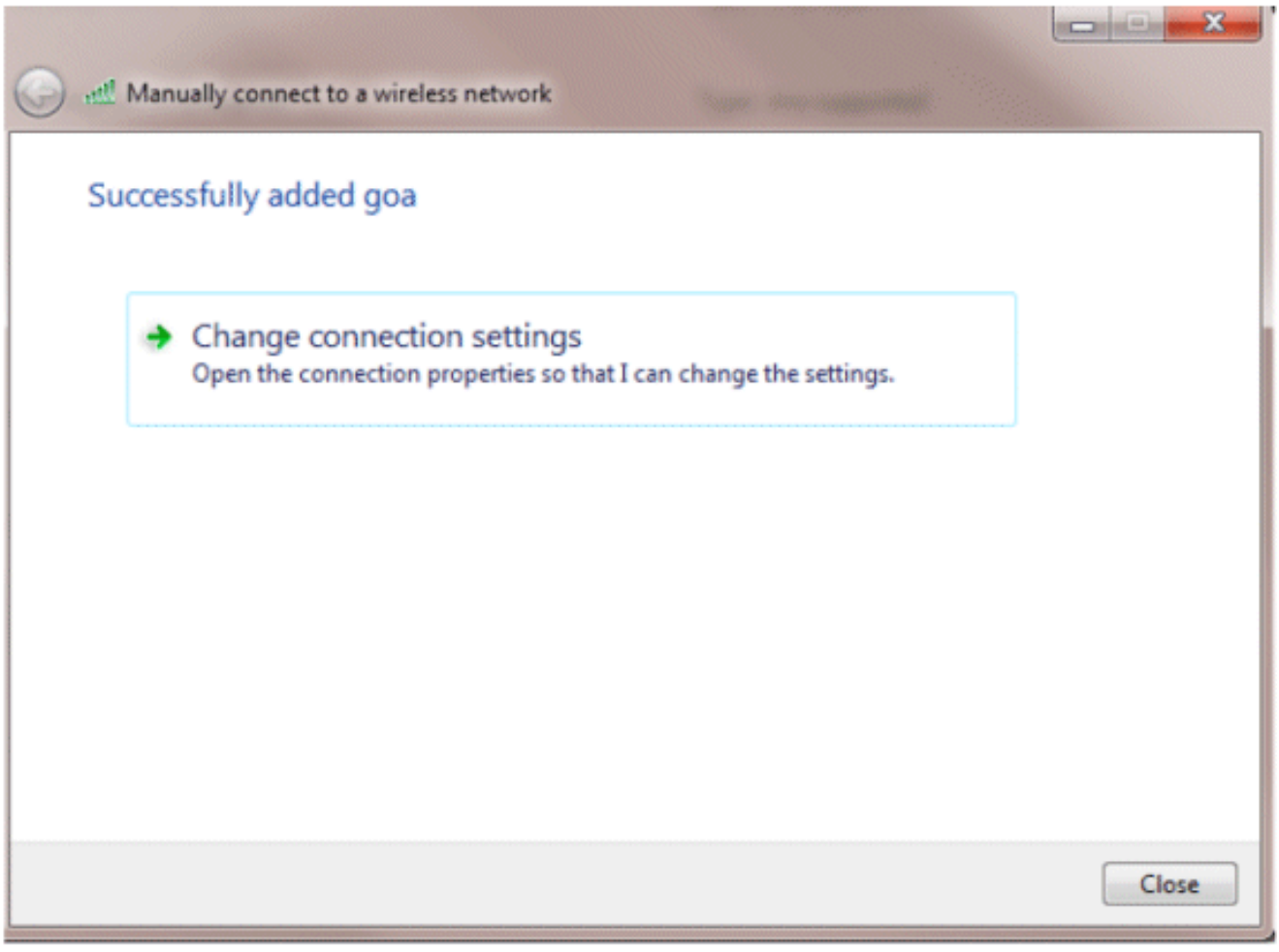
1. Selezionare **Pannello di controllo > Rete e Internet > Gestisci reti wireless**.
2. Fare clic sulla scheda **Aggiungi**.
3. Fare clic su **Crea manualmente un profilo di rete**.



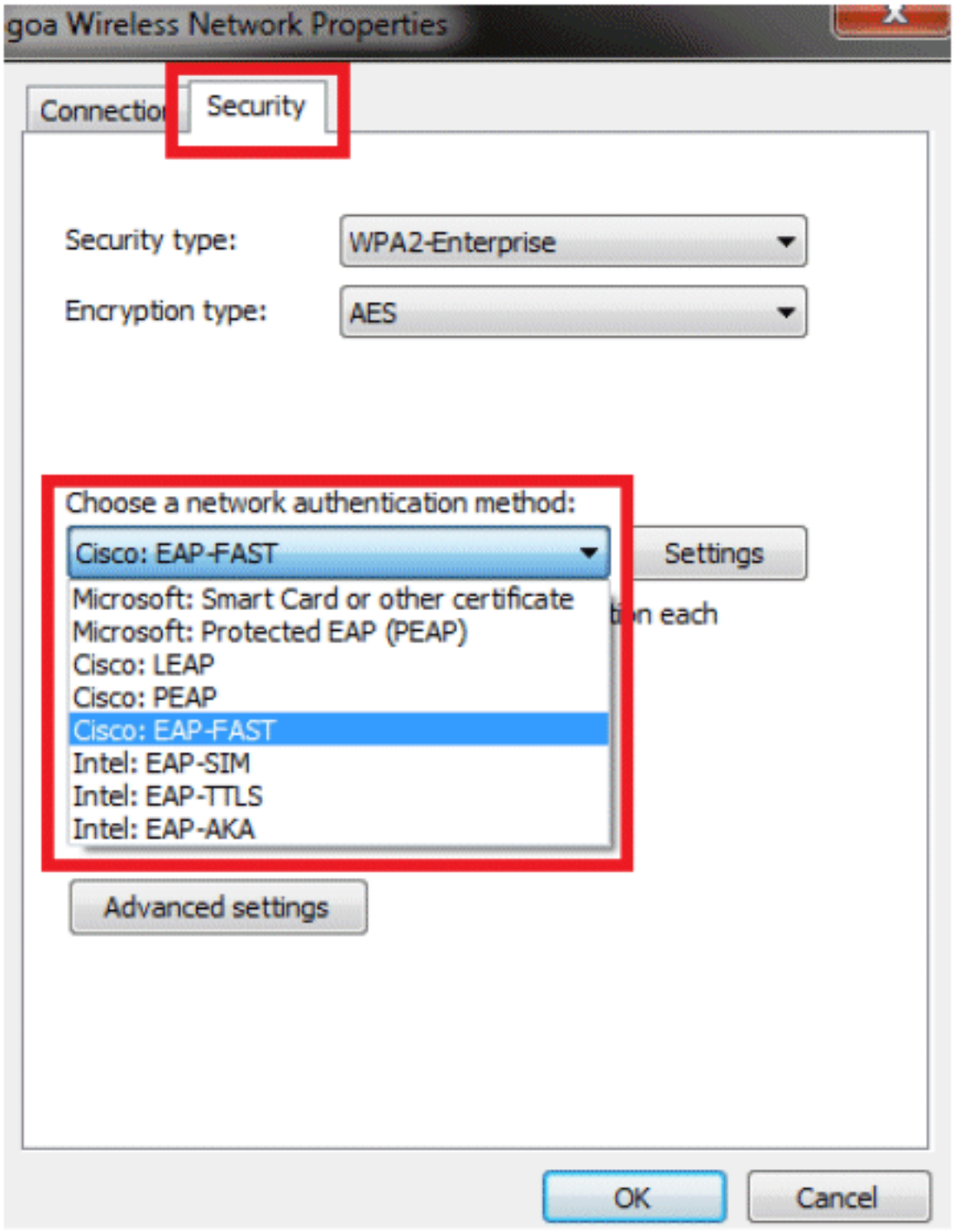
4. Aggiungere i dettagli come configurato sul WLC.**Nota:** per SSID viene fatta distinzione tra maiuscole e minuscole.
5. Fare clic su **Next**
   (Avanti).



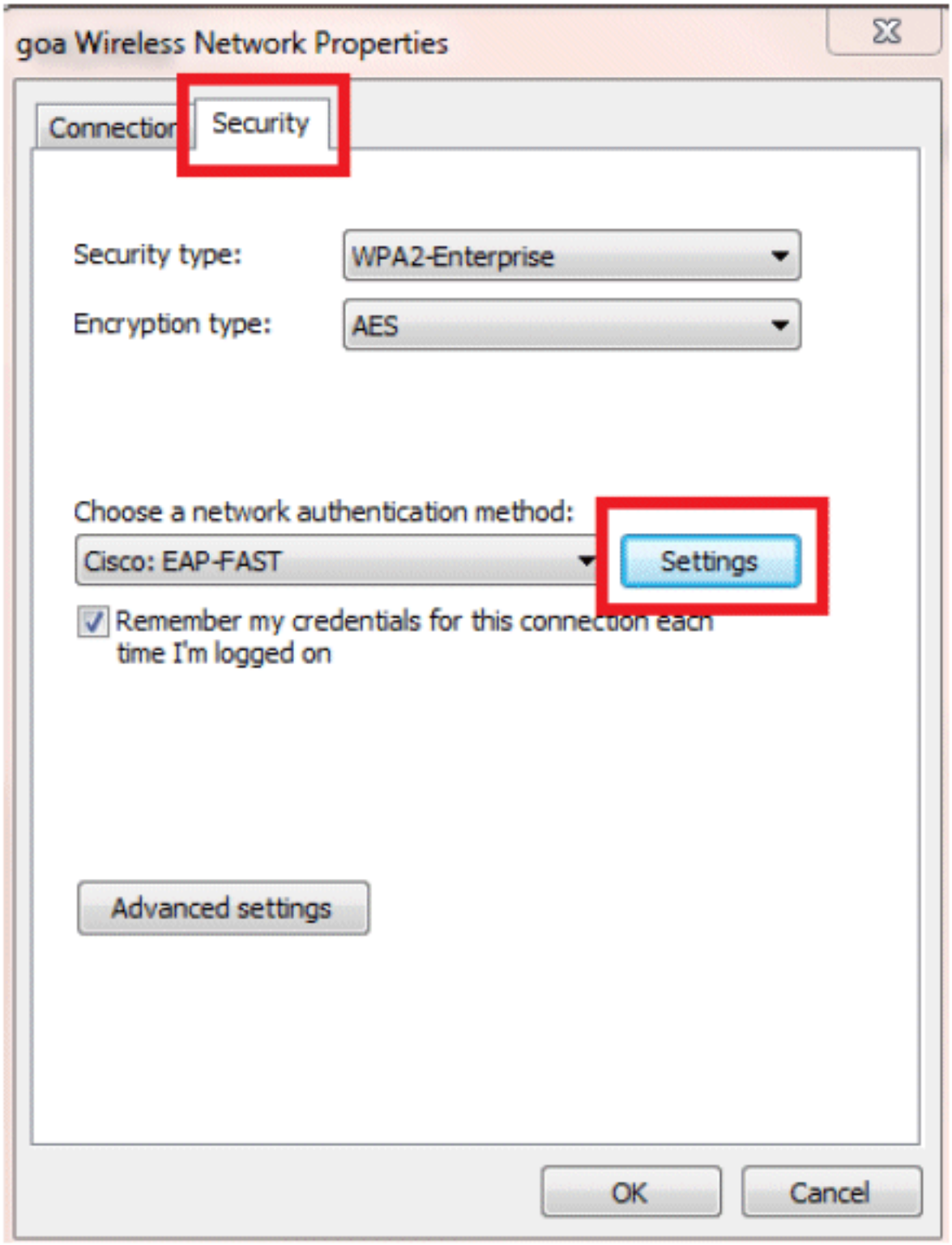
6. Fare clic su **Cambia impostazioni di connessione** per ricontrollare le impostazioni.



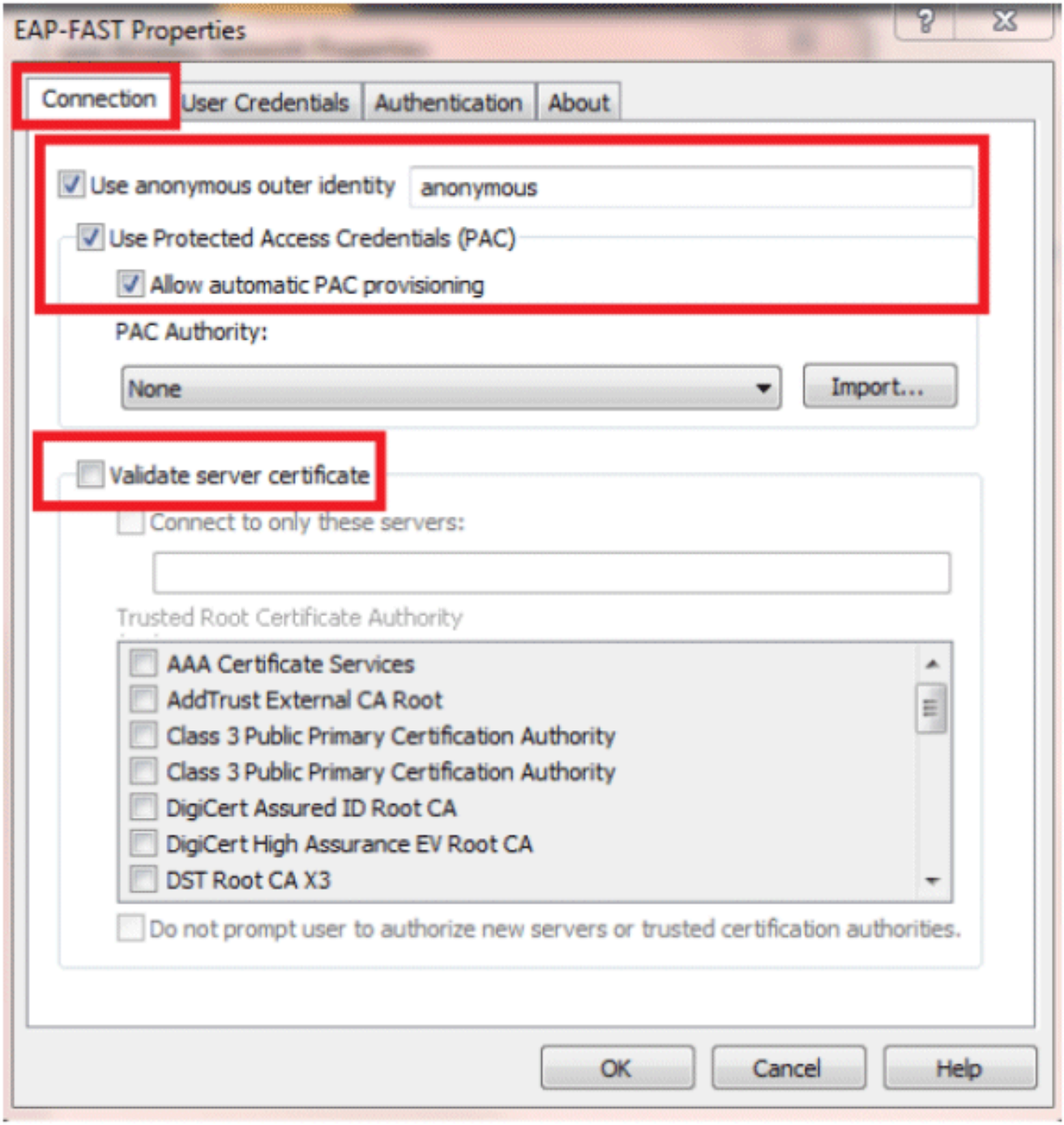
7. Assicurarsi che EAP-FAST sia abilitato.**Nota:** per impostazione predefinita, WZC non dispone di EAP-FAST come metodo di autenticazione. È necessario scaricare l'utility da un fornitore esterno. In questo esempio, poiché si tratta di una scheda Intel, Intel PROSet è installato sul



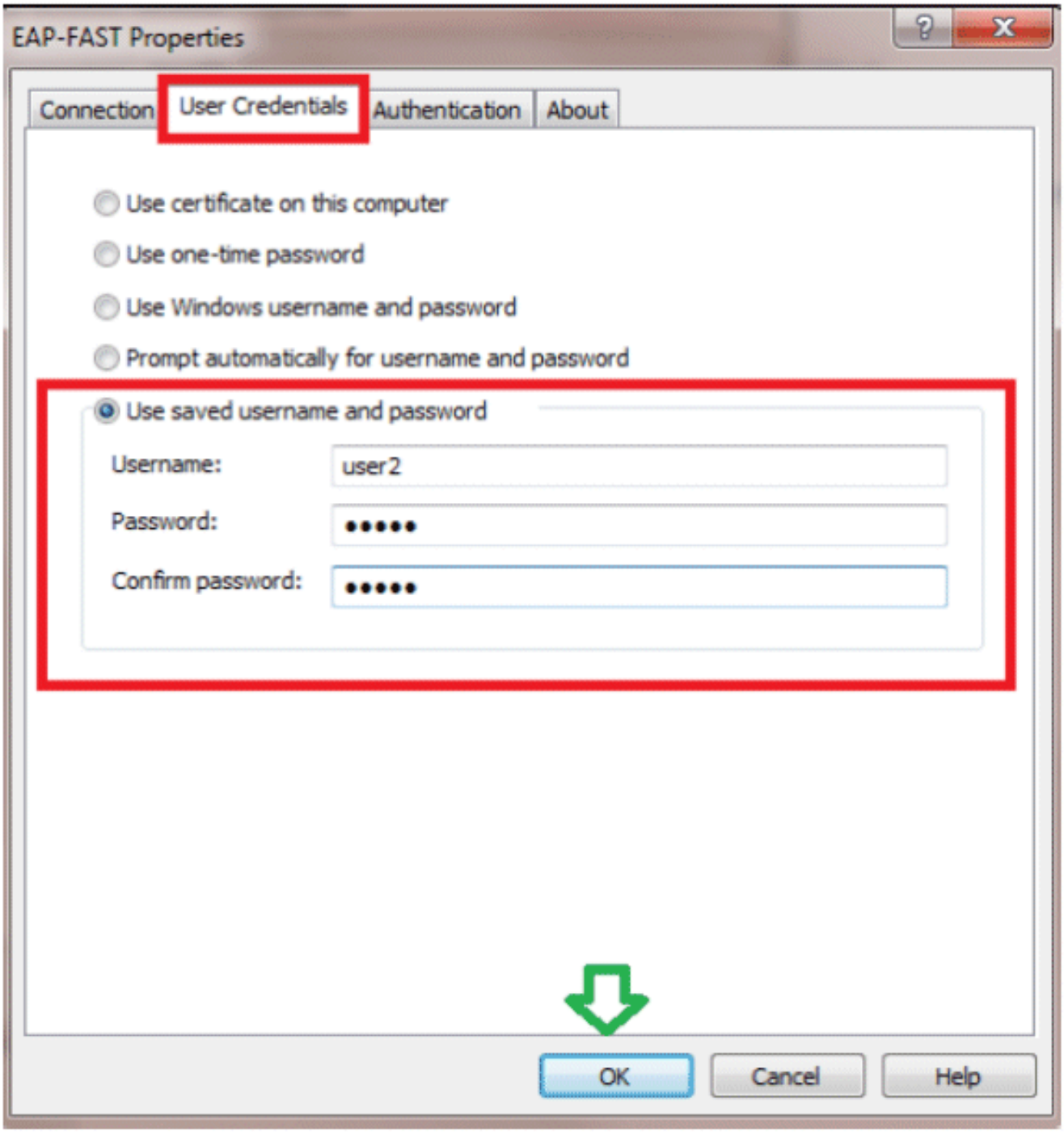
sistema.



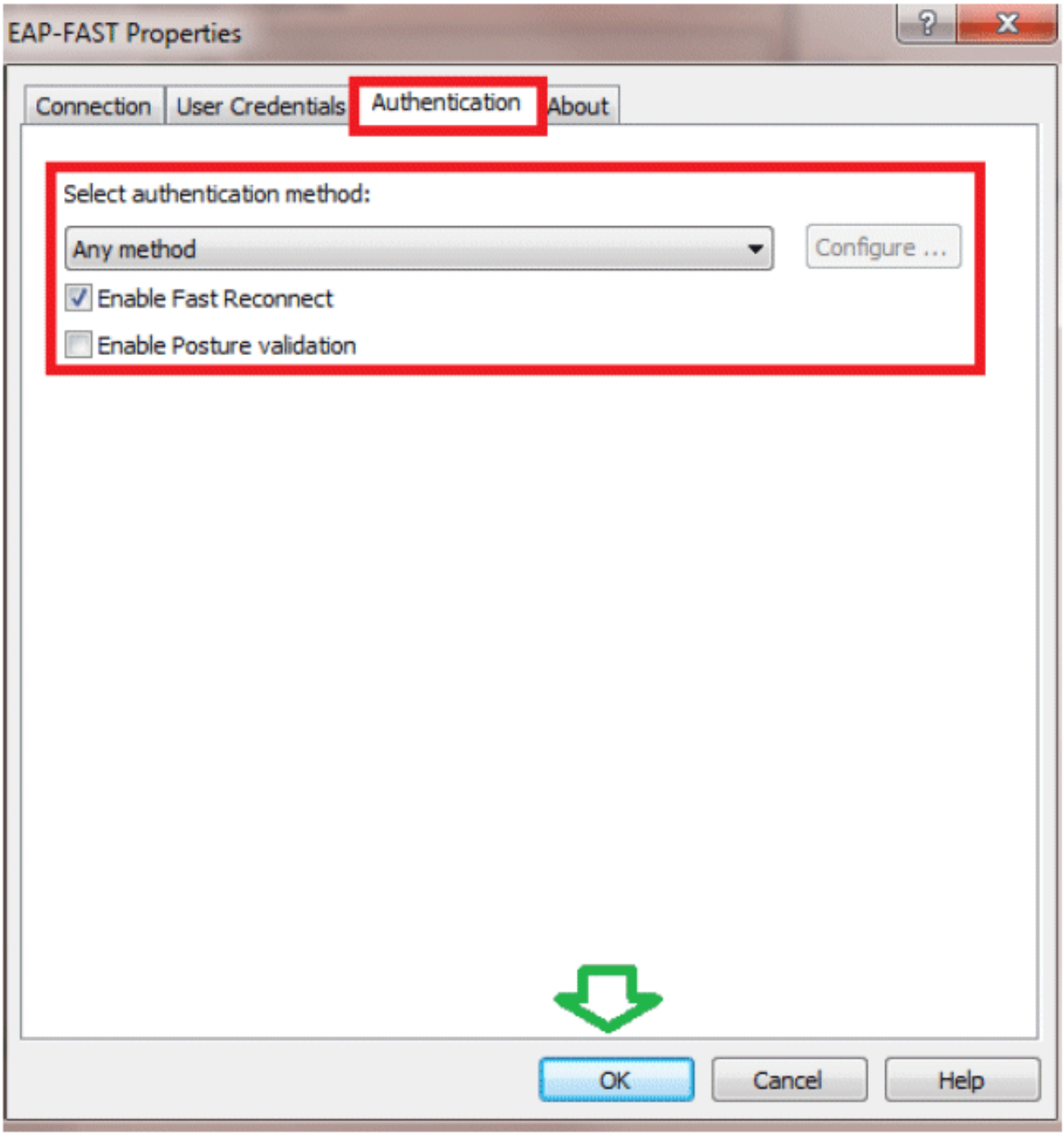
8. Abilitare **Consenti preparazione automatica PAC** e verificare che **Convalida certificato server** sia
deselezionato.



9. Fare clic sulla scheda **Credenziali utente** e immettere le credenziali dell'utente 2. In alternativa, è possibile utilizzare le credenziali di Windows per eseguire l'accesso. Tuttavia, in questo esempio non useremo questo
metodo.

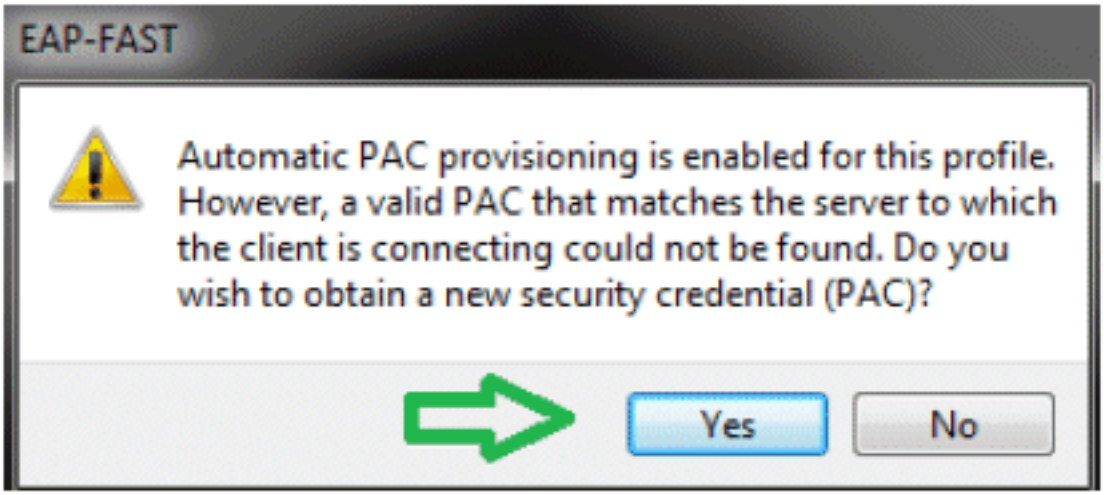


10. Fare clic su **OK**.



L'utilità Client è ora pronta per la connessione per l'utente 2.

Nota: quando l'utente 2 tenta di eseguire l'autenticazione, il server RADIUS invia una PAC. Accettare la PAC per completare l'autenticazione.



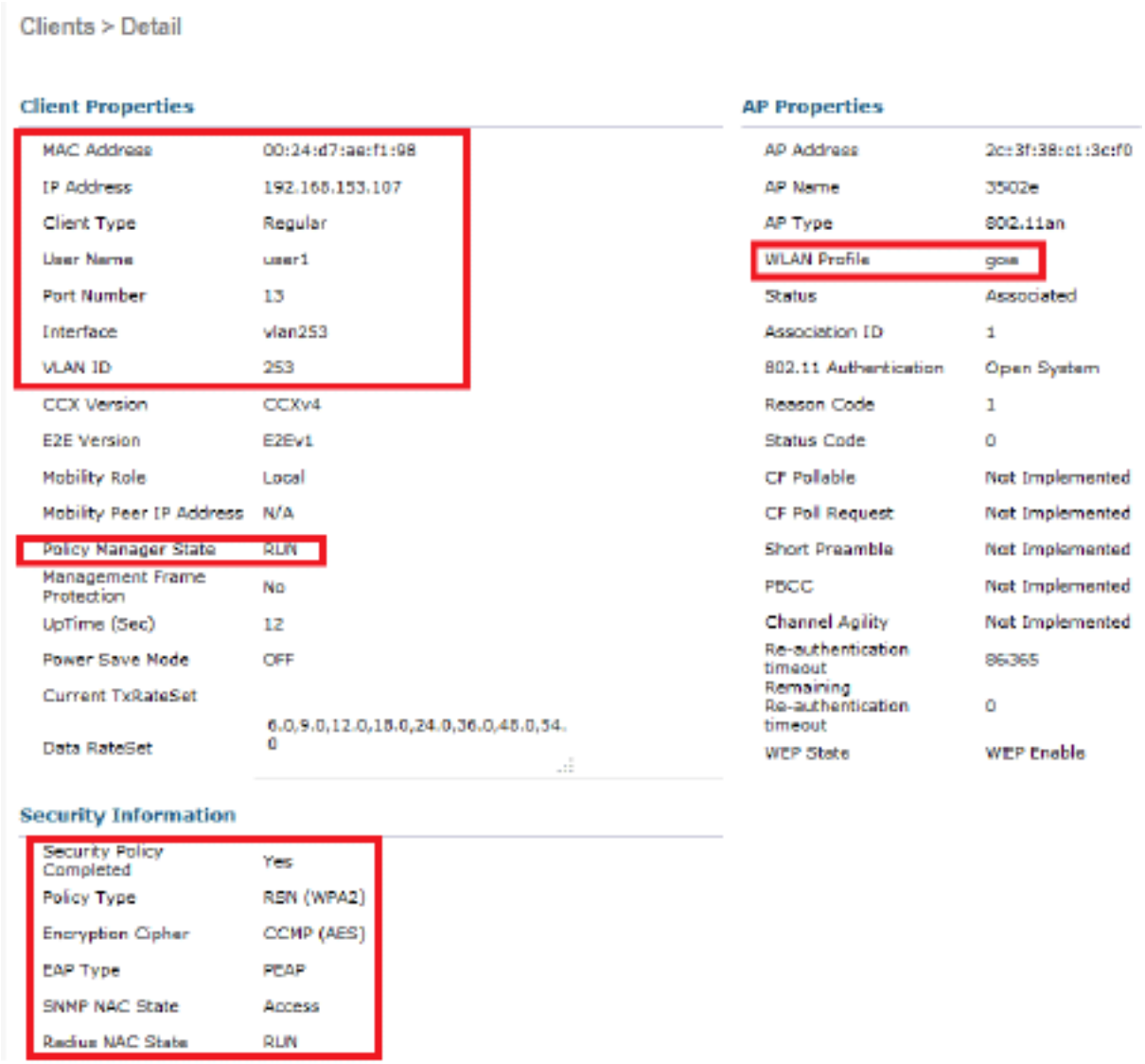
Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Verifica utente1 (PEAP-MSCHAPv2)

Dalla GUI del WLC, selezionare **Monitor** > **Clients**, quindi selezionare l'indirizzo MAC.

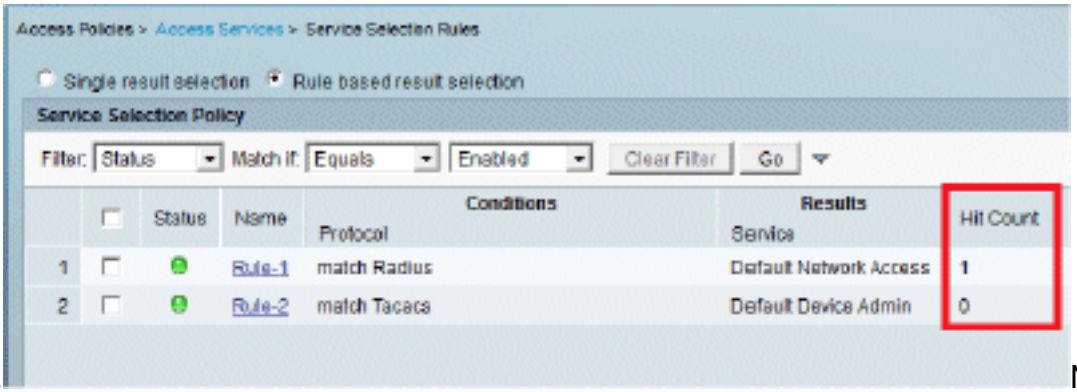


Statistiche RADIUS WLC:

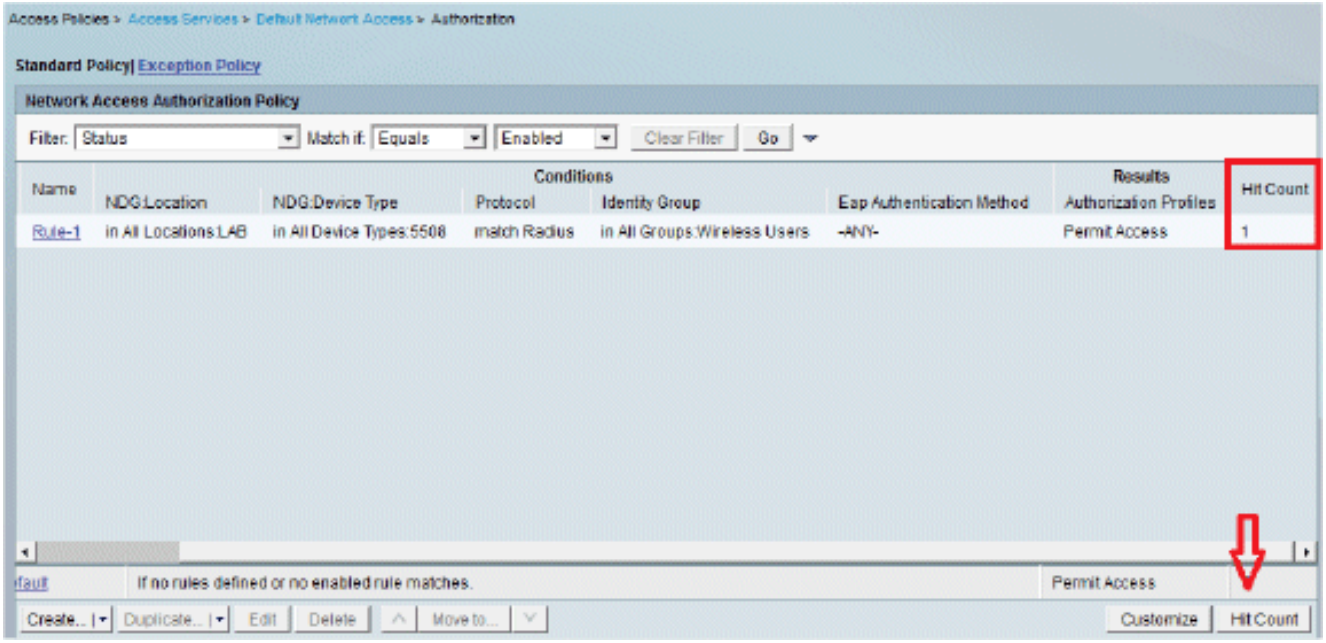
```
(Cisco Controller) >show radius auth statistics
Authentication Servers:
Server Index..................................... 1
Server Address................................... 192.168.150.24
Msg Round Trip Time.............................. 1 (msec)
First Requests................................... 8
Retry Requests................................... 0
Accept Responses................................. 1
Reject Responses................................. 0
Challenge Responses.............................. 7
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Pending Requests................................. 0
Timeout Requests................................. 0
Unknowntype Msgs................................. 0
Other Drops...................................... 0
```

Log ACS:

1. Completare questi passaggi per visualizzare i conteggi visite:Se si controllano i registri entro 15 minuti dall'autenticazione, assicurarsi di aggiornare il numero di

accessi. 

Nella parte inferiore della stessa pagina è presente una scheda per **Conteggio visite**.



2. Fare clic su **Monitoraggio e report** per visualizzare una nuova finestra popup. Andare su **Autenticazioni -Radius -Today**. È inoltre possibile fare clic su **Dettagli** per verificare quale regola di selezione del servizio è stata applicata.

Verifica utente2 (EAP-FAST)

Dalla GUI del WLC, selezionare **Monitor > Clients**, quindi selezionare l'indirizzo MAC.

Clients > Detail

Client Properties

MAC Address	00:24:d7:ae:f1:98
IP Address	192.168.153.111
Client Type	Regular
User Name	user2
Port Number	13
Interface	vlan253
VLAN ID	253
CCX Version	CCXv4
E2E Version	E2Ev1
Mobility Role	Local
Mobility Peer IP Address	N/A
Policy Manager State	RUN
Management Frame Protection	No
UpTime (Sec)	29
Power Save Mode	OFF
Current TxRateSet	m15
Data RateSet	6.0,9.0,12.0,18.0,24.0,36.0,48.0,54.0

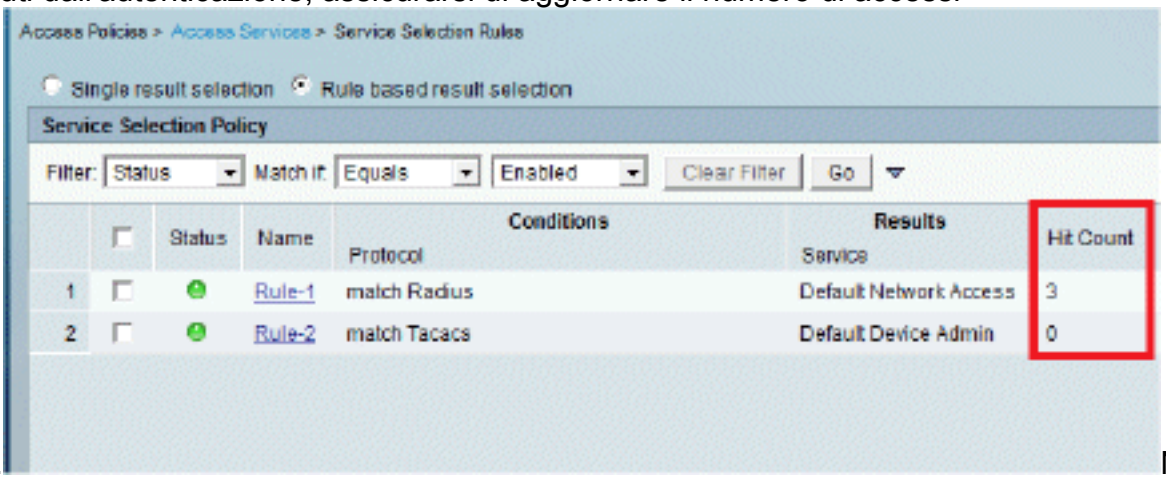
AP Properties

AP Address	2c:3f:38:c1:3c:f0
AP Name	3502e
AP Type	802.11an
WLAN Profile	goa
Status	Associated
Association ID	1
802.11 Authentication	Open System
Reason Code	1
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Not Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Re-authentication timeout	86392
Remaining Re-authentication timeout	0
WEP State	WEP Enable

Security Information

Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Encryption Cipher	CCMP (AES)
EAP Type	EAP-FAST
SNMP NAC State	Access
Radius NAC State	RUN

Log ACS:

1. Completare questi passaggi per visualizzare i conteggi visite:Se si controllano i registri entro 15 minuti dall'autenticazione, assicurarsi di aggiornare il numero di accessi riusciti. 
Access Policies > Access Services > Service Selection Rules

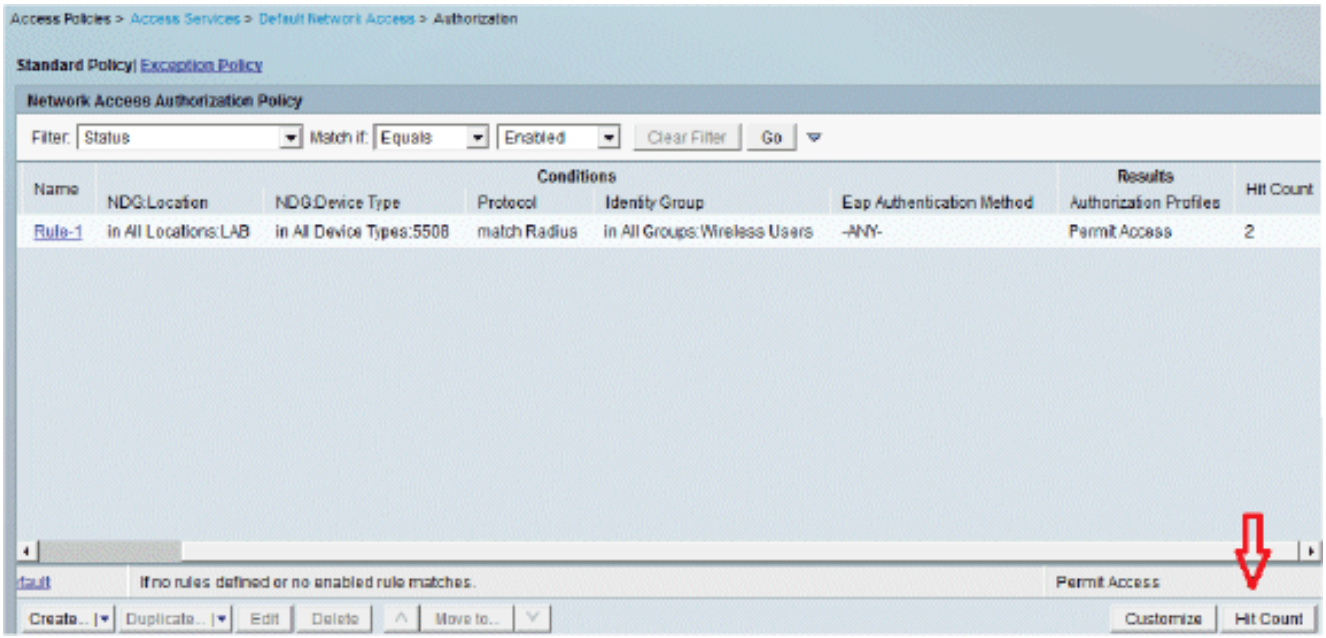
Single result selection Rule based result selection

Service Selection Policy

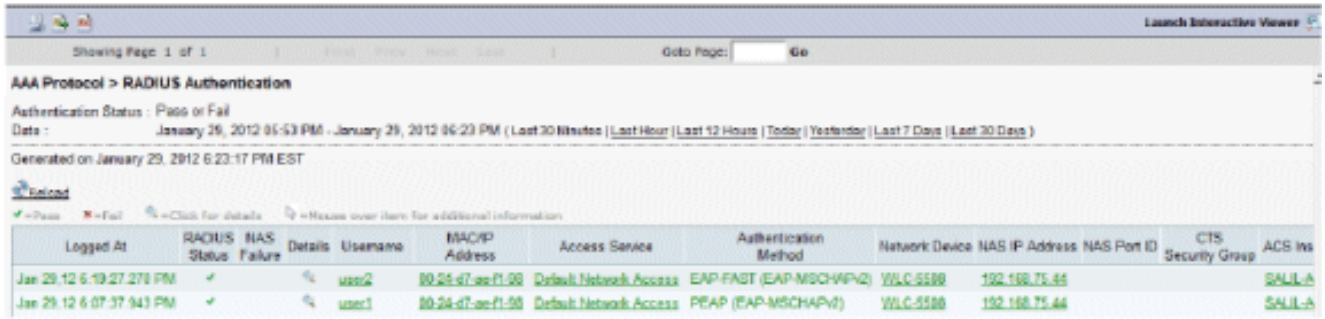
Filter: Status Match if: Equals Enabled Clear Filter Go

		Status	Name	Conditions: Protocol	Results: Service	Hit Count
1			Rule-1	match Radius	Default Network Access	3
2			Rule-2	match Tacacs	Default Device Admin	0

Nella parte inferiore della stessa pagina è presente una scheda per **Conteggio visite**.



2. Fare clic su **Monitoraggio e report** per visualizzare una nuova finestra popup. Andare su **Autenticazioni -Radius -Today**. È inoltre possibile fare clic su **Dettagli** per verificare quale regola di selezione del servizio è stata applicata.



Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Comandi per la risoluzione dei problemi

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

1. In caso di problemi, usare questi comandi sul WLC:**debug client** *<mac add of the client>***debug aaa all enableshow client detail** *<mac addr>* - Verificare lo stato di policy manager.**show radius auth statistics** - Verifica il motivo dell'errore.**debug disable-all** - Disattiva i debug.**clear stats radius auth all**: cancella le statistiche sul raggio del WLC.
2. Verificare i log nel server ACS e annotare il motivo dell'errore.

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems

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).