BYOD wireless con Identity Services Engine

Sommario

Introduzione

Cisco Identity Services Engine (ISE) è il server delle policy Cisco di nuova generazione che fornisce l'infrastruttura di autenticazione e autorizzazione alla soluzione Cisco TrustSec. Offre inoltre altri due servizi critici:

- Il primo servizio consiste nel fornire un modo per profilare automaticamente il tipo di dispositivo dell'endpoint in base agli attributi che Cisco ISE riceve da diverse fonti di informazioni. Questo servizio (denominato Profiler) offre funzioni equivalenti a quelle offerte precedentemente da Cisco con l'appliance Cisco NAC Profiler.
- Un altro servizio importante offerto da Cisco ISE è la scansione della conformità dell'endpoint, ad esempio l'installazione del software AV/AS e la validità del file di definizione (nota come Postura). In precedenza Cisco aveva fornito questa esatta funzione di postura solo con l'appliance Cisco NAC.

Cisco ISE fornisce un livello equivalente di funzionalità ed è integrato con il meccanismo di autenticazione 802.1X.

Cisco ISE integrato con WLC (Wireless LAN Controller) può fornire meccanismi di profiling di dispositivi mobili come Apple iDevices (iPhone, iPad e iPod), smartphone basati su Android e altri. Per gli utenti 802.1X, Cisco ISE può fornire lo stesso livello di servizi, come la profilatura e la scansione della postura. I servizi guest su Cisco ISE possono essere integrati anche con Cisco WLC reindirizzando le richieste di autenticazione Web a Cisco ISE per l'autenticazione.

In questo documento viene presentata la soluzione wireless BYOD (Bring Your Own Device), che consente ad esempio di differenziare l'accesso in base agli endpoint noti e alle policy dell'utente. Questo documento non fornisce la soluzione completa di BYOD, ma serve a dimostrare un semplice caso d'uso di accesso dinamico. Altri esempi di configurazione includono l'uso del portale degli sponsor ISE, dove un utente con privilegi può sponsorizzare un guest per il provisioning dell'accesso guest wireless.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

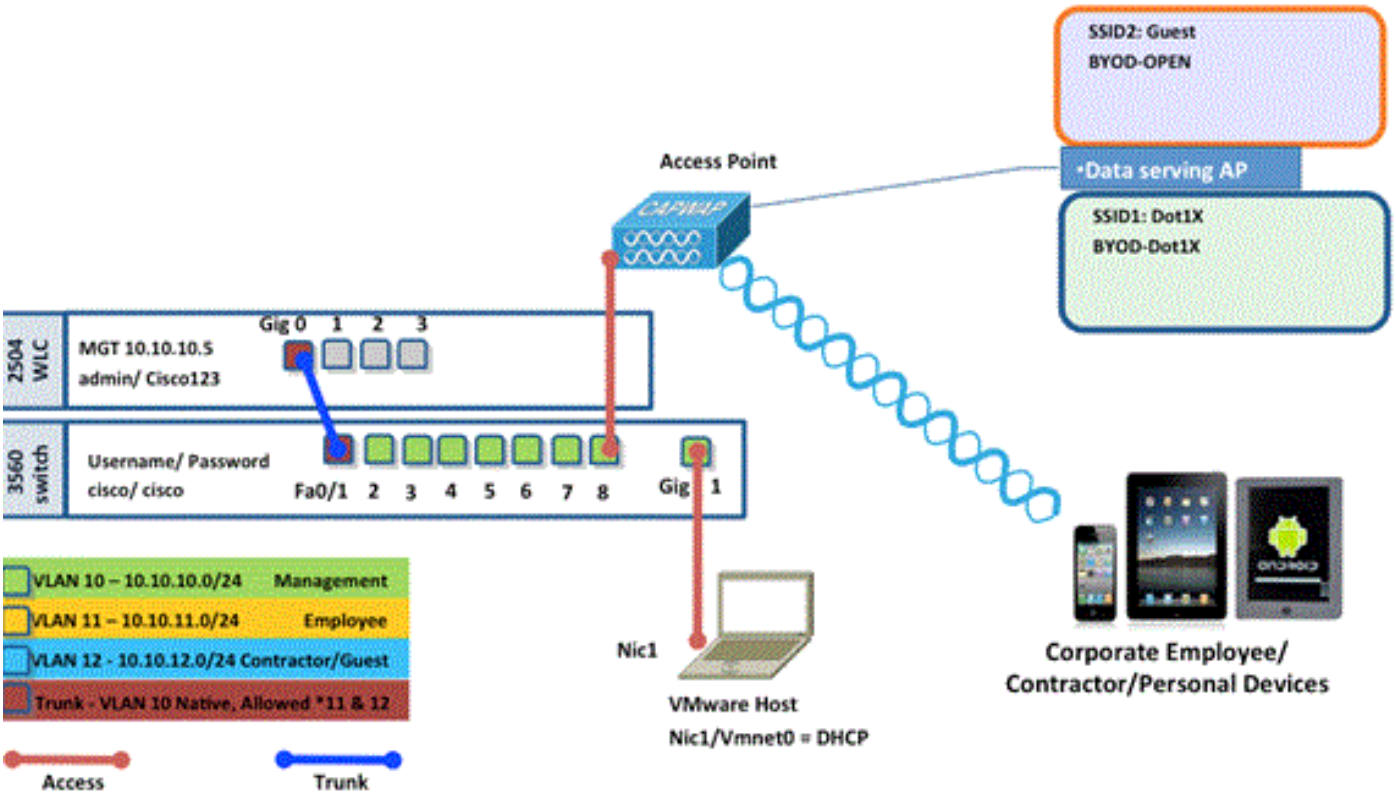
Componenti usati

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

hardware:

- Cisco Wireless LAN Controller 2504 o 2106 con versione software 7.2.103
- Catalyst 3560 - 8 porte
- WLC 2504
- Identity Services Engine 1.0MR (versione immagine server VMware)
- Windows 2008 Server (immagine VMware): disco da 20 GB, 512 MBActive DirectoryDNSDHCPServizi certificati

Topologia



Name	IP Address	Credential
Vmware Host	10.10.10.2	*(Machine used to host the ISE 1.0 MR vmware server files)*
Identity Service Engine	10.10.10.70	admin/ default1A
Active Directory/ DNS/ DHCP/ CA Server	10.10.10.10	*(Machine used to host Active Directory/ DNS/ DHCP/ CA Server)*

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Panoramica di RADIUS NAC e CoA Controller LAN wireless

Questa impostazione consente al WLC di cercare le coppie AV di reindirizzamento URL provenienti dal server ISE RADIUS. Questa condizione si verifica solo su una WLAN collegata a un'interfaccia con l'impostazione RADIUS NAC abilitata. Quando si riceve la coppia AV Cisco per il reindirizzamento URL, il client viene messo nello stato POSTURE_REQD. In pratica,

corrisponde allo stato WEBAUTH_REQD internamente al controller.

Quando il server ISE RADIUS ritiene che il client sia Posture_Compliant, emette una nuova autenticazione CoA. Il valore Session_ID viene utilizzato per collegarlo. Con la nuova funzione AuthC (re-Auth), non viene inviata alcuna coppia AV URL-Redirect. Poiché non sono presenti coppie AV di reindirizzamento URL, il WLC sa che il client non richiede più la postura.

Se l'impostazione RADIUS NAC non è abilitata, il WLC ignora i VSA di reindirizzamento dell'URL.

CoA-ReAuth: abilitata con l'impostazione RFC 3576. La funzionalità ReAuth è stata aggiunta ai comandi CoA esistenti supportati in precedenza.

L'impostazione RADIUS NAC si esclude a vicenda da questa funzionalità, sebbene sia necessaria per il funzionamento del CoA.

ACL pre-postura: quando un client si trova nello stato POSTURE_REQ, il comportamento predefinito del WLC è bloccare tutto il traffico eccetto DHCP/DNS. L'ACL pre-postura (chiamato nell'URL-redirect-acl AV-Pair) viene applicato al client e ciò che è permesso in quell'ACL è ciò che il client può raggiungere.

Override di ACL pre-autenticazione e VLAN: una VLAN di quarantena o authC diversa dalla VLAN di accesso non è supportata in 7.0MR1. Se si imposta una VLAN dal Policy Server, sarà la VLAN per l'intera sessione. Non sono necessarie modifiche alla VLAN dopo la prima AuthZ.

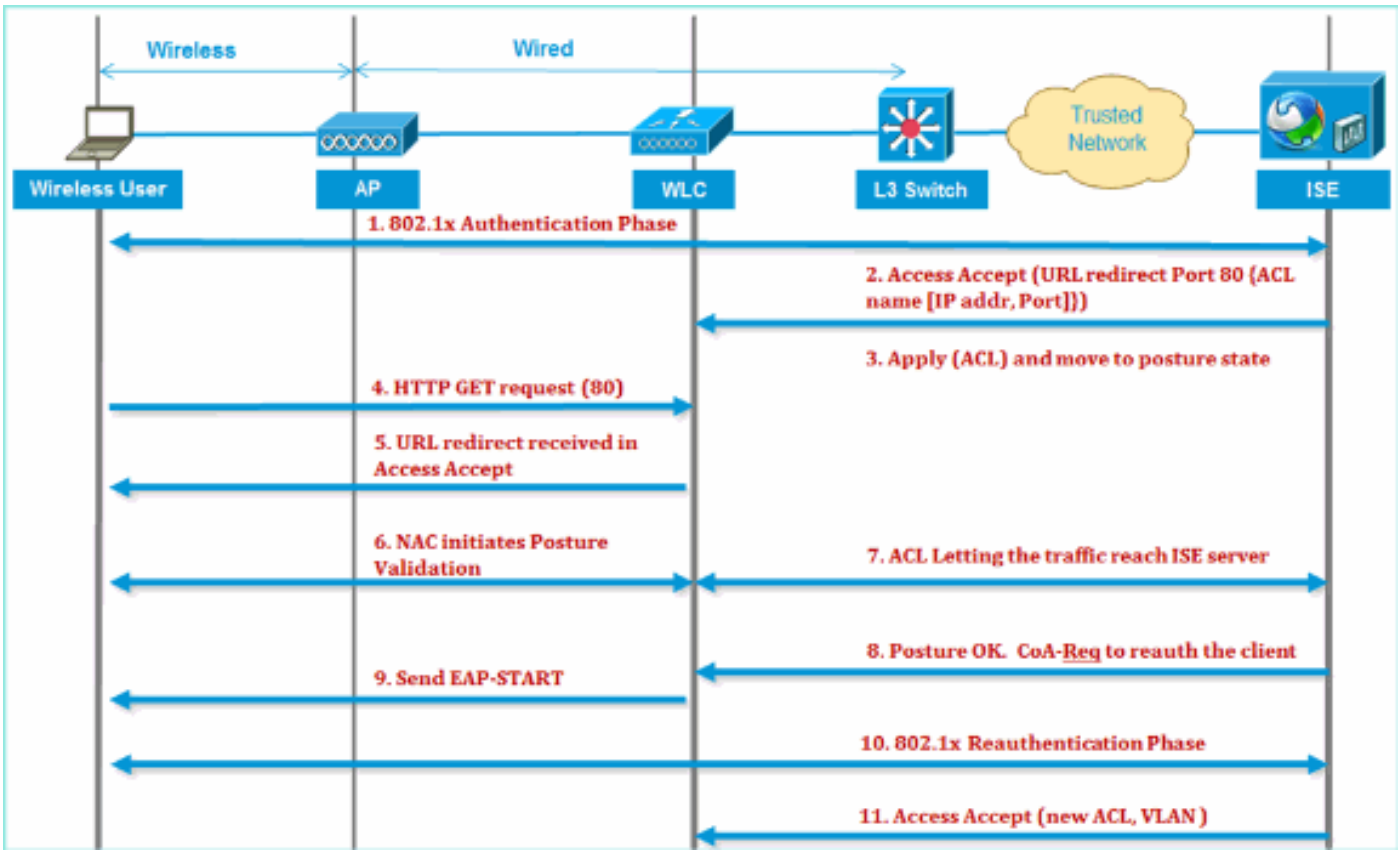
Flusso delle funzionalità RADIUS NAC e CoA del controller LAN wireless

La figura seguente fornisce i dettagli dello scambio di messaggi quando il client viene autenticato sul server back-end e la convalida della postura NAC.

1. Il client esegue l'autenticazione con dot1x.
2. L'autorizzazione di accesso RADIUS porta l'URL reindirizzato per la porta 80 e gli ACL di pre-autenticazione, che includono la possibilità di usare indirizzi IP e porte o di mettere in quarantena le VLAN.
3. Il client verrà reindirizzato all'URL specificato in Accetta accesso e messo in un nuovo stato fino a quando non viene eseguita la convalida della postura. In questo stato, il client comunica con il server ISE e si convalida rispetto alle policy configurate sul server ISE NAC.
4. L'agente NAC sul client avvia la convalida della postura (traffico verso la porta 80): l'agente invia una richiesta di individuazione HTTP alla porta 80 che il controller reindirizza all'URL fornito in accettazione accesso. L'ISE sa che il cliente cerca di raggiungere il cliente e risponde direttamente a quest'ultimo. In questo modo il client viene a conoscenza dell'IP del server ISE e da ora in poi comunica direttamente con il server ISE.
5. Il WLC consente questo traffico perché l'ACL è configurato per consentire questo traffico. In caso di override della VLAN, il traffico viene bloccato in modo che raggiunga il server ISE.
6. Una volta che il client ISE ha completato la valutazione, un CoA-Req RADIUS con servizio di riautenticazione viene inviato al WLC. In questo modo viene avviata la riautenticazione del client (inviando EAP-START). Se la riautenticazione ha esito positivo, ISE invia un messaggio di accettazione dell'accesso con un nuovo ACL (se presente) e senza reindirizzamento dell'URL o accesso alla VLAN.

7. WLC supporta CoA-Req e Disconnect-Req come da RFC 3576. Il WLC deve supportare CoA-Req per il servizio di riautenticazione, come da RFC 5176.
8. Anziché ACL scaricabili, sul WLC vengono utilizzati ACL preconfigurati. Il server ISE invia semplicemente il nome ACL, già configurato nel controller.
9. Questa progettazione deve funzionare sia con le VLAN che con gli ACL. In caso di override della VLAN, è sufficiente reindirizzare la porta 80 per consentire al resto del traffico sulla VLAN di quarantena. Per l'ACL, viene applicato l'ACL di preautenticazione ricevuto in accettazione dell'accesso.

La figura seguente fornisce una rappresentazione visiva di questo flusso di funzionalità:



Presentazione del Profiling ISE

Il servizio Cisco ISE profiler offre la funzionalità di rilevamento, individuazione e determinazione delle funzionalità di tutti gli endpoint collegati alla rete, indipendentemente dal tipo di dispositivo, in modo da garantire e mantenere un accesso appropriato alla rete aziendale. Raccoglie principalmente un attributo o un set di attributi di tutti gli endpoint della rete e li classifica in base ai relativi profili.

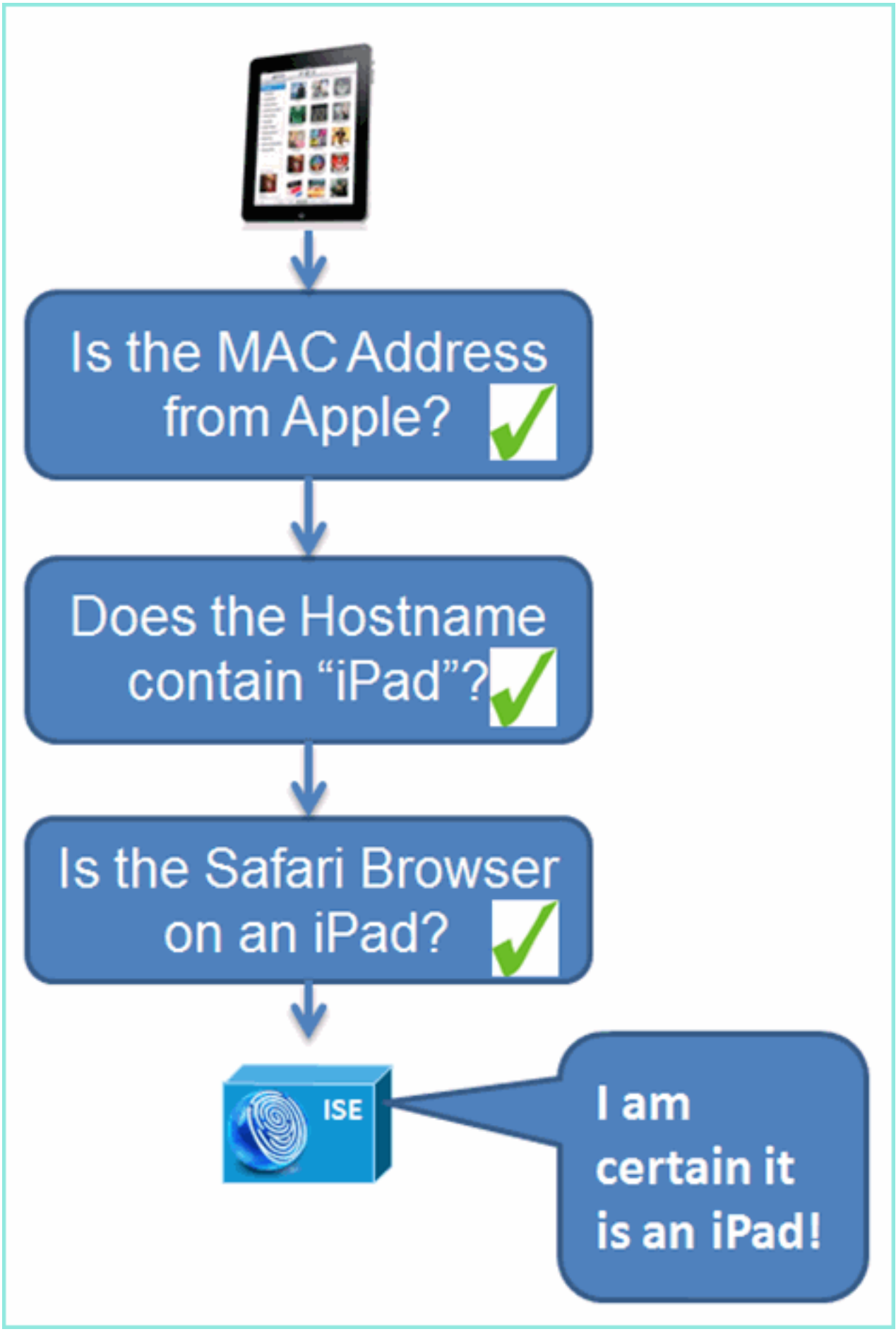
Il profiler è costituito dai componenti seguenti:

- Il sensore contiene un certo numero di sonde. I probe acquisiscono i pacchetti di rete interrogando i dispositivi di accesso alla rete e inoltrano all'analizzatore gli attributi e i relativi valori di attributo raccolti dagli endpoint.
- Un analizzatore valuta gli endpoint utilizzando i criteri configurati e i gruppi di identità in modo che corrispondano agli attributi e ai valori dei relativi attributi raccolti, classificando gli endpoint nel gruppo specificato e memorizzando gli endpoint con il profilo corrispondente nel database Cisco ISE.

Per il rilevamento dei dispositivi mobili, si consiglia di utilizzare una combinazione di queste sonde per una corretta identificazione del dispositivo:

- RADIUS (Calling-Station-ID): fornisce l'indirizzo MAC (OUI)
- DHCP (nome-host): Hostname - il nome host predefinito può includere il tipo di dispositivo; ad esempio: jsmith-ipad
- DNS (ricerca IP inversa): FQDN - il nome host predefinito può includere il tipo di dispositivo
- HTTP (agente utente): dettagli sul tipo di dispositivo mobile specifico

In questo esempio di iPad, il profiler acquisisce le informazioni del browser Web dall'attributo User-Agent, nonché altri attributi HTTP dai messaggi di richiesta e li aggiunge all'elenco degli attributi dell'endpoint.



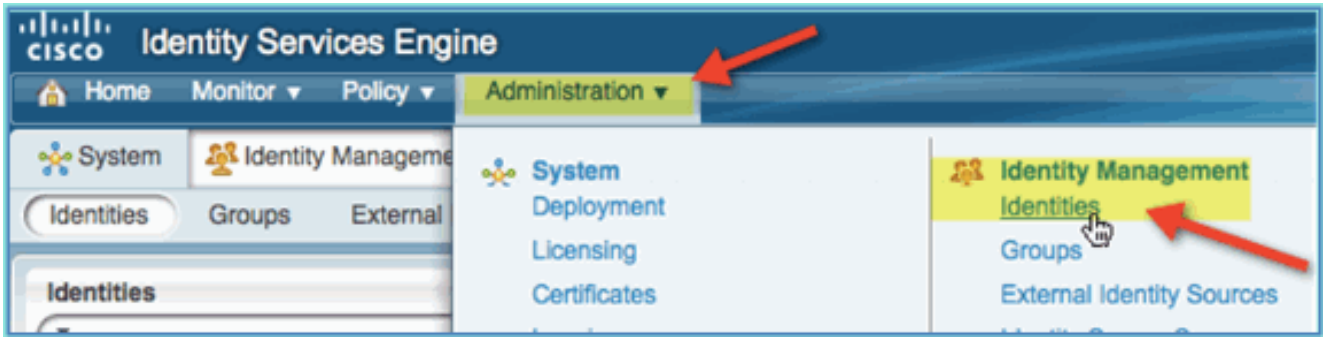
[Crea utenti identità interna]

MS Active Directory (AD) non è richiesto per un proof of concept semplice. L'ISE può essere utilizzato come unico archivio di identità, che include la differenziazione dell'accesso degli utenti per l'accesso e il controllo granulare delle policy.

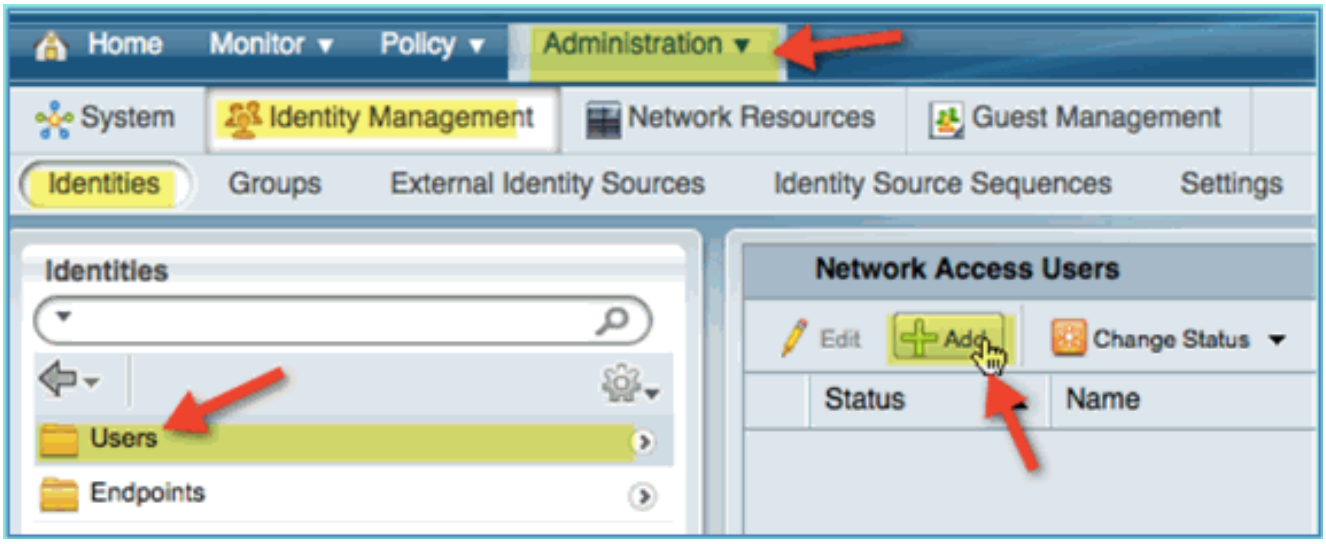
Nella release di ISE 1.0, utilizzando l'integrazione AD, ISE può utilizzare i gruppi AD nei criteri di autorizzazione. Se si usa l'archivio utenti interno ISE (senza integrazione AD), i gruppi non possono essere usati nei criteri insieme ai gruppi di identità dei dispositivi (bug identificato da risolvere in ISE 1.1). Pertanto, è possibile distinguere solo i singoli utenti, ad esempio i dipendenti o i collaboratori esterni quando vengono utilizzati in aggiunta ai gruppi di identità dei dispositivi.

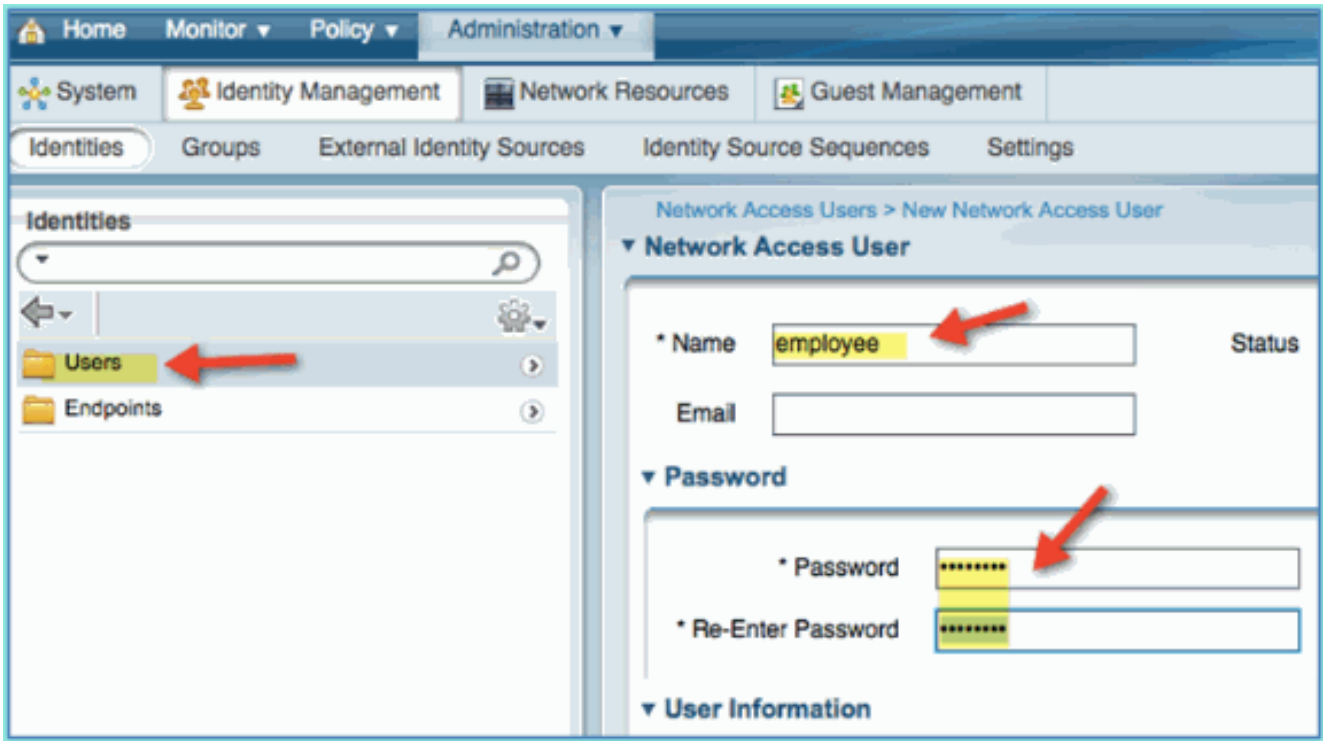
Attenersi alla seguente procedura:

1. Aprire una finestra del browser all'indirizzo https://ISEip.
2. Passare a **Amministrazione > Gestione delle identità > Identità**.

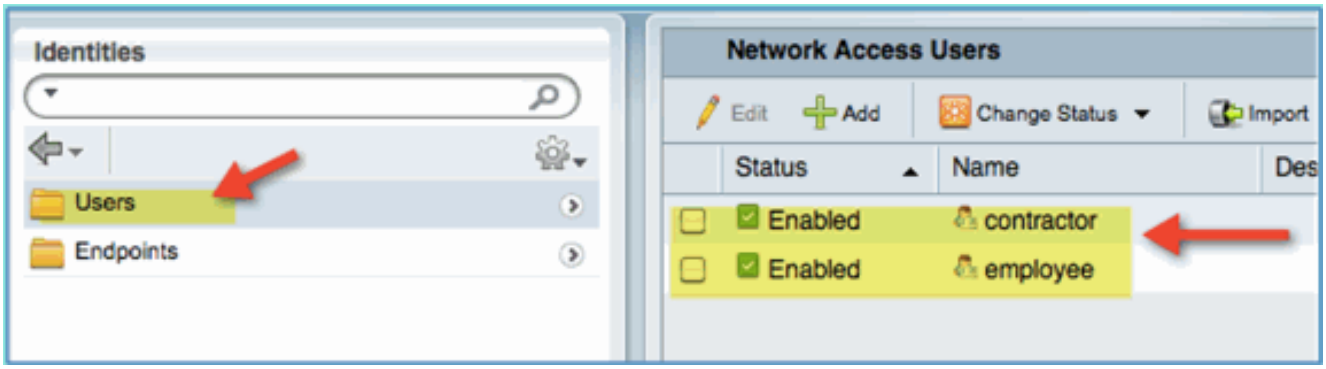


3. Selezionare **Users**, quindi fare clic su **Add** (Network Access User). Immettere i seguenti valori utente e assegnarli al gruppo Employee:Nome: dipendentePassword: XXXX





4. Fare clic su **Invia**.Nome: contraentePassword: XXXX
5. Confermare la creazione di entrambi gli account.



Aggiunta del controller LAN wireless all'ISE

Ogni dispositivo che avvia richieste RADIUS all'ISE deve avere una definizione in ISE. Questi dispositivi di rete vengono definiti in base all'indirizzo IP. Le definizioni dei dispositivi di rete ISE possono specificare intervalli di indirizzi IP consentendo in tal modo alla definizione di rappresentare più dispositivi effettivi.

Oltre a quanto richiesto per la comunicazione RADIUS, le definizioni dei dispositivi di rete ISE contengono impostazioni per altre comunicazioni ISE/dispositivi, quali SNMP e SSH.

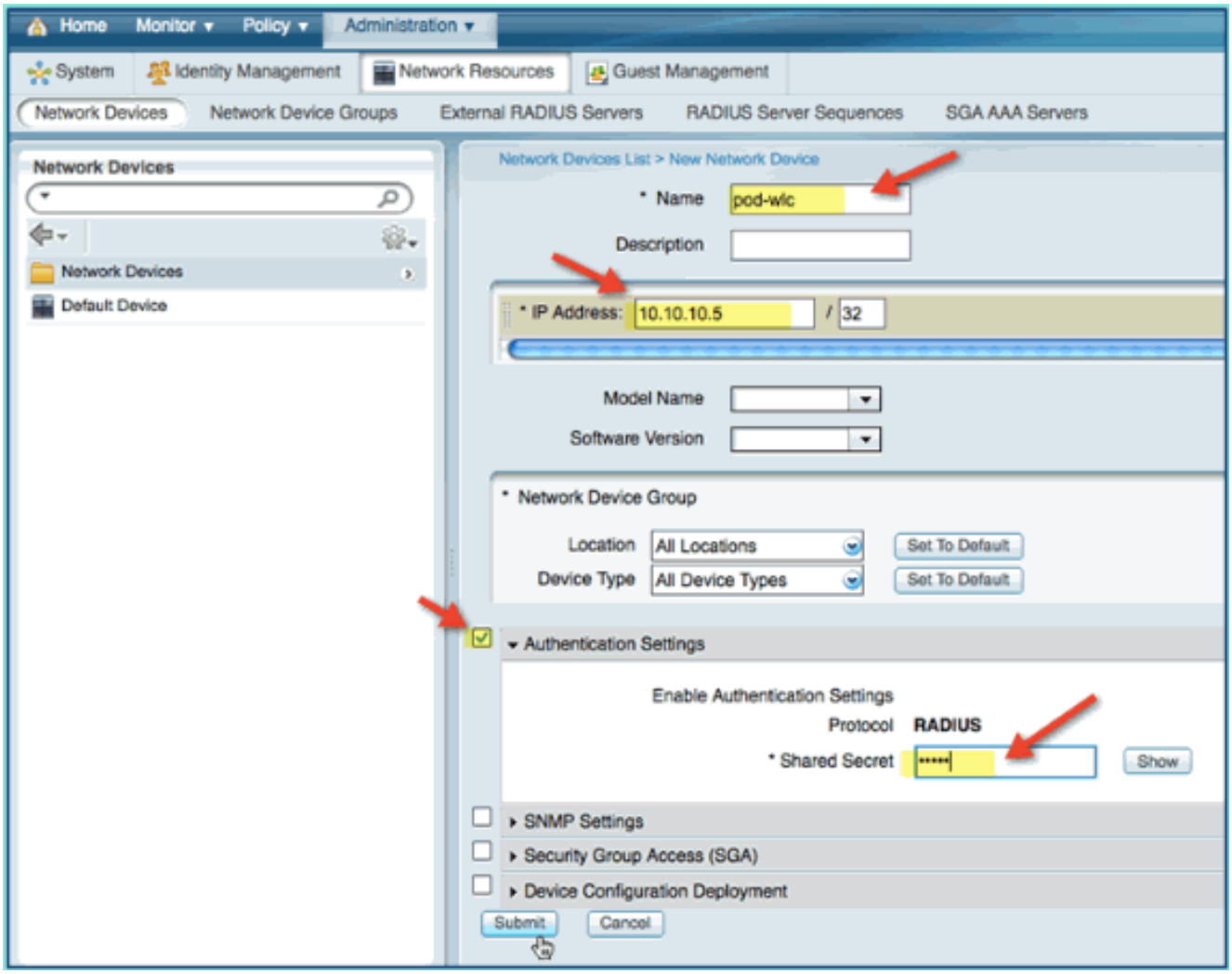
Un altro aspetto importante della definizione dei dispositivi di rete è il raggruppamento appropriato dei dispositivi in modo che questo raggruppamento possa essere utilizzato nei criteri di accesso alla rete.

In questo esercizio vengono configurate le definizioni dei dispositivi necessarie per il laboratorio.

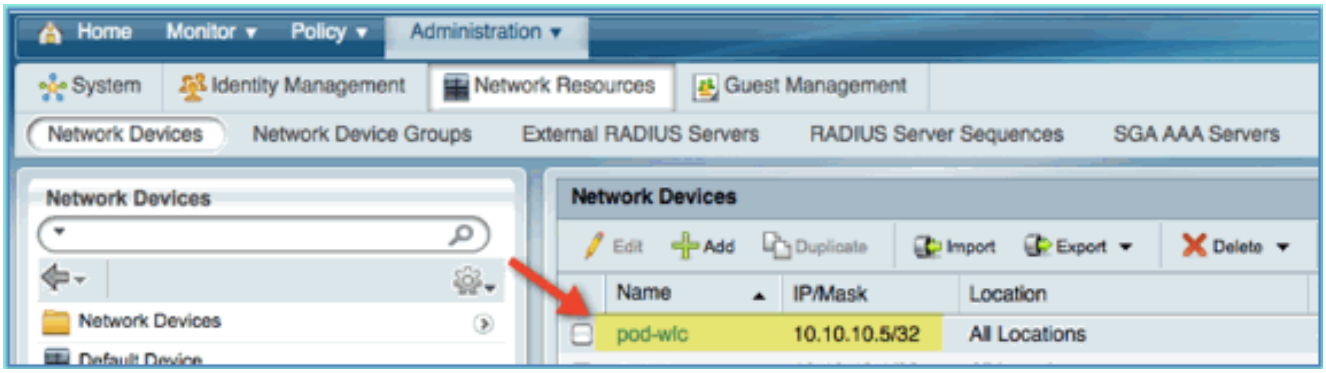
Attenersi alla seguente procedura:

1. Da ISE andare a **Amministrazione > Risorse di rete > Dispositivi di**

rete.



2. Da Periferiche di rete, fare clic su **Aggiungi**. Immettere l'indirizzo IP, controllare l'impostazione di autenticazione della maschera, quindi immettere ‘cisco’ per il segreto condiviso.
3. Salvare la voce WLC e confermare il controller nell'elenco.

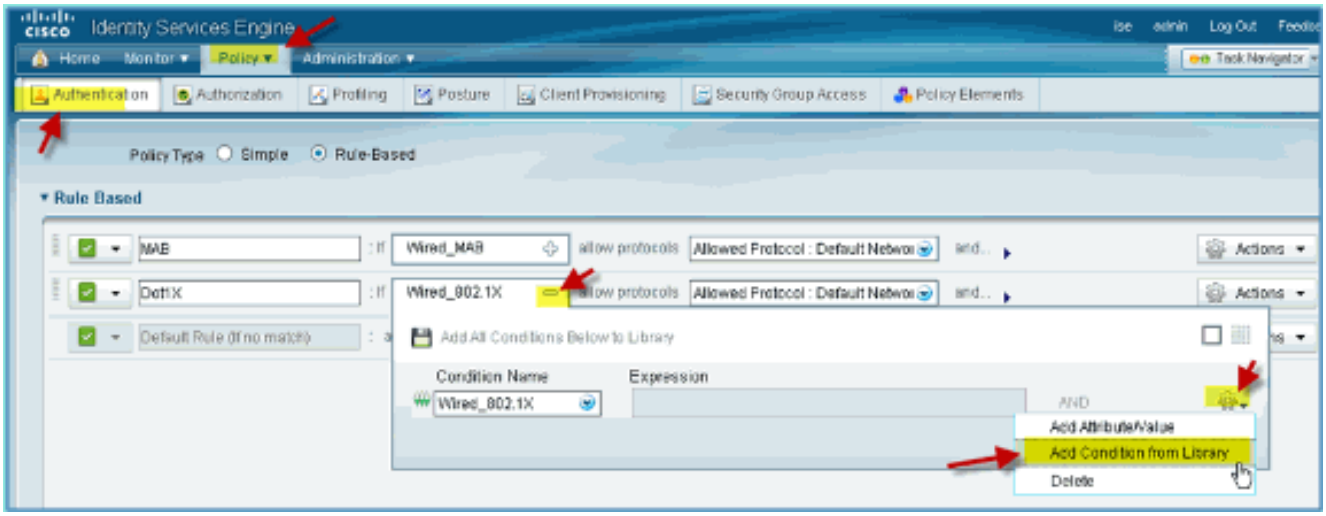


Configurazione di ISE per l'autenticazione wireless

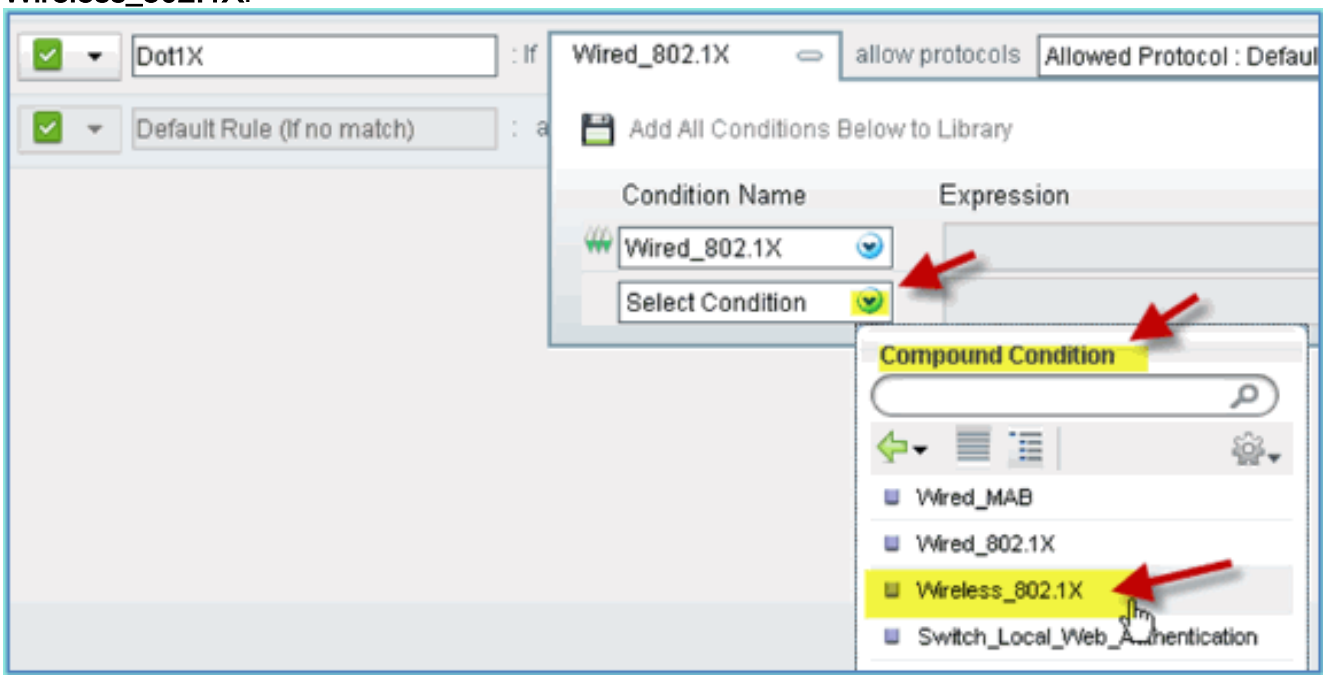
Ènecessario configurare ISE per l'autenticazione dei client wireless 802.1x e per utilizzare Active Directory come archivio identità.

Attenersi alla seguente procedura:

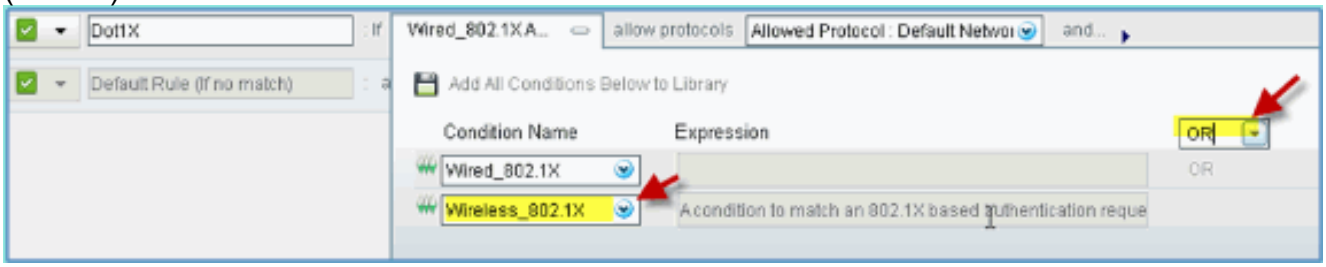
1. Da ISE selezionare **Policy > Authentication** (Policy > Autenticazione).
2. Fate clic su per espandere Dot1x > Wired_802.1X (-).
3. Fate clic sull'icona dell'ingranaggio per **aggiungere una condizione dalla libreria**.

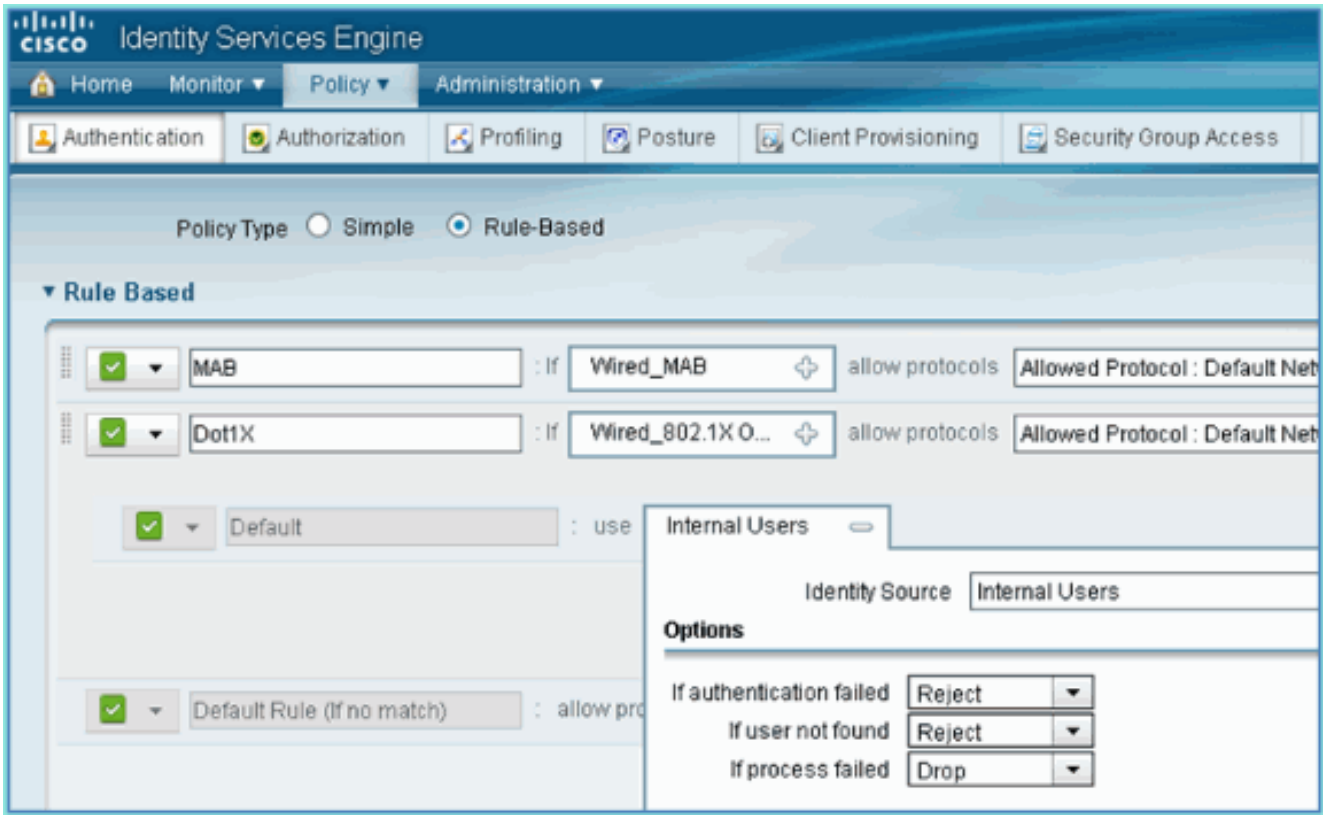


4. Dall'elenco a discesa per la selezione della condizione, scegliere **Condizione composta > Wireless_802.1X**.



5. Impostare la condizione Express su **OR**.
6. Espandere l'opzione dopo consenti protocolli e accettare l'opzione predefinita Utenti interni (default).





7. Lasciare tutto il resto in posizione predefinita. Fare clic su **Save** (Salva) per completare la procedura.

Controller LAN wireless bootstrap

Connessione di WLC a una rete

Una guida all'installazione di Cisco Wireless LAN Controller 2500 è disponibile anche nella guida all'installazione di Cisco Wireless Controller serie 2500.

Configurare il controller utilizzando la Configurazione guidata

```
(Cisco Controller)
 Welcome to the Cisco Wizard Configuration Tool Use the '-' character to backup
 Would you like to terminate autoinstall? [yes]: yes AUTO-INSTALL: process terminated
-- no configuration loaded System Name [Cisco_d9:24:44] (31 characters max):
   ISE-Podx Enter Administrative User Name (24 characters max): admin
   Enter Administrative Password
   (3 to 24 characters): Cisco123
   Re-enter Administrative Password: Cisco123
Management Interface IP Address: 10.10.10.5
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.10.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 10.10.10.10
 Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: ISE
 Network Name (SSID): PODx
Configure DHCP Bridging Mode [yes][NO]: no
Allow Static IP Addresses [YES][no]: no
 Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
```

```
Please see documentation for more details.
 Enter Country Code list (enter 'help' for a list of countries) [US]: US

Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes
 Configure a NTP server now? [YES][no]: no
Configure the ntp system time now? [YES][no]: yes
Enter the date in MM/DD/YY format: mm/dd/yy
Enter the time in HH:MM:SS format: hh:mm:ss
Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
 Configuration saved!
 Resetting system with new configuration...
Restarting system.
```

Configurazione switch adiacente

Il controller è collegato alla porta Ethernet dello switch adiacente (Fast Ethernet 1). La porta dello switch adiacente è configurata come trunk 802.1Q e consente tutte le VLAN sul trunk. La VLAN nativa 10 consente di connettere l'interfaccia di gestione del WLC.

La configurazione della porta dello switch 802.1Q è la seguente:

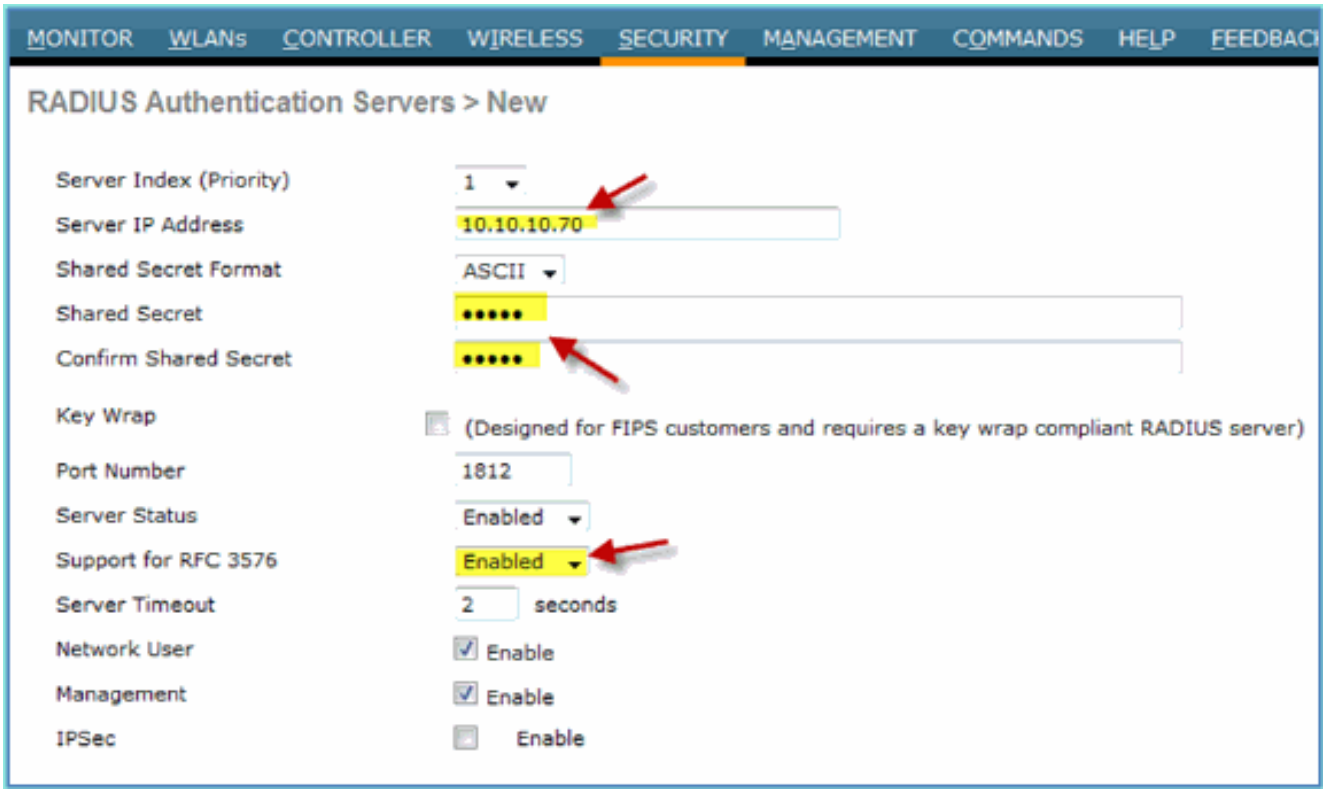
```
switchport
switchport trunk encapsulation dot1q
switchport trunk native VLAN 10
switchport mode trunk
end
```

Add Authentication Server (ISE) to WLC

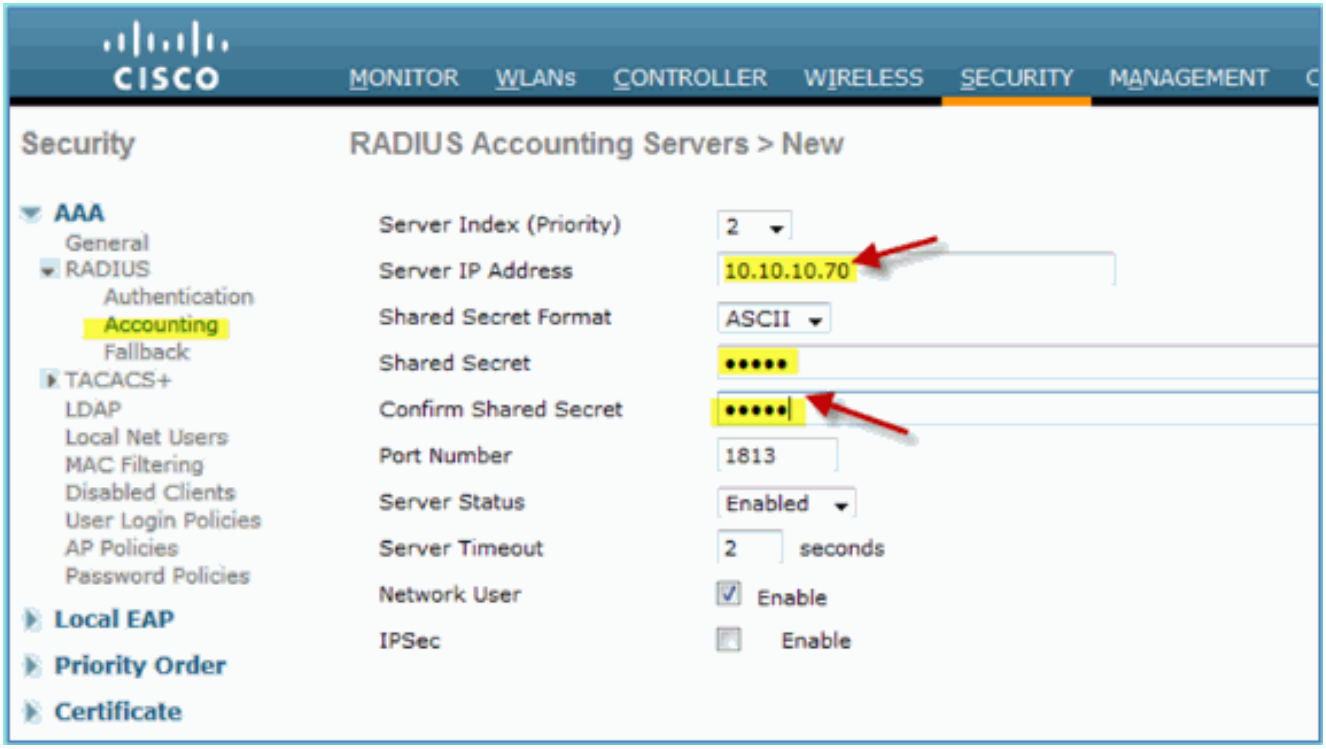
Per abilitare 802.1X e la funzione CoA per gli endpoint wireless, è necessario aggiungere l'ISE al WLC.

Attenersi alla seguente procedura:

1. Aprire un browser, quindi collegarsi al pod WLC (usando il protocollo HTTP protetto) > https://wlc.
2. Selezionare **Protezione > Autenticazione > Nuovo**.



3. Immettere i seguenti valori:Indirizzo IP server: 10.10.10.70 (controllare l'assegnazione)Segreto condiviso: ciscoSupporto per RFC 3576 (CoA): abilitato (predefinito)Tutto il resto: Predefinito
4. Fare clic su **Apply** (Applica) per continuare.
5. Selezionare **Accounting RADIUS > aggiungi NUOVO**.

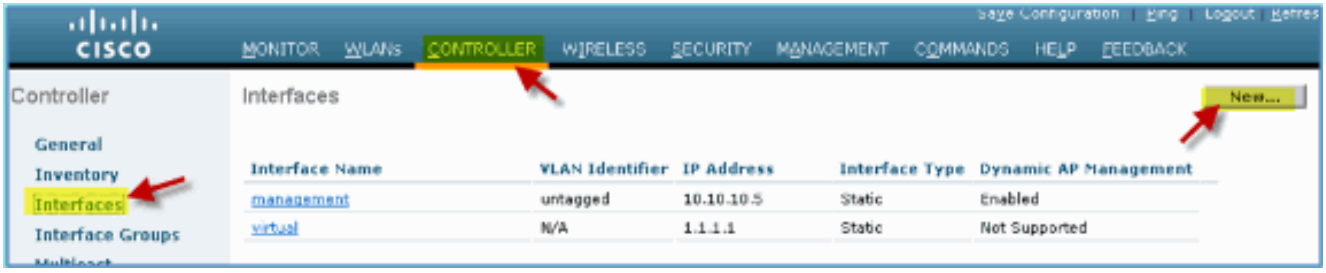


6. Immettere i seguenti valori:Indirizzo IP server: 10.10.10.70Segreto condiviso: ciscoTutto il resto: Predefinito
7. Fare clic su **Apply** (Applica), quindi salvare la configurazione per il WLC.

Crea interfaccia dinamica dipendente WLC

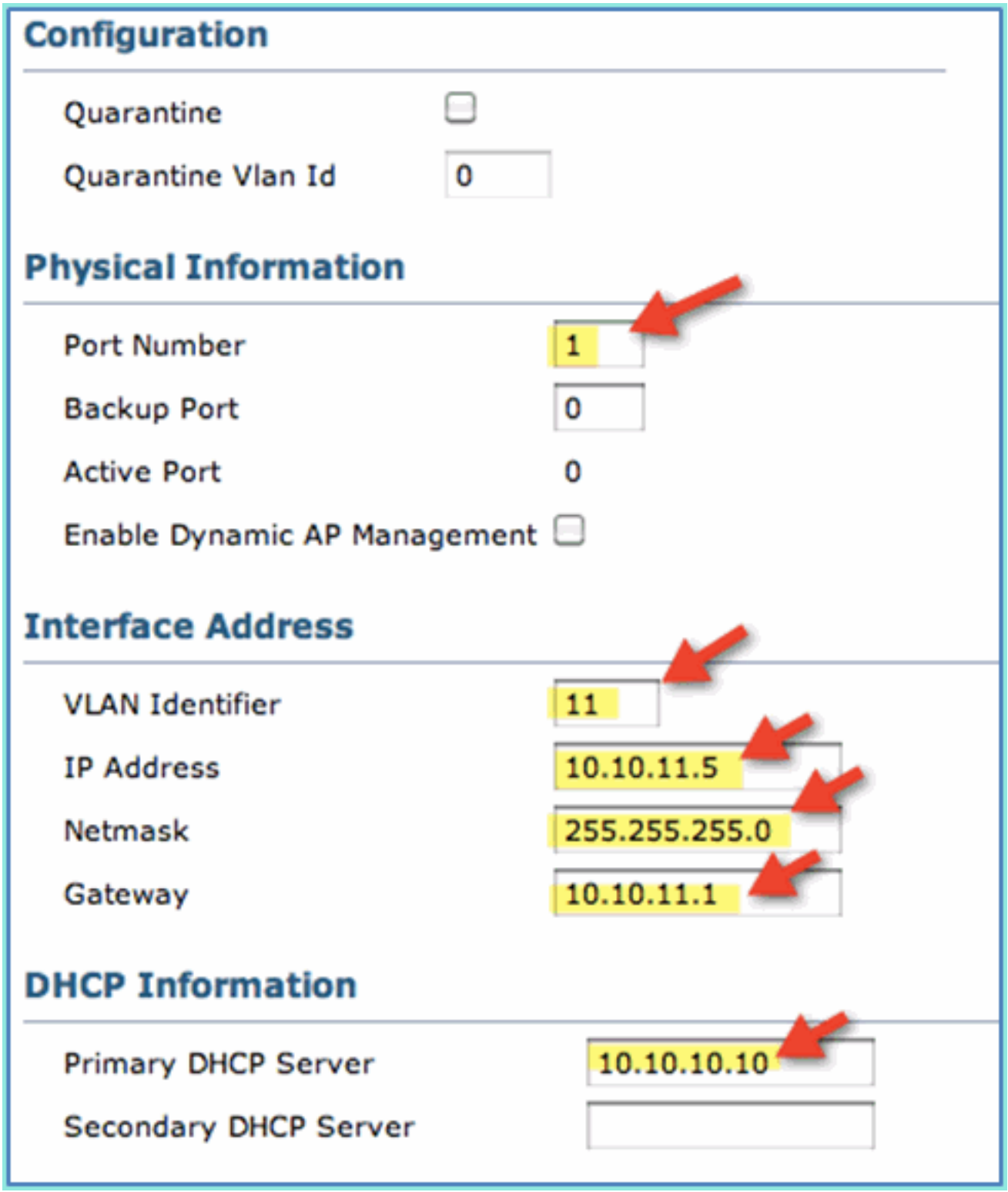
Completare questi passaggi per aggiungere una nuova interfaccia dinamica per il WLC e mapparla alla VLAN del dipendente:

1. Da WLC, selezionare **Controller > Interfaces**. Fare quindi clic su **Nuovo**.



2. Da WLC, selezionare **Controller > Interfaces**. Immettere quanto segue:Nome interfaccia: dipendenteID VLAN:
   11

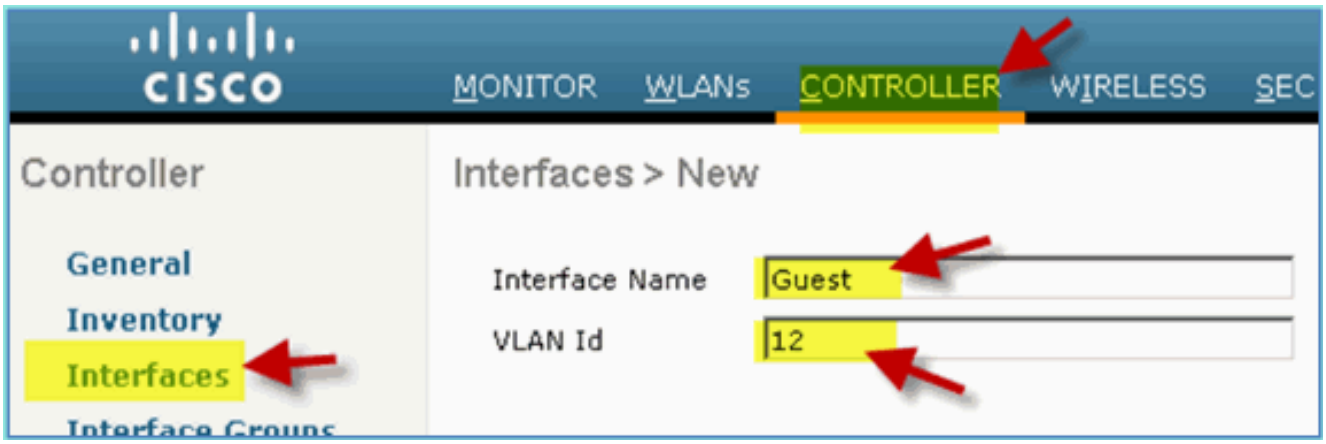
3. Immettere quanto segue per l'interfaccia dipendente:Numero porta: 1Identificatore VLAN: 11Indirizzo IP: 10.10.11.5Maschera di rete: 255.255.255.0Gateway: 10.10.11.1DHCP: 10.10.10.10



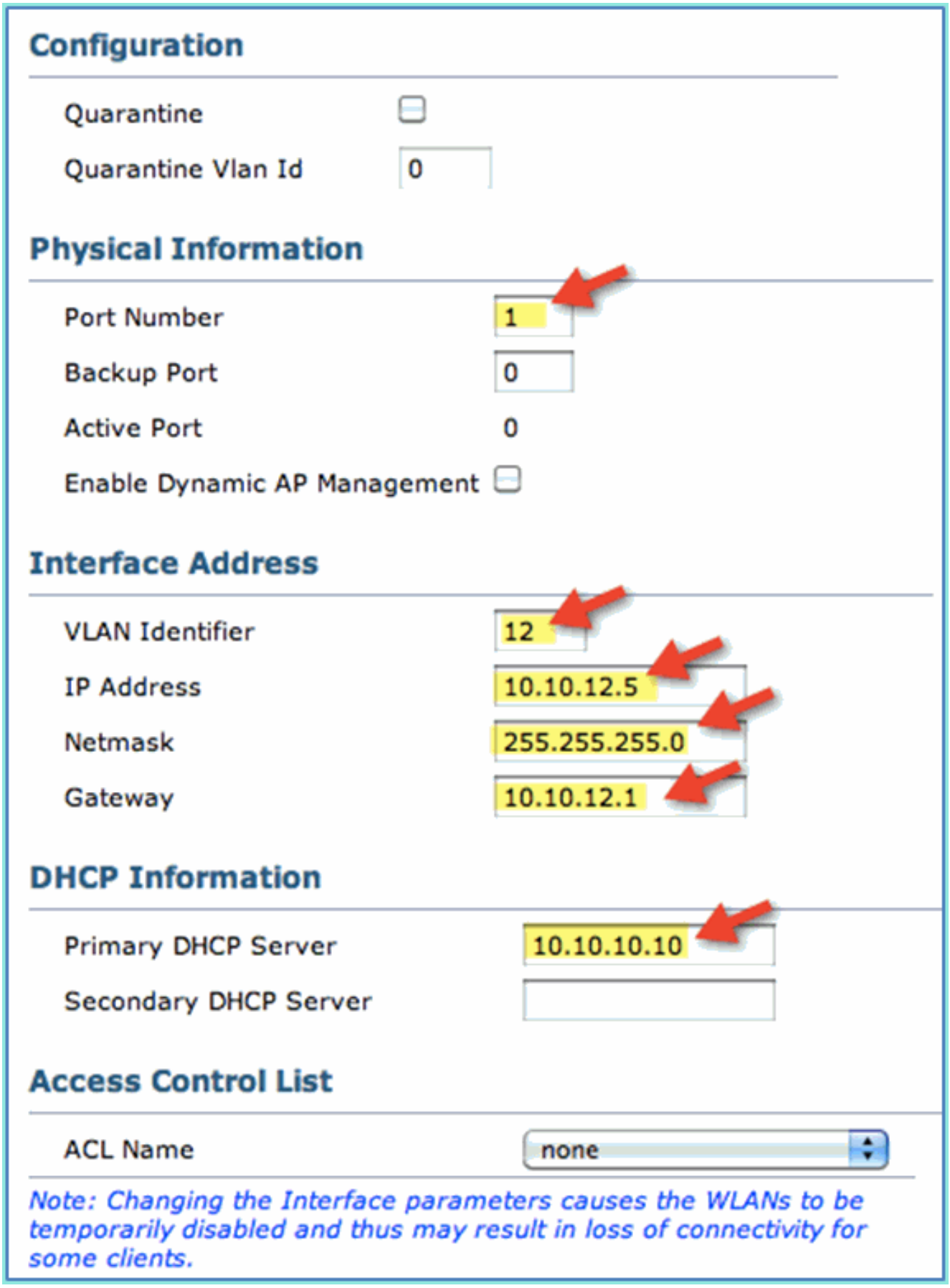
4. Confermare la creazione della nuova interfaccia dinamica dipendente.

Crea interfaccia dinamica guest WLC

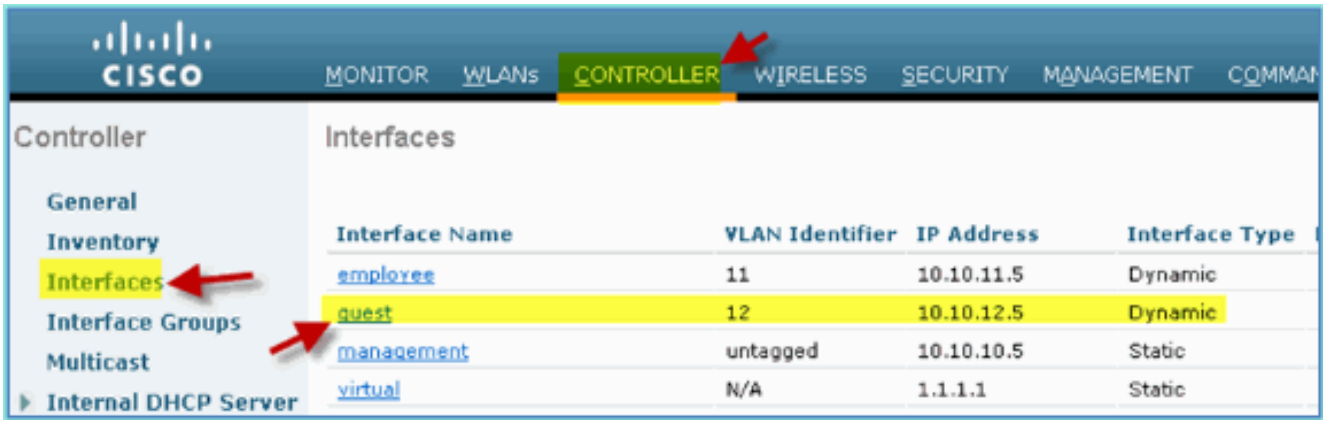
Completare questi passaggi per aggiungere una nuova interfaccia dinamica per il WLC e mapparla alla VLAN guest:

1. Da WLC, selezionare **Controller > Interfaces**. Fare quindi clic su **Nuovo**.
2. Da WLC, selezionare **Controller > Interfaces**. Immettere quanto segue:Nome interfaccia: GuestID VLAN:
   12
   

3. Immettere quanto segue per l'interfaccia Guest:Numero porta: 1Identificatore VLAN: 12Indirizzo IP: 10.10.12.5Maschera di rete: 255.255.255.0Gateway: 10.10.12.1DHCP: 10.10.10.10



4. Confermare che l'interfaccia guest è stata aggiunta.



Aggiungi WLAN 802.1x

Dal bootstrap iniziale del WLC, potrebbe essere stata creata una WLAN predefinita. In tal caso, modificarla o creare una nuova WLAN che supporti l'autenticazione wireless 802.1X come indicato nella guida.

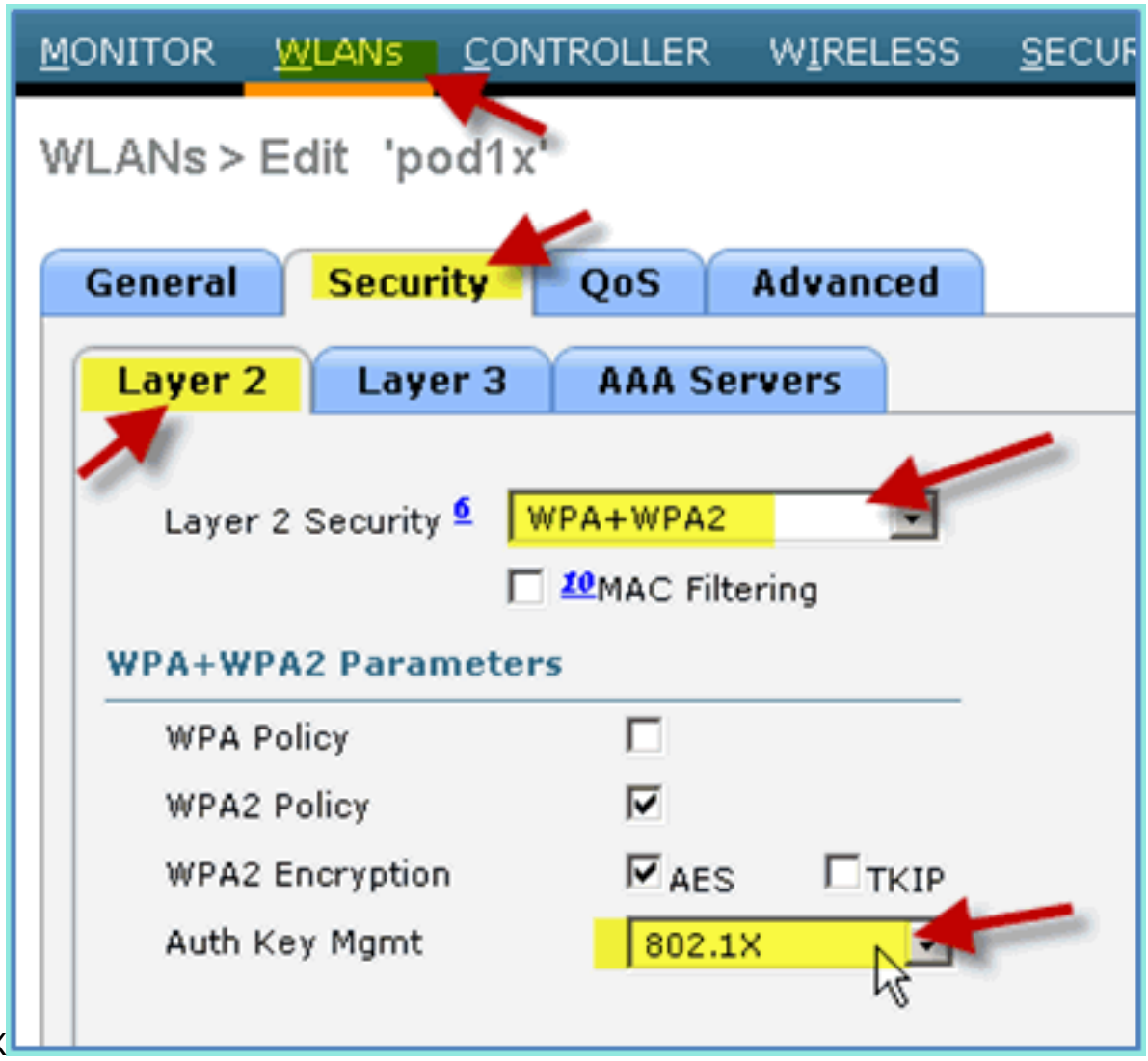
Attenersi alla seguente procedura:

1. Da WLC, selezionare **WLAN > Create New**
   (WLC).


2. Per la WLAN, immettere quanto segue:Nome profilo: pod1xSSID:
   uguale

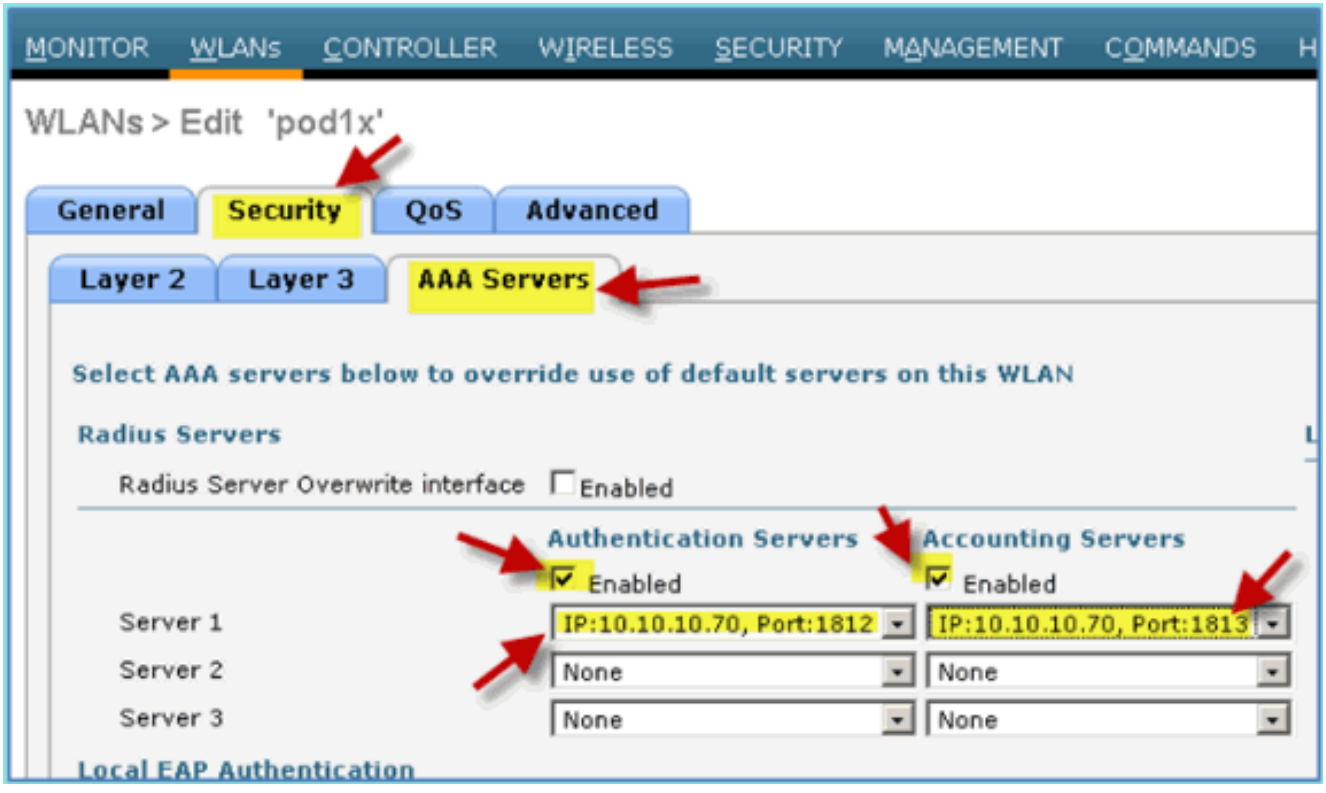

3. Per la scheda Impostazioni WLAN > Generale, usare quanto segue:Criterio radio:
   tuttoInterfaccia/Gruppo: gestioneTutto il resto:
   predefinito

4. Per la scheda WLAN > Protezione > Layer 2, impostare quanto segue:Sicurezza di livello 2:WPA+WPA2Criterio WPA2 / Crittografia: attivata / AESGestione Chiavi Auth:

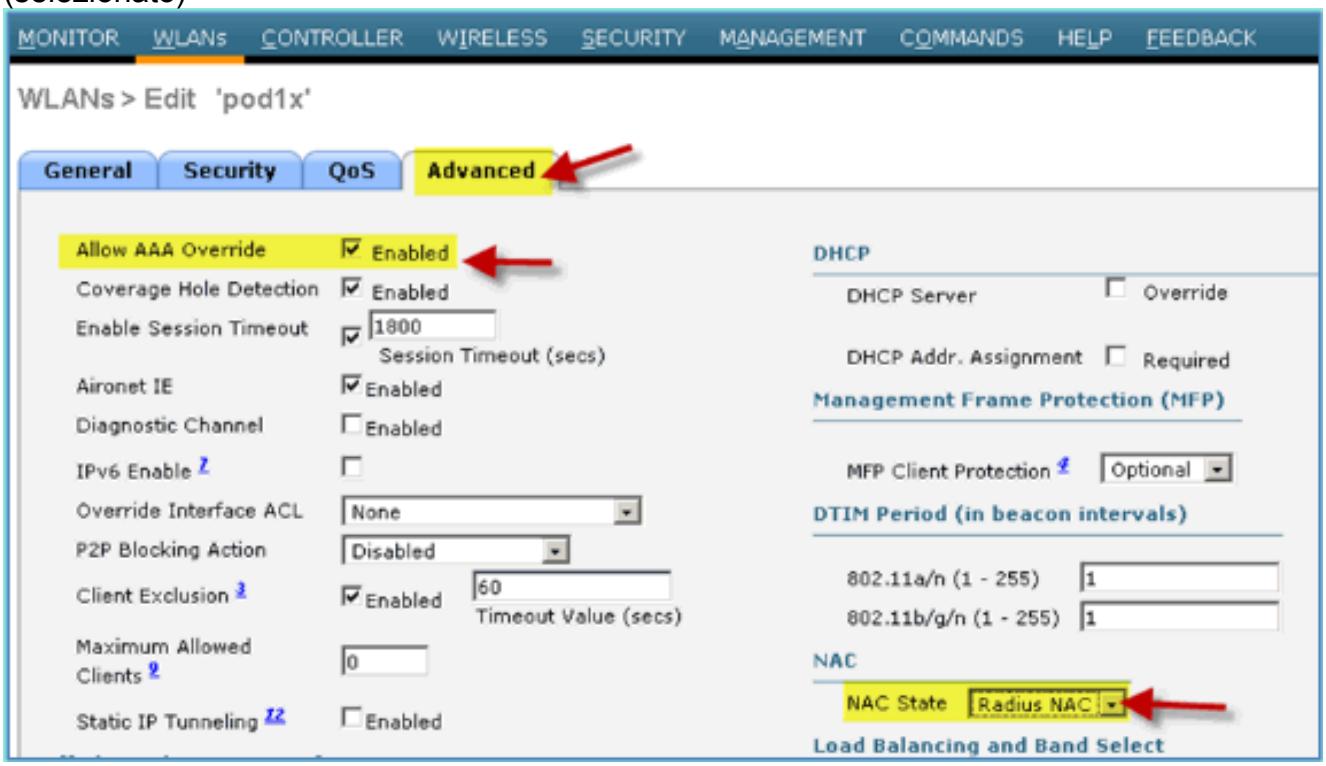


802.1X

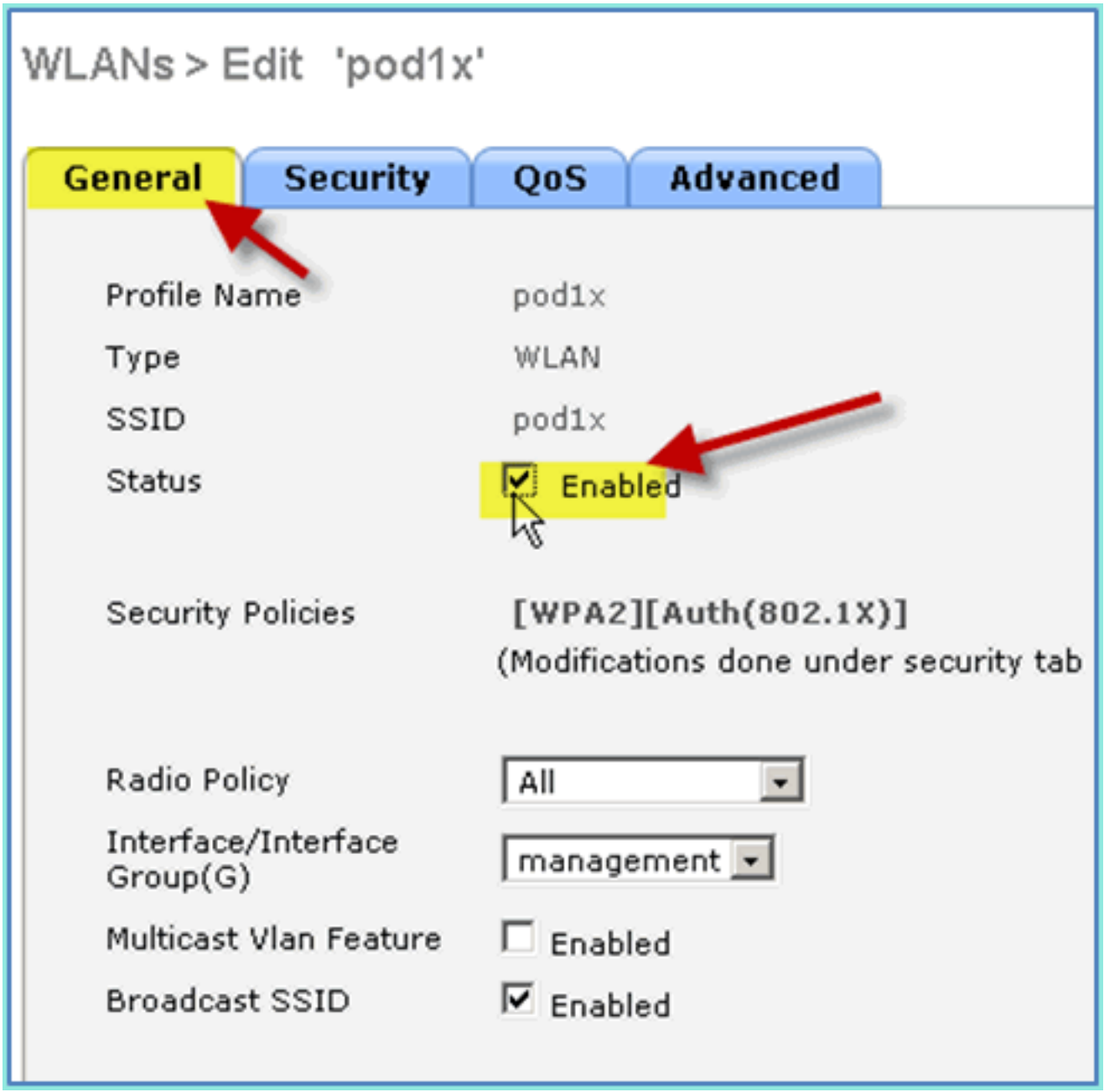
5. Per la scheda WLAN > Sicurezza > Server AAA, impostare quanto segue:Interfaccia di sovrascrittura del server radio: disabilitataServer di autenticazione/accounting: AbilitatoServer 1:
10.10.10.70



6. Per la scheda WLAN > Avanzate, impostare quanto segue:Consenti sostituzione AAA: abilitataStato NAC: Radius NAC
   (selezionato)



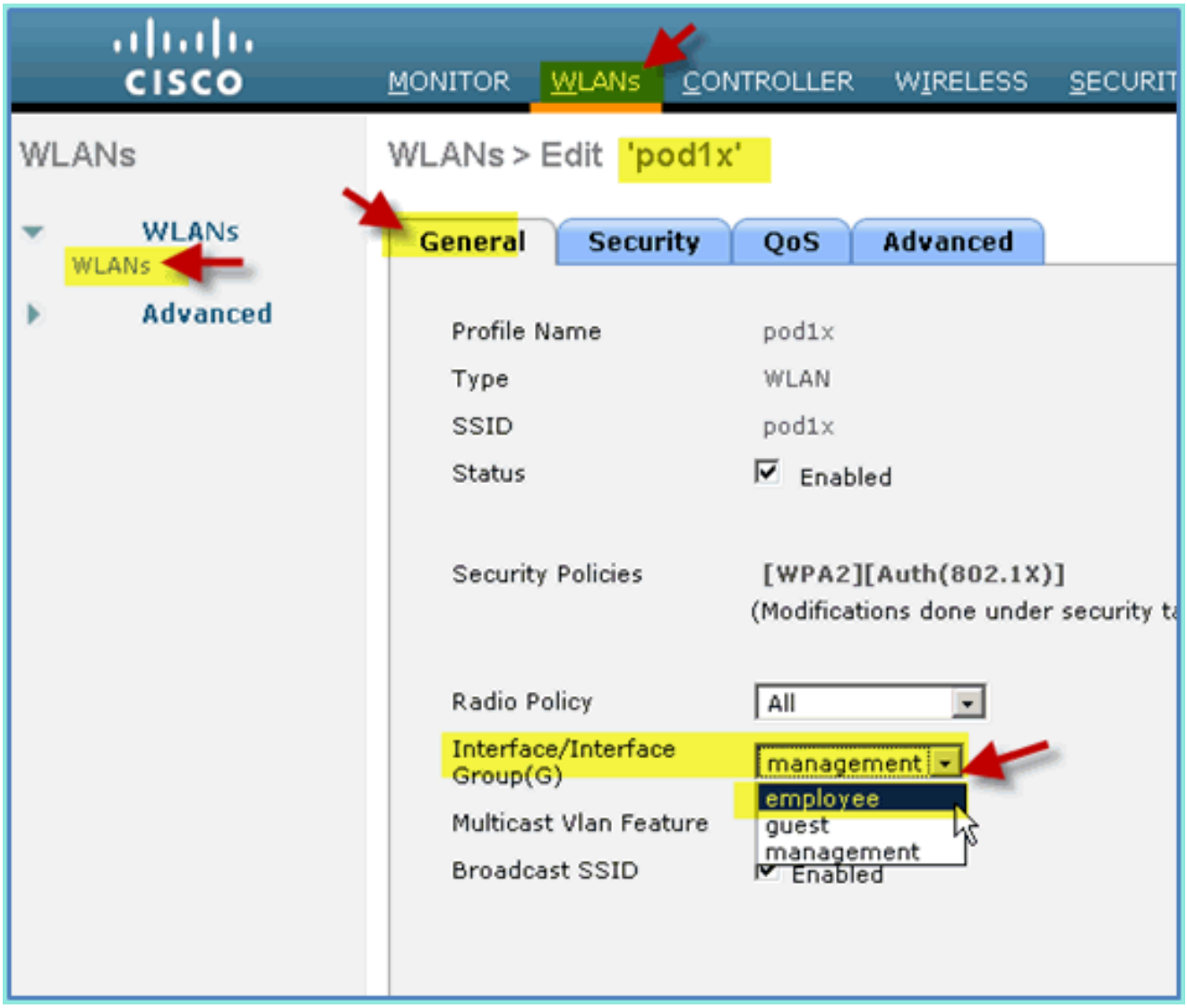
7. Tornare alla scheda WLAN > Generale > Abilita WLAN (casella di controllo).



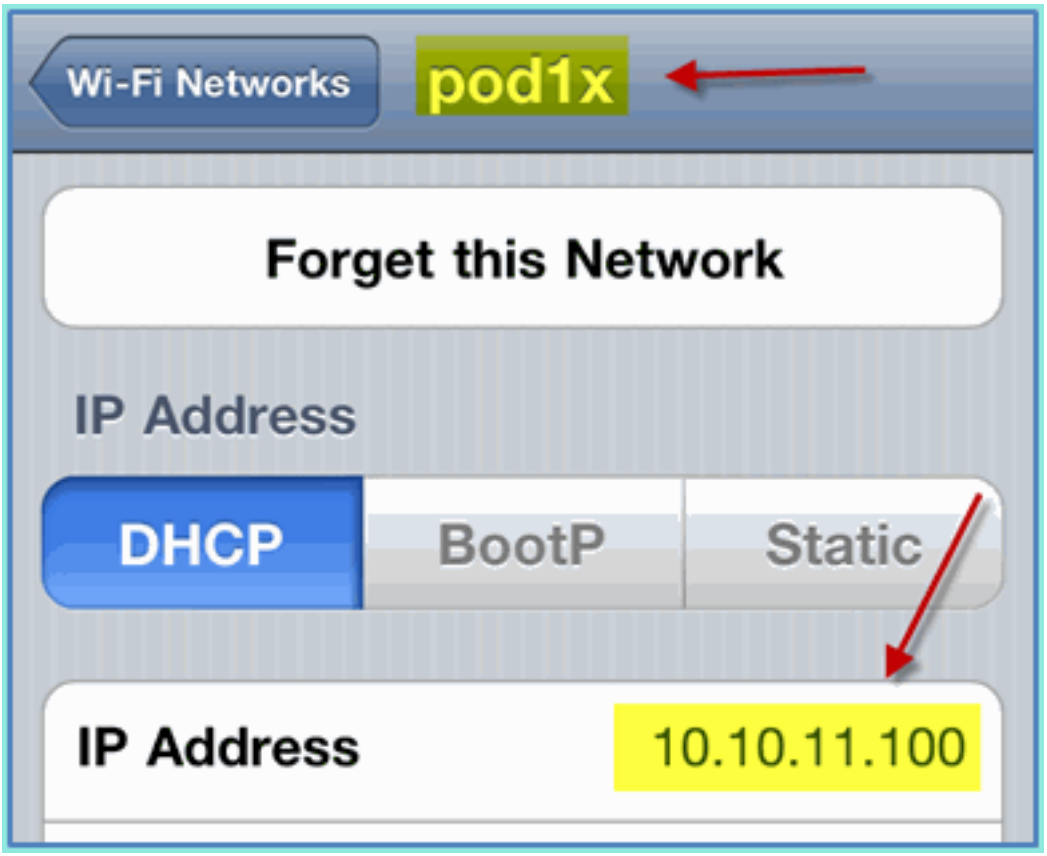
Test interfacce dinamiche WLC

Ènecessario verificare rapidamente le interfacce utente e guest valide. Usare un dispositivo qualsiasi da associare alla WLAN, quindi modificare l'assegnazione dell'interfaccia WLAN.

1. Da WLC, selezionare **WLAN > WLAN**. Fare clic per modificare il SSID sicuro creato nell'esercizio precedente.
2. Modificare il gruppo interfaccia/interfaccia in **Dipendente**, quindi fare clic su **Applica**.

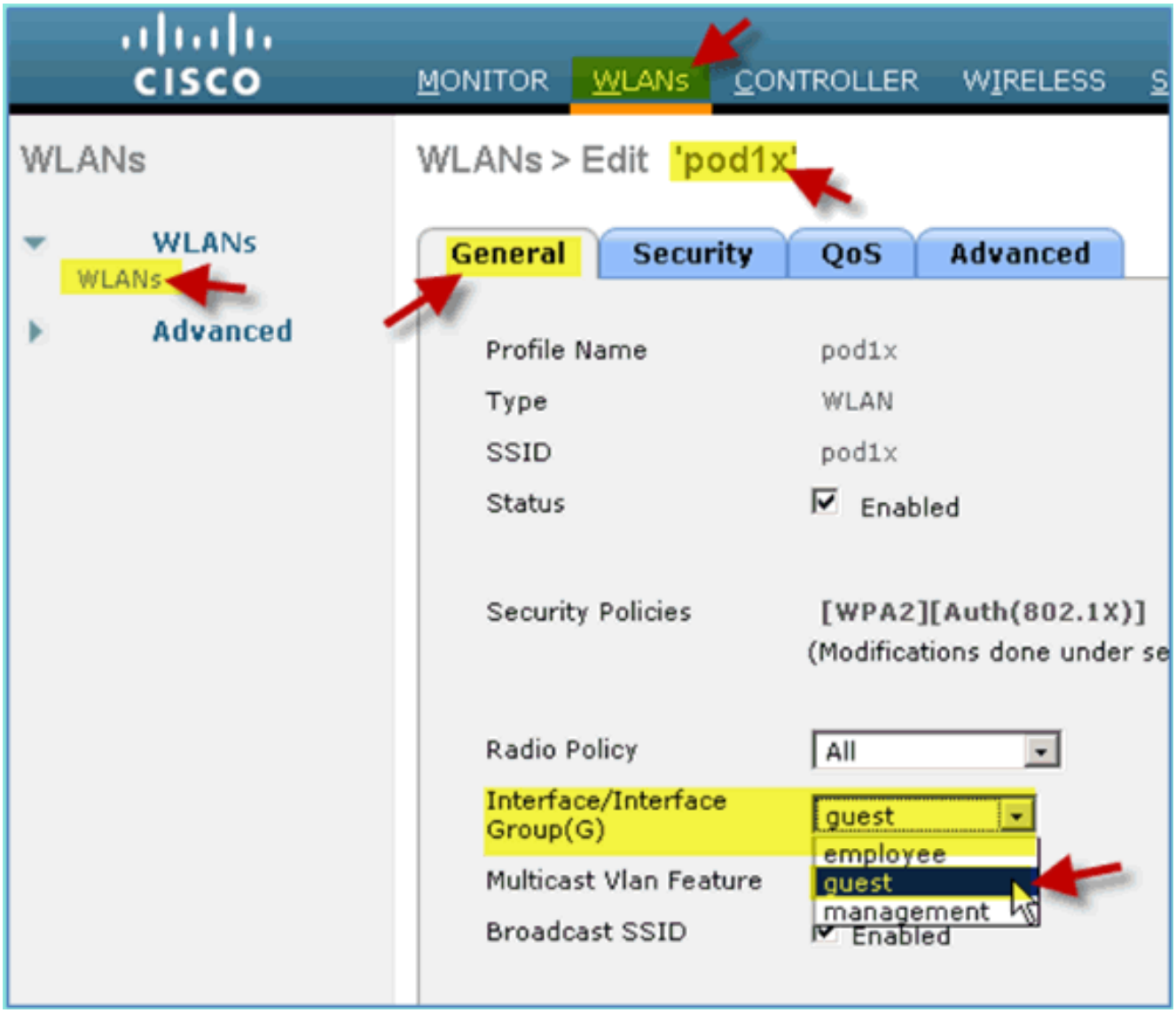


3. Se configurato correttamente, un dispositivo riceve un indirizzo IP dalla VLAN del dipendente (10.10.11.0/24). Nell'esempio viene mostrato un dispositivo iOS che ottiene un nuovo

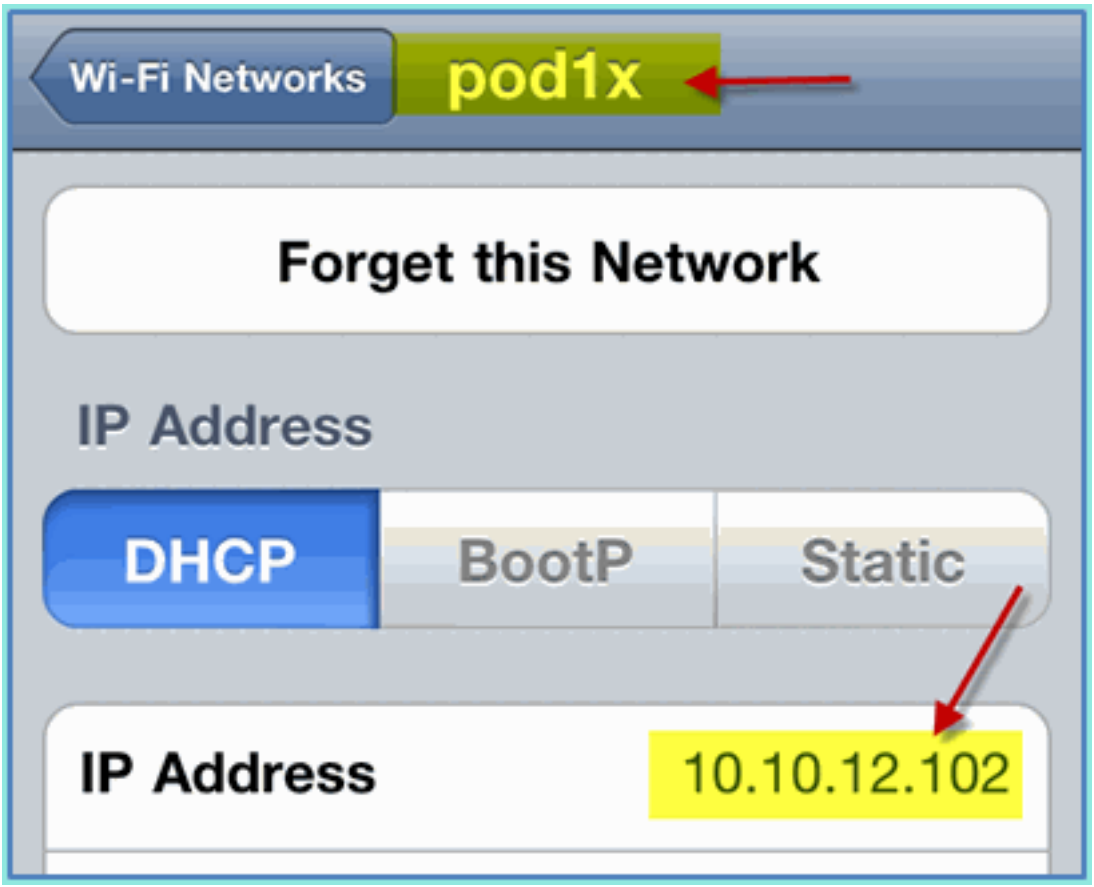


indirizzo IP.

4. Una volta confermata l'interfaccia precedente, modificare l'assegnazione dell'interfaccia WLAN in **Guest**, quindi fare clic su **Apply** (Applica).



5. Se configurato correttamente, un dispositivo riceve un indirizzo IP dalla VLAN guest (10.10.12.0/24). Nell'esempio viene mostrato un dispositivo iOS che ottiene un nuovo



indirizzo IP.

6. **IMPORTANTE:** ripristinare l'assegnazione originale dell'interfaccia.
7. Fare clic su **Apply** (Applica) e salvare la configurazione per il WLC.

Autenticazione wireless per iOS (iPhone/iPad)

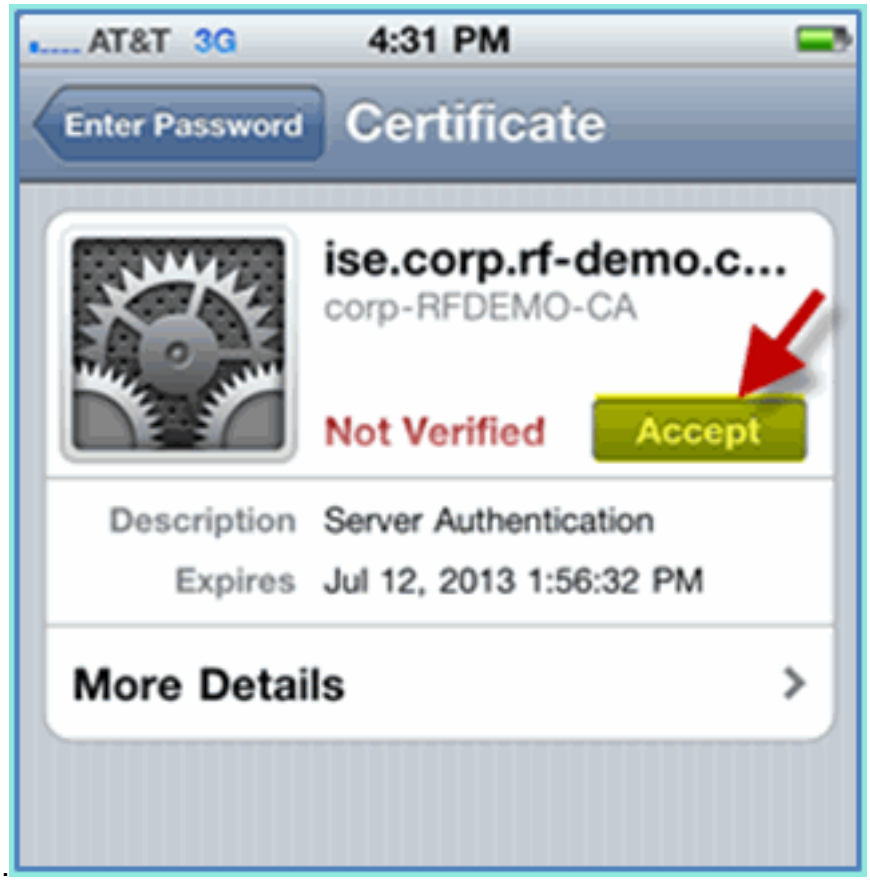
Associare al WLC tramite un SSID autenticato un utente INTERNO (o un utente AD integrato) utilizzando un dispositivo iOS come un iPhone, iPad o iPod. Se non applicabile, ignorare questi passaggi.

1. Sul dispositivo iOS, passare alle impostazioni WLAN. Attivare WIFI, quindi selezionare il SSID abilitato 802.1X creato nella sezione precedente.
2. Fornire queste informazioni per la connessione:Nome utente: dipendente (interno - dipendente) o terzista (interno - terzista)Password:

XXXX

3. Fare clic per accettare il certificato

ISE.

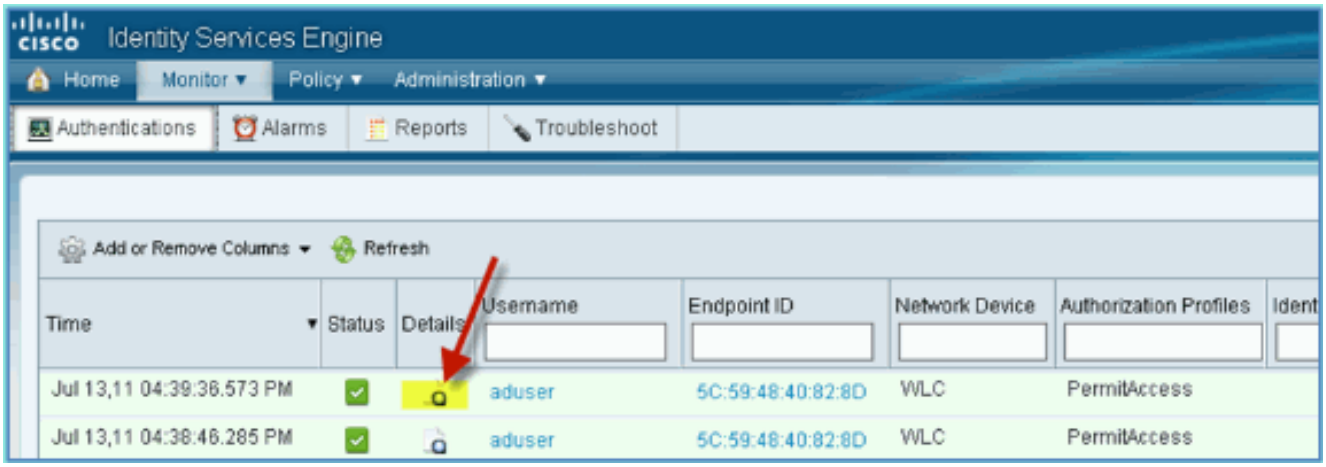


4. Verificare che il dispositivo iOS riceva un indirizzo IP dall'interfaccia di gestione

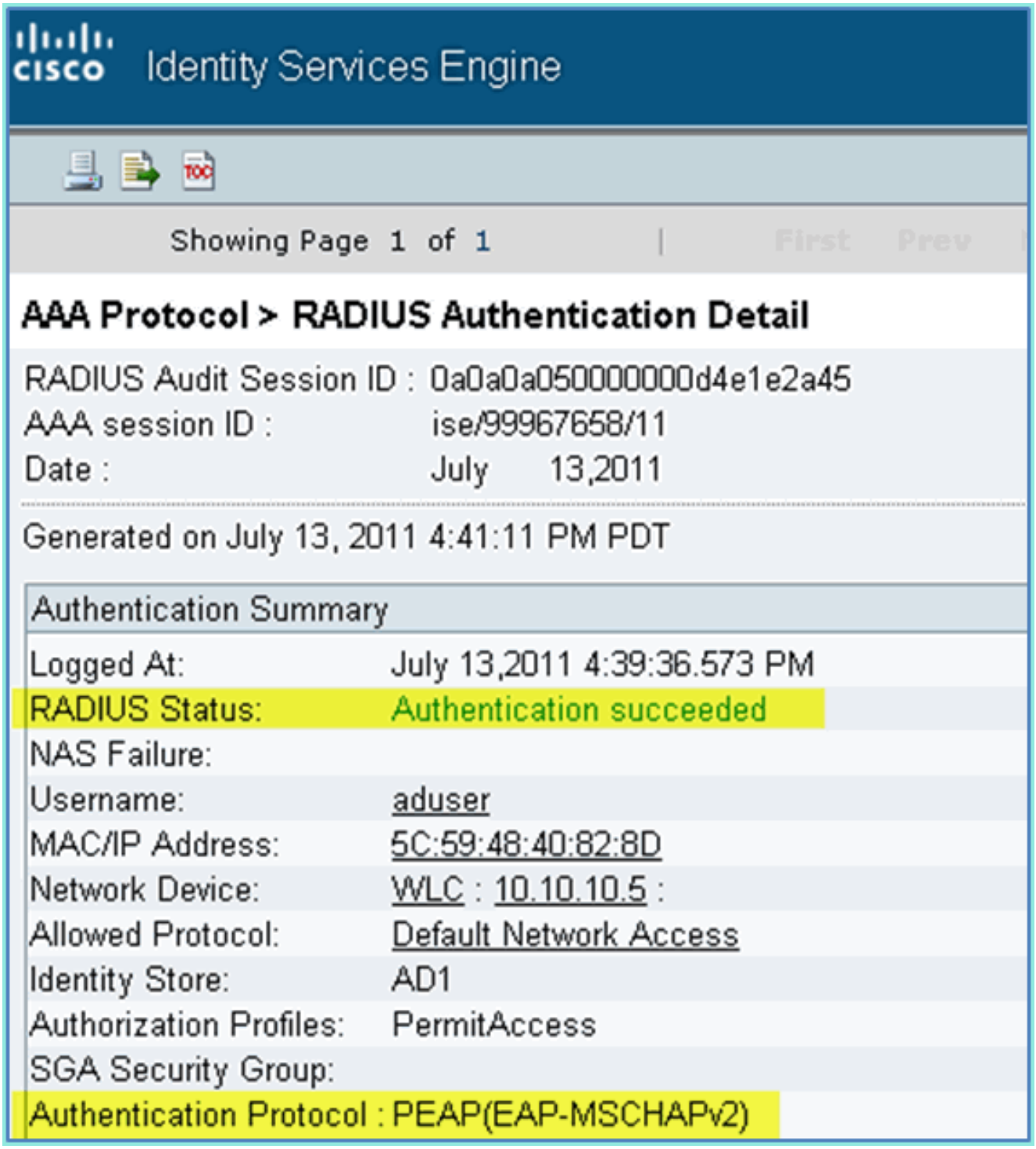
(VLAN10).

5. In WLC > Monitor > Clients (WLC > Monitor > Client), verificare le informazioni sull'endpoint, inclusi l'uso, lo stato e il tipo
   EAP.

6. Analogamente, le informazioni sul client possono essere fornite da ISE > Monitor > pagina Autenticazione.



7. Fare clic sull'icona **Dettagli** per espandere la sessione e ottenere informazioni dettagliate sulla
sessione.



Aggiungi ACL di reindirizzamento della postura al WLC

L'ACL di reindirizzamento della postura è configurato sul WLC, da dove ISE verrà usato per limitare la postura del client. L'ACL permette il traffico tra ISE in modo efficace e minimo. Se necessario, è possibile aggiungere regole facoltative in questo ACL.

1. Passare a **WLC > Sicurezza > Access Control Lists > Access Control Lists**. Fare clic su **New**.

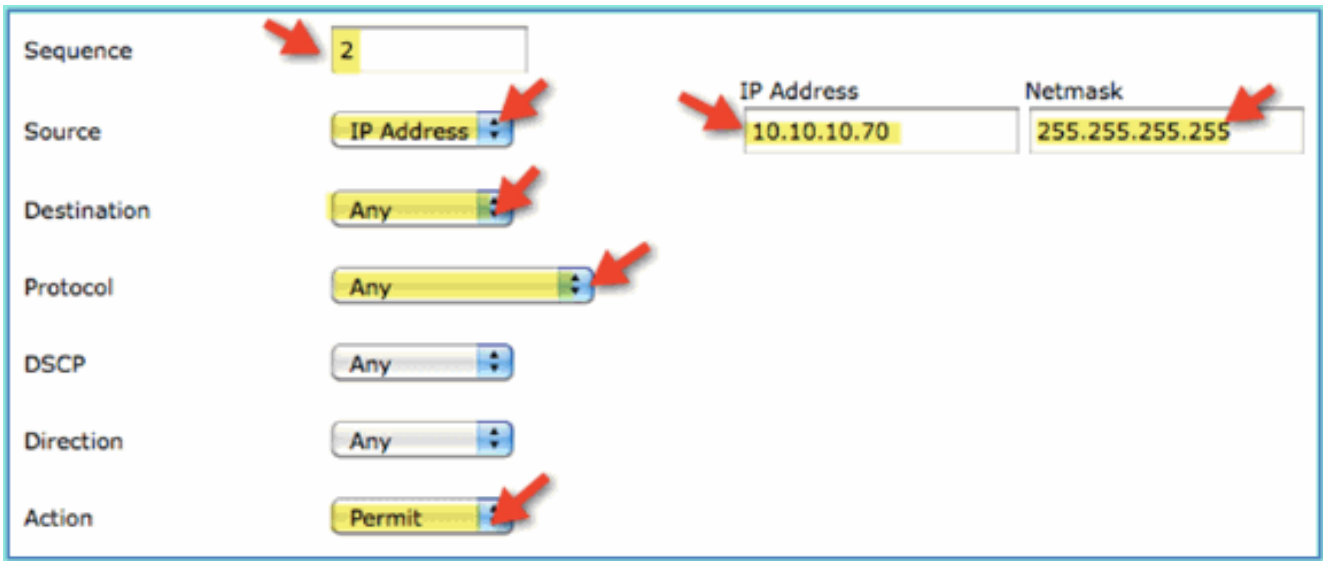
2. Specificare un nome (ACL-POSTURE-REDIRECT) per l'ACL.

3. Fare clic su **Add New Rule** (Aggiungi nuova regola) per il nuovo ACL. Impostare i seguenti valori sulla sequenza ACL n. 1. Al termine, fare clic su **Apply** (Applica).Fonte: AnyDestinazione: indirizzo IP 10.10.10.70, 255.255.255.255Protocollo: AnyAzione: Autorizza

4. La sequenza di conferma è stata aggiunta.

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	10.10.10.70 / 255.255.255.255	Any	Any	Any	Any	Any	0

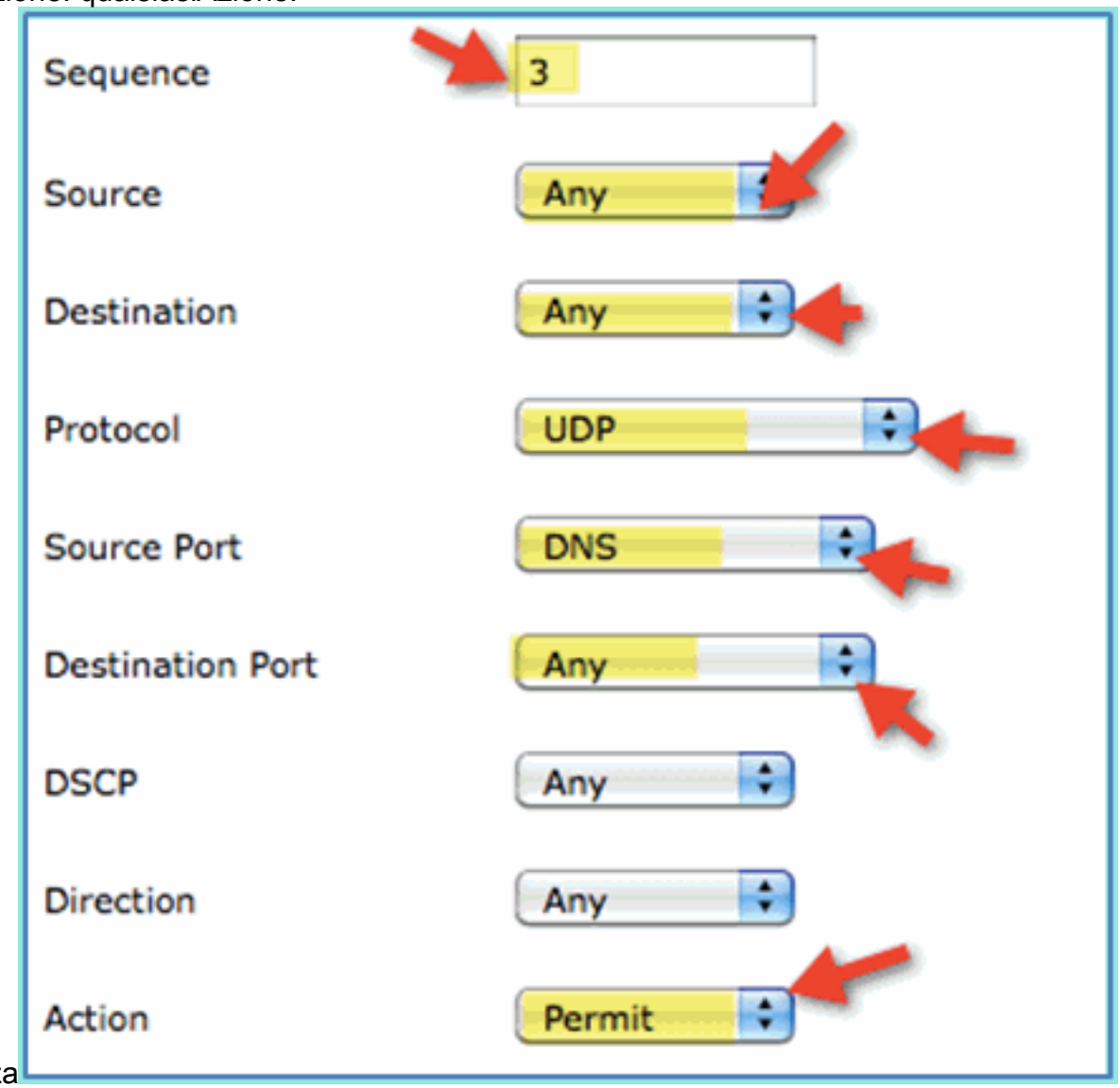
5. Fare clic su **Aggiungi nuova regola**. Impostare i seguenti valori sulla sequenza ACL n. 2. Al termine, fare clic su **Apply** (Applica).Fonte: indirizzo IP 10.10.10.70, 255.255.255.255Destinazione: QualsiasiProtocollo: AnyAzione: Autorizza



6. La sequenza di conferma è stata aggiunta.

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	0.0.0.0 / 0.0.0.0	10.10.10.70 / 255.255.255.255	Any	Any	Any	Any	Any
2	Permit	10.10.10.70 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any

7. Impostare i seguenti valori sulla sequenza ACL n. 3. Al termine, fare clic su **Apply** (Applica).Fonte: AnyDestinazione: QualsiasiProtocollo: UDPPorta di origine: DNSPorta di destinazione: qualsiasiAzione:



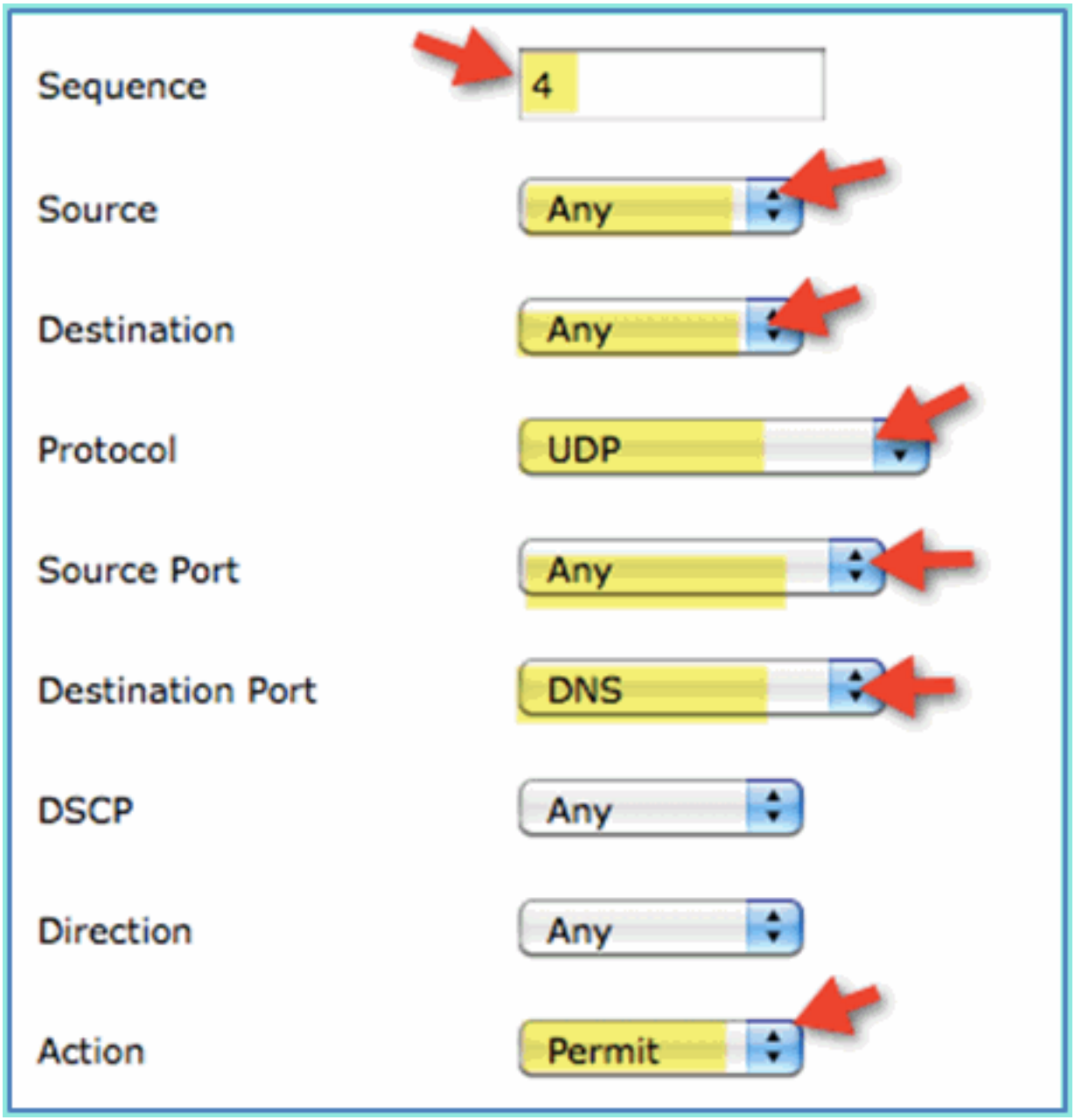
Autorizza

8. La sequenza di conferma è stata aggiunta.

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	0.0.0.0 / 0.0.0.0	10.10.10.70 / 255.255.255.255	Any	Any	Any	Any	Any
2	Permit	10.10.10.70 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any
3	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any

9. Fare clic su **Aggiungi nuova regola**. Impostare i seguenti valori sulla sequenza ACL n. 4. Al

termine, fare clic su **Apply** (Applica).Fonte: AnyDestinazione: QualsiasiProtocollo: UDPPorta di origine: qualsiasiPorta di destinazione: DNSAzione: Autorizza



10. La sequenza di conferma è stata aggiunta.

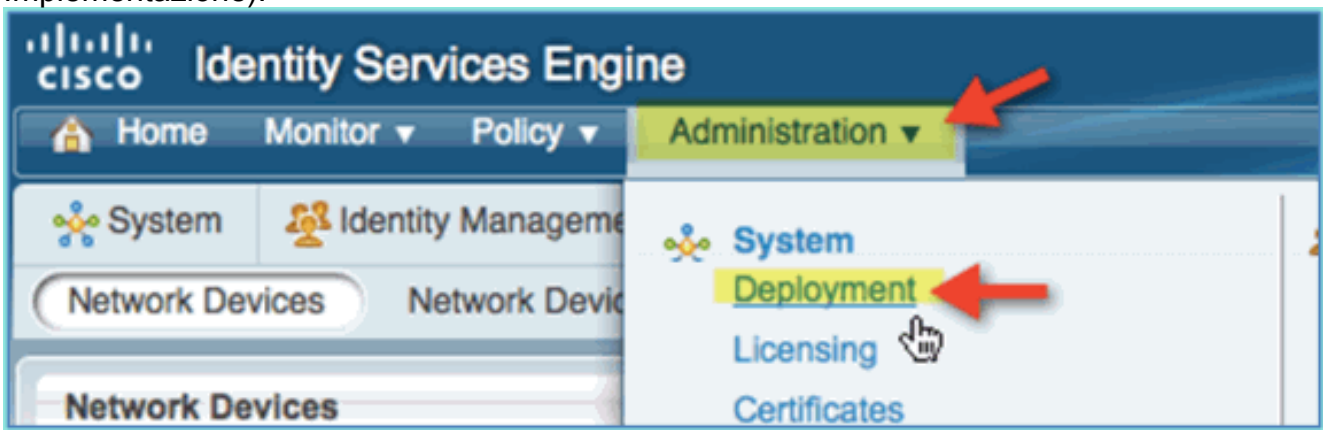
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	0.0.0.0 / 0.0.0.0	10.10.10.70 / 255.255.255.255	Any	Any	Any	Any	Any
2	Permit	10.10.10.70 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any
3	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any
4	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any

11. Salvare la configurazione WLC corrente.

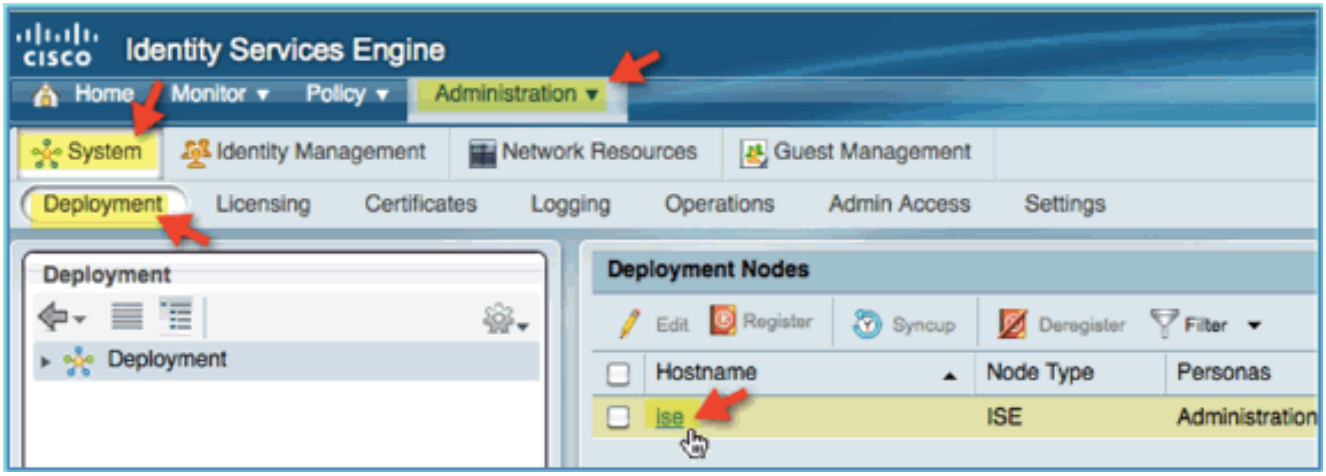
Abilitazione delle sonde di profilatura su ISE

L'ISE deve essere configurato come sonde per profilare in modo efficace gli endpoint. Per impostazione predefinita, queste opzioni sono disattivate. Questa sezione illustra come configurare ISE come sonde.

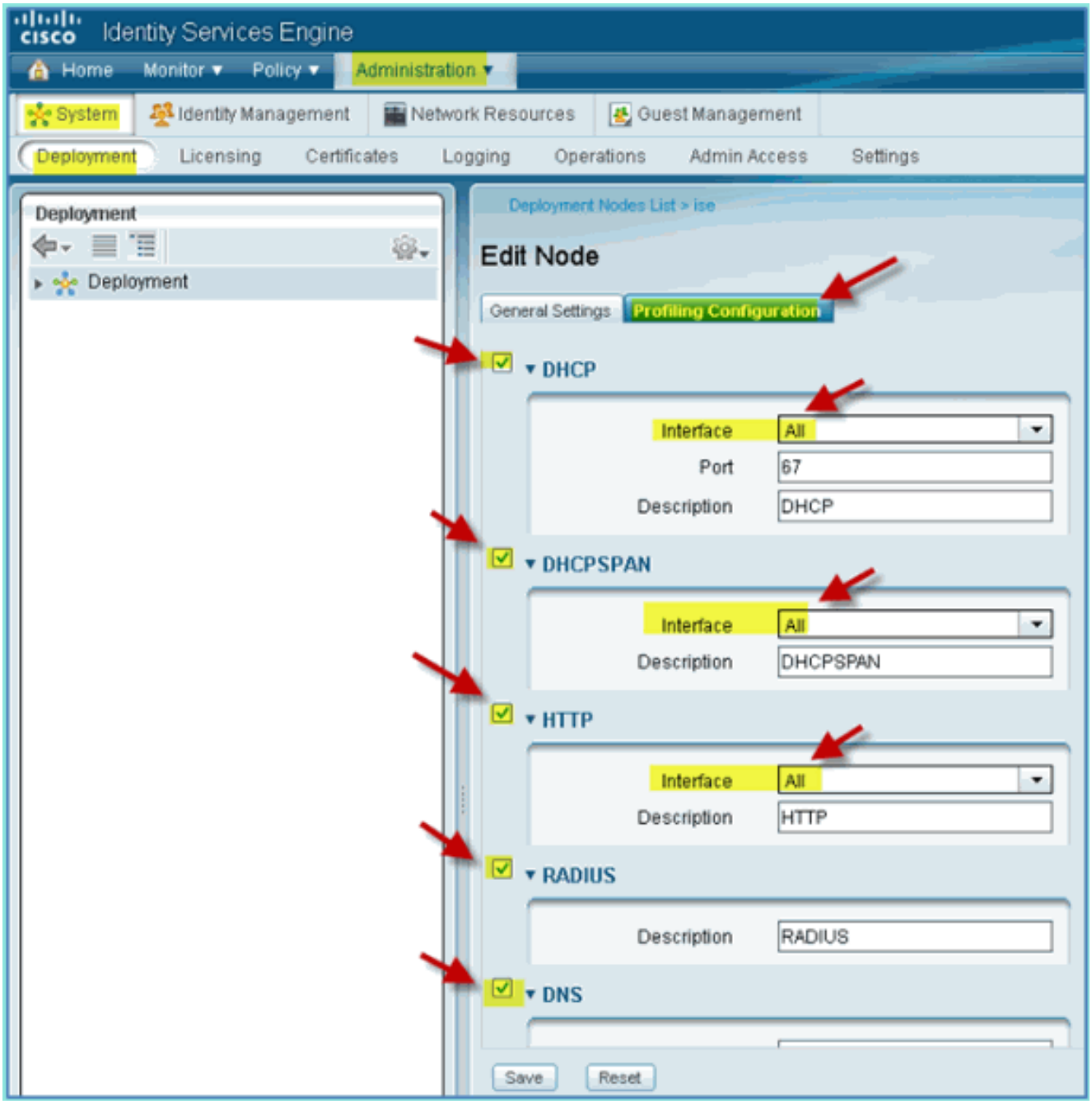
1. Da ISE management, selezionare **Administration > System > Deployment** (Amministrazione > Sistema > Implementazione).



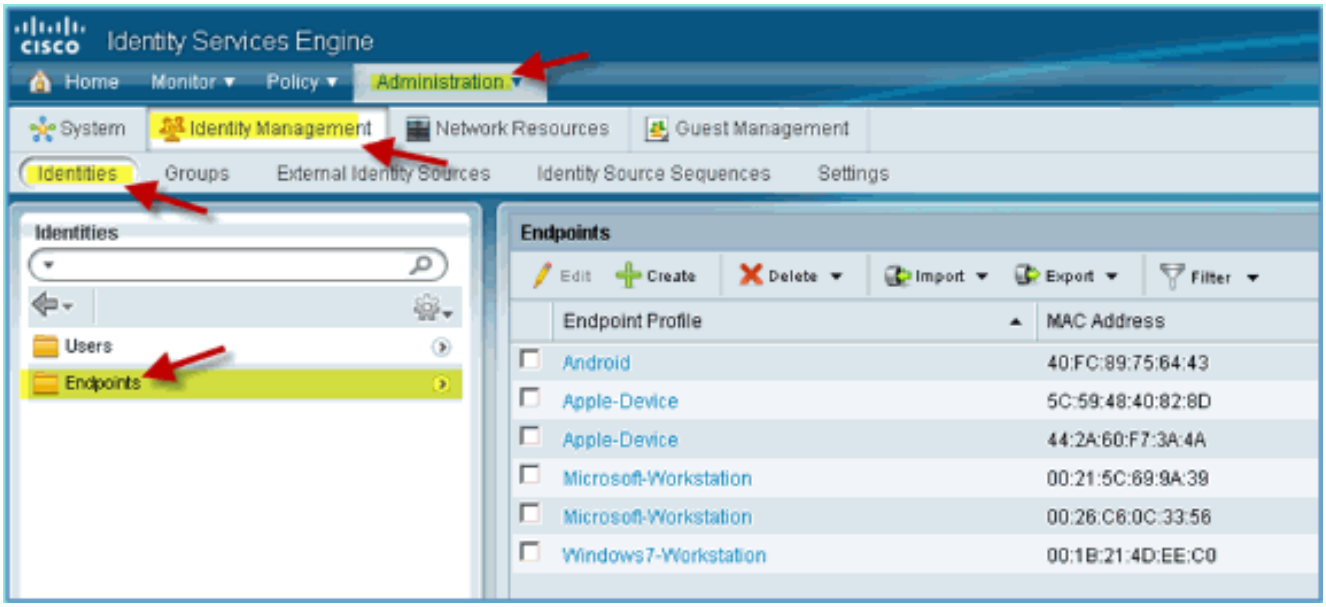
2. Scegliere **ISE**. Fare clic su **Edit ISE host**.



3. Nella pagina Modifica nodo, selezionare Configurazione profilatura e configurare quanto segue:DHCP: Enabled, All (abilitato, tutti) (predefinito)DHCPSPAN: Attivato, Tutto (o predefinito)HTTP: Attivato, Tutto (o predefinito)RADIUS: attivato, N/DDNS: abilitato, N/D



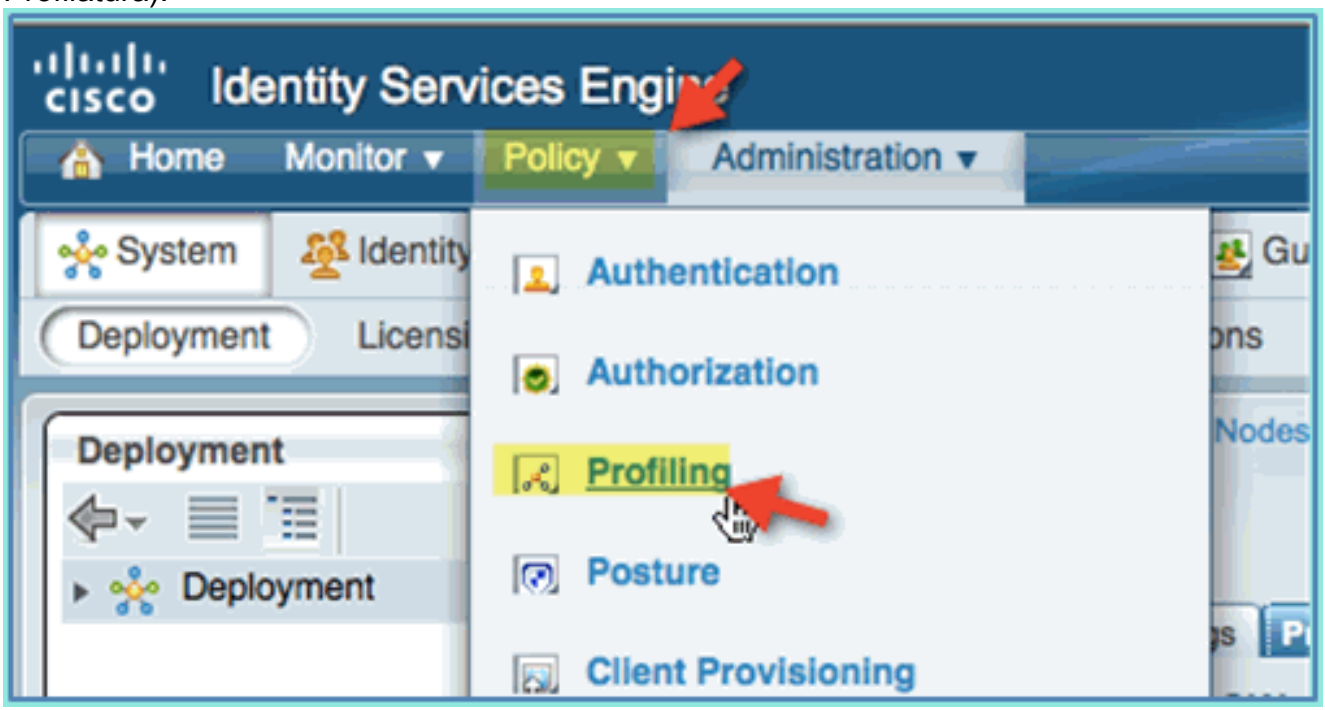
4. Riassociare i dispositivi (iPhone/iPads/Droids/Mac, ecc.).
5. Confermare le identità degli endpoint ISE. Passare a **Amministrazione > Gestione delle identità > Identità**. Fare clic su Endpoint per elencare i profili.**Nota:** la profilatura iniziale viene eseguita da sonde
   RADIUS.



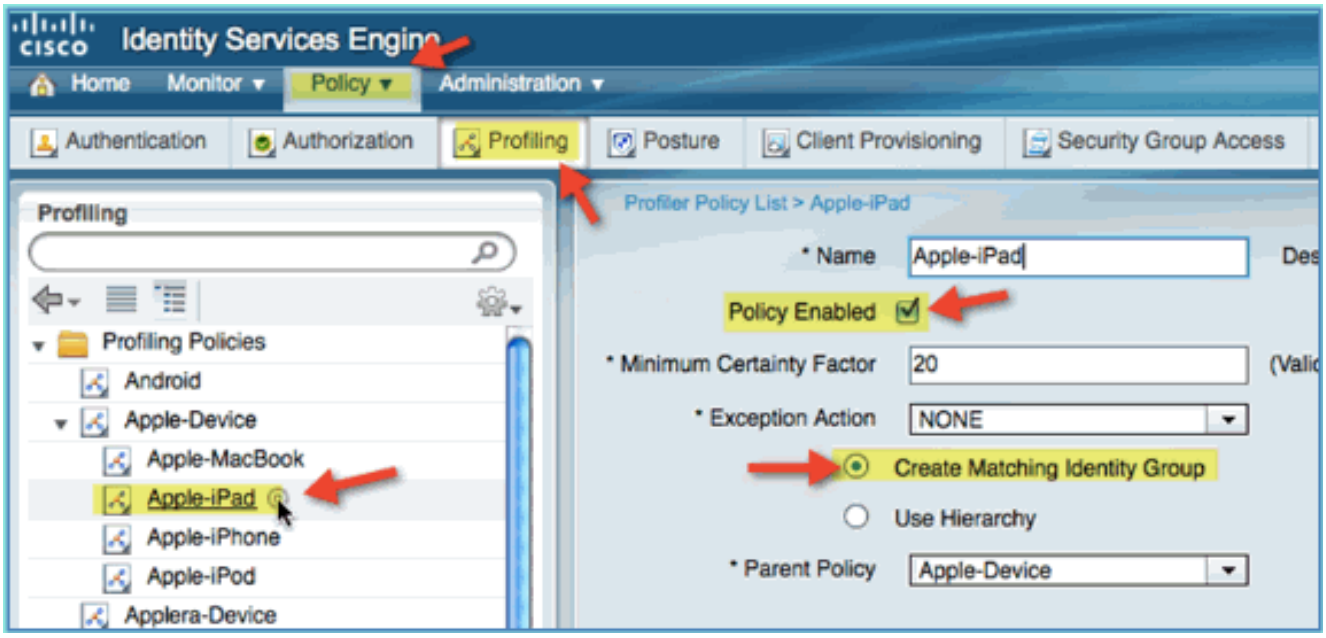
Abilita ISE Profile Policies for Devices

ISE offre una libreria di vari profili di endpoint. Completare questi passaggi per abilitare i profili per i dispositivi:

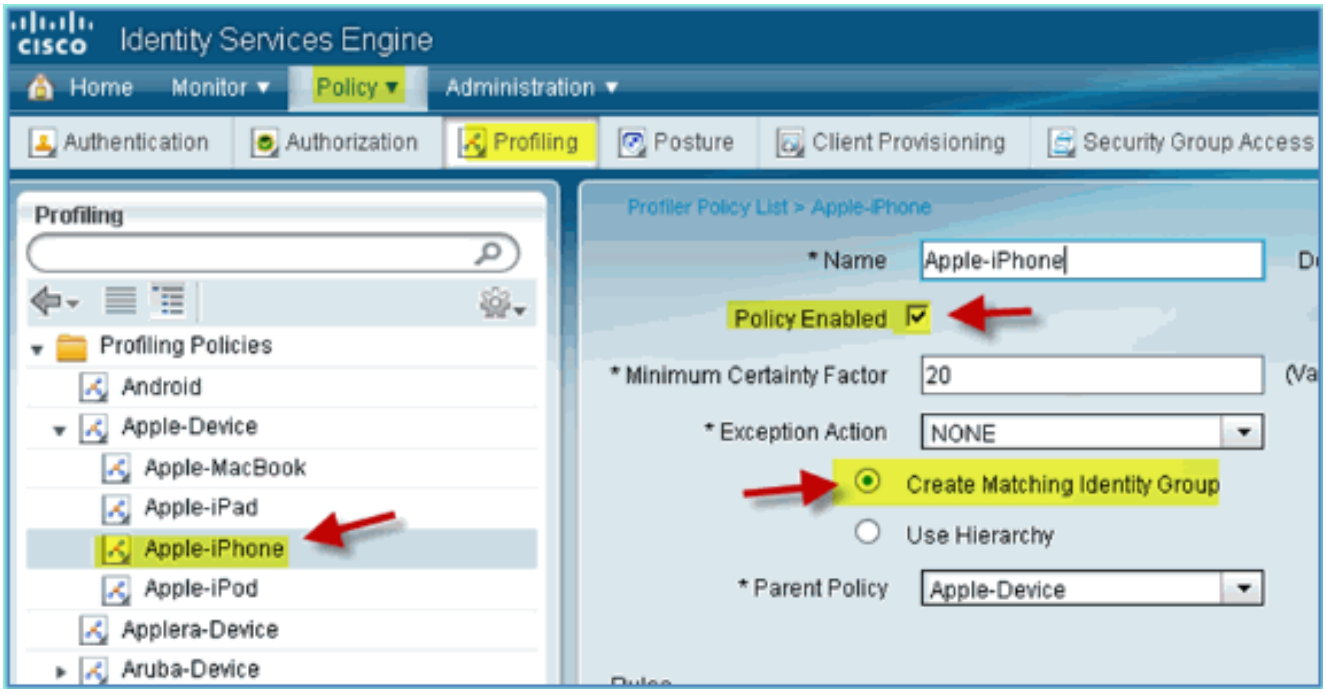
1. Da ISE, selezionare **Policy > Profiling** (Policy > Profilatura).



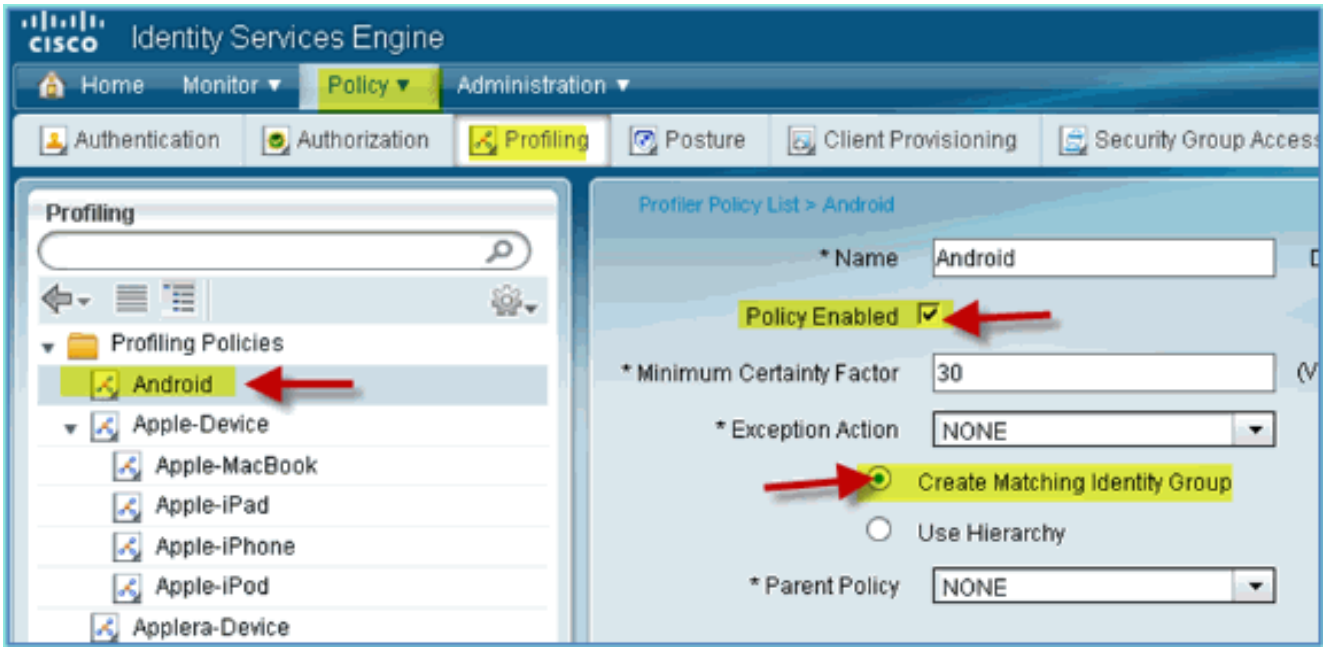
2. Nel riquadro di sinistra espandere **Criteri di profilatura**.
3. Fare clic su **Apple Device > Apple iPad** e impostare quanto segue:Criterio abilitato: AbilitatoCrea gruppo di identità corrispondente: selezionato



4. Fare clic su **Apple Device > Apple iPhone**, impostare quanto segue:Criterio abilitato: AbilitatoCrea gruppo di identità corrispondente:
selezionato



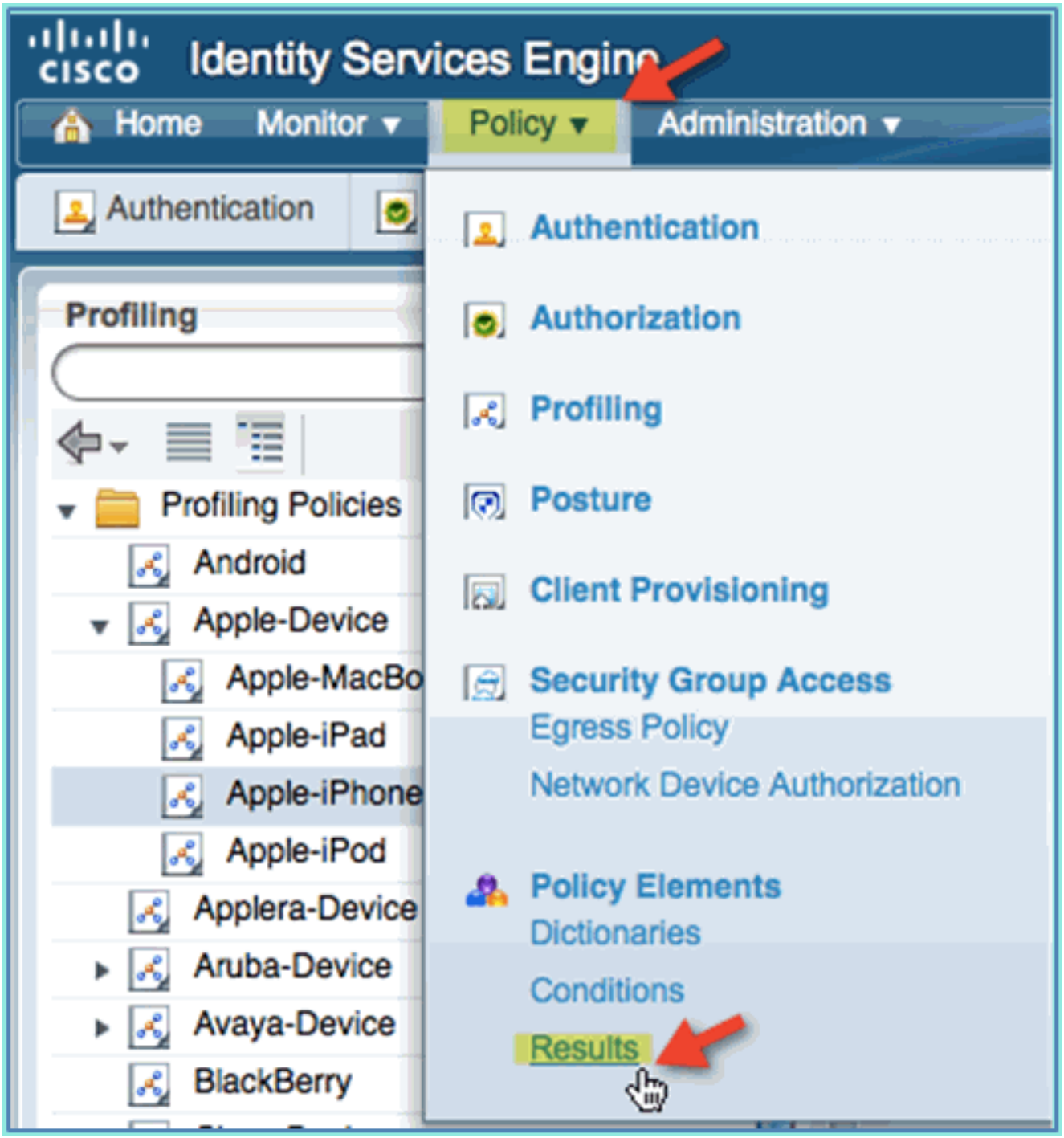
5. Fare clic su **Android**, impostare quanto segue:Criterio abilitato: AbilitatoCrea gruppo di identità corrispondente:
selezionato



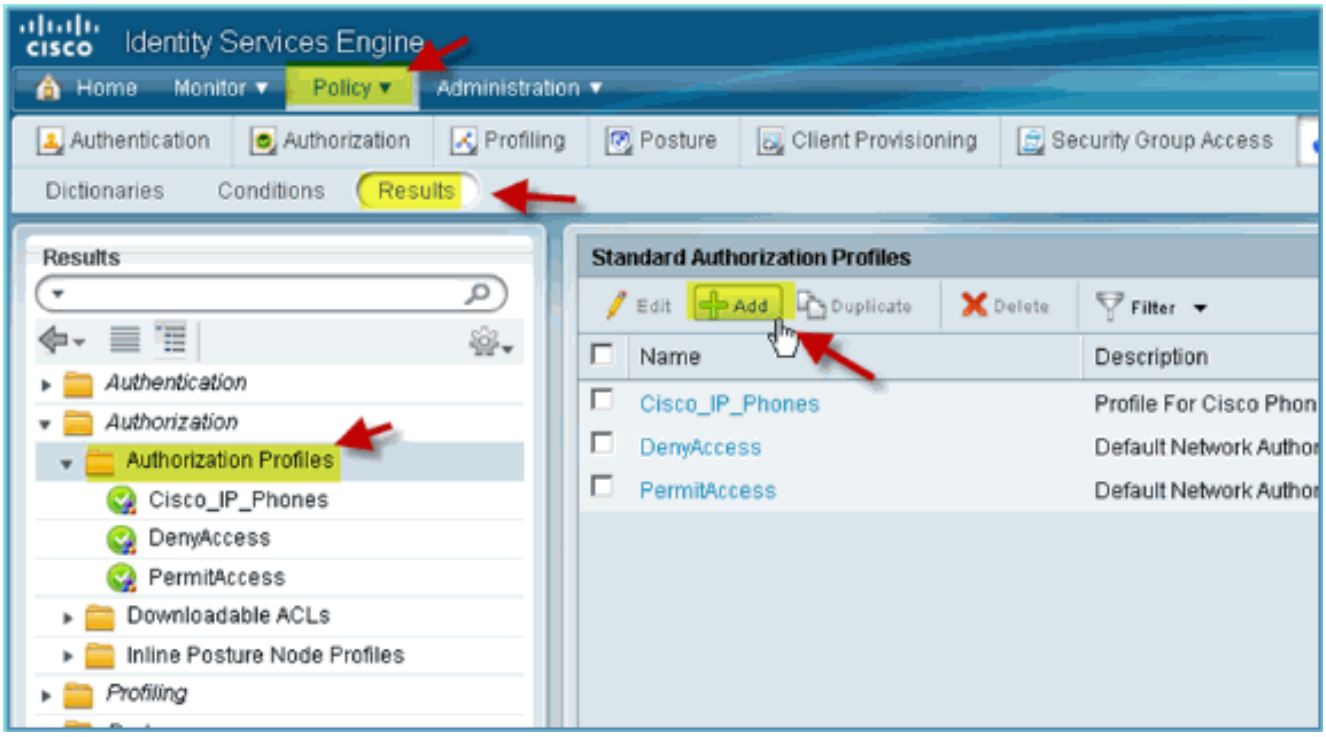
Profilo di autorizzazione ISE per Posture Discovery Redirect

Completare questa procedura per configurare un reindirizzamento della postura dei criteri di autorizzazione che consenta il reindirizzamento di nuovi dispositivi all'ISE per il rilevamento e la profilatura corretti:

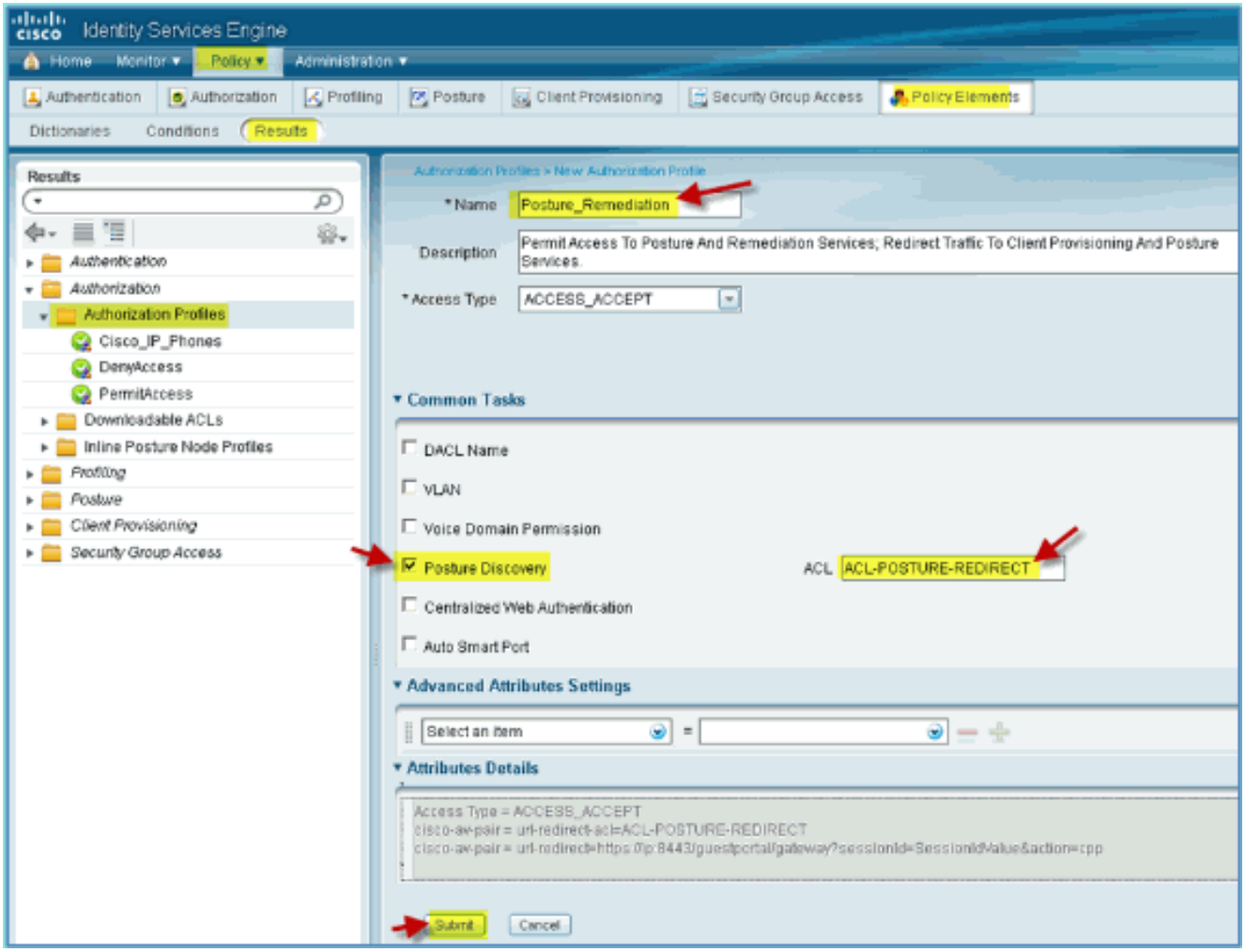
1. Da ISE, selezionare **Policy > Policy Elements > Results** (Policy > Elementi della policy > Risultati).



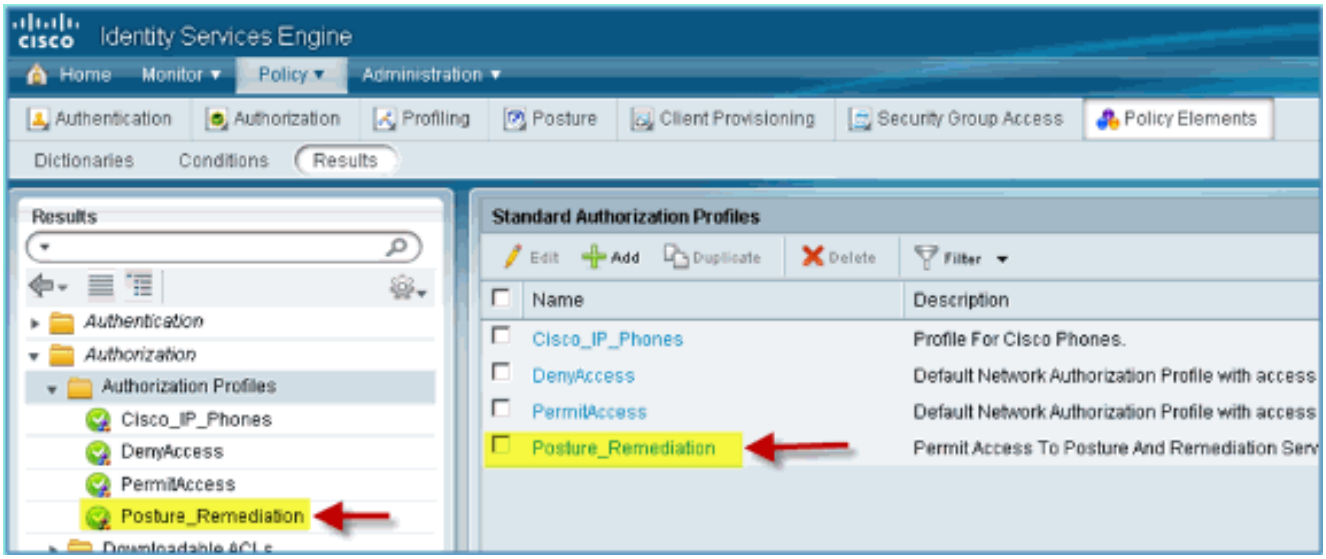
2. Espandere **Autorizzazione**. Fare clic su **Profili di autorizzazione** (riquadro sinistro) e fare clic su
Aggiungi.



3. Creare il profilo di autorizzazione con:Nome: Posture_RemediationTipo di accesso: Access_AcceptStrumenti comuni:Rilevamento postura, abilitatoRilevamento postura, ACL-POSTURE-
REDIRECT



4. Fare clic su **Invia** per completare l'attività.
5. Confermare l'aggiunta del nuovo profilo di autorizzazione.

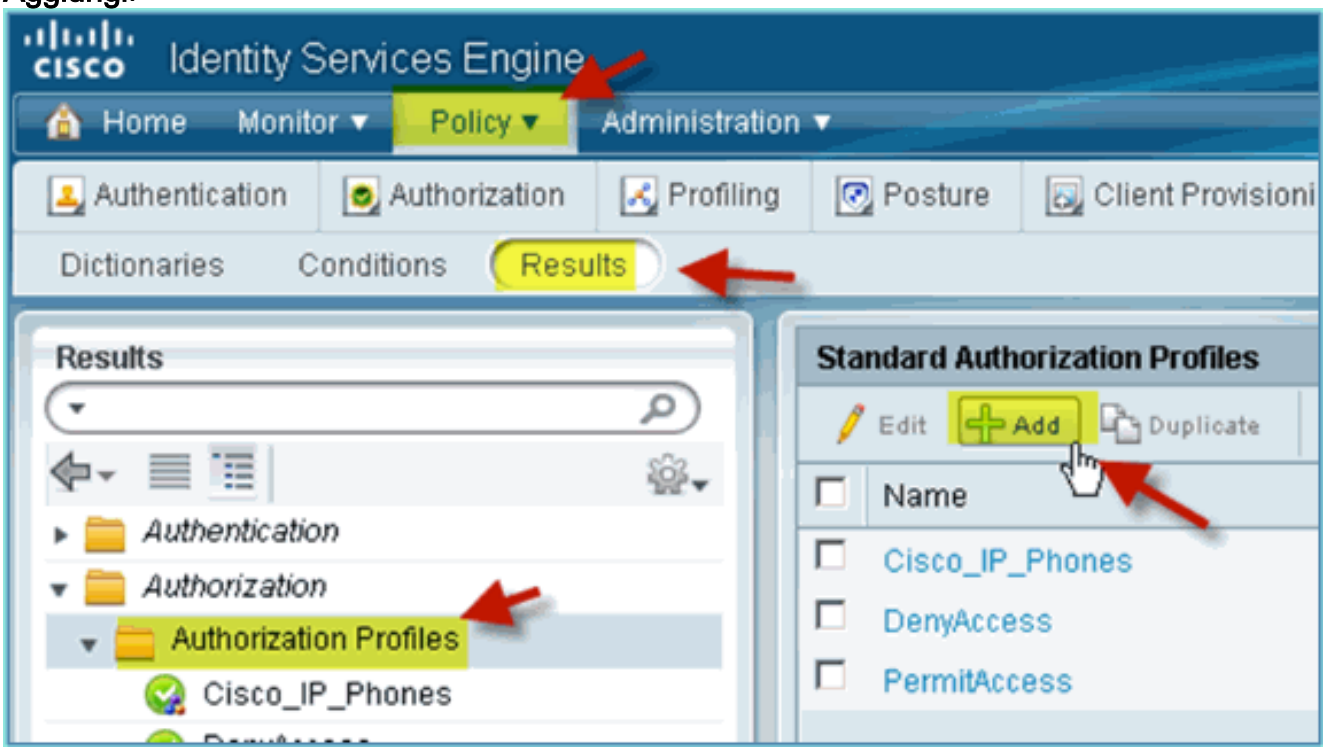


Crea profilo di autorizzazione ISE per dipendente

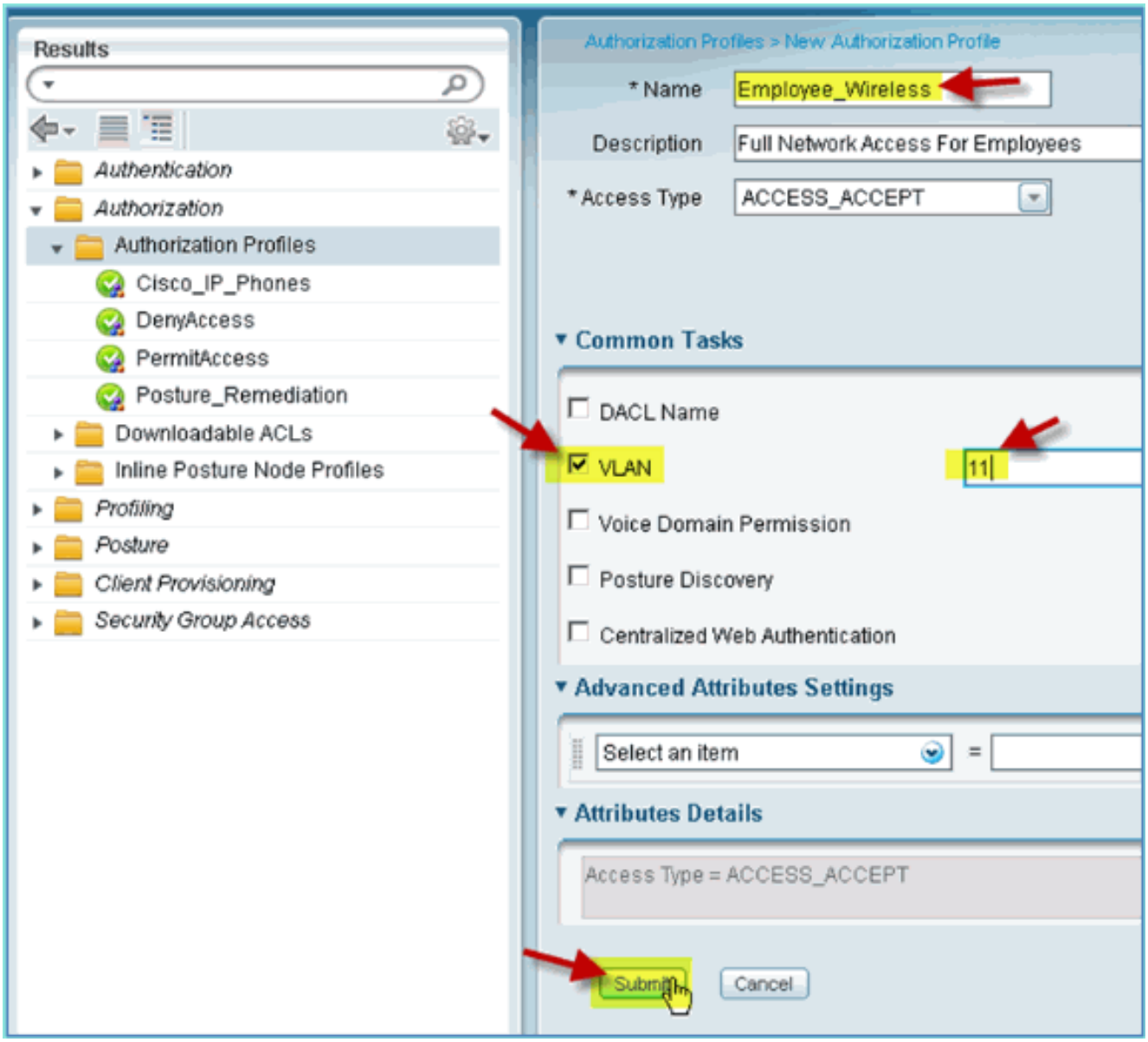
L'aggiunta di un profilo di autorizzazione per un dipendente consente ad ISE di autorizzare e permettere l'accesso con gli attributi assegnati. In questo caso, viene assegnata la VLAN 11 del dipendente.

Attenersi alla seguente procedura:

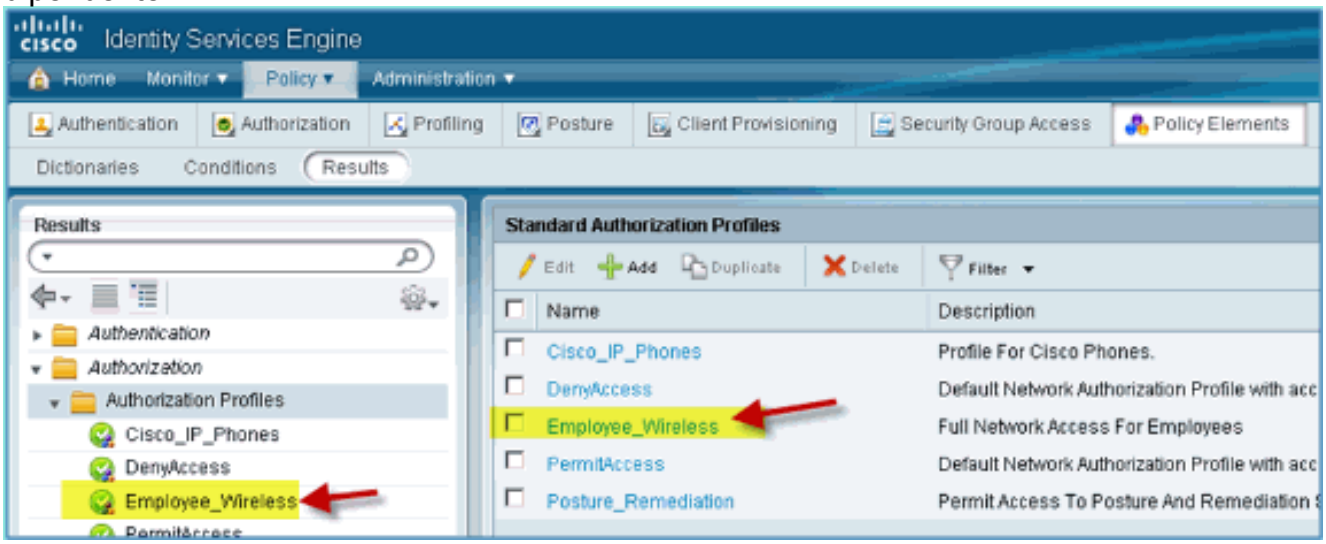
1. Da ISE, selezionare **Policy > Results** (Policy > Risultati). Espandere **Autorizzazione**, quindi fare clic su **Profili di autorizzazione** e fare clic su **Aggiungi**.



2. Immettere quanto segue per il profilo di autorizzazione dipendente:Nome: Employee_WirelessAttività comuni:VLAN, abilitataVLAN, valore secondario 11
3. Fare clic su **Invia** per completare l'attività.



4. Confermare la creazione del nuovo profilo di autorizzazione dipendente.



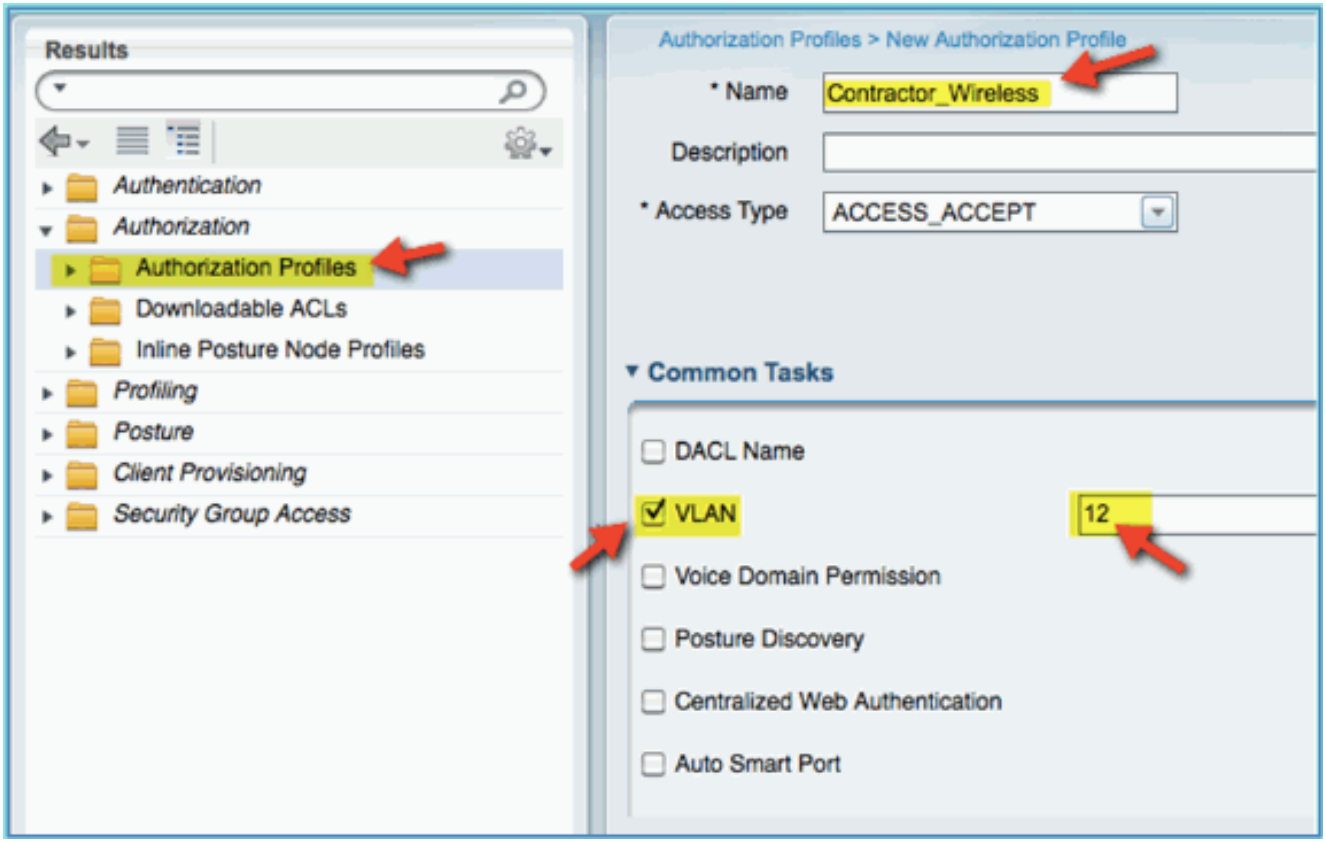
Crea profilo di autorizzazione ISE per collaboratore esterno

L'aggiunta di un profilo di autorizzazione per un collaboratore esterno consente ad ISE di autorizzare e permettere l'accesso con gli attributi assegnati. In questo caso, è assegnata la VLAN

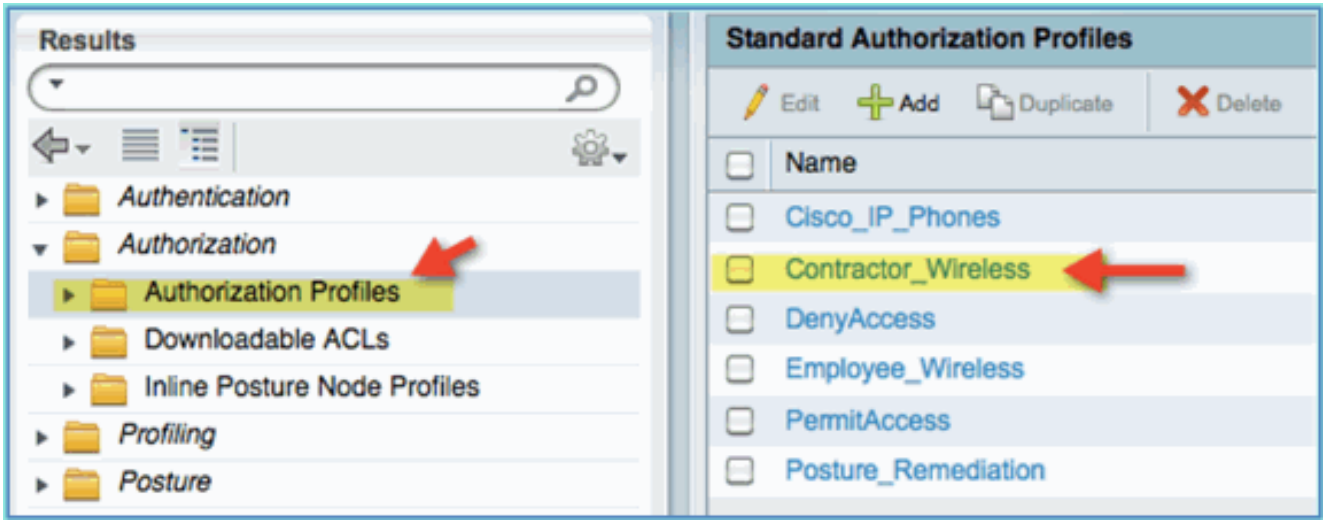
12 del terzista.

Attenersi alla seguente procedura:

1. Da ISE, selezionare **Policy > Results** (Policy > Risultati). Espandere **Autorizzazione**, quindi fare clic su **Profili di autorizzazione** e fare clic su **Aggiungi**.
2. Immettere quanto segue per il profilo di autorizzazione dipendente:Nome: Employee_WirelessAttività comuni:VLAN, abilitataVLAN, valore secondario 12



3. Fare clic su **Invia** per completare l'attività.
4. Confermare la creazione del profilo di autorizzazione collaboratore esterno.



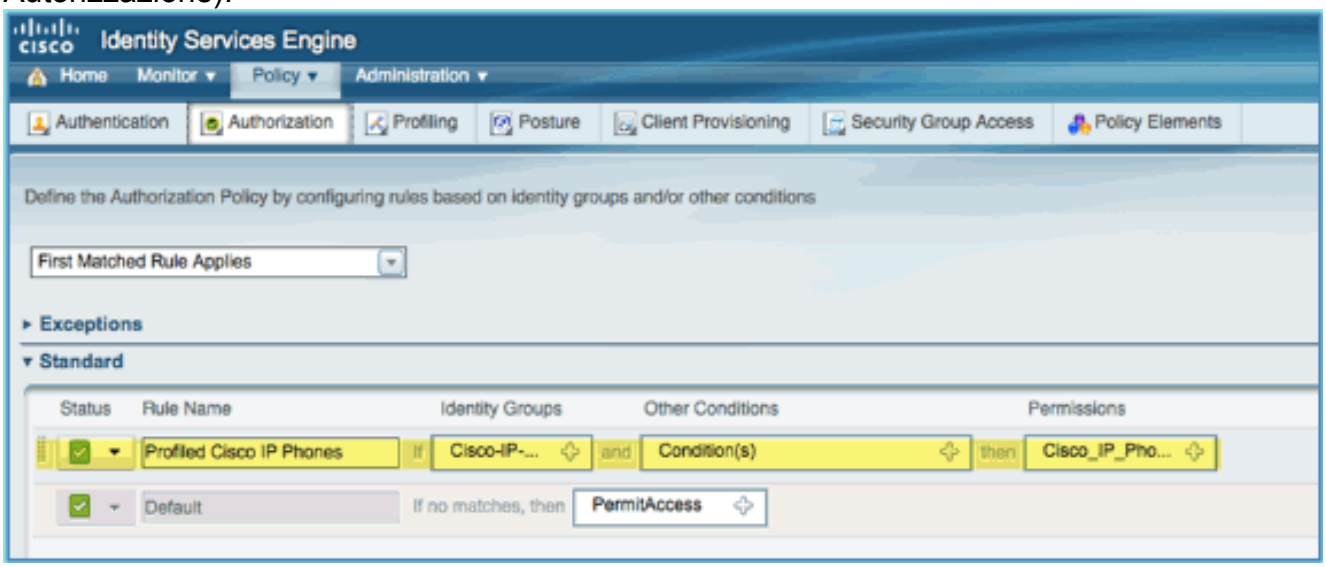
Criteri di autorizzazione per postura/profilatura dispositivo

Quando un nuovo dispositivo viene connesso alla rete per la prima volta, si conoscono poche

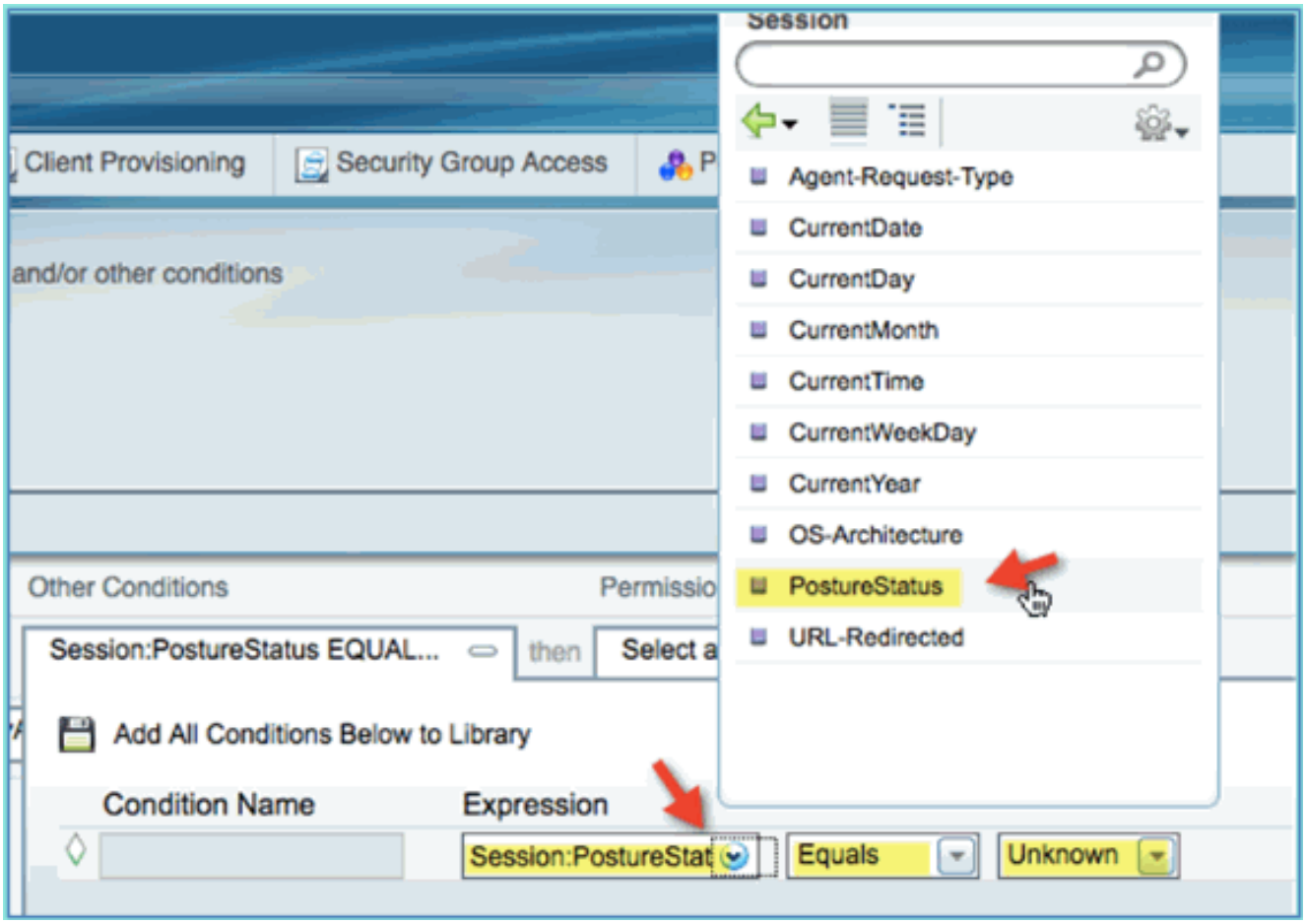
informazioni. L'amministratore creerà i criteri appropriati per consentire l'identificazione degli endpoint sconosciuti prima di concedere l'accesso. In questo esercizio, la policy di autorizzazione verrà creata in modo che un nuovo dispositivo venga reindirizzato all'ISE per la valutazione della postura (per i dispositivi mobili non è necessario l'agente, quindi è importante solo la profilatura); gli endpoint verranno reindirizzati al portale per le risorse ISE e identificati.

Attenersi alla seguente procedura:

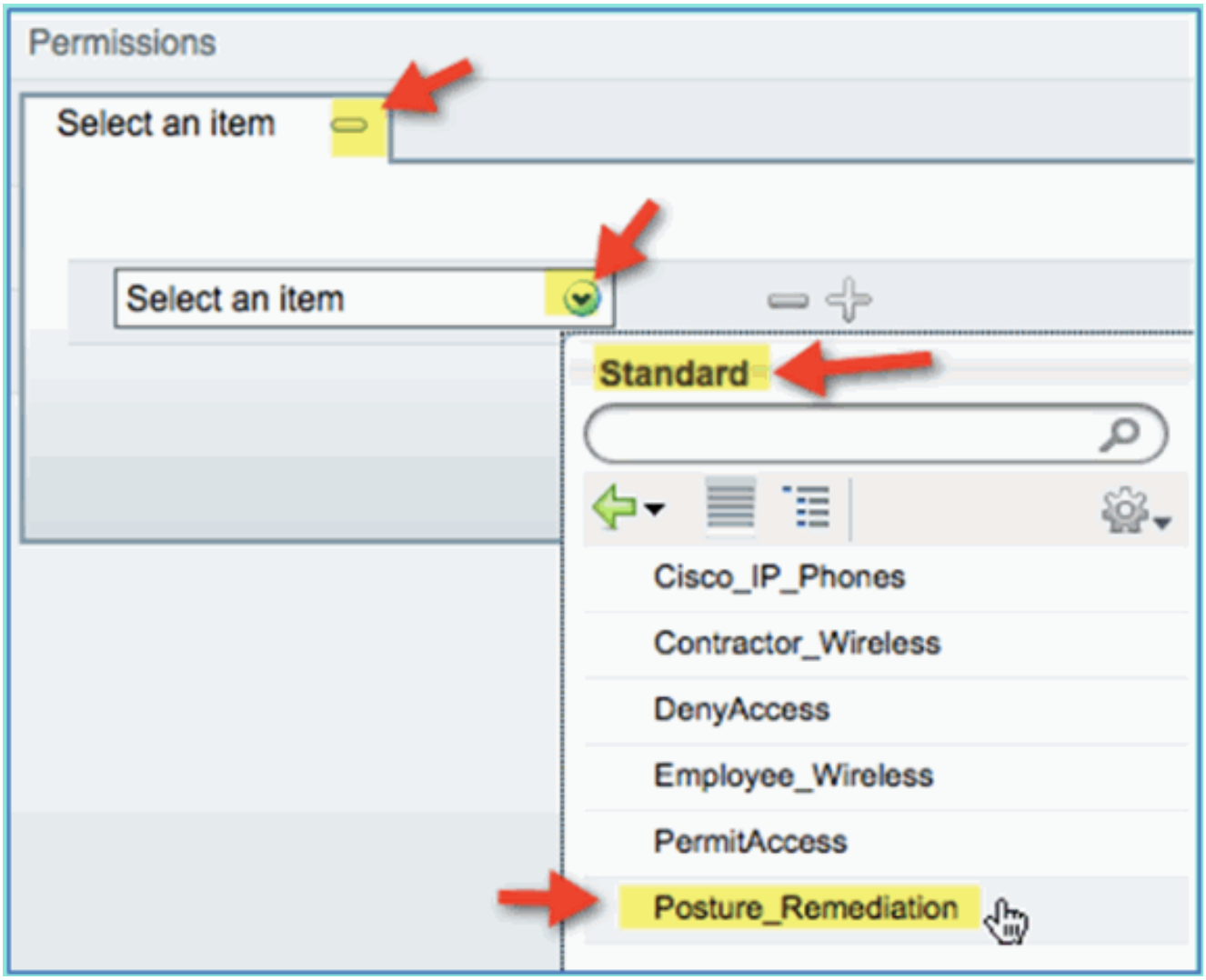
1. Da ISE, selezionare **Policy > Authorization** (Policy > Autorizzazione).



2. Esiste una policy per i telefoni IP Cisco con profilo. Questo è fuori dagli schemi. Modifica come criterio di postura.
3. Immettere i valori seguenti per il criterio:Nome regola: Posture_RemediationGruppi di identità: qualsiasiAltre condizioni > Crea nuovo: Sessione (avanzata) > Stato posturaPostureStatus > Uguale a:
sconosciuto



4. Impostare quanto segue per le autorizzazioni:Autorizzazioni > Standard: Posture_Remediation

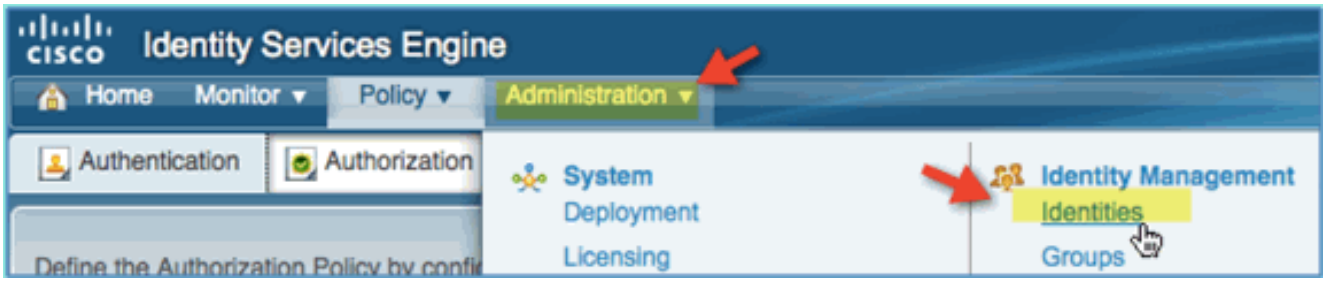


5. Fare clic su **Salva**.**Nota: in** alternativa, è possibile creare elementi di criteri personalizzati per rendere più semplice l'utilizzo.

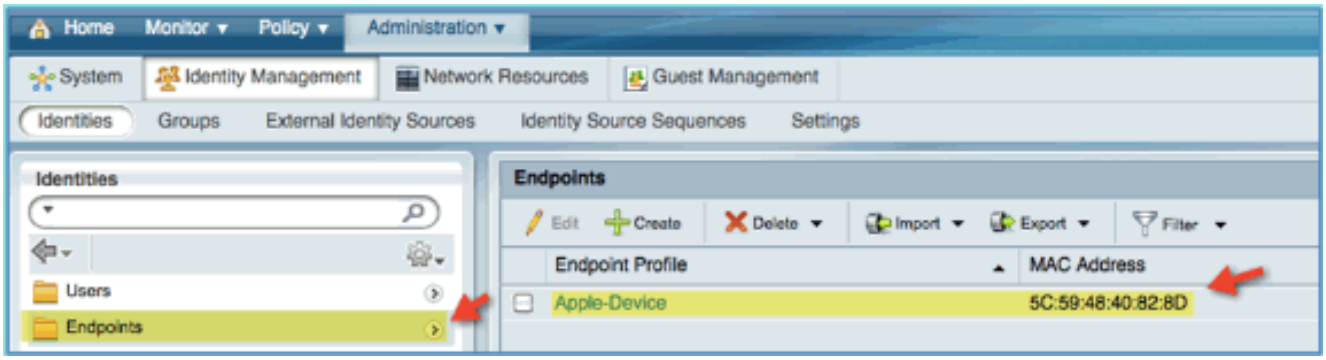
Verifica criteri di correzione postura

Èpossibile eseguire una semplice dimostrazione per dimostrare che ISE sta creando correttamente il profilo di un nuovo dispositivo in base alla policy di postura.

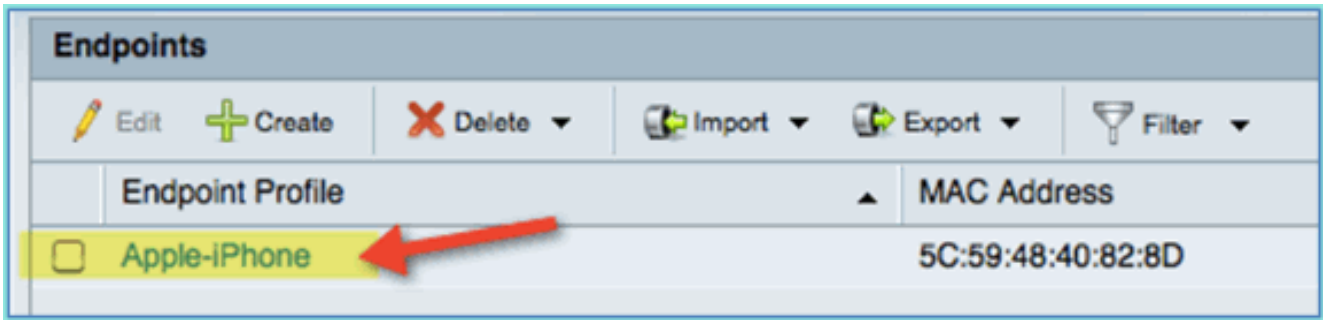
1. Da ISE, selezionare **Amministrazione > Gestione delle identità > Identità**.



2. Fare clic su **Endpoint**. Associare e connettere un dispositivo (un iPhone in questo esempio).



3. Aggiornare l'elenco Endpoints. Osservate quali informazioni vengono fornite.
4. Dal dispositivo endpoint, selezionare:URL: http://www (o 10.10.10.10)Il dispositivo viene reindirizzato. Accettare qualsiasi richiesta di certificati.
5. Dopo il reindirizzamento completo del dispositivo mobile, da ISE aggiornare di nuovo l'elenco Endpoints. Osservate cosa è cambiato. L'endpoint precedente (ad esempio, Apple-Device) avrebbe dovuto essere modificato in 'Apple-iPhone'ecc. Il motivo è che il probe HTTP ottiene in modo efficace informazioni sull'agente utente, come parte del processo di reindirizzamento al portale
vincolato.

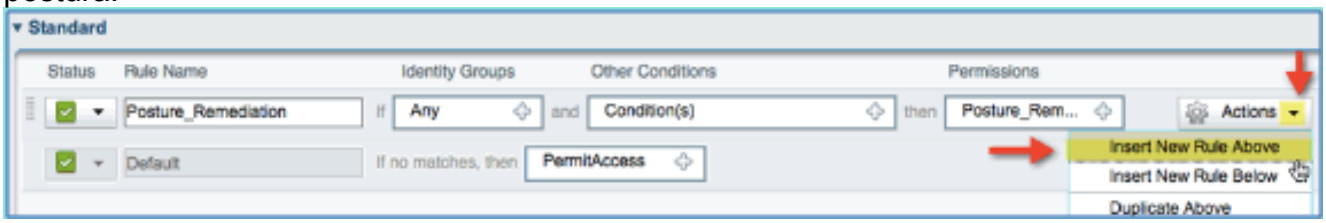


Criteri di autorizzazione per l'accesso differenziato

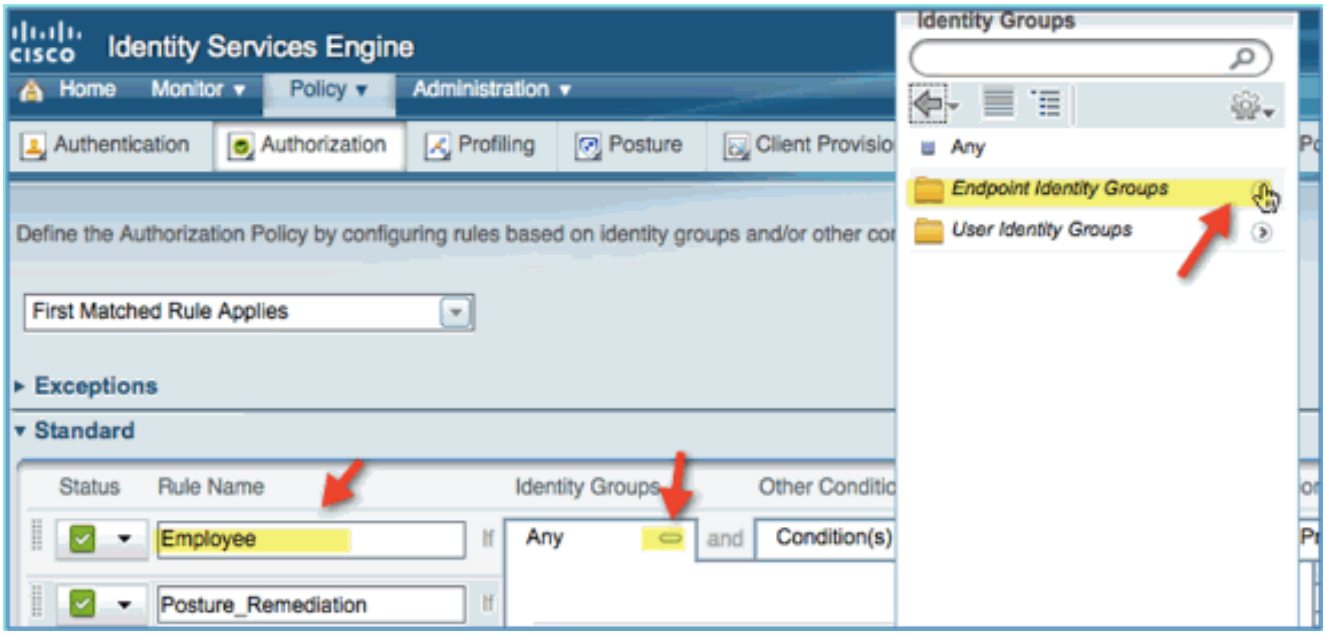
Dopo aver verificato correttamente l'autorizzazione della postura, continuare a creare policy per supportare l'accesso differenziato per il dipendente e il terzista con dispositivi noti e diverse assegnazioni VLAN specifiche per il ruolo utente (in questo scenario, dipendente e terzista).

Attenersi alla seguente procedura:

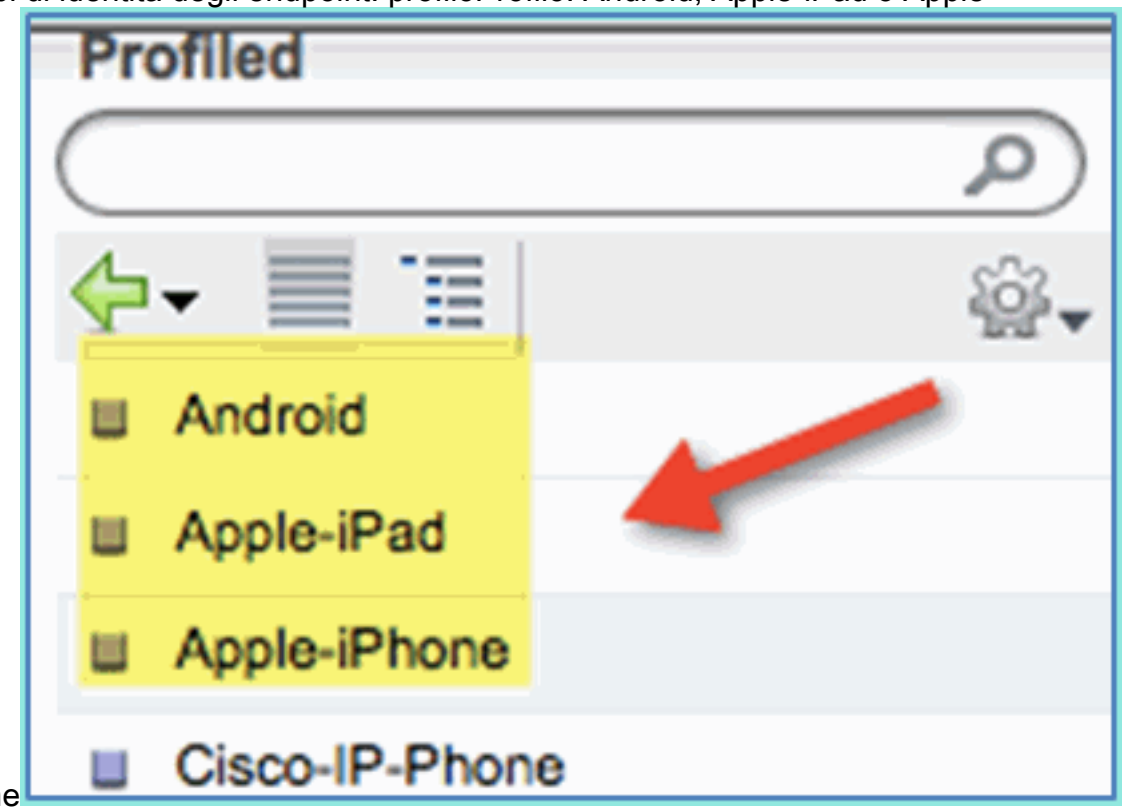
1. Selezionare **ISE > Policy > Authorization**.
2. Aggiunge/inserisce una nuova regola sopra la riga/il criterio di correzione della postura.



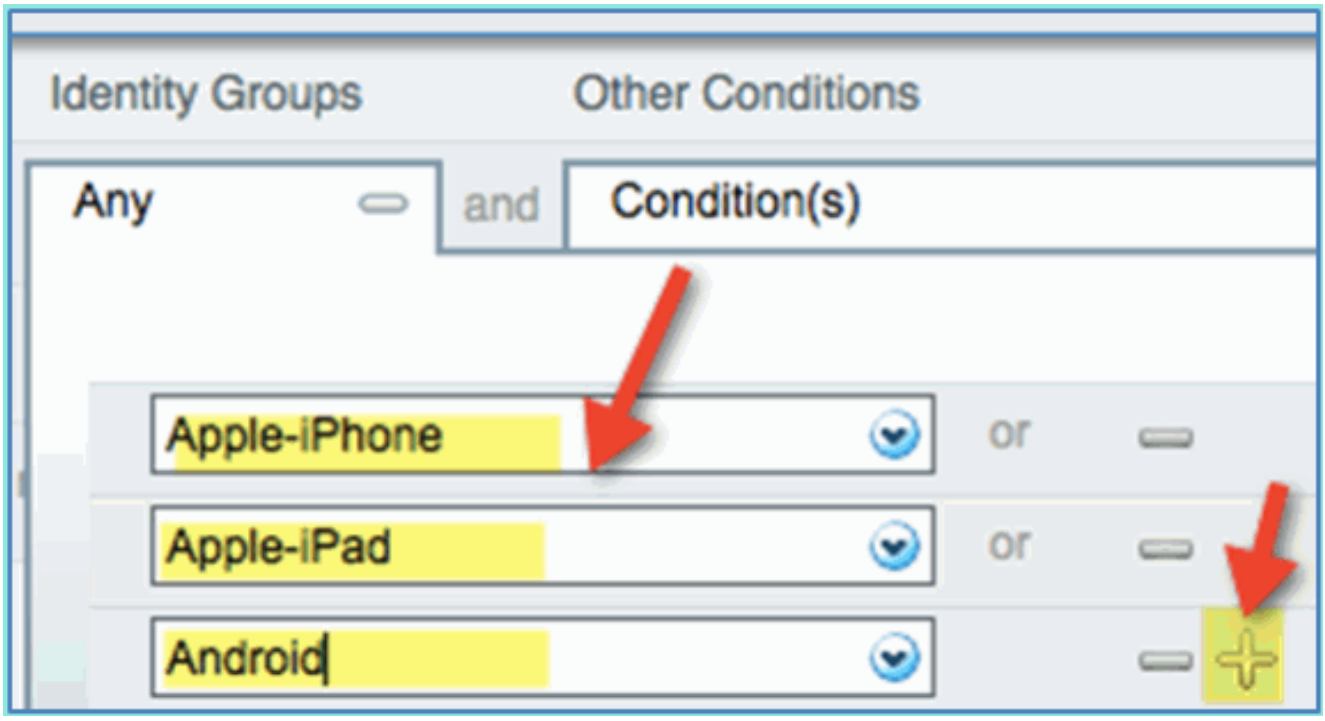
3. Immettere i valori seguenti per il criterio:Nome regola: dipendenteGruppi di identità (espandere): Gruppi di identità degli
endpoint



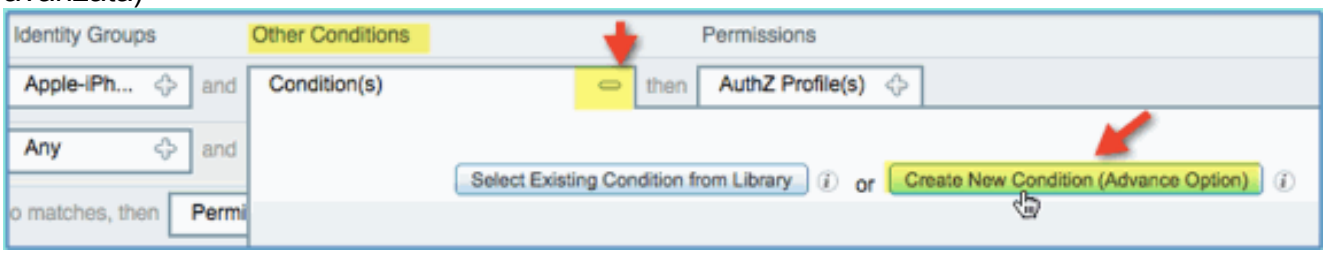
Gruppi di identità degli endpoint: profiloProfilo: Android, Apple-iPad o Apple-iPhone



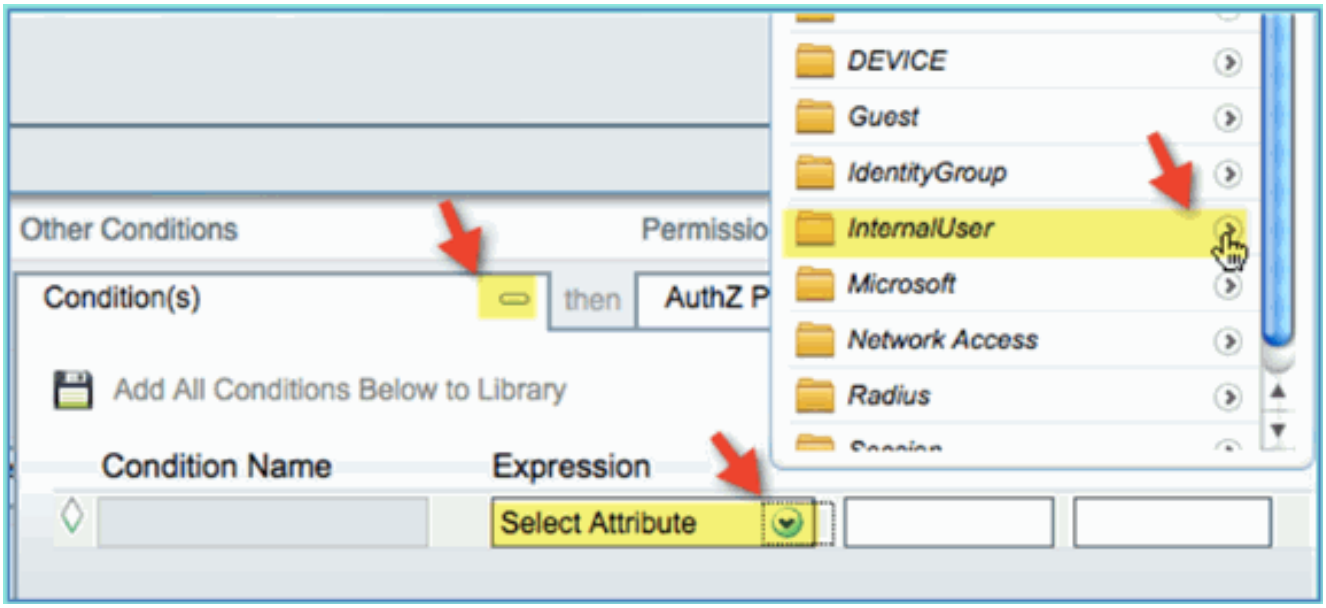
4. Per specificare altri tipi di dispositivi, fare clic sul segno **+** e aggiungere altri dispositivi (se necessario):Gruppi di identità degli endpoint: profiloProfilo: Android, Apple-iPad o Apple-iPhone



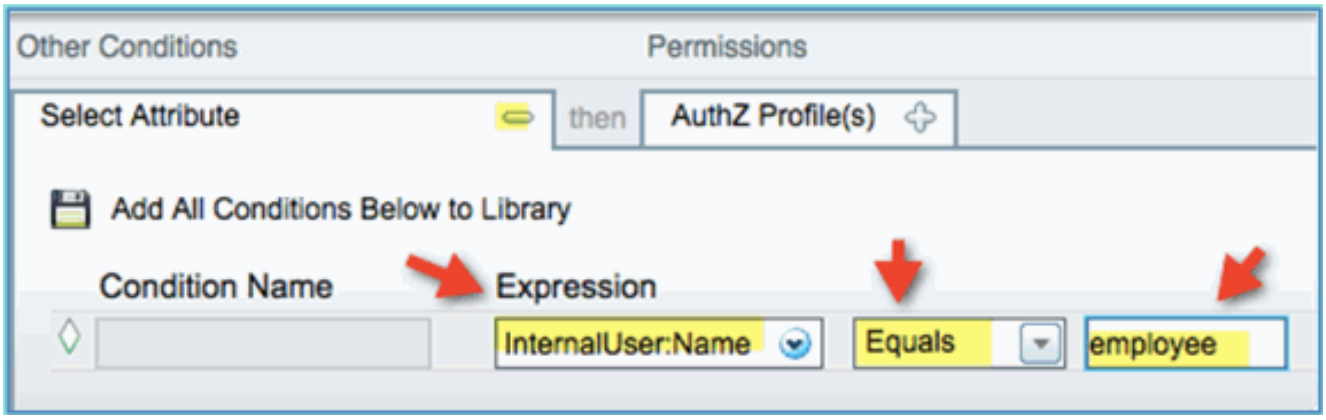
5. Specificare i valori di Autorizzazioni seguenti per il criterio:Altre condizioni (espandere): Crea nuova condizione (opzione avanzata)



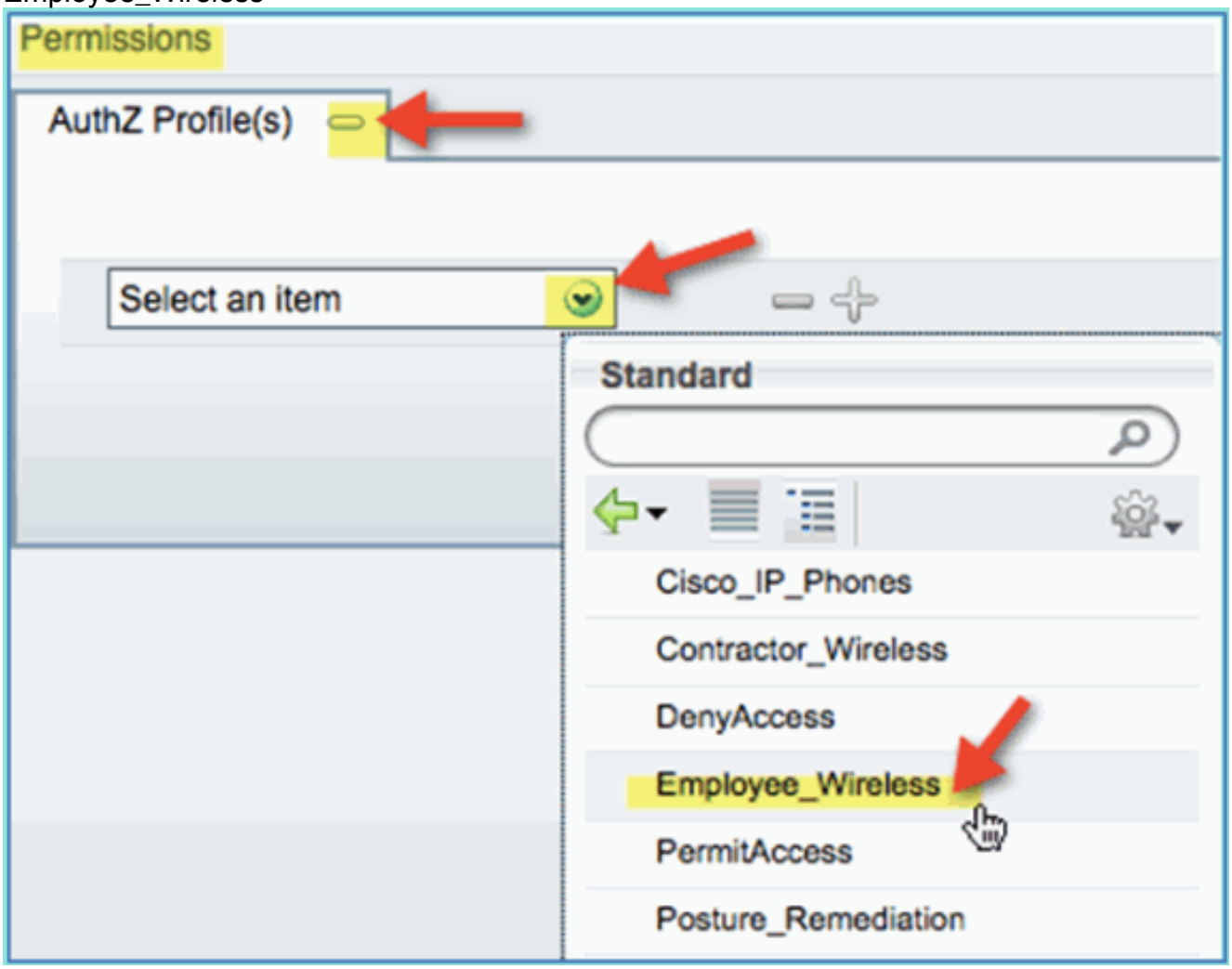
Condizione > Espressione (dall'elenco): InternalUser > Nome



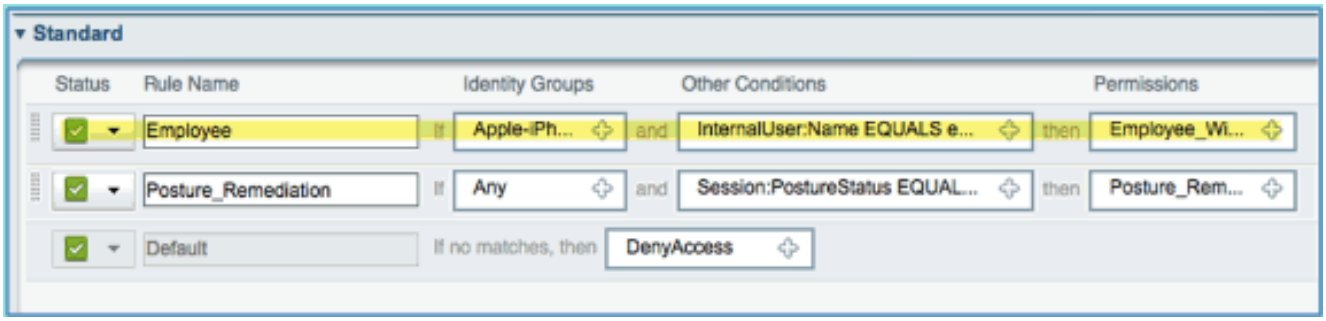
InternalUser > Nome: dipendente



6. Aggiungere una condizione per la sessione di postura conforme:Autorizzazioni > Profili > Standard:
   Employee_Wireless

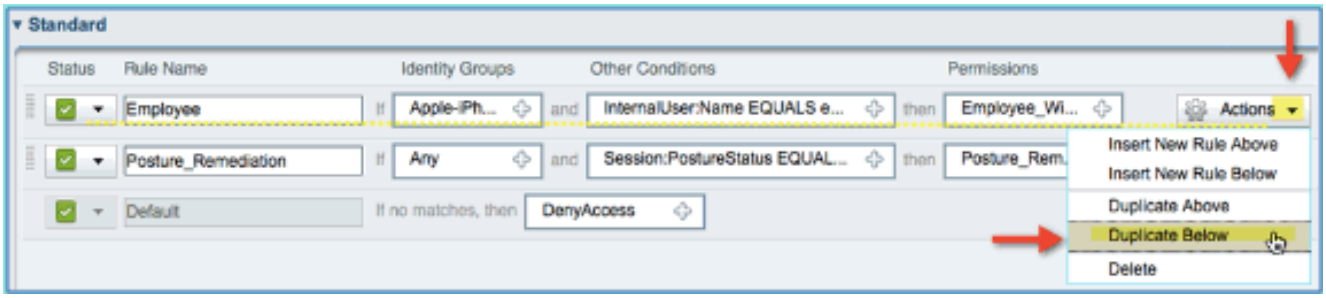


7. Fare clic su **Salva**. Confermare che il criterio è stato aggiunto correttamente.

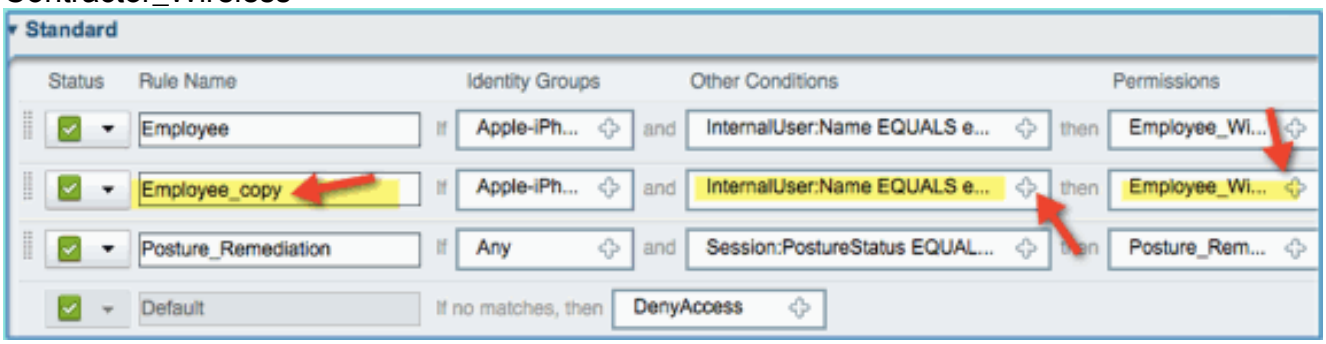


8. Continuare aggiungendo il criterio Terzista. In questo documento, i criteri precedenti vengono

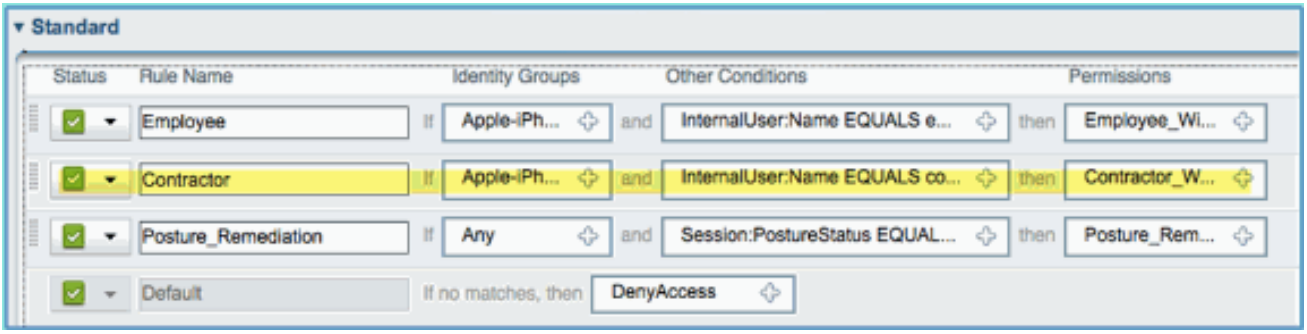
duplicati per velocizzare il processo (oppure è possibile configurarli manualmente per ottenere risultati ottimali).Da Politica dipendente > Azioni, fare clic su **Duplica sotto**.



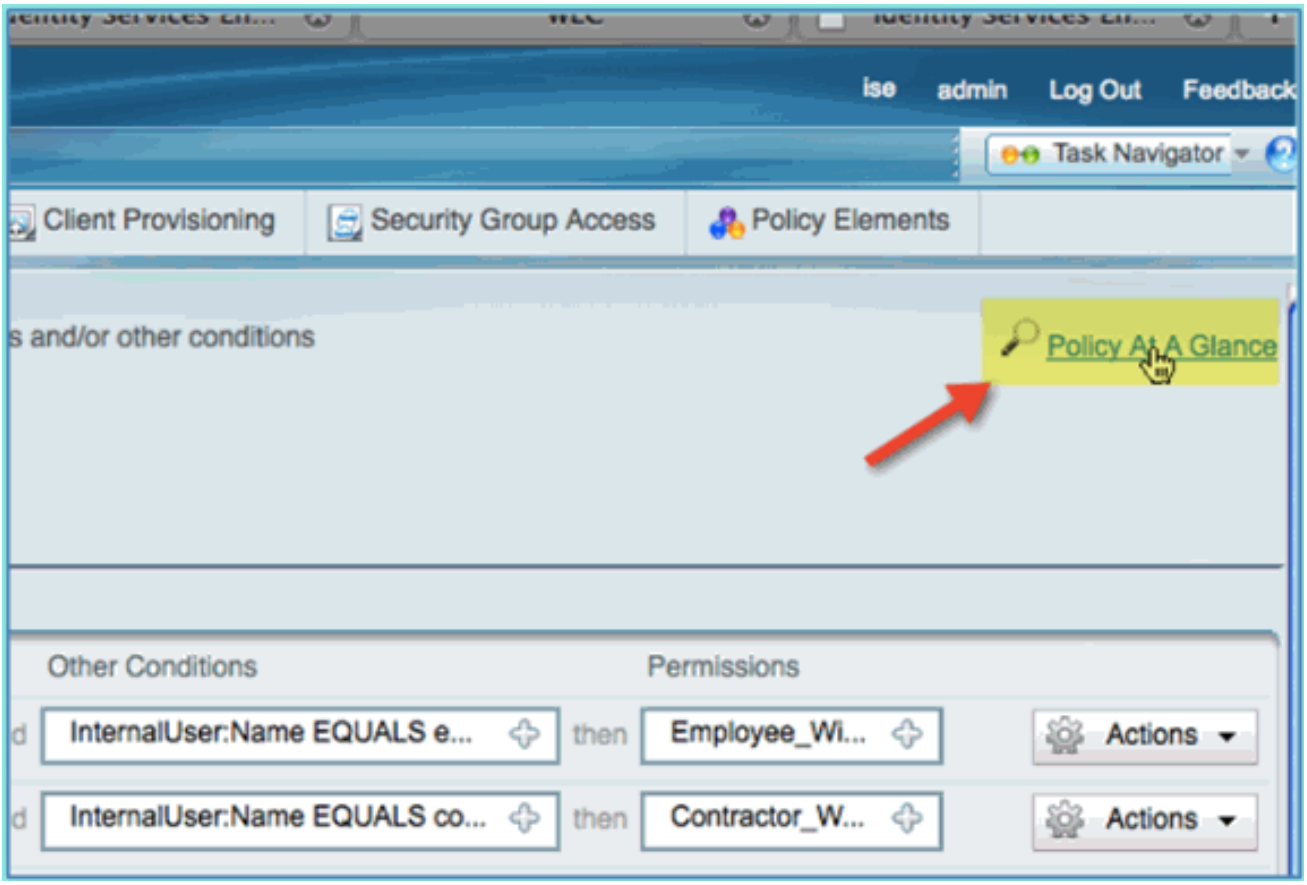
9. Modifica i campi seguenti per questo criterio (copia duplicata):Nome regola: terzistaAltre condizioni > Utente interno > Nome: terzistaAutorizzazioni: Contractor_Wireless



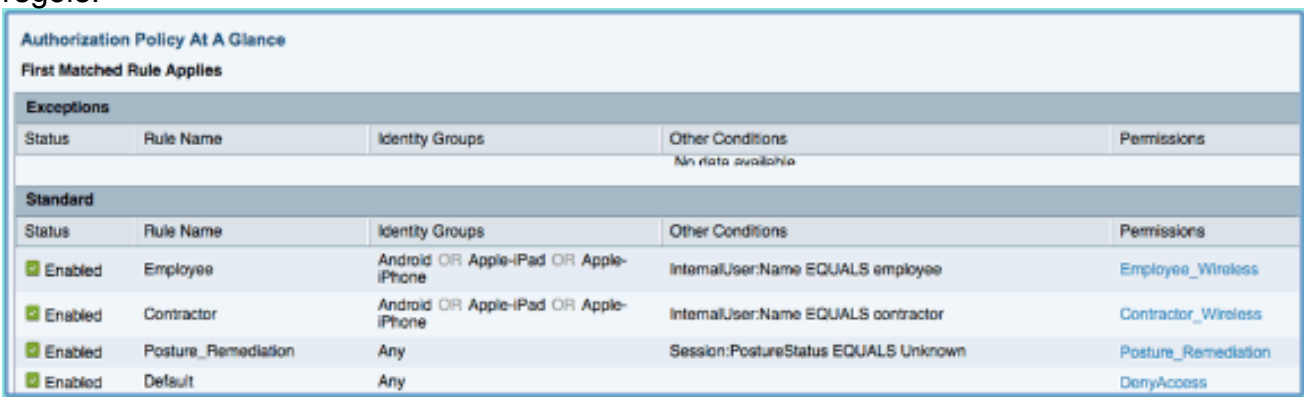
10. Fare clic su **Salva**. Verificare che la copia duplicata precedente (o il nuovo criterio) sia configurata correttamente.



11. Per visualizzare l'anteprima dei criteri, fare clic su **Panoramica dei criteri**.



La visualizzazione Panoramica delle regole fornisce un riepilogo consolidato e una facile visualizzazione delle
regole.



Authorization Policy At A Glance

First Matched Rule Applies

Exceptions

Status	Rule Name	Identity Groups	Other Conditions	Permissions
			No data available	

Standard

Status	Rule Name	Identity Groups	Other Conditions	Permissions
Enabled	Employee	Android OR Apple-iPad OR Apple-iPhone	InternalUser:Name EQUALS employee	Employee_Wireless
Enabled	Contractor	Android OR Apple-iPad OR Apple-iPhone	InternalUser:Name EQUALS contractor	Contractor_Wireless
Enabled	Posture_Remediation	Any	Session:PostureStatus EQUALS Unknown	Posture_Remediation
Enabled	Default	Any		DenyAccess

Verifica di CoA per l'accesso differenziato

Con i profili di autorizzazione e le politiche predisposte per differenziare l'accesso, è giunto il momento di testare. Con un'unica WLAN protetta, a un dipendente verrà assegnata la VLAN del dipendente e per la VLAN del collaboratore esterno verrà designato un collaboratore esterno. Nei prossimi esempi verrà utilizzato un iPhone/iPad Apple.

Attenersi alla seguente procedura:

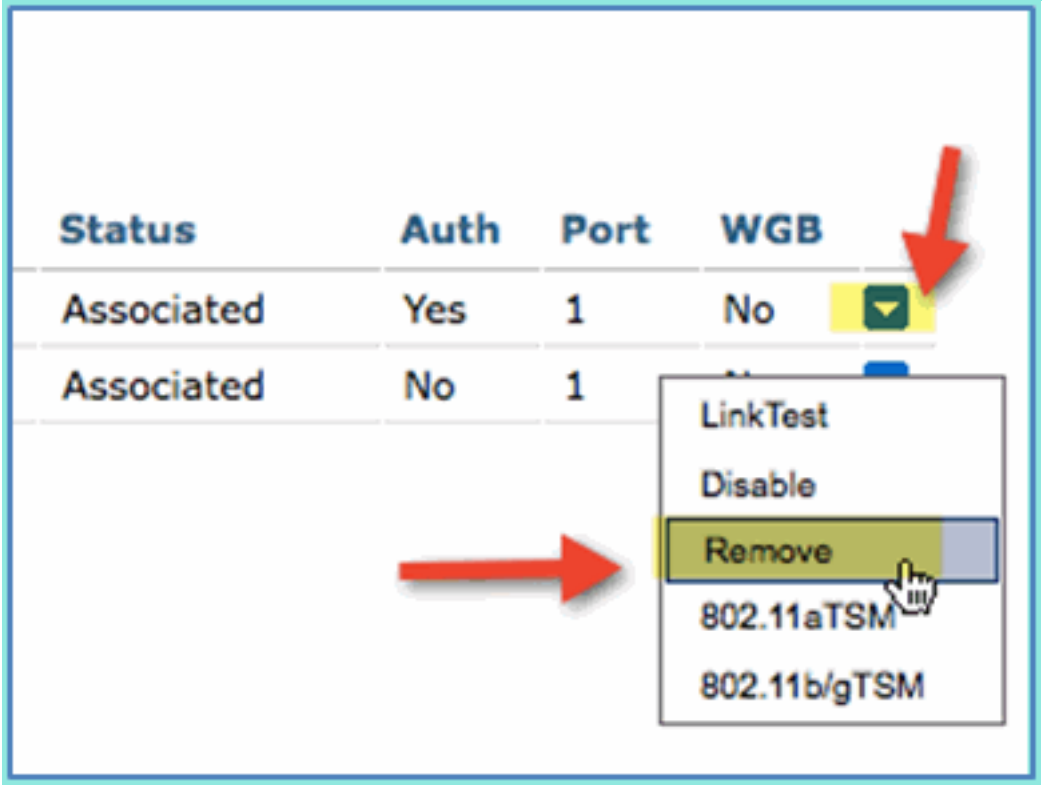
1. Connettersi alla rete WLAN protetta (POD1x) con il dispositivo mobile e utilizzare le seguenti credenziali:Nome utente: dipendentePassword:
   XXXXX

2. Fare clic su **Partecipa**. Confermare che al dipendente sia assegnata la VLAN 11 (VLAN dipendente).

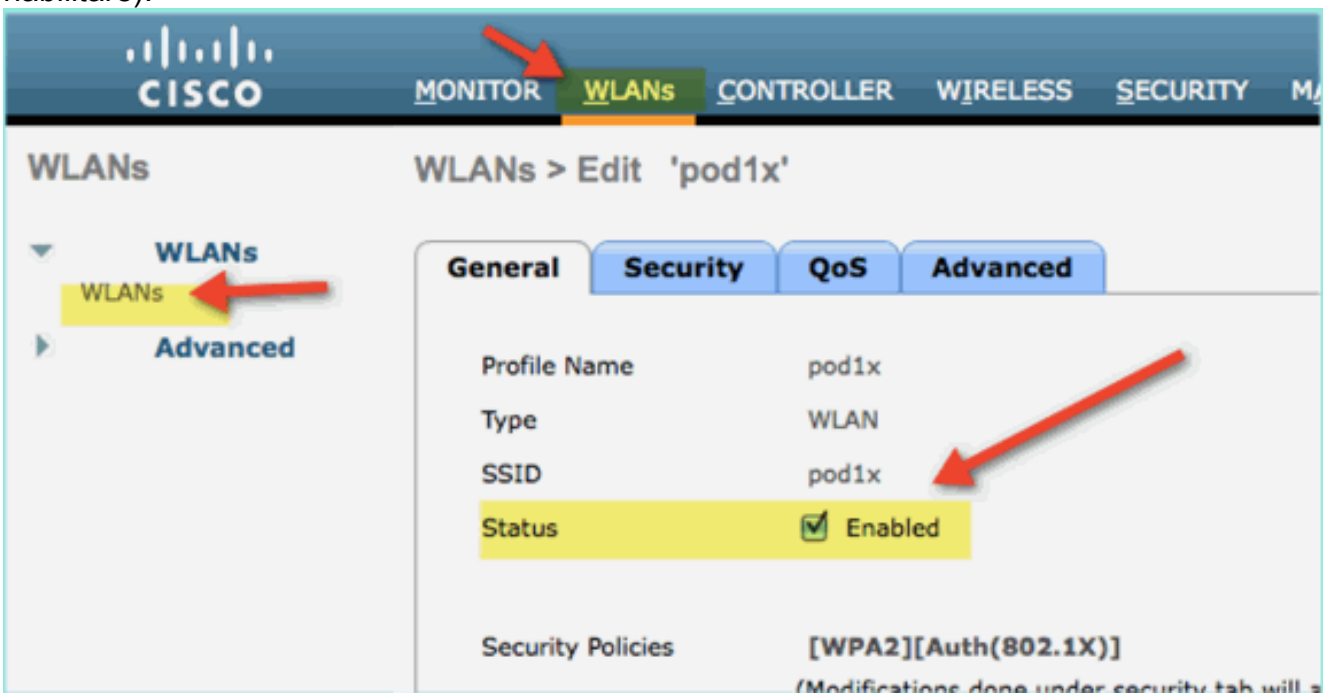
3. Fare clic su **Dimentica questa rete**. Confermare facendo clic su **Dimentica**.

4. Andare a WLC e rimuovere le connessioni client esistenti (se lo stesso è stato utilizzato nei passaggi precedenti). Selezionare **Monitor > Client > Indirizzo MAC**, quindi fare clic su **Rimuovi**.


CISCO
MONITOR
WLANs
Monitor
Clients
Summary
Current Filter
Access Points
Cisco CleanAir
Client MAC Addr
Statistics
44:2a:60:f7:3a:4a
CDP
5c:59:48:40:82:8d
Rogues
Clients
Multicast


Status
Auth
Port
WGB
Associated
Yes
1
No
Associated
No
1
LinkTest
Disable
Remove
802.11aTSM
802.11b/gTSM

5. Un altro modo sicuro per cancellare le sessioni client precedenti è disabilitare/abilitare la WLAN.Andare su **WLC > WLAN > WLAN**, quindi fare clic sulla WLAN da modificare.Deselezionare **Abilitato > Applica** (per disabilitare).Selezionare la casella per **Abilitato > Applica** (per riabilitare).

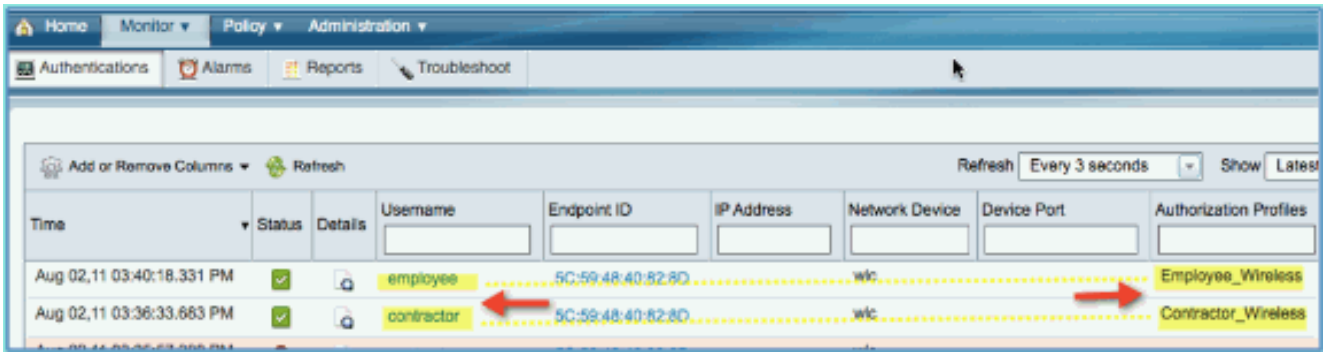


6. Torna al dispositivo mobile. Connettersi di nuovo alla stessa WLAN con queste credenziali:Nome utente: appaltatorePassword:

XXXX

7. Fare clic su **Partecipa**. Confermare che all'utente terzista sia assegnata la VLAN 12 (VLAN terzista/ospite).

8. La visualizzazione del log in tempo reale di ISE si trova in **ISE > Monitor > Authorizations**. Dovrebbe essere possibile vedere singoli utenti (dipendente, terzista) ottenere profili di autorizzazione differenziati (Employee_Wireless vsContractor_Wireless) in VLAN diverse.



WLC Guest WLAN

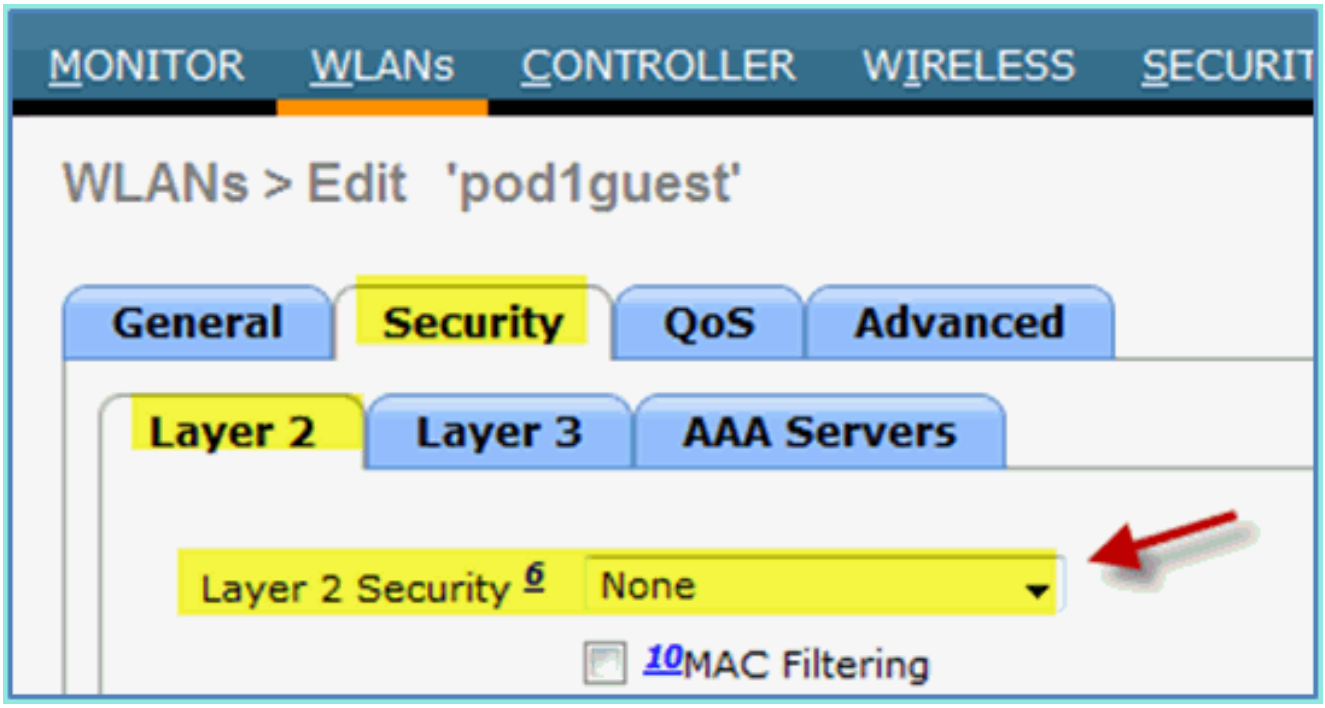
Completare questi passaggi per aggiungere una WLAN guest e consentire agli utenti non

autorizzati di accedere al portale per gli ospiti dello sponsor ISE:

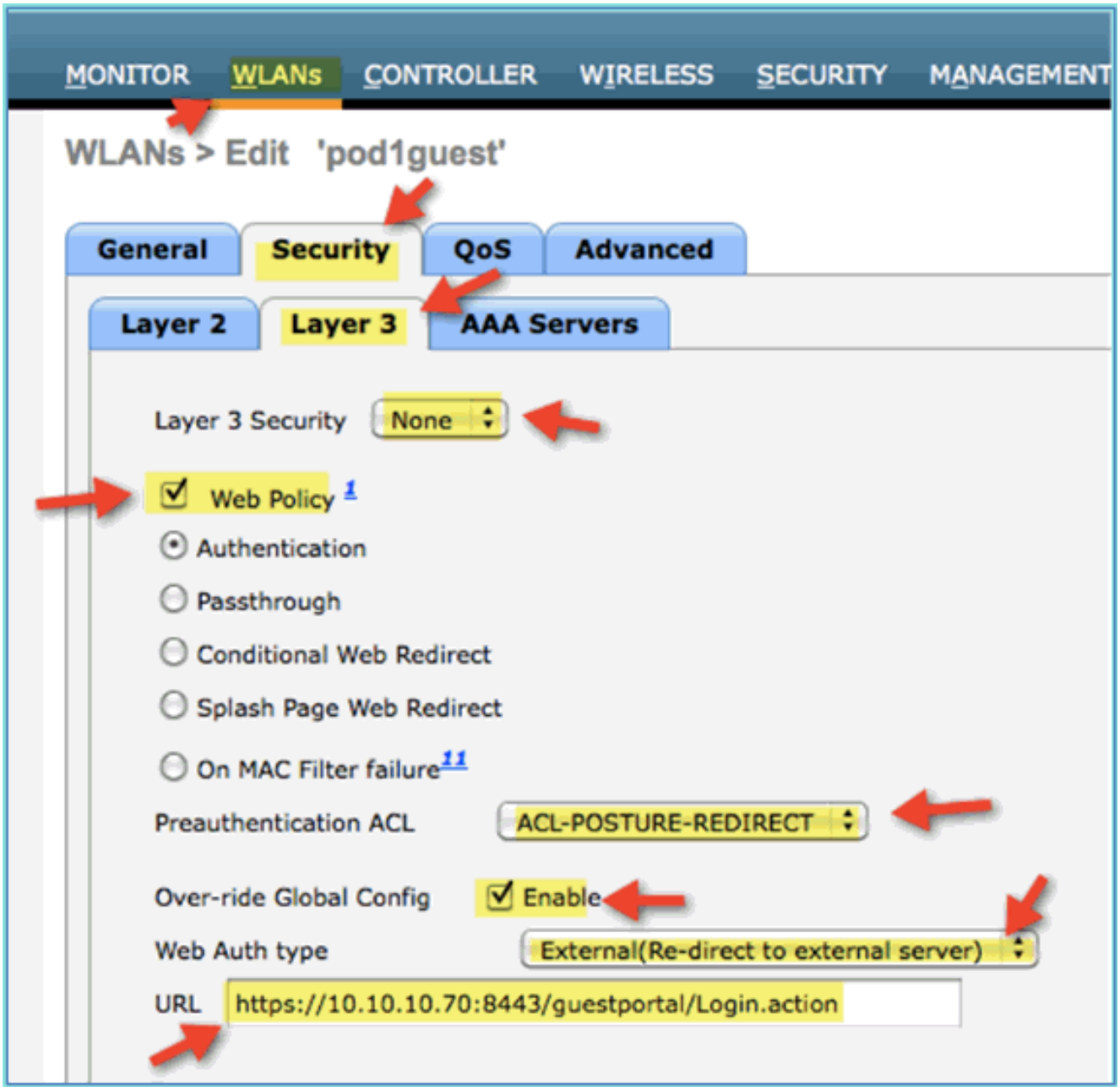
1. Da WLC, selezionare **WLAN > WLAN > Add New** (WLC),
2. Immettere quanto segue per la nuova WLAN guest:Nome profilo: pod1guestSSID: pod1 guest

3. Fare clic su **Apply** (Applica).
4. Immettere quanto segue nella scheda WLAN guest > Generale:Stato: disattivatoInterfaccia/Gruppo di interfacce:
   Guest

5. Passare a **WLAN** guest **> Sicurezza > Layer2** e immettere quanto segue:Sicurezza di livello 2:
   nessuna



6. Passare a **WLAN** guest **> Sicurezza >** scheda **Layer3** e immettere quanto segue:Sicurezza di livello 3: nessunaCriterio Web: AbilitatoValore secondario criteri Web: AutenticazioneACL preautenticazione: ACL-POSTURE-REDIRECTTipo di autenticazione Web: esterna (reindirizzamento a server esterno)URL: https://10.10.10.70:8443/guestportal/Login.action



7. Fare clic su **Apply** (Applica).
8. Accertarsi di **salvare la configurazione WLC**.

Test della WLAN guest e del portale guest

A questo punto, è possibile eseguire il test della configurazione della WLAN guest. Gli ospiti devono essere reindirizzati al portale ISE.

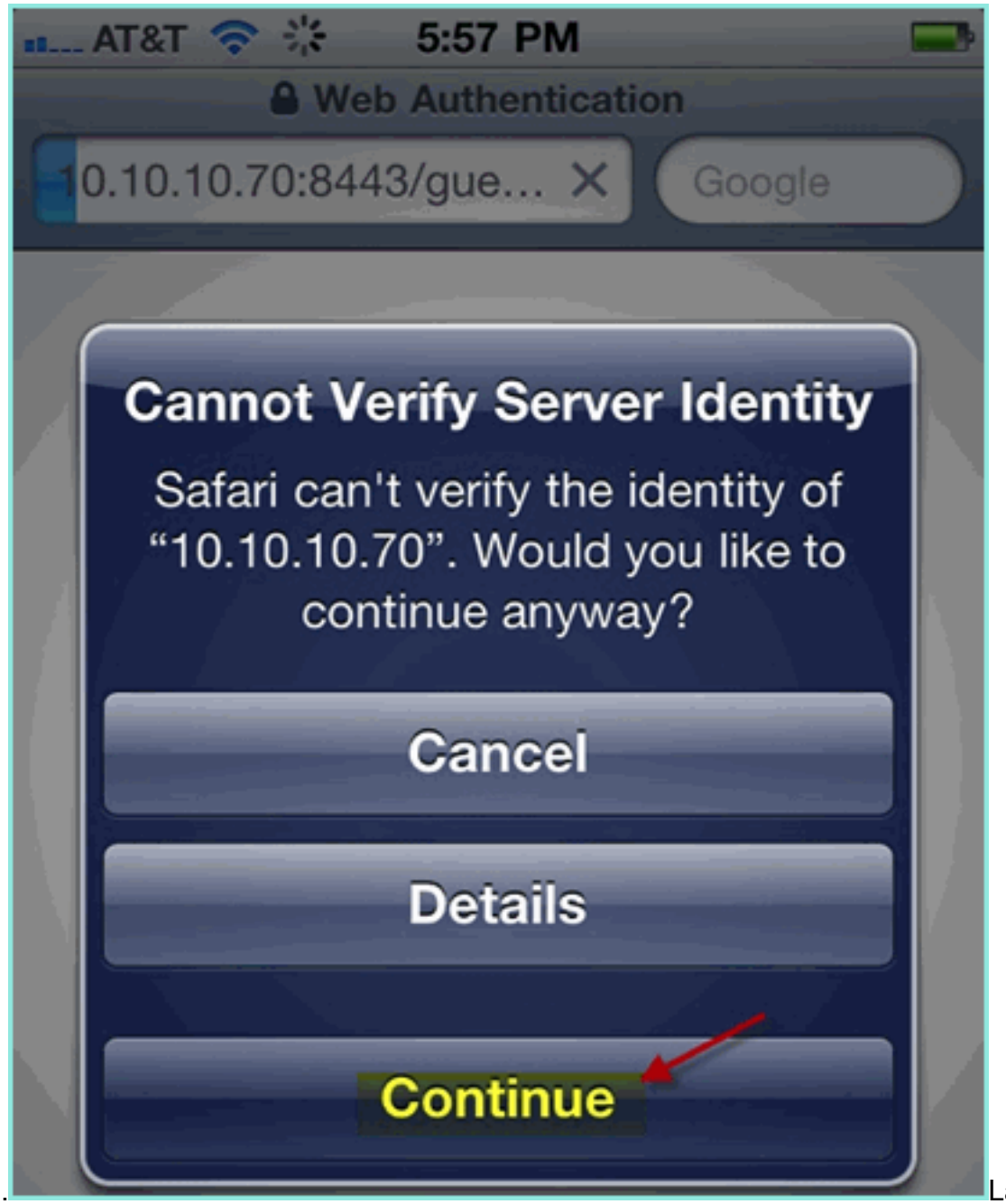
Attenersi alla seguente procedura:

1. Da un dispositivo iOS come un iPhone, selezionare **Reti Wi-Fi > Abilita**. Quindi, selezionare la rete guest

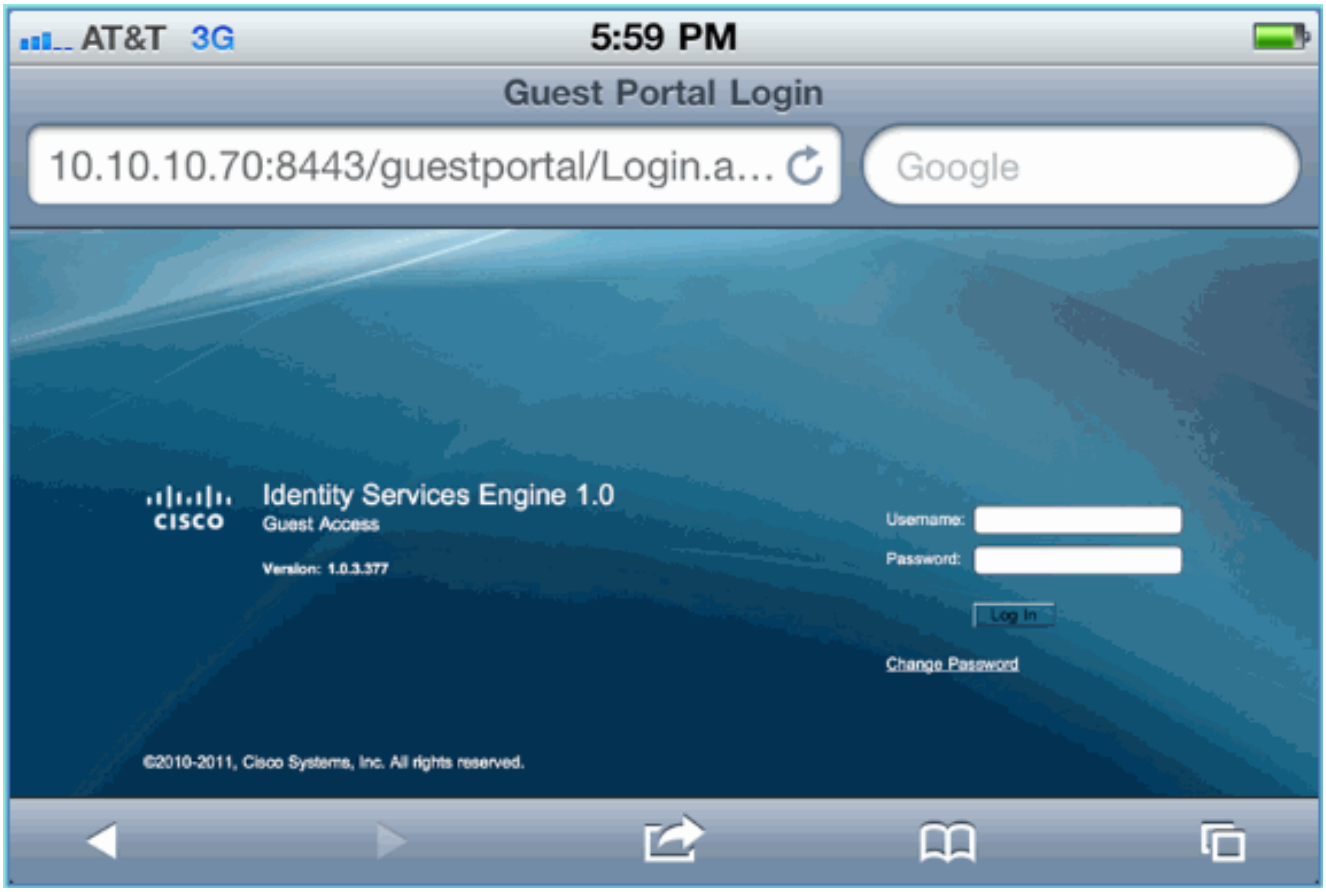
POD.

2. Sul dispositivo iOS deve essere visualizzato un indirizzo IP valido della VLAN guest (10.10.12.0/24).

3. Apri il browser Safari e connettiti a:URL: http://10.10.10.10Verrà visualizzato un reindirizzamento dell'autenticazione Web.
4. Fare clic su **Continue** (Continua) fino ad arrivare alla pagina ISE Guest



Portal. La schermata di esempio successiva mostra il dispositivo iOS su un login al portale guest. In questo modo si conferma che l'impostazione corretta per il portale WLAN e ISE Guest è attiva.

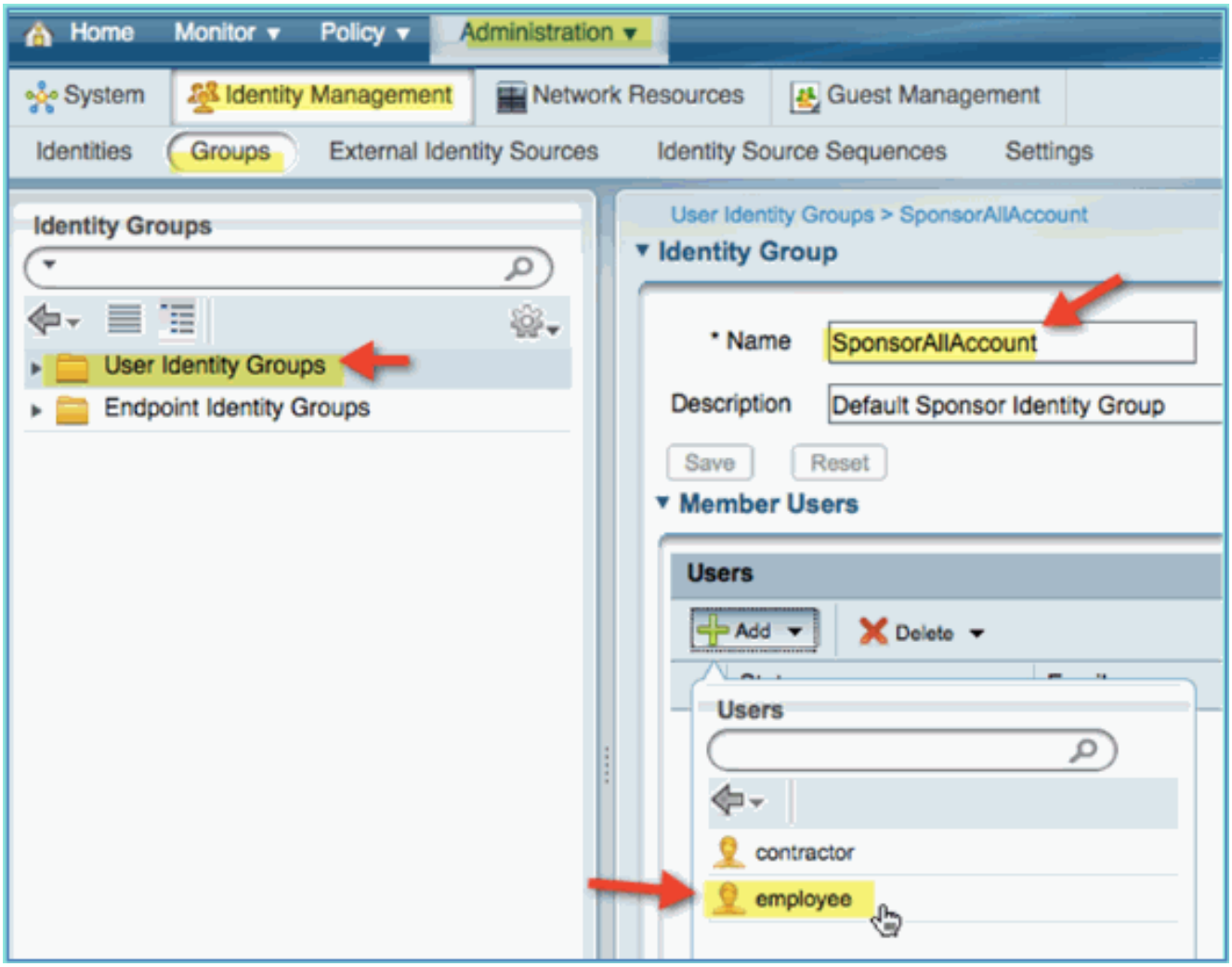


ISE Wireless Sponsored Guest Access

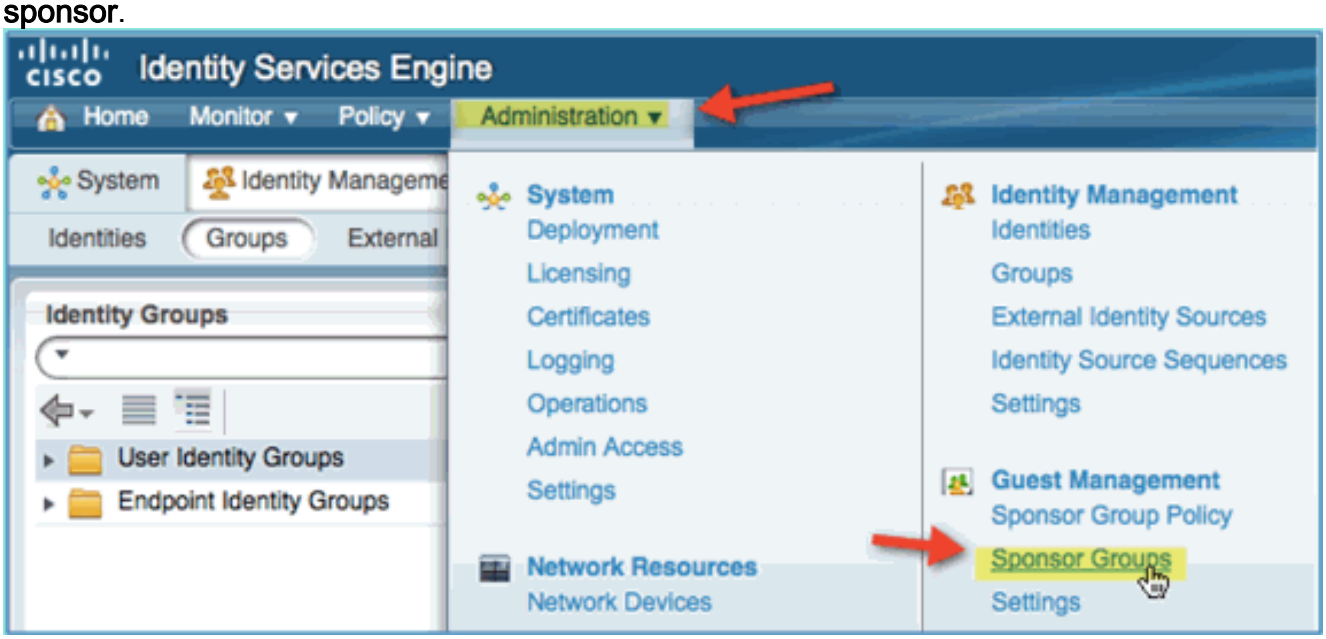
L'ISE può essere configurata per offrire il patrocinio agli ospiti. In questo caso sarà necessario configurare le policy ISE per gli utenti guest in modo da consentire agli utenti interni o del dominio Active Directory (se integrati) di sponsorizzare l'accesso guest. Configurerete anche l'ISE in modo da permettere agli sponsor di visualizzare la password dell'ospite (opzionale), una funzione utile in questa esercitazione.

Attenersi alla seguente procedura:

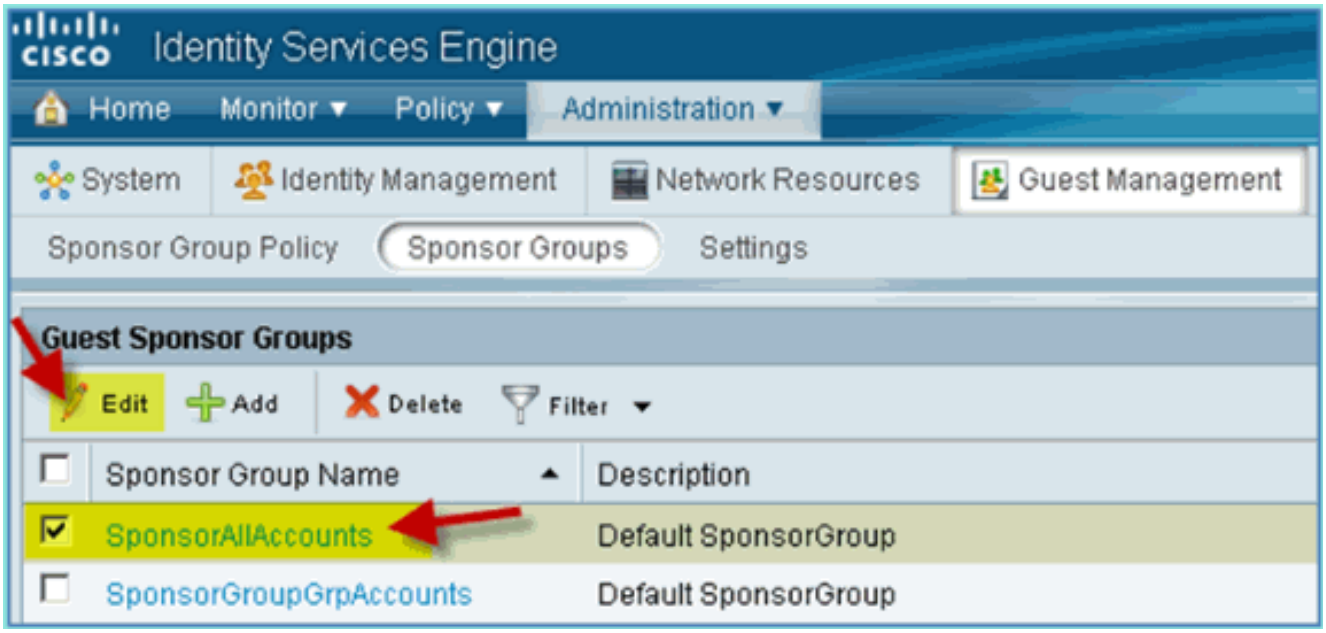
1. Aggiungere l'utente del dipendente al gruppo SponsorAllAccount. A tale scopo, è possibile passare direttamente al gruppo oppure modificare l'utente e assegnare il gruppo. Per questo esempio, passare a **Amministrazione > Gestione delle identità > Gruppi > Gruppi identità utente**. Quindi, fare clic su **SponsorAllAccount** e aggiungere l'utente del dipendente.



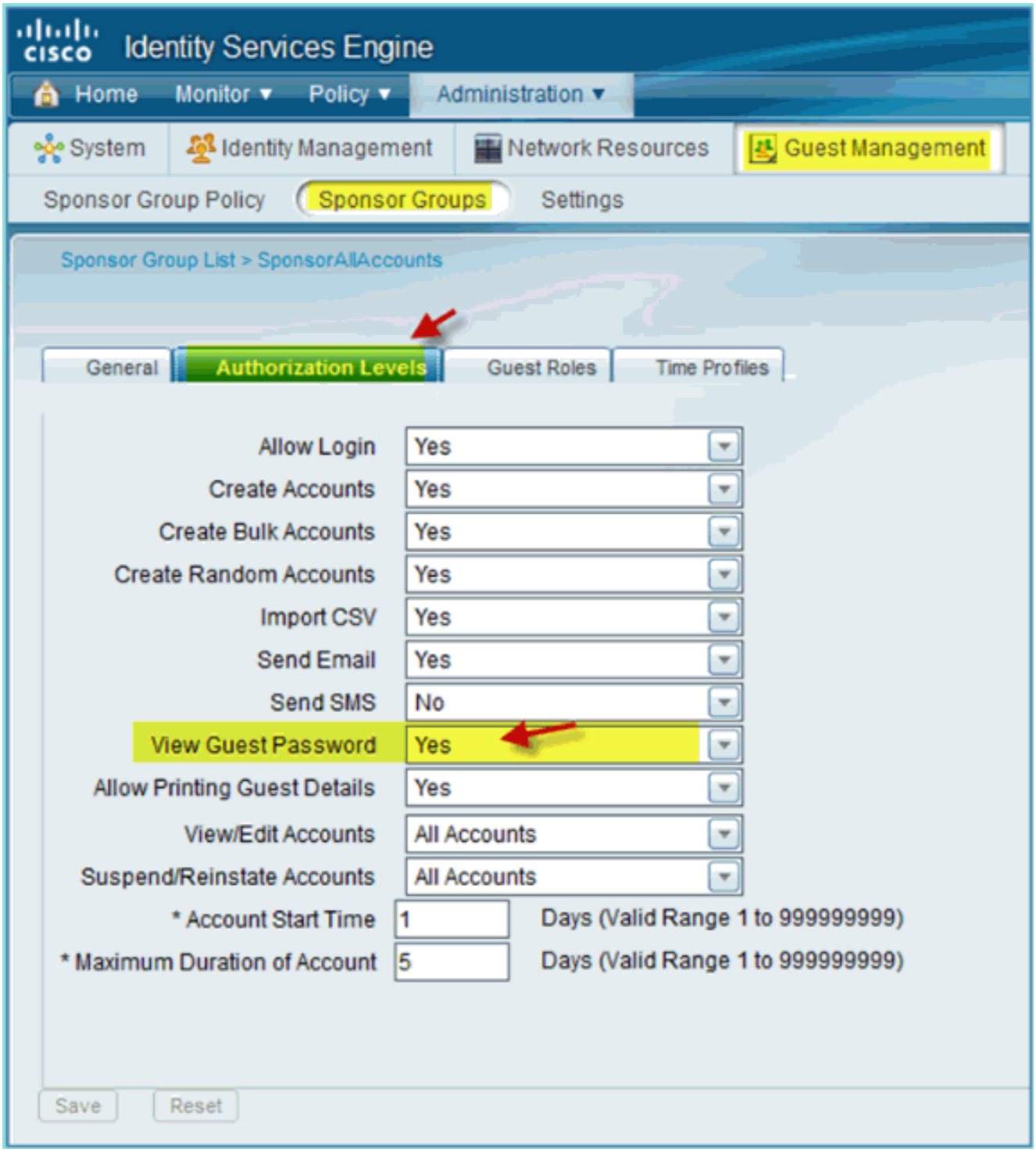
2. Passare a **Amministrazione > Gestione guest > Gruppi sponsor**.



3. Fare clic su **Modifica**, quindi scegliere **SponsorAllAccounts**.



4. Selezionare Livelli di autorizzazione e impostare quanto segue:Visualizza password guest: Sì



5. Per completare l'operazione, fare clic su **Save** (Salva).

Sponsorizzazione Guest

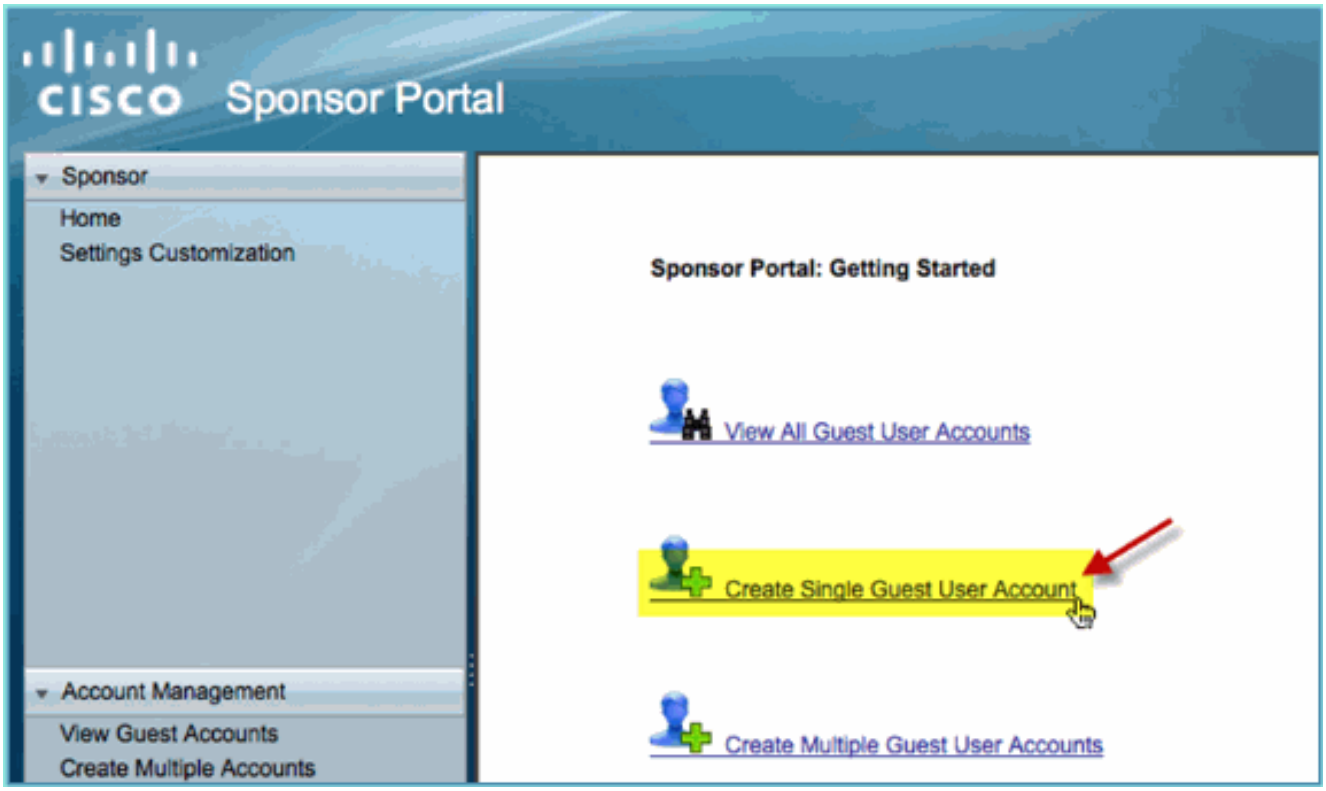
In precedenza, sono stati configurati i criteri e i gruppi guest appropriati per consentire agli utenti del dominio Active Directory di sponsorizzare utenti guest temporanei. Successivamente, si accederà al portale degli sponsor e si creerà un accesso guest temporaneo.

Attenersi alla seguente procedura:

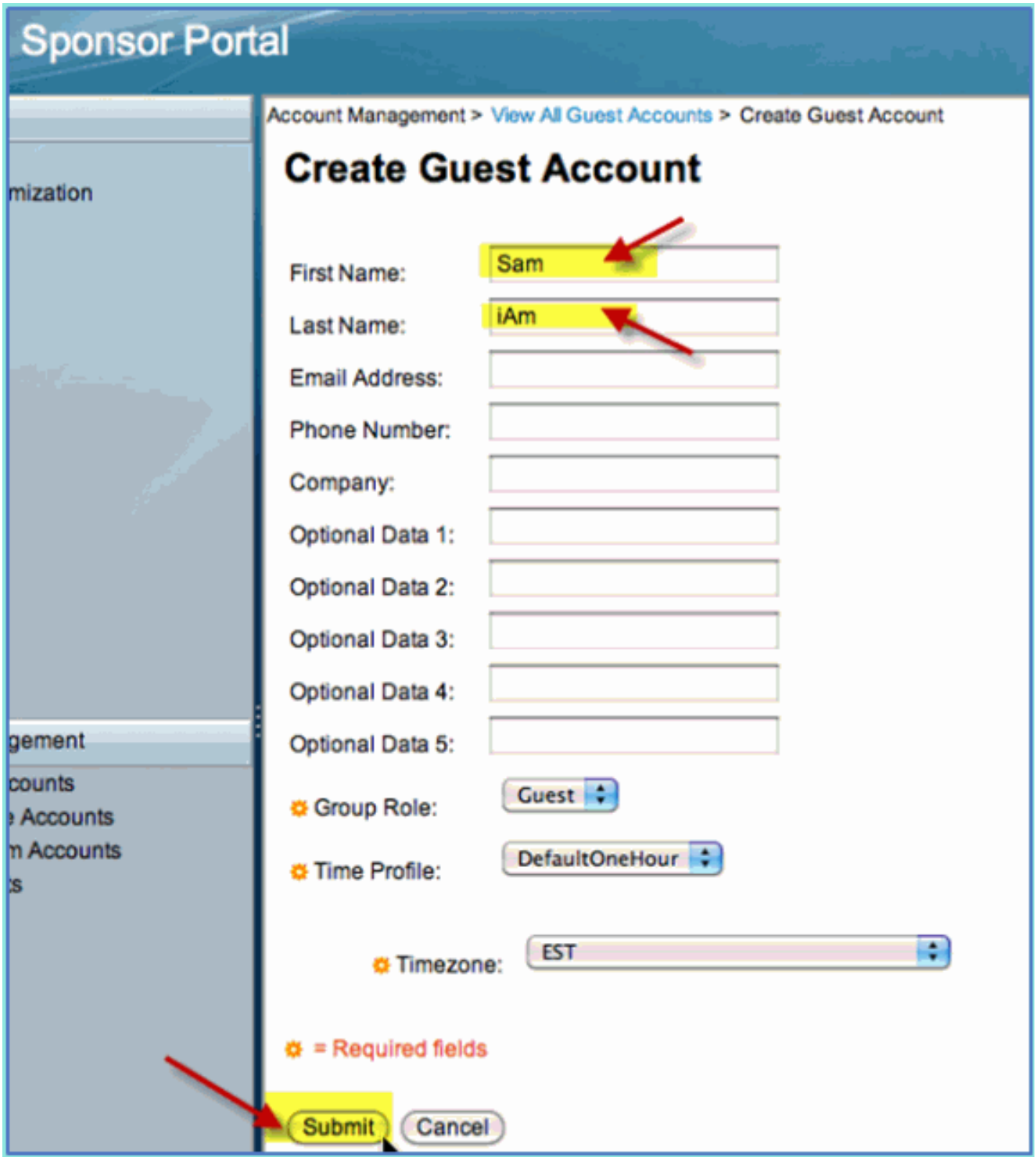
1. Da un browser, selezionare uno dei seguenti URL: http://<ise ip>:8080/sponsorportal/ **o** https://<ise ip>:8443/sponsorportal/. Quindi, eseguire il login con:Nome utente: aduser (Active Directory), employee (Internal User)Password:

XXXX

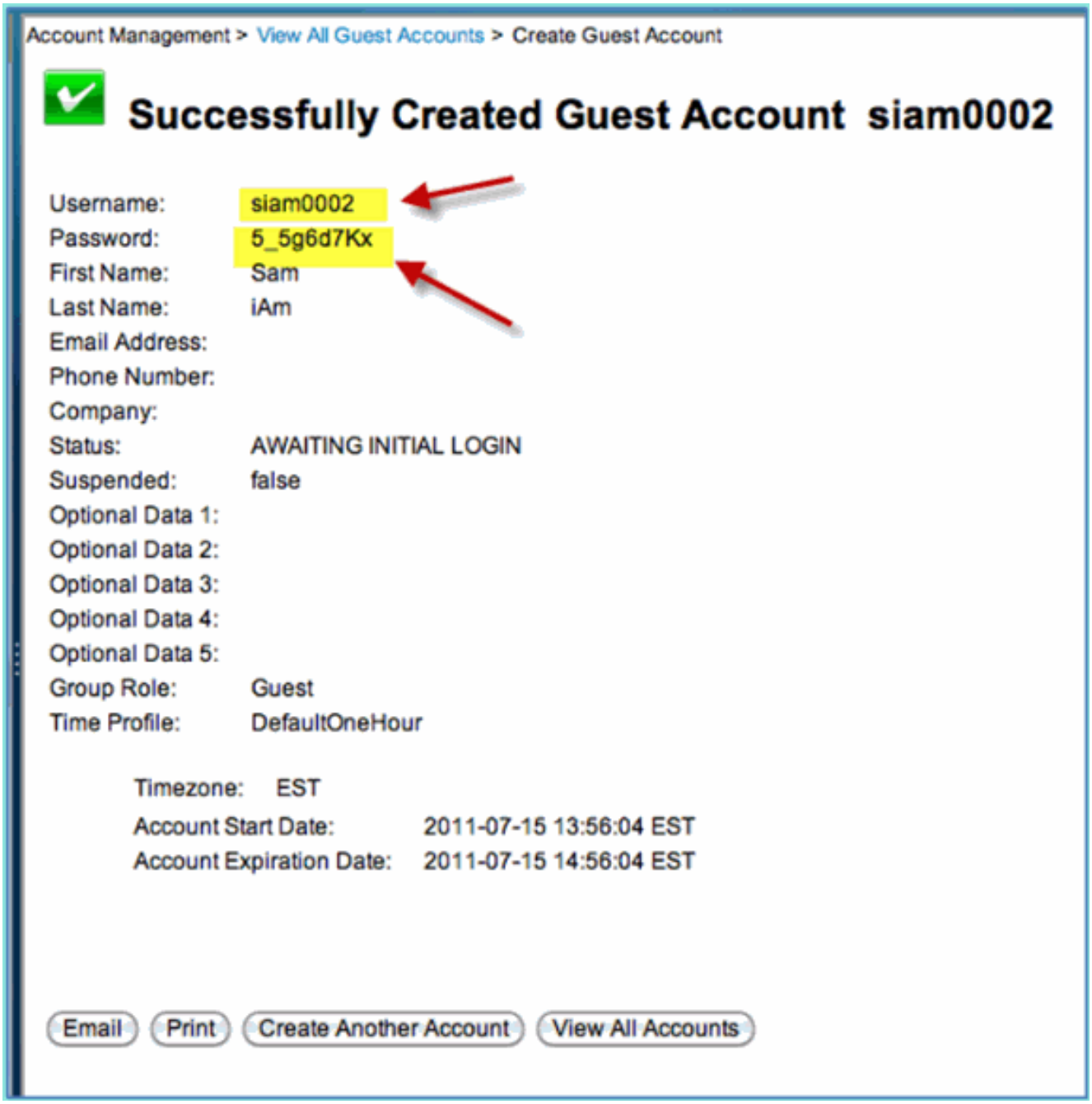
2. Nella pagina Sponsor, fare clic su **Create Single Guest User Account** (Crea account utente guest
singolo).



3. Per un guest temporaneo, aggiungere quanto segue:Nome: obbligatorio (ad esempio, Sam)Cognome: obbligatorio (ad esempio, Rossi)Ruolo gruppo: GuestProfilo temporale: DefaultOneHourFuso orario:
   Qualsiasi/Predefinito



4. Fare clic su **Invia**.
5. Viene creato un account Guest in base alla voce precedente. Si noti che la password è visibile (dall'esercizio precedente) anziché l'hash ***.
6. Lasciare aperta questa finestra che mostra il nome utente e la password per il guest. Le utilizzerete per verificare l'accesso al portale guest (successivo).



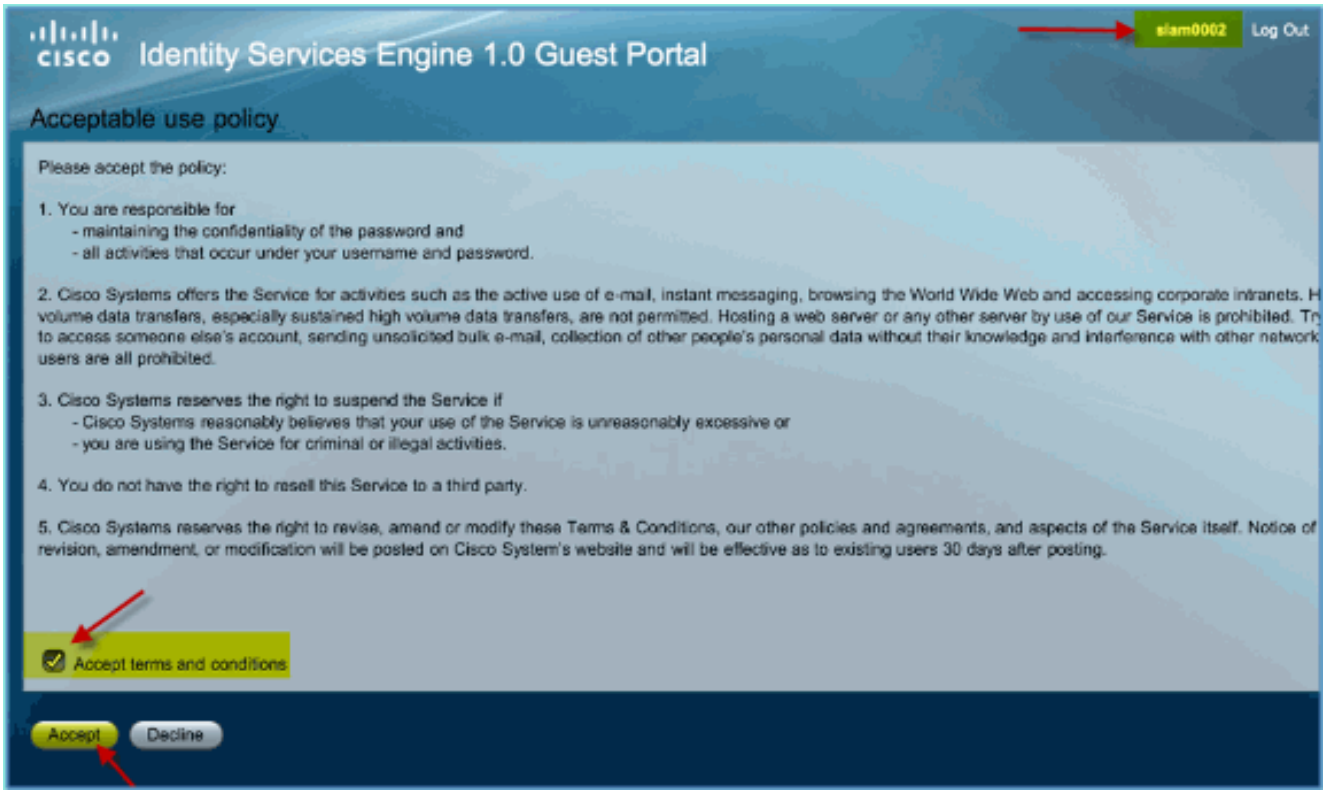
Verifica dell'accesso al portale guest

Con il nuovo account guest creato da un utente/sponsor di Active Directory, è il momento di testare il portale guest e l'accesso.

Attenersi alla seguente procedura:

1. Su un dispositivo preferito (in questo caso un Apple iOS / iPad), collegarsi al Pod Guest SSID e controllare indirizzo IP /connettività.
2. Utilizzare il browser e tentare di passare a http://www.Viene visualizzata la pagina Login al portale
guest.

3. Accedere utilizzando l'account Guest creato nell'esercizio precedente.Se l'operazione ha esito positivo, viene visualizzata la pagina Criterio d'uso accettabile.
4. Selezionare **Accetta termini e condizioni**, quindi fare clic su **Accetta**.



L'URL originale è stato completato e all'endpoint è consentito l'accesso come guest.

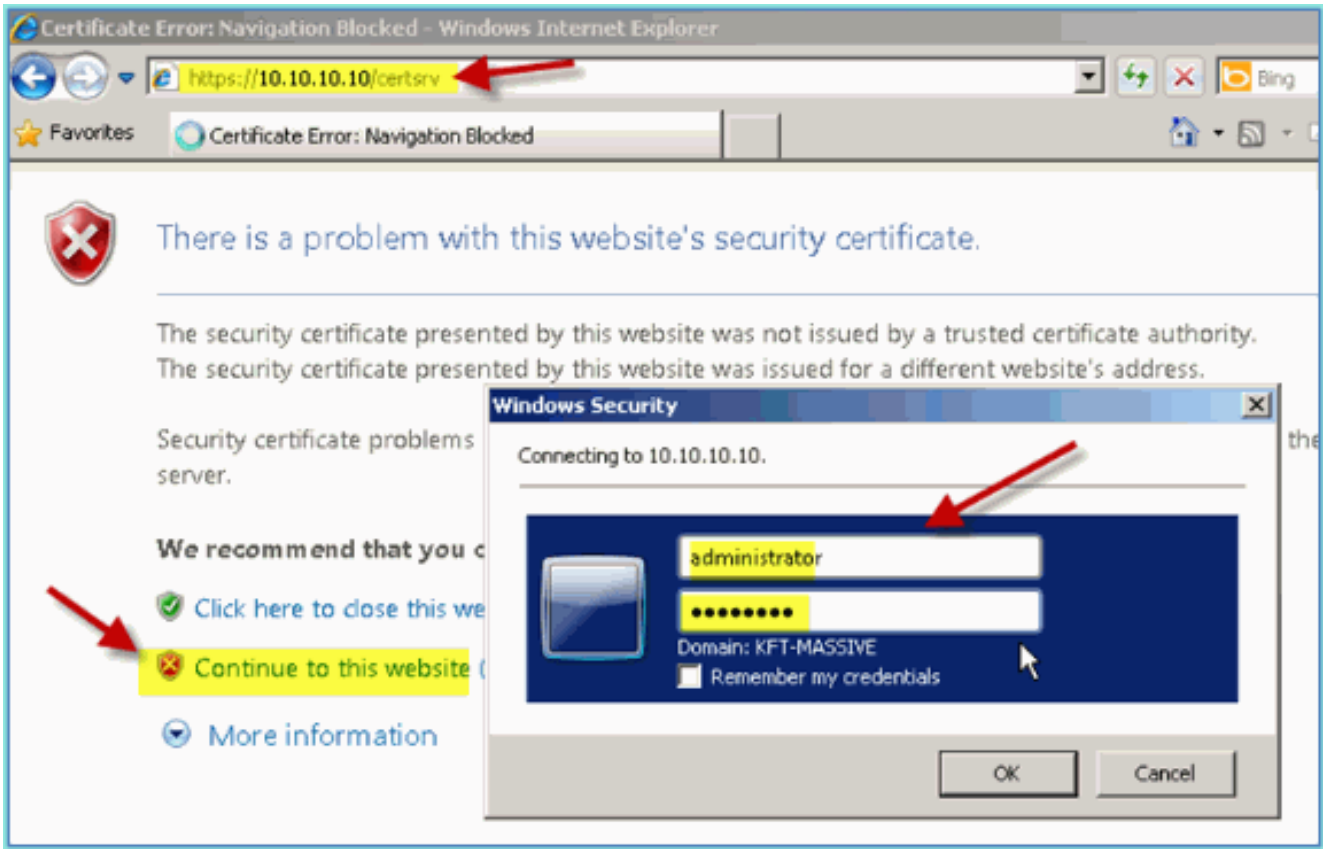
Configurazione certificato

Per proteggere le comunicazioni con ISE, stabilire se la comunicazione è correlata all'autenticazione o per la gestione di ISE. Ad esempio, per la configurazione che utilizza l'interfaccia utente Web ISE, è necessario configurare i certificati X.509 e le catene di certificati per abilitare la crittografia asimmetrica.

Attenersi alla seguente procedura:

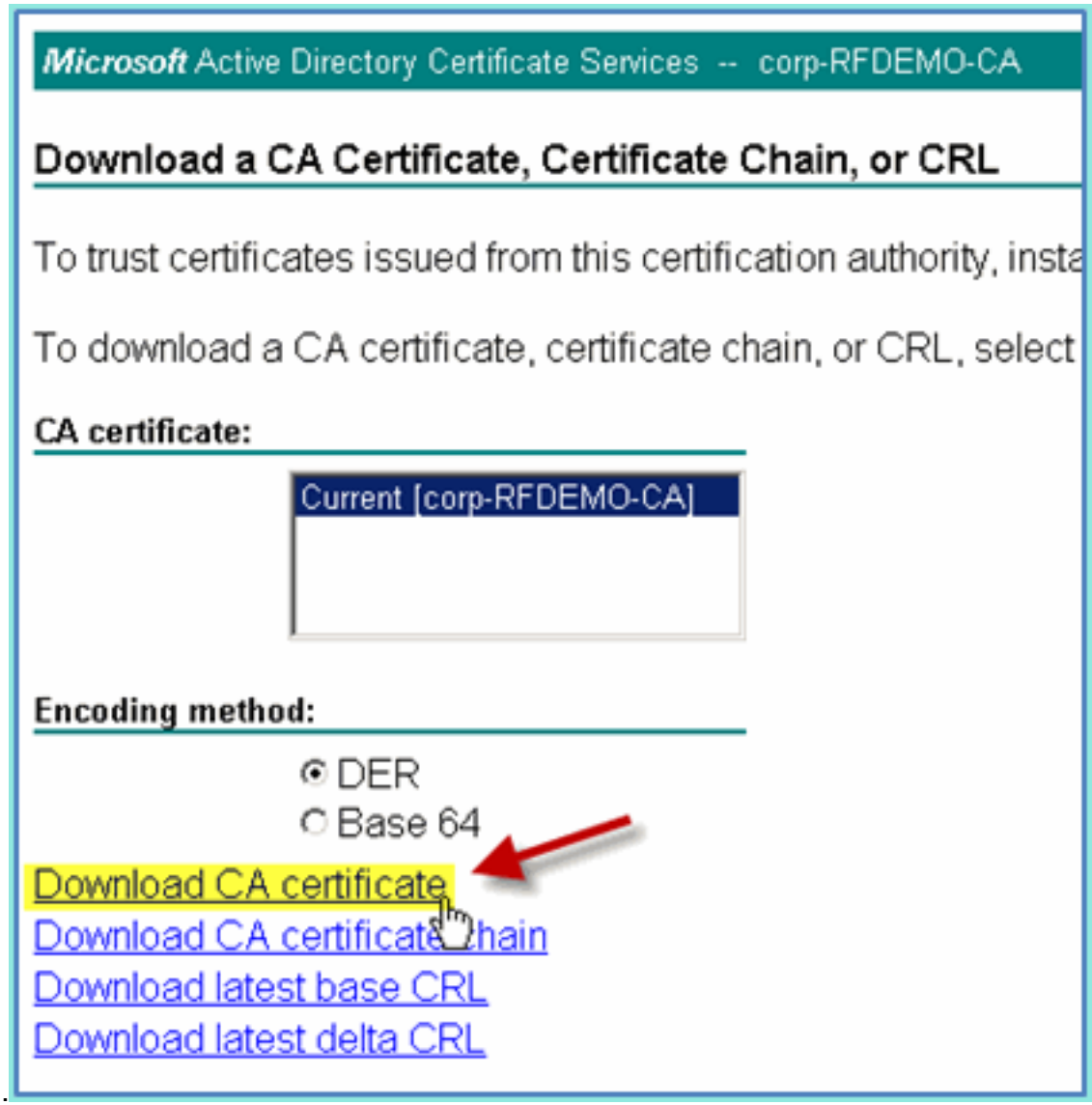
1. Dal PC connesso via cavo, aprire una finestra del browser in https://AD/certsrv.**Nota:** utilizzare il protocollo HTTP protetto.**Nota:** per accedere ad ISE, usare Mozilla Firefox o MS Internet Explorer.
2. Accedere come

amministratore/Cisco123.



3. Fare clic su **Scarica un certificato CA, una catena di certificati o un CRL**.

4. Fare clic su **Scarica certificato CA** e salvarlo (annotare il percorso di

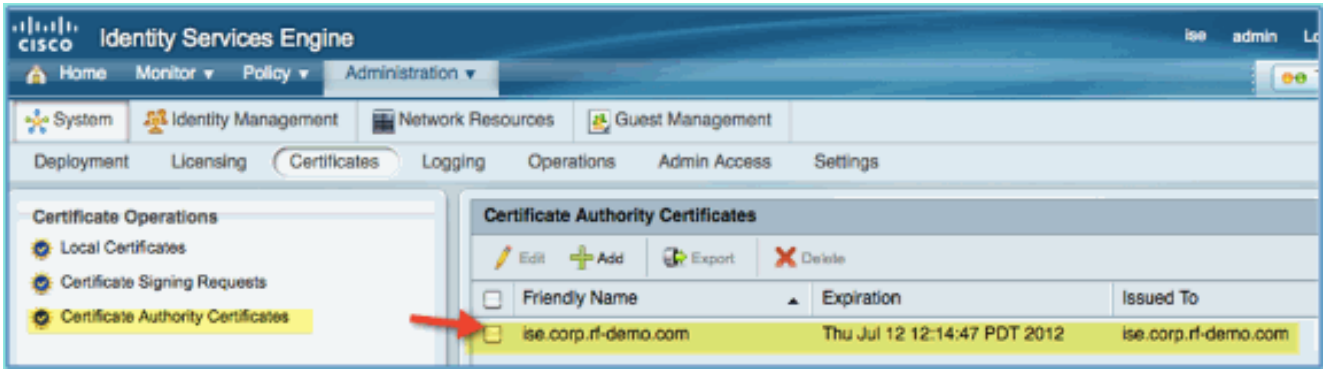


salvataggio).

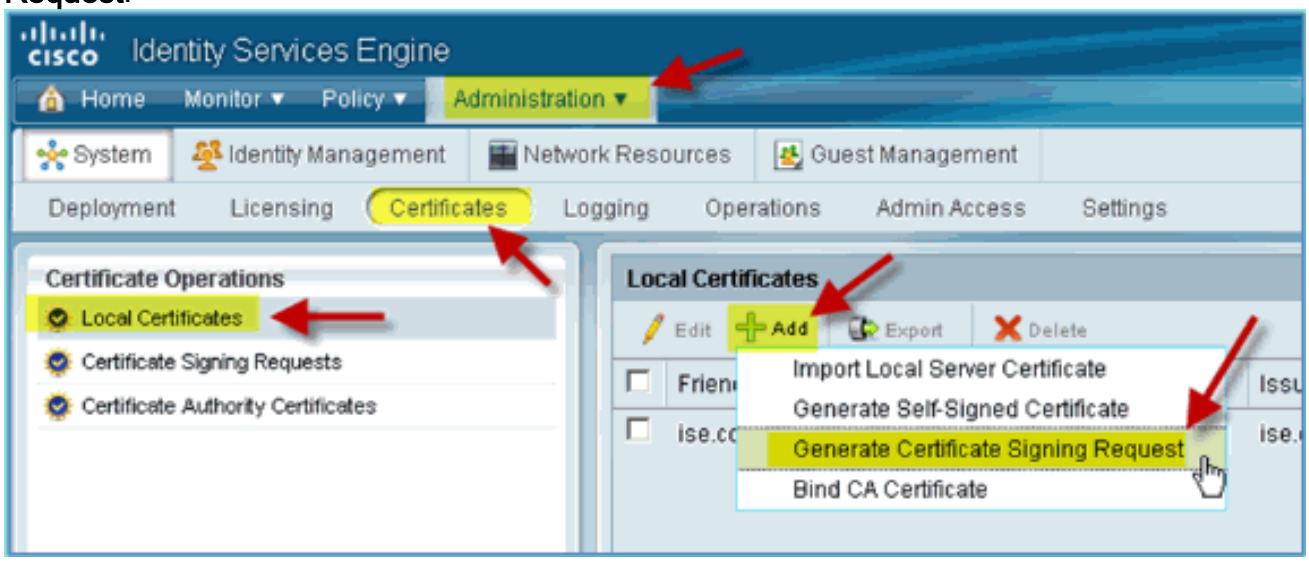
5. Aprire una finestra del browser in https://<Pod-ISE>.
6. Selezionare **Amministrazione > Sistema > Certificati > Certificati autorità di certificazione**.

7. Selezionare l'operazione **Certificati Autorità di certificazione** e selezionare il certificato CA scaricato in precedenza.
8. Selezionare **Considera attendibile il client con EAP-TLS**, quindi eseguire l'invio.

9. Confermare che la CA è stata aggiunta come attendibile come CA radice.



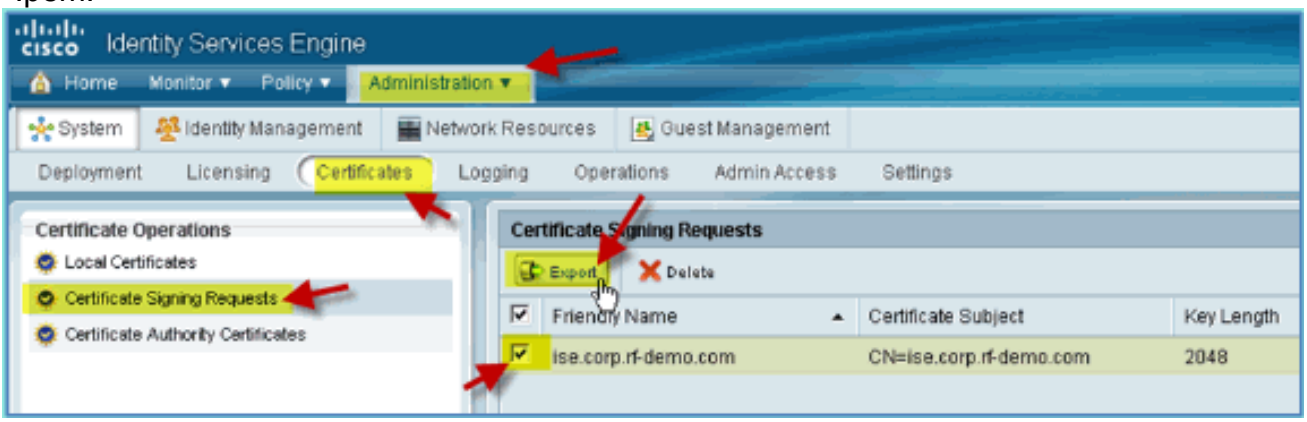
10. Da un browser, selezionare **Amministrazione > Sistema > Certificati > Certificati Autorità di certificazione**.
11. Fare clic su **Add**, quindi su **Generate Certificate Signing Request**.



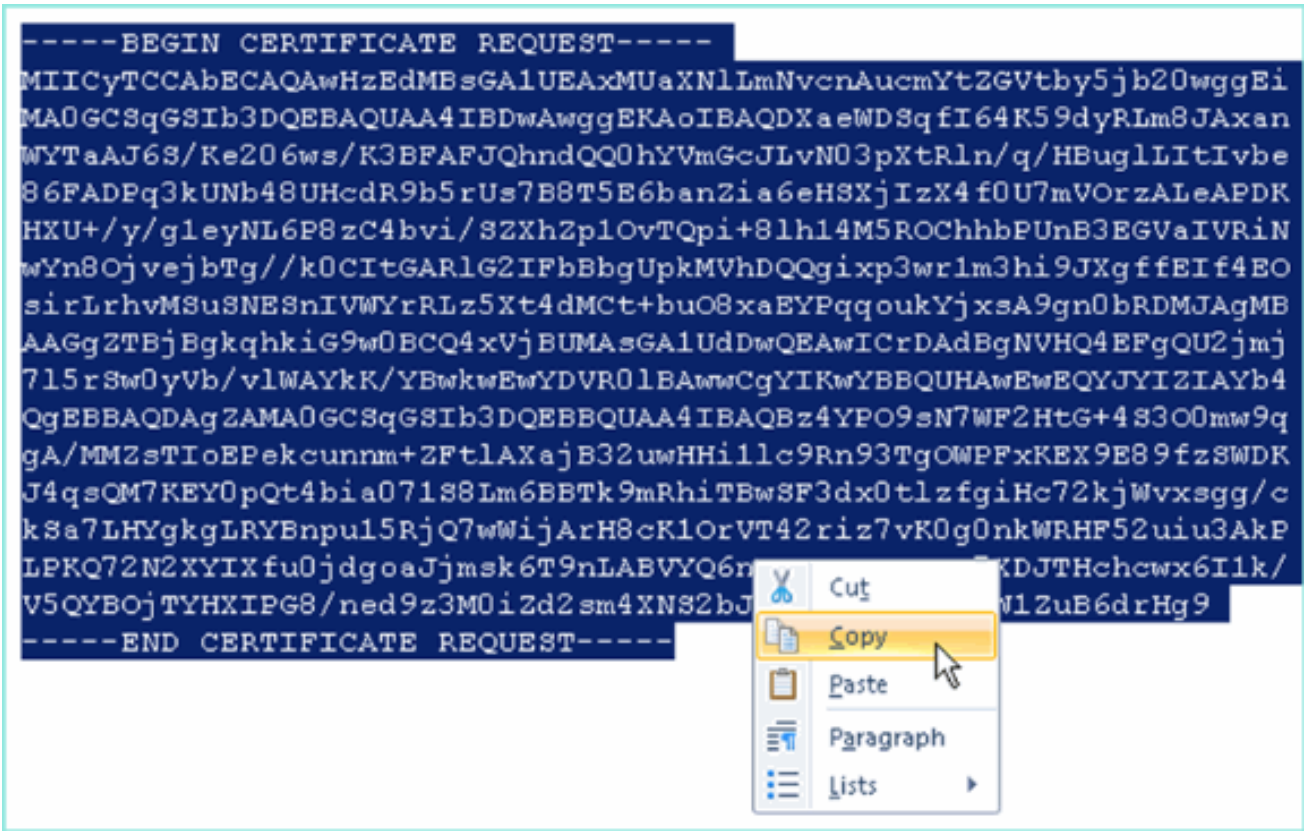
12. Invia i seguenti valori:Oggetto certificato: CN=ise.corp.rf-demo.comLunghezza chiave: 2048

13. ISE richiede che il CSR sia disponibile nella pagina CSR. Fare clic su **OK**.

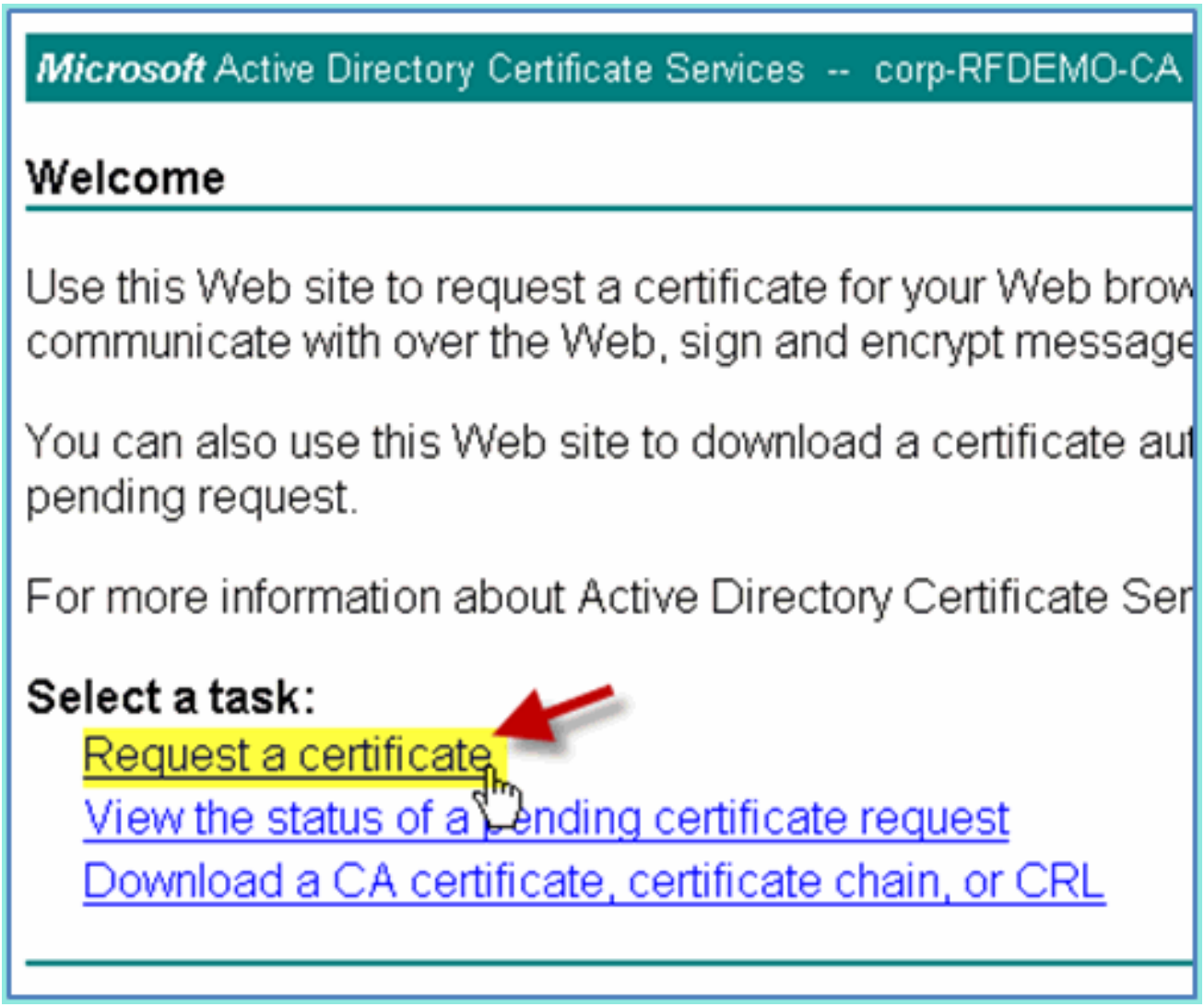
14. Selezionare il CSR dalla pagina ISE CSR e fare clic su **Esporta**.
15. Salvare il file in qualsiasi percorso (ad esempio, Download e così via)
16. Il file verrà salvato come *.pem.



17. Individuare il file CSR e modificarlo con Blocco note/Wordpad/TextEdit.
18. Copiare il contenuto (Seleziona tutto > Copia).

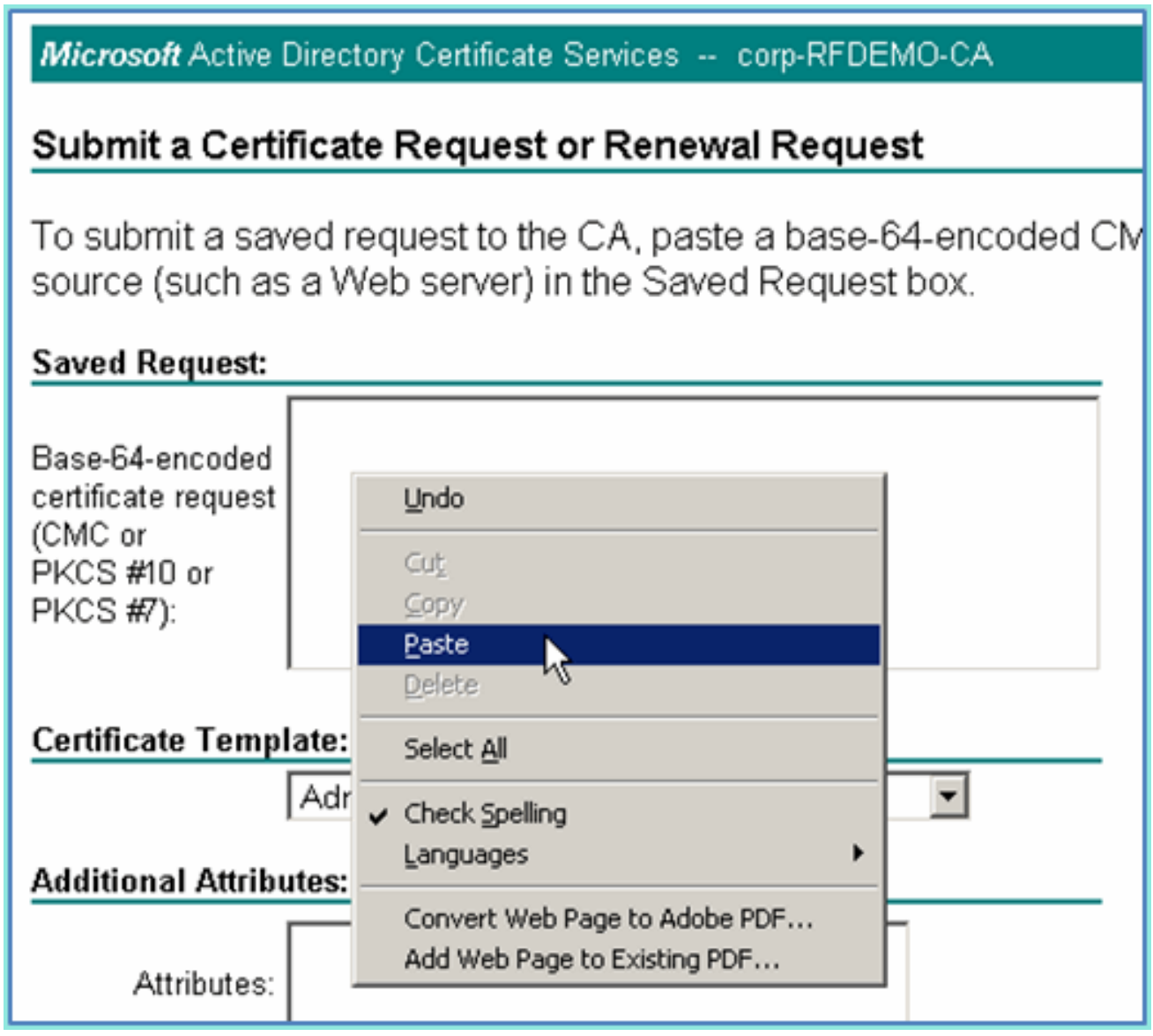


19. Aprire una finestra del browser in https://<Pod-AD>/certsrv.
20. Fare clic su **Richiedi certificato**.

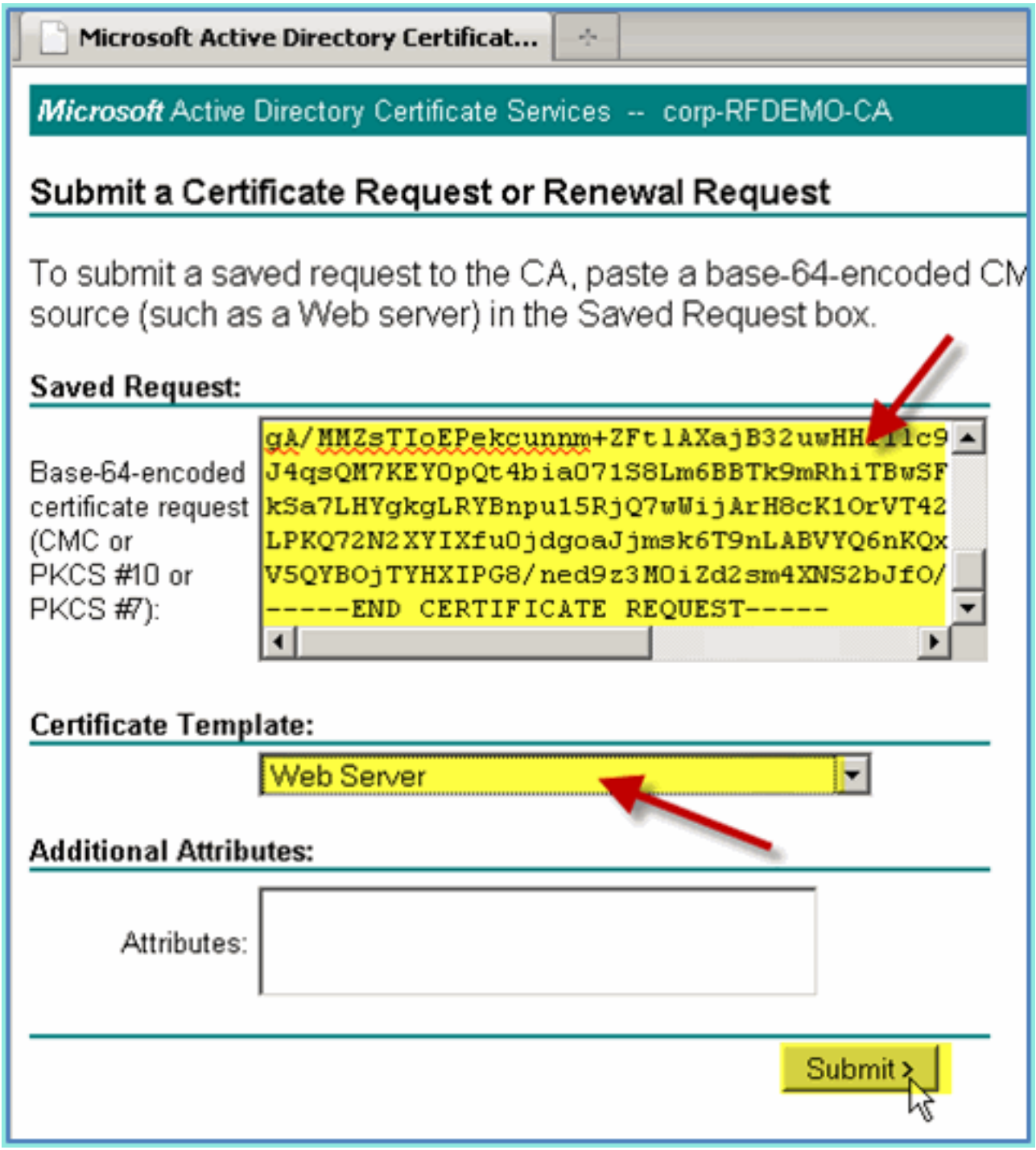


21. Fare clic per inviare una **richiesta di certificato avanzata**.

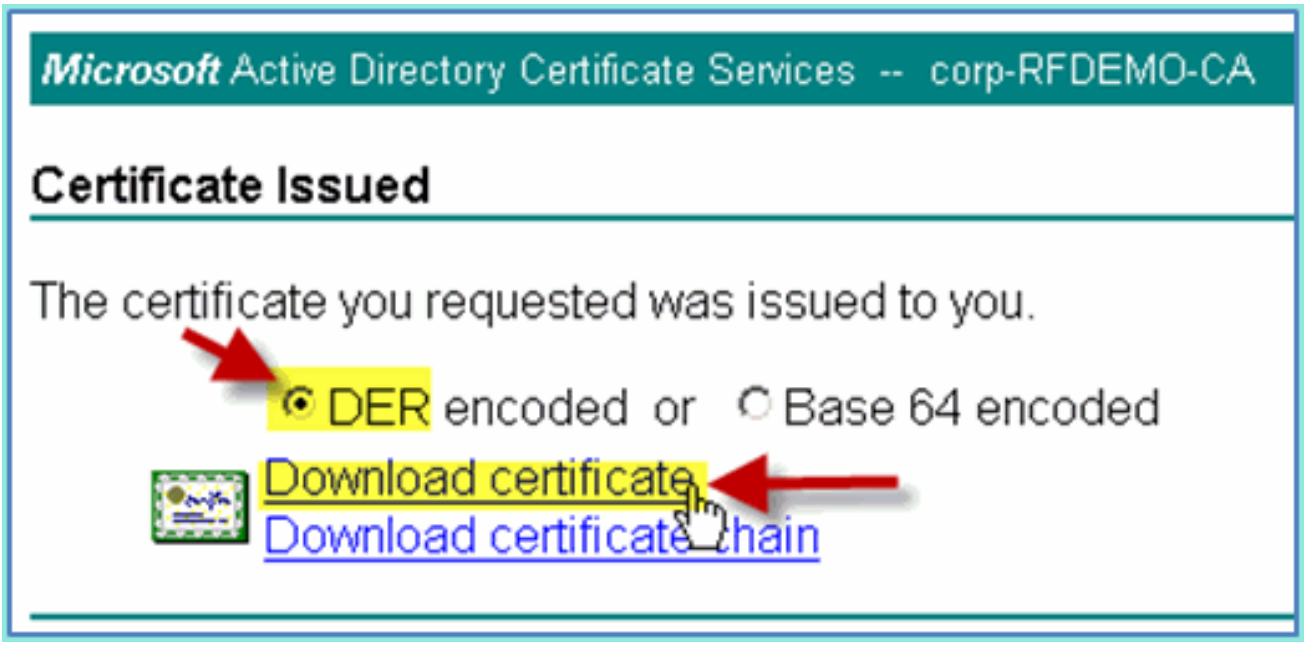
22. Incollare il contenuto CSR nel campo Richiesta salvata.



23. Selezionare **Server Web** come modello di certificato, quindi fare clic su **Invia**.

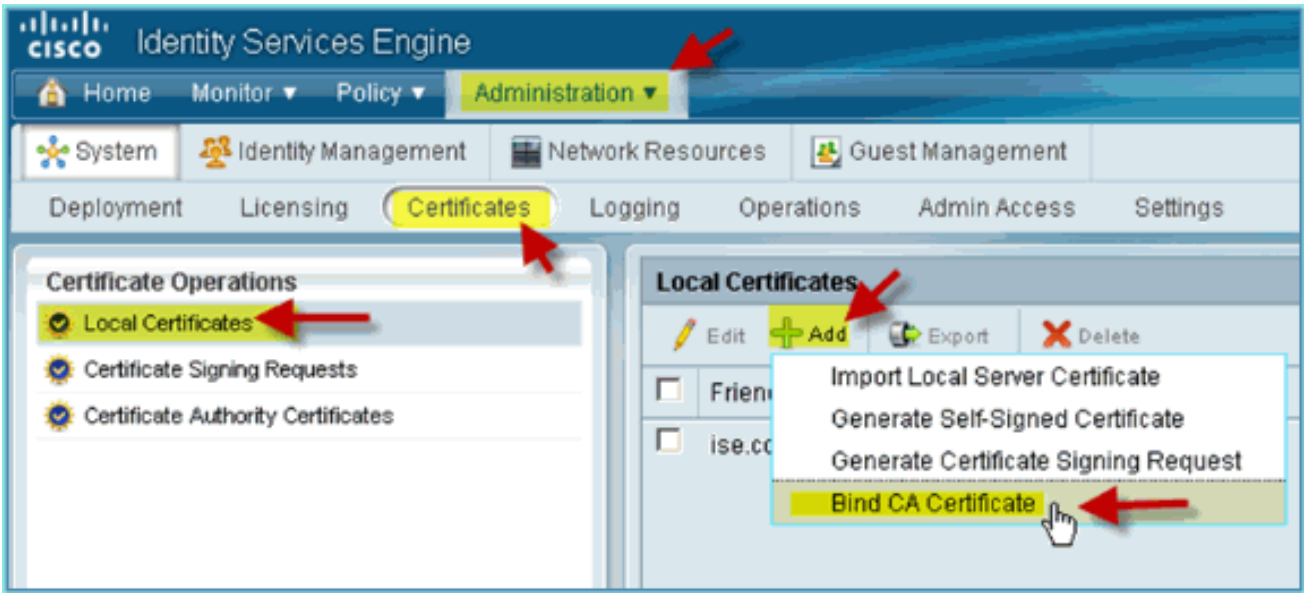


24. Selezionare **Codificato DER**, quindi fare clic su **Scarica certificato**.

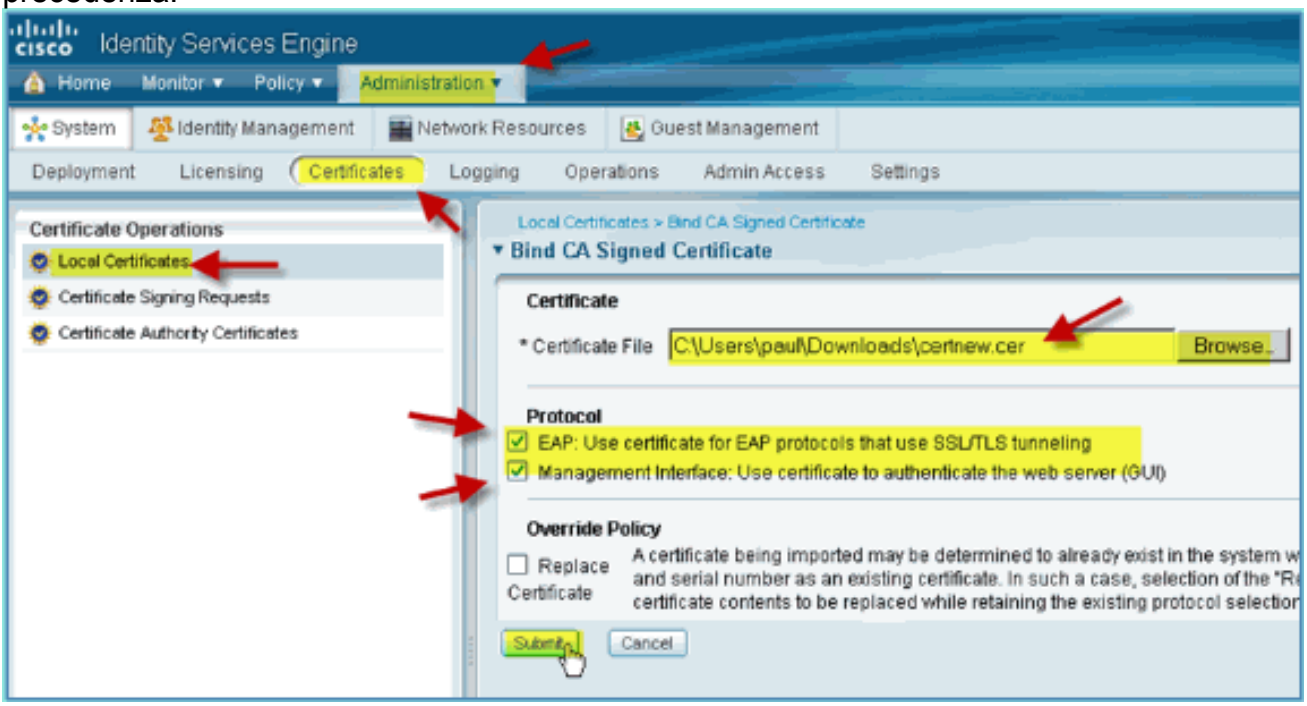


25. Salvare il file in una posizione nota (ad esempio, Download)
26. Selezionare **Amministrazione > Sistema > Certificati > Certificati autorità di certificazione**.

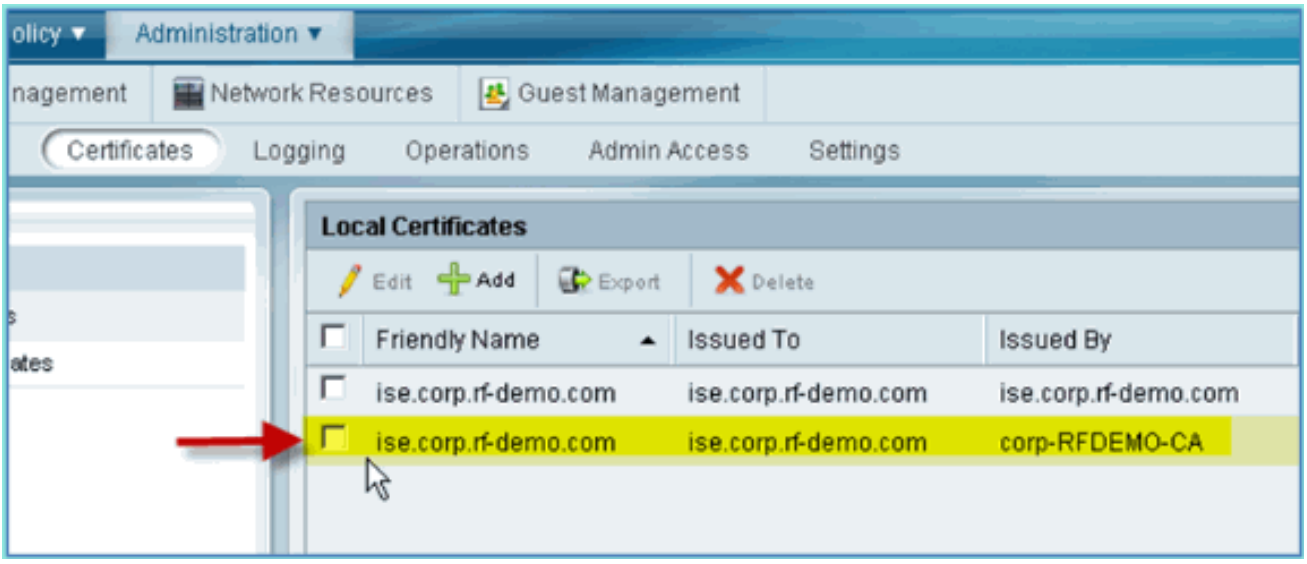
27. Fare clic su **Aggiungi > Associa certificato CA**.



28. Selezionare il certificato CA scaricato in precedenza.



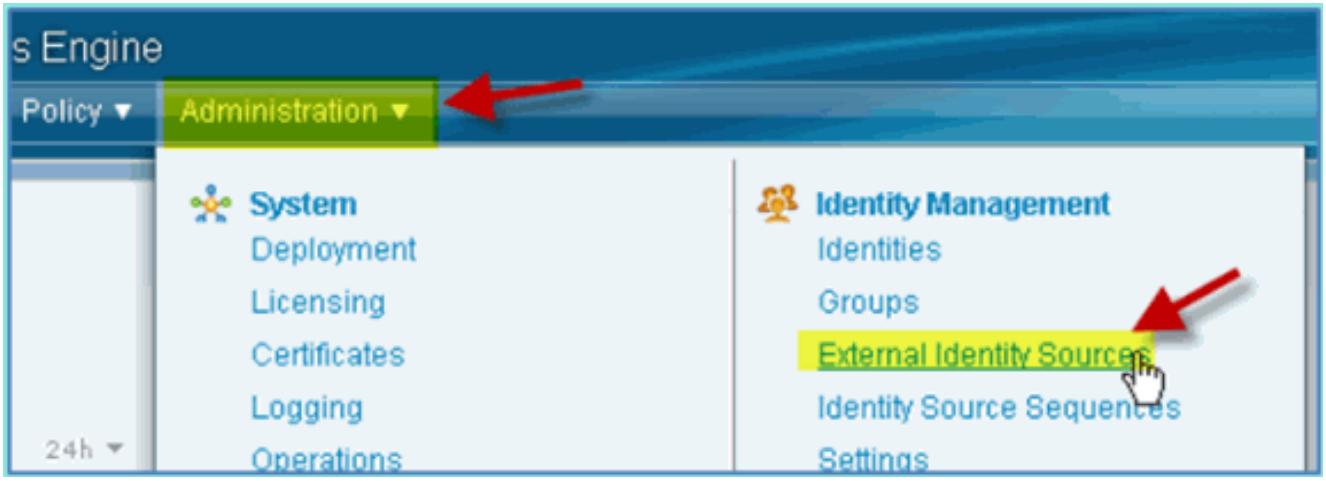
29. Selezionare **Protocol EAP** e **Management Interface**, quindi fare clic su **Submit** (Invia).
30. Confermare che la CA è stata aggiunta come attendibile come CA radice.



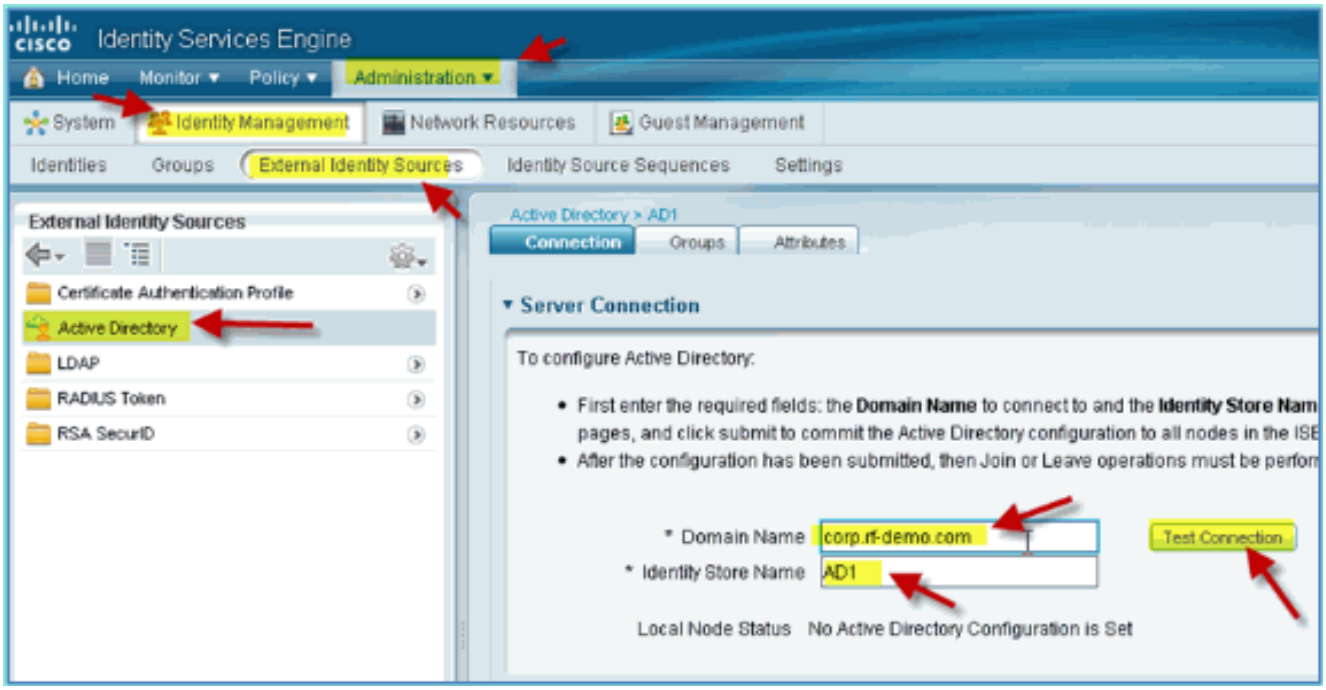
Integrazione con Active Directory in Windows 2008

ISE può comunicare direttamente con Active Directory (AD) per l'autenticazione di utenti/computer o per il recupero delle informazioni di autorizzazione e degli attributi utente. Per comunicare con AD, ISE deve essere 'aggiunto' a un dominio AD. In questo esercizio si aggiungerà ISE a un dominio AD e si verificherà che la comunicazione AD funzioni correttamente.

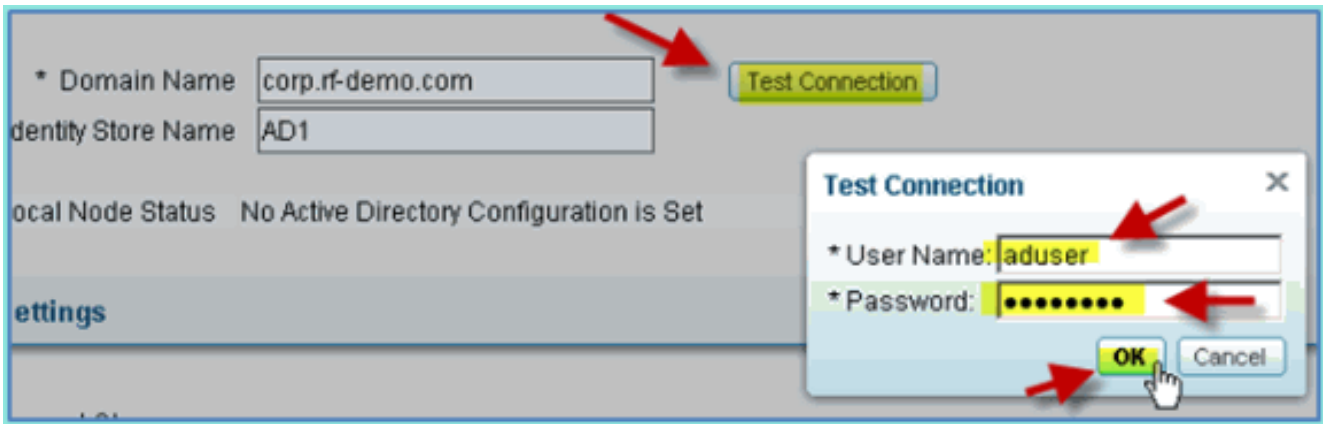
Attenersi alla seguente procedura:

1. Per aggiungere ISE al dominio AD, da ISE andare in **Amministrazione > Gestione delle identità > Origini identità esterne**.


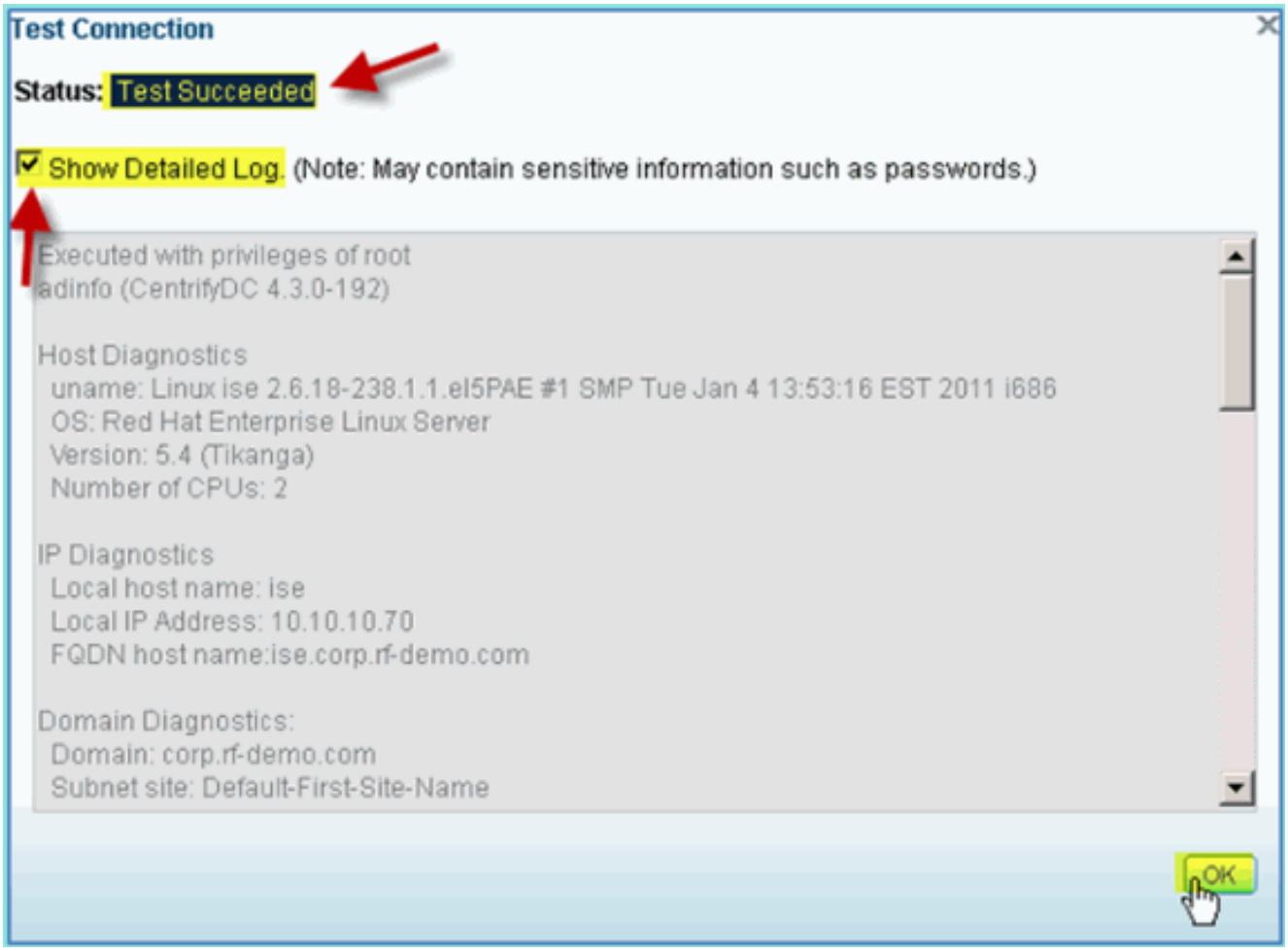
2. Nel riquadro di sinistra (Origini identità esterne), selezionare **Active Directory**.
3. Sul lato destro, selezionare la scheda **Connessione** e immettere quanto segue:Nome dominio: corp.rf-demo.comNome archivio identità:
AD1



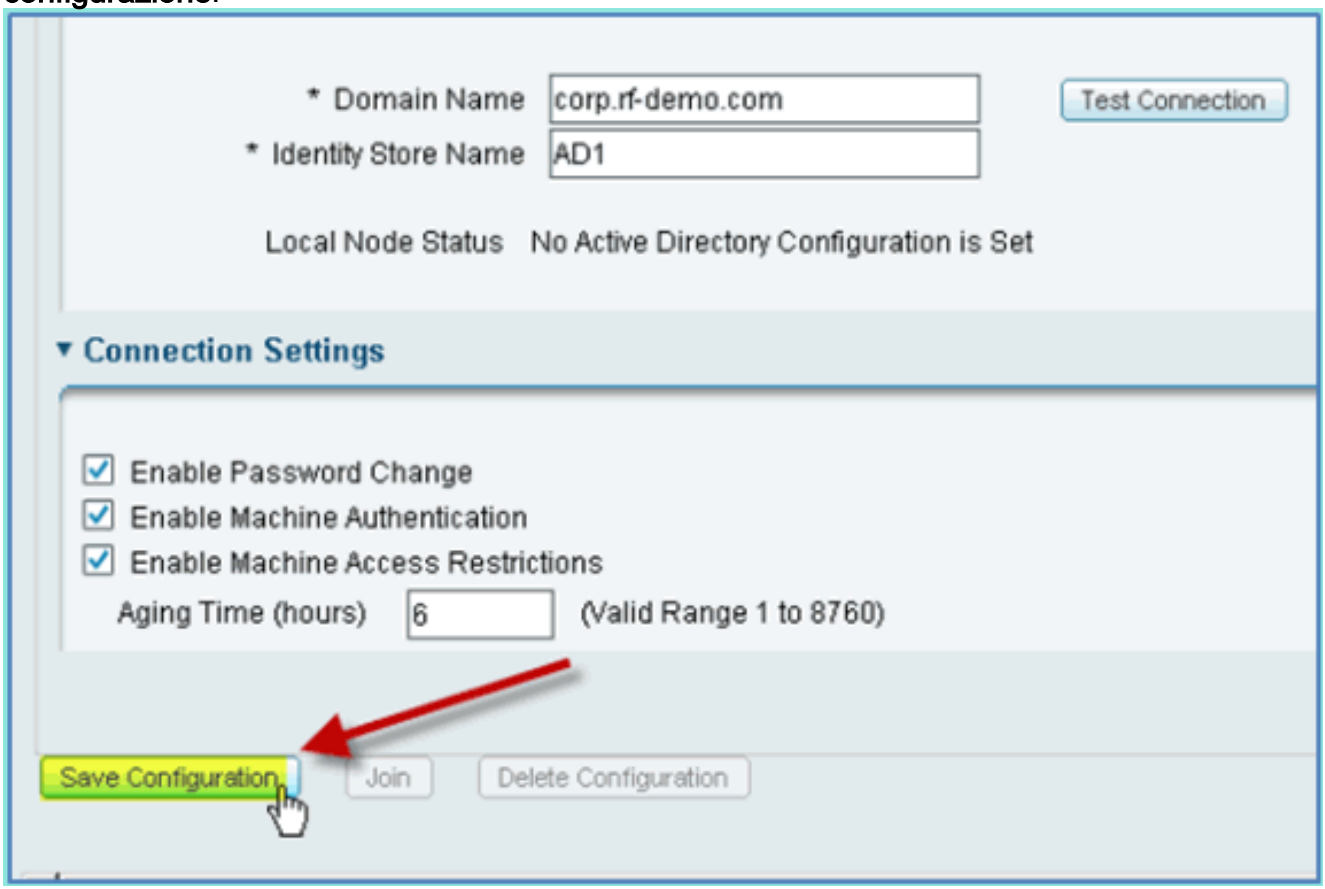
4. Fare clic su **Test connessione**. Immettere il nome utente AD (aduser/Cisco123), quindi fare clic su
OK.



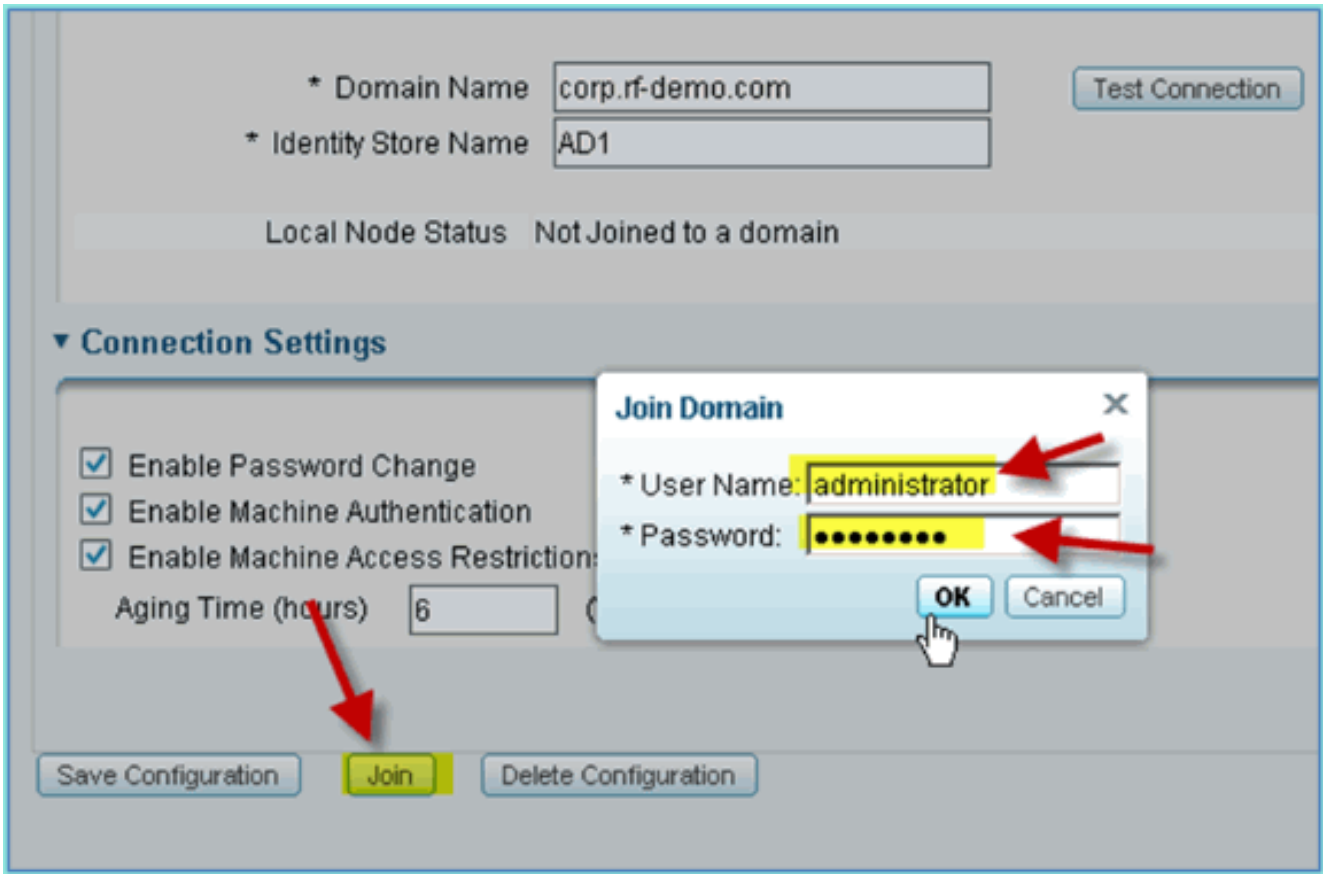
5. Confermare che in Stato test sia visualizzato **Test riuscito**.
6. Selezionare Mostra registro dettagliato e osservare i dettagli utili per la risoluzione dei problemi. Fare clic su **OK** per
continuare.



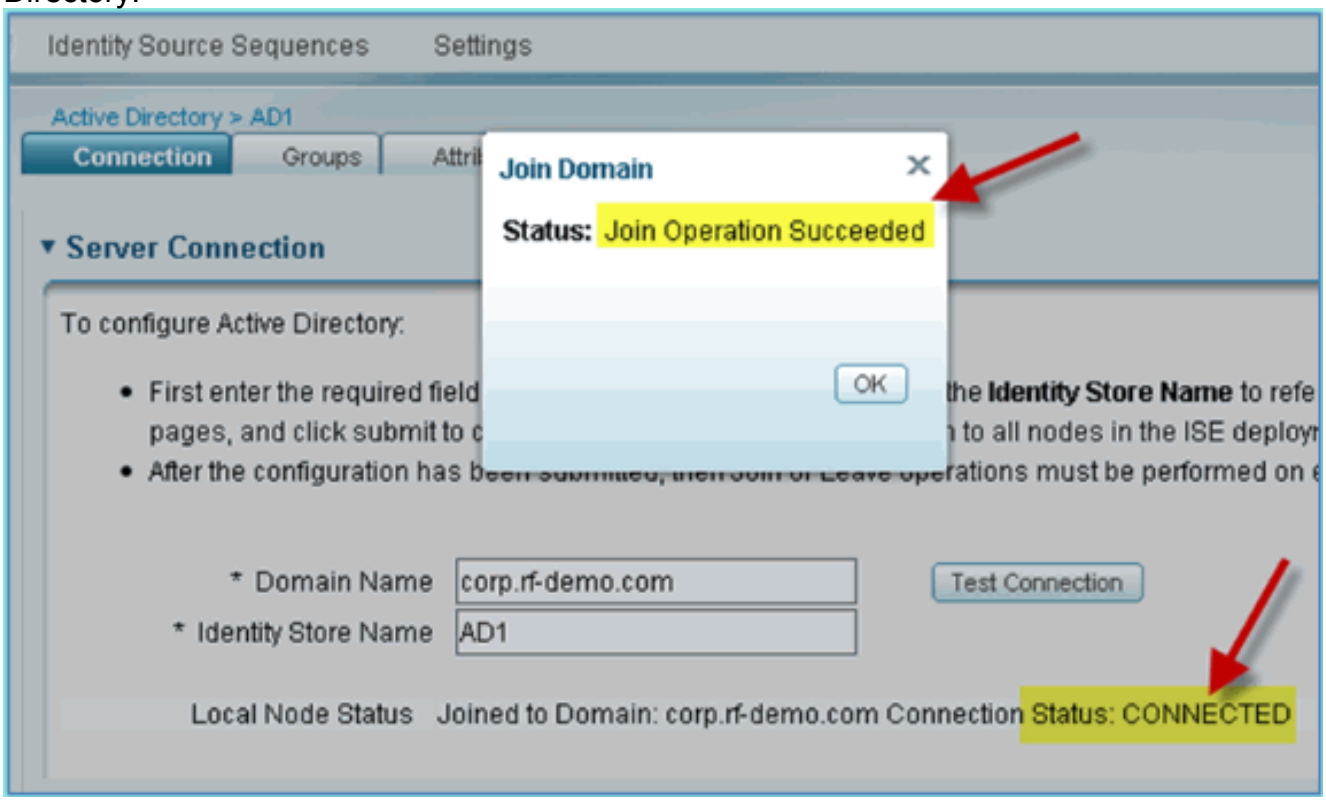
7. Fare clic su **Salva configurazione**.



8. Fare clic su **Partecipa**. Immettere l'utente AD (administrator/Cisco123), quindi fare clic su **OK**.



9. Confermare che in Stato operazione di join sia indicato **Completato**, quindi fare clic su **OK** per continuare.Nel campo Stato connessione server viene visualizzato **CONNESSO**. Se lo stato cambia in qualsiasi momento, una connessione di prova consente di risolvere i problemi relativi alle operazioni di Active Directory.



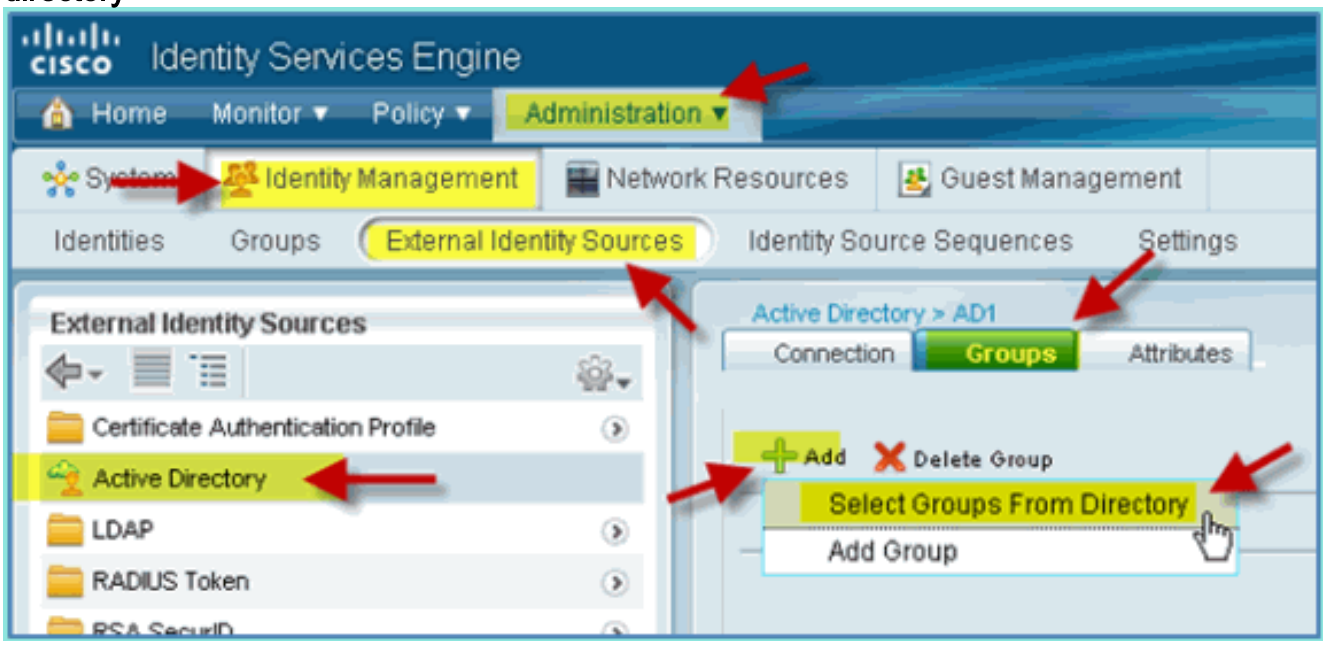
Aggiungi gruppi di Active Directory

Quando si aggiungono gruppi AD, è consentito un controllo più granulare sui criteri ISE. Ad esempio, i gruppi AD possono essere differenziati in base ai ruoli funzionali, come i gruppi Dipendente o Appaltatore, senza che il bug correlato venga riscontrato nelle precedenti esercitazioni ISE 1.0 in cui le policy erano limitate solo agli utenti.

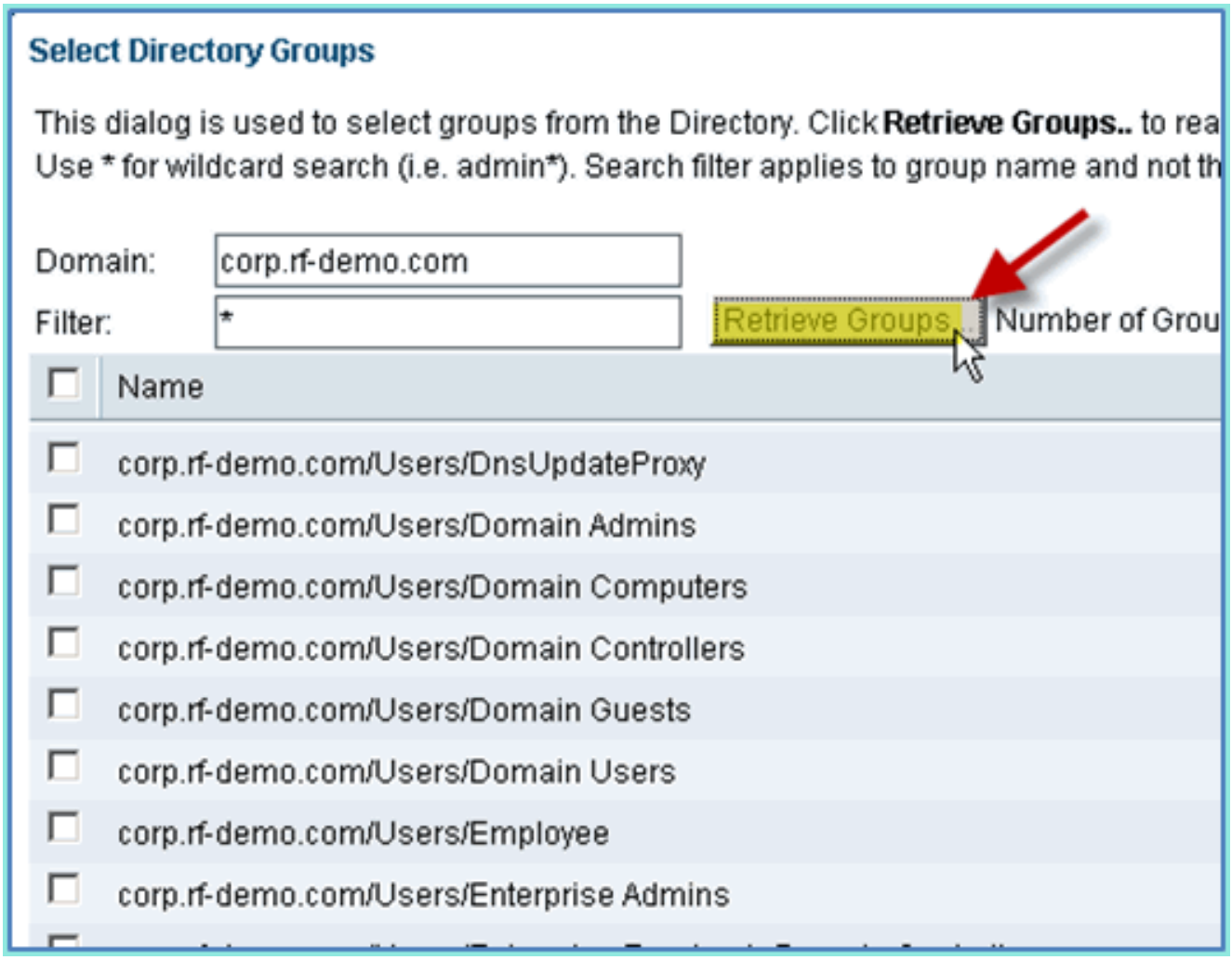
In questa esercitazione vengono utilizzati solo il gruppo Domain Users e/o il gruppo Employee.

Attenersi alla seguente procedura:

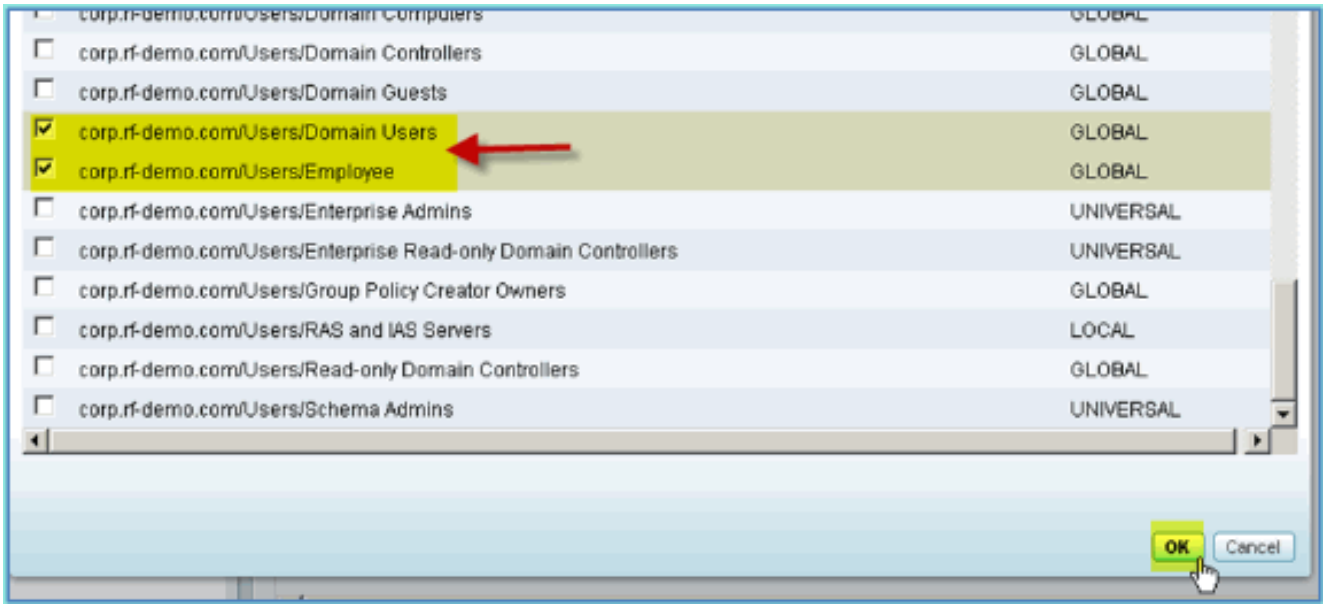
1. Da ISE, andare a **Amministrazione > Gestione delle identità > Origini identità esterne**.
2. Selezionare **Active Directory >** scheda **Gruppi**.
3. Fare clic su **+Aggiungi**, quindi su **Seleziona gruppi dalla directory**.



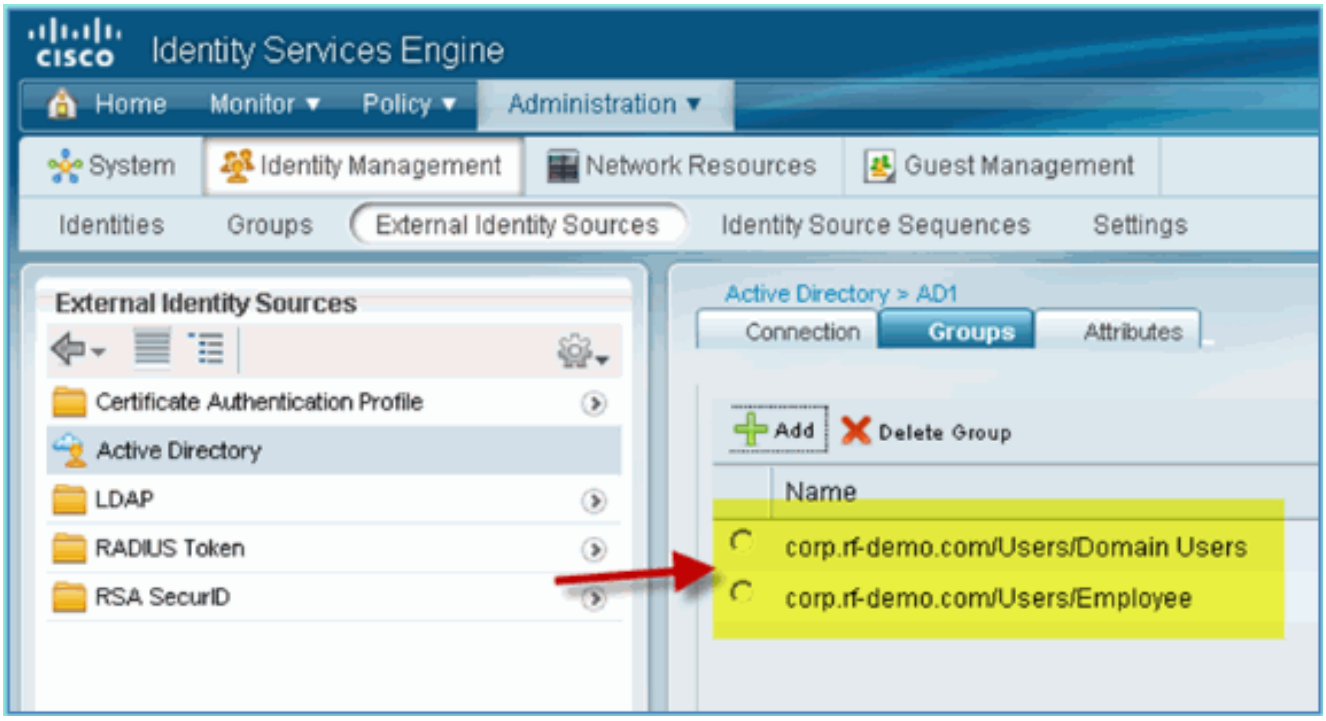
4. Nella finestra di completamento (Seleziona gruppi di directory), accettare le impostazioni predefinite per dominio (corp-rf-demo.com) e Filtro (*). Quindi, fare clic su **Recupera gruppi**.



5. Selezionare le caselle relative ai gruppi **Domain Users** e **Employee**. Al termine, fare clic su **OK**.



6. Confermare che i gruppi sono stati aggiunti all'elenco.

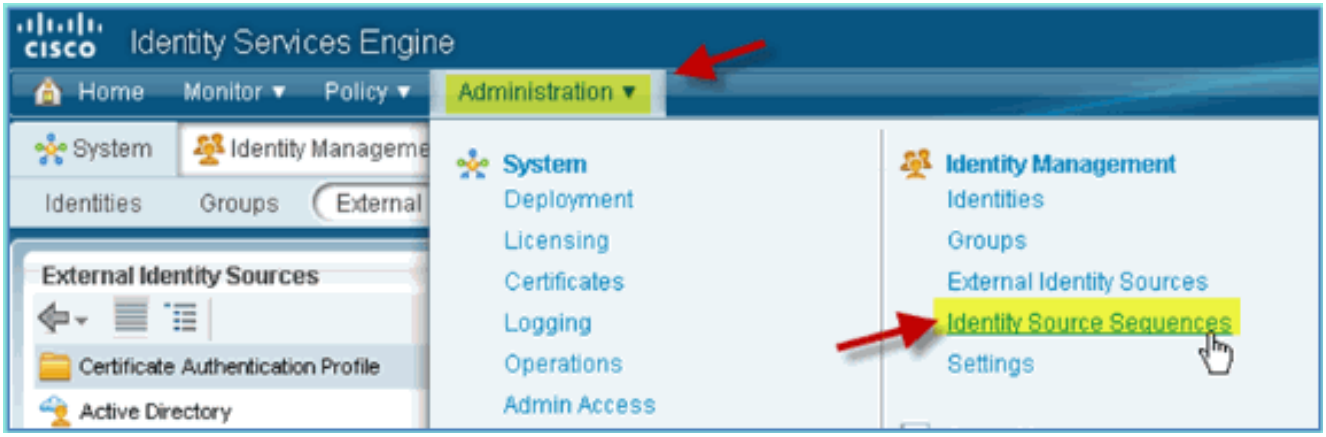


Aggiungi sequenza origine identità

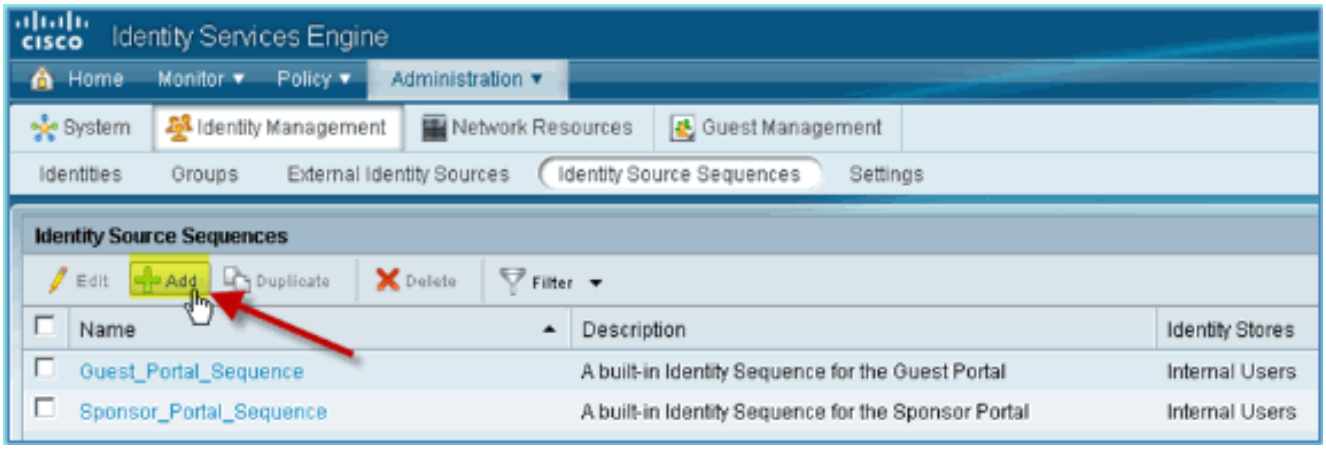
Per impostazione predefinita, ISE è impostato per l'utilizzo di Internal Users per l'archivio di autenticazione. Se si aggiunge AD, è possibile creare un ordine di priorità della sequenza per includere l'AD che ISE utilizzerà per verificare l'autenticazione.

Attenersi alla seguente procedura:

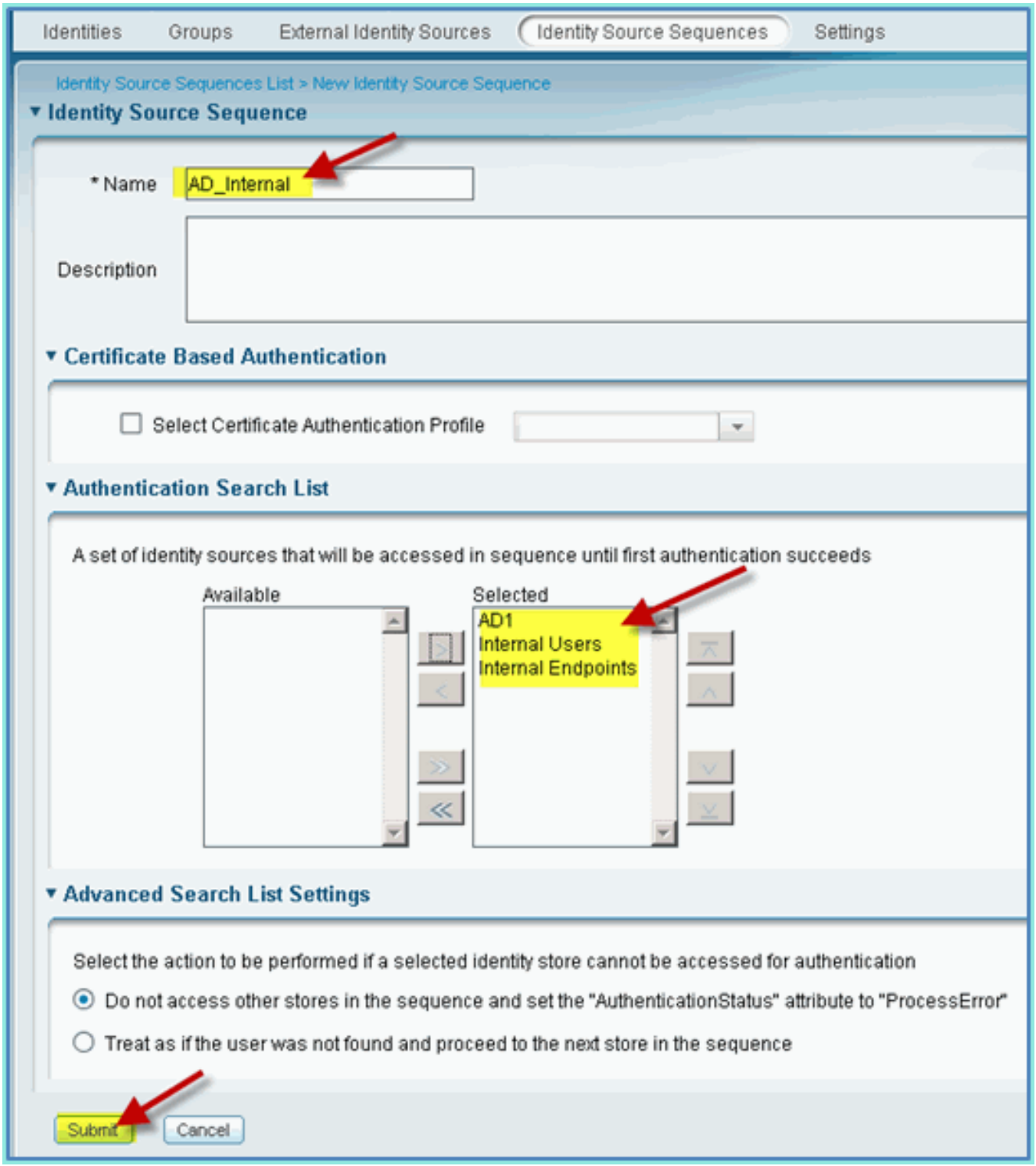
1. Da ISE, passare a **Amministrazione > Gestione delle identità > Sequenze origine identità**.



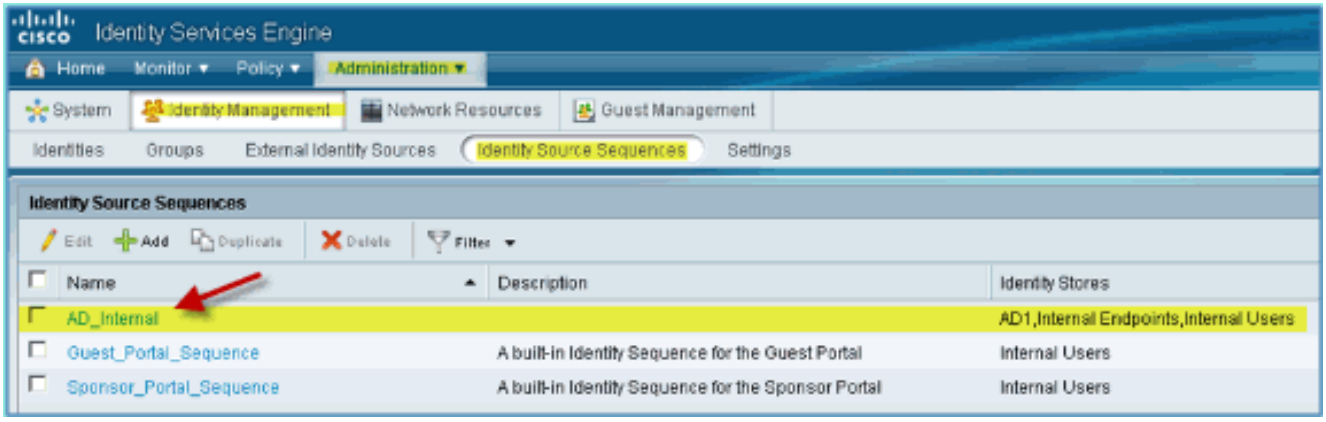
2. Per aggiungere una nuova sequenza, fare clic su **+Aggiungi**.



3. Immettere il nuovo nome: **AD_Internal**. Aggiungere tutte le origini disponibili al campo Selezionato. Riordinare quindi in base alle esigenze in modo che AD1 venga spostato all'inizio dell'elenco. Fare clic su **Invia**.



4. Confermare che la sequenza è stata aggiunta all'elenco.

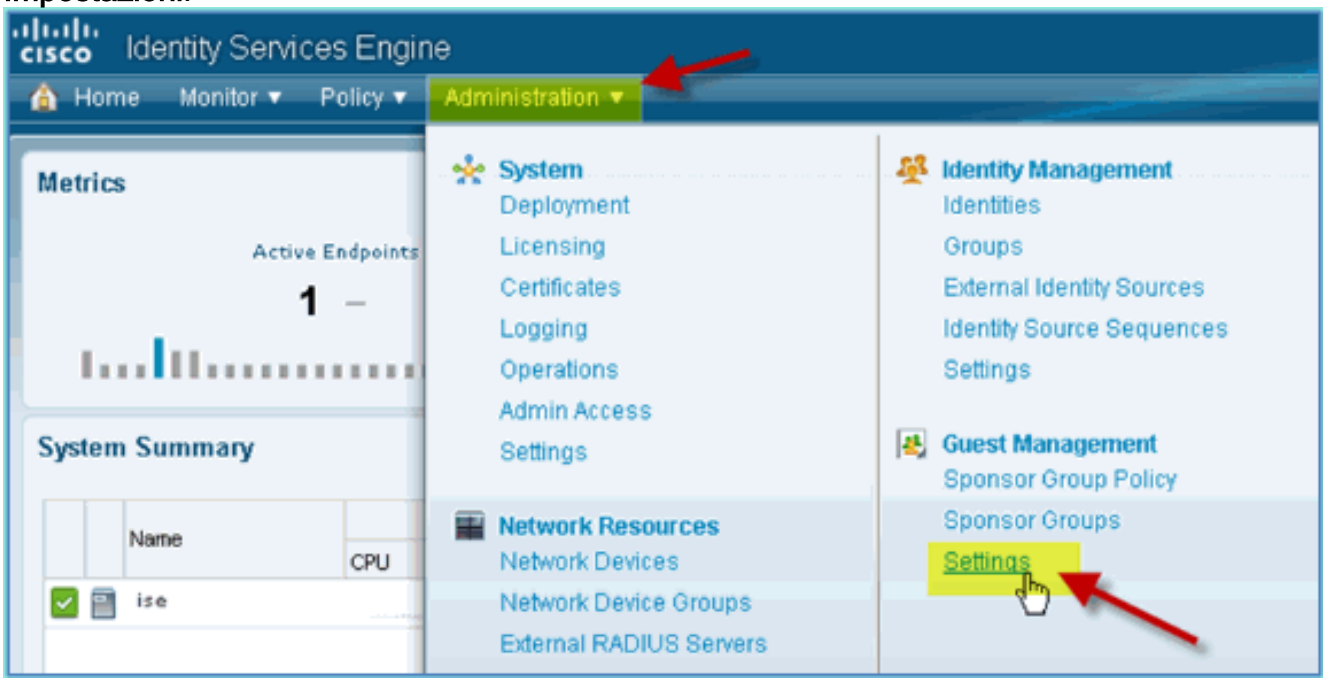


ISE Wireless Sponsored Guest Access con AD integrato

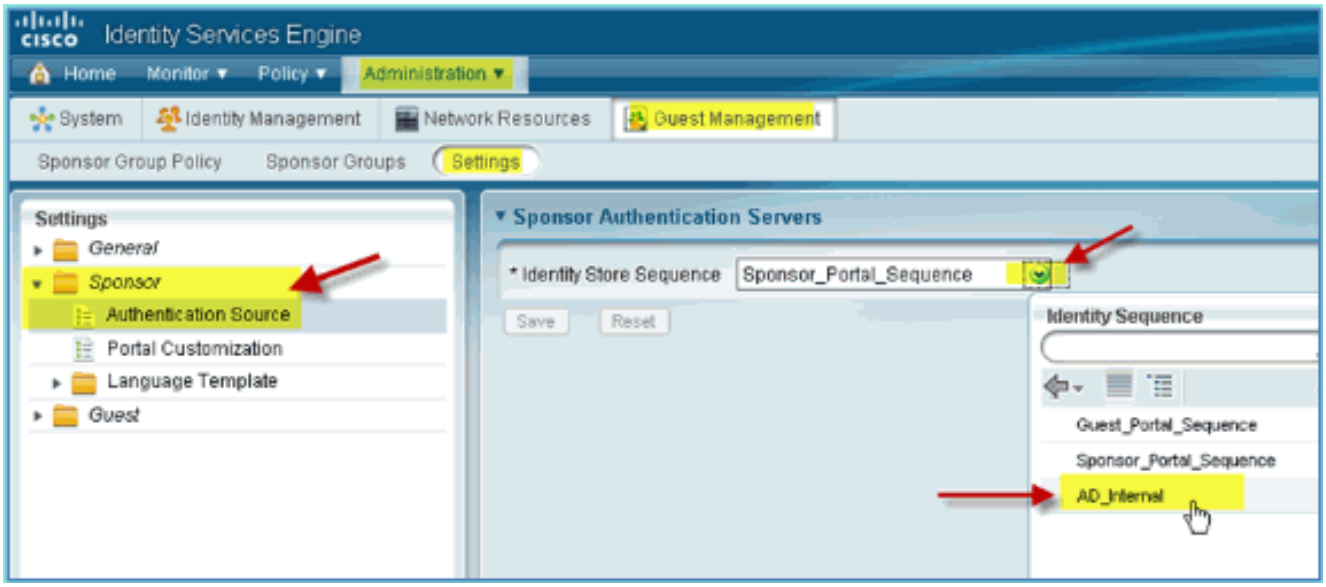
Èpossibile configurare ISE in modo da consentire agli utenti guest di essere sponsorizzati con policy che consentano agli utenti del dominio AD di sponsorizzare l'accesso guest.

Attenersi alla seguente procedura:

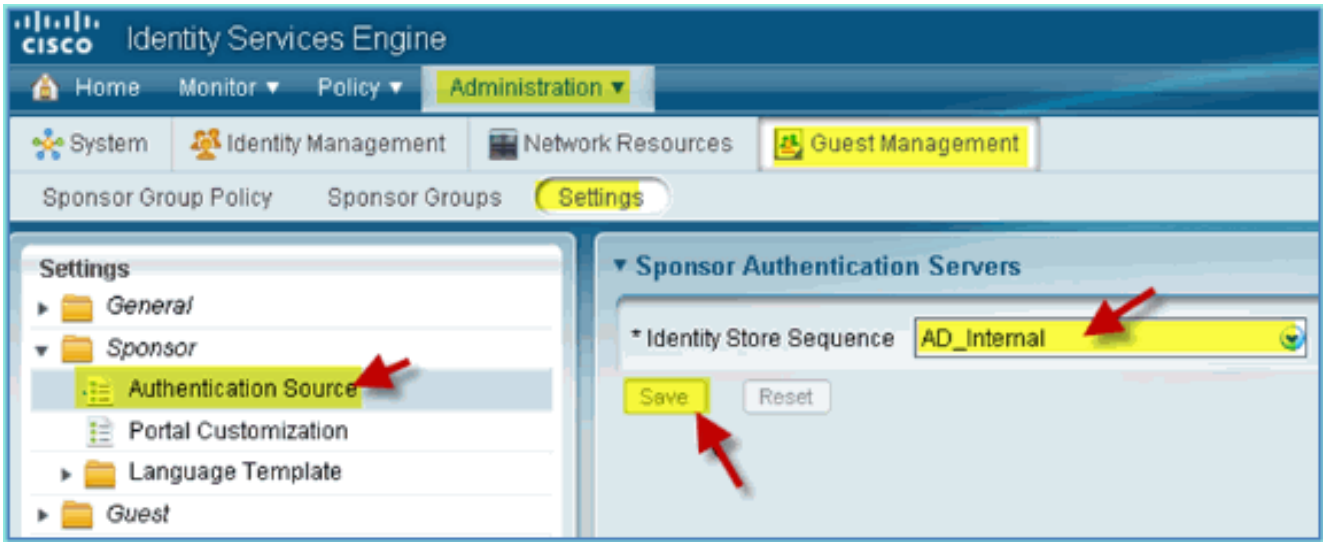
1. Da ISE, selezionare **Amministrazione > Gestione guest > Impostazioni**.



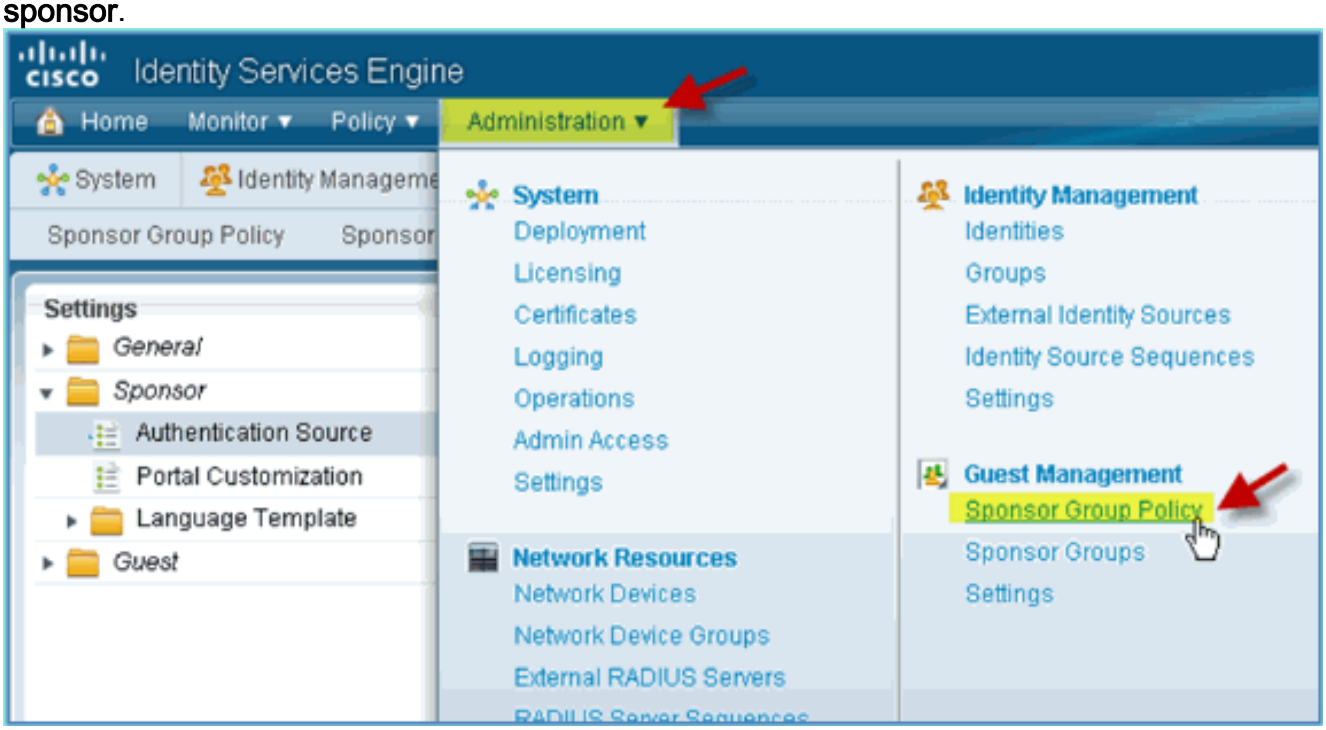
2. Espandere **Sponsor**, quindi fare clic su **Origine autenticazione**. Quindi, selezionare **AD_Internal** come Sequenza archivio identità.



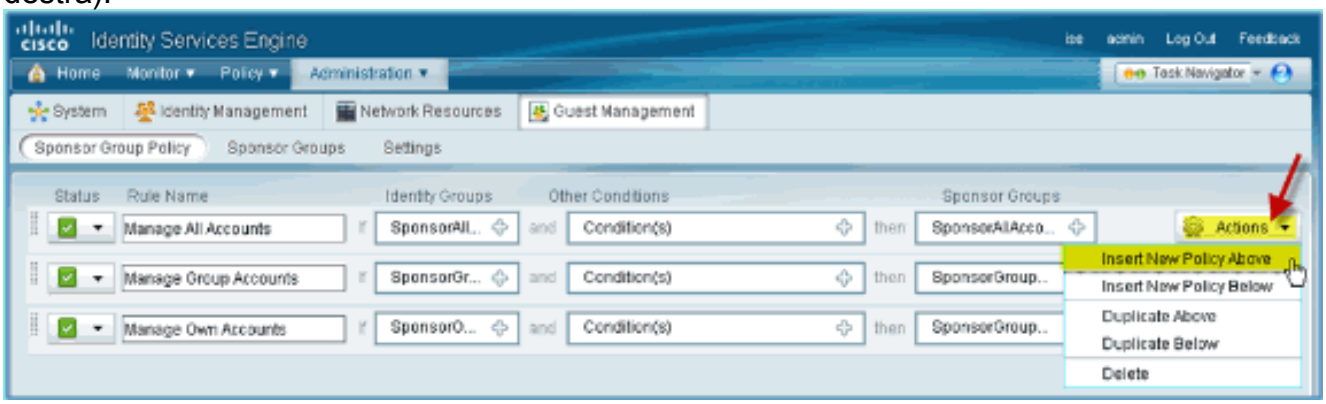
3. Confermare AD_Internal come sequenza archivio identità. Fare clic su **Salva**.



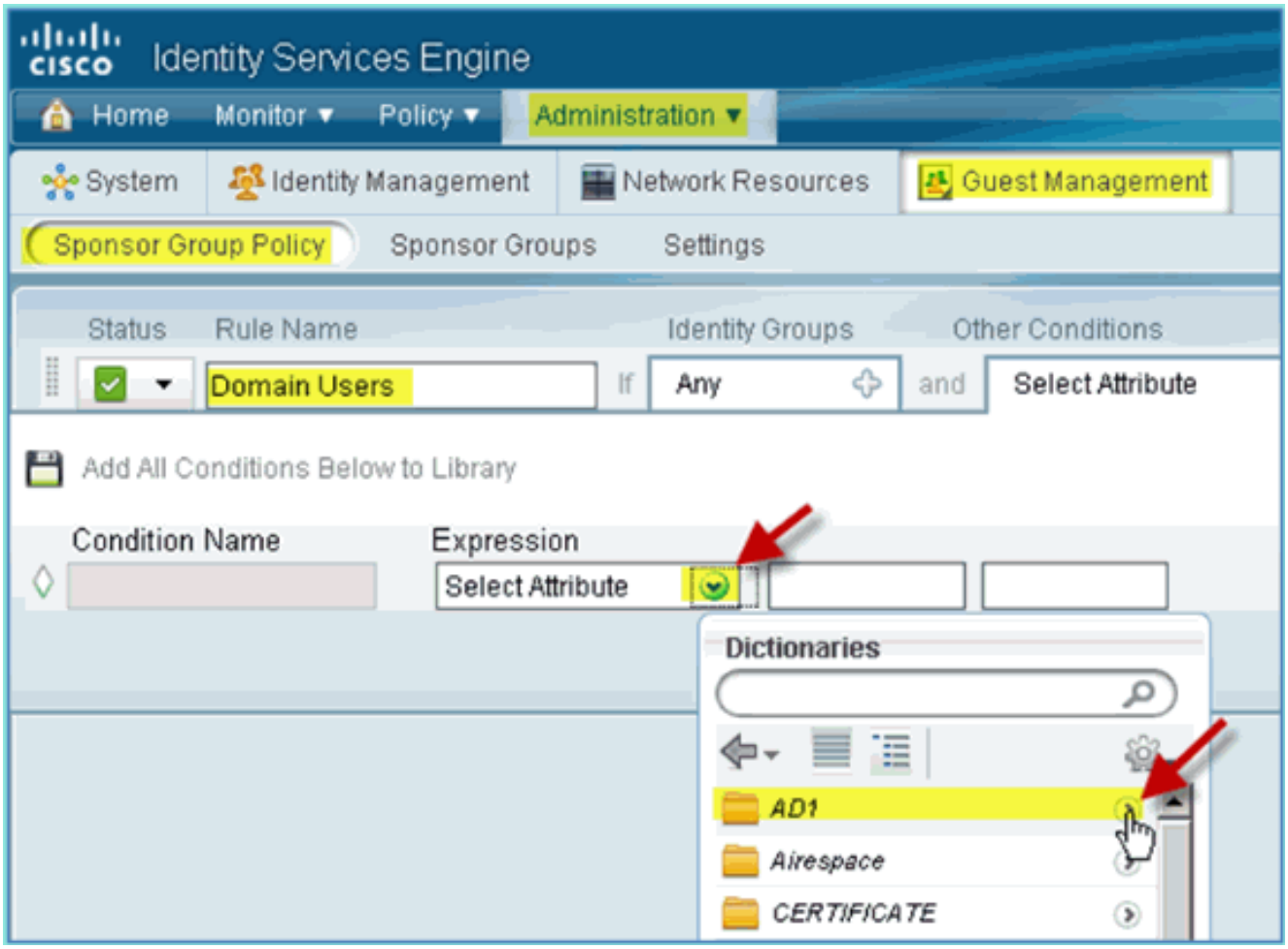
4. Passare a **Amministrazione > Gestione guest > Criteri di gruppo sponsor**.



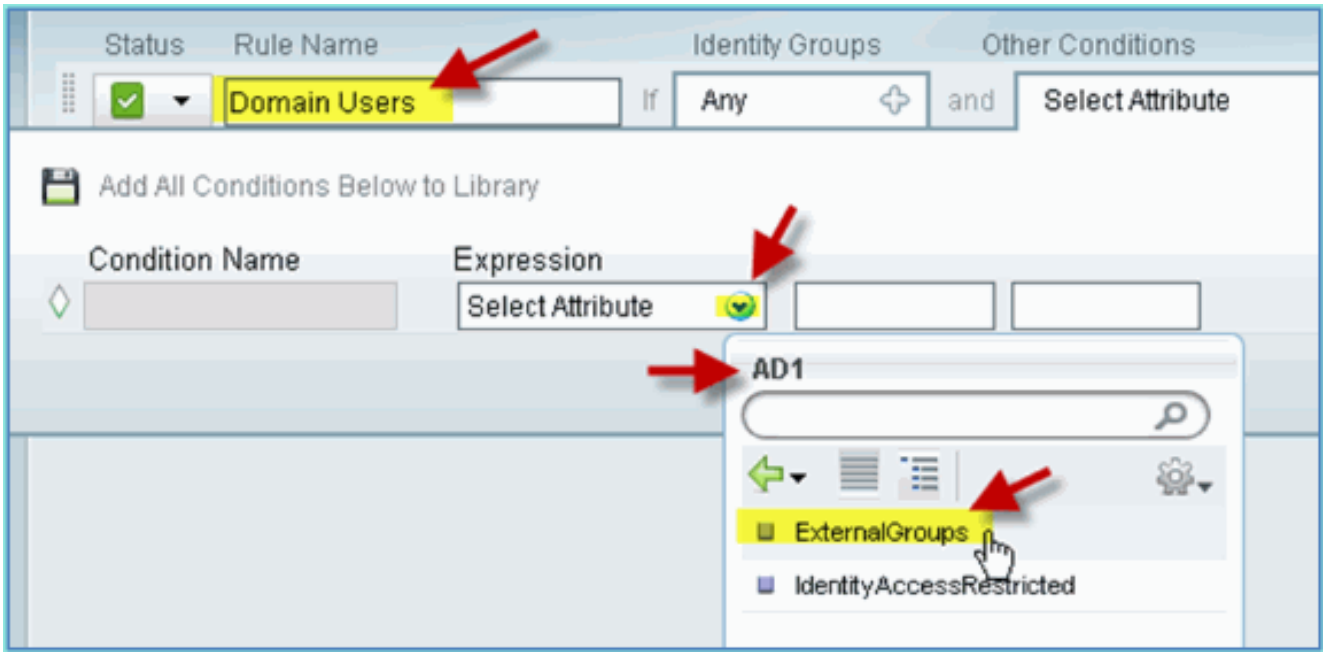
5. Inserisci nuovo criterio sopra la prima regola (fare clic sull'icona **Azioni** a destra).



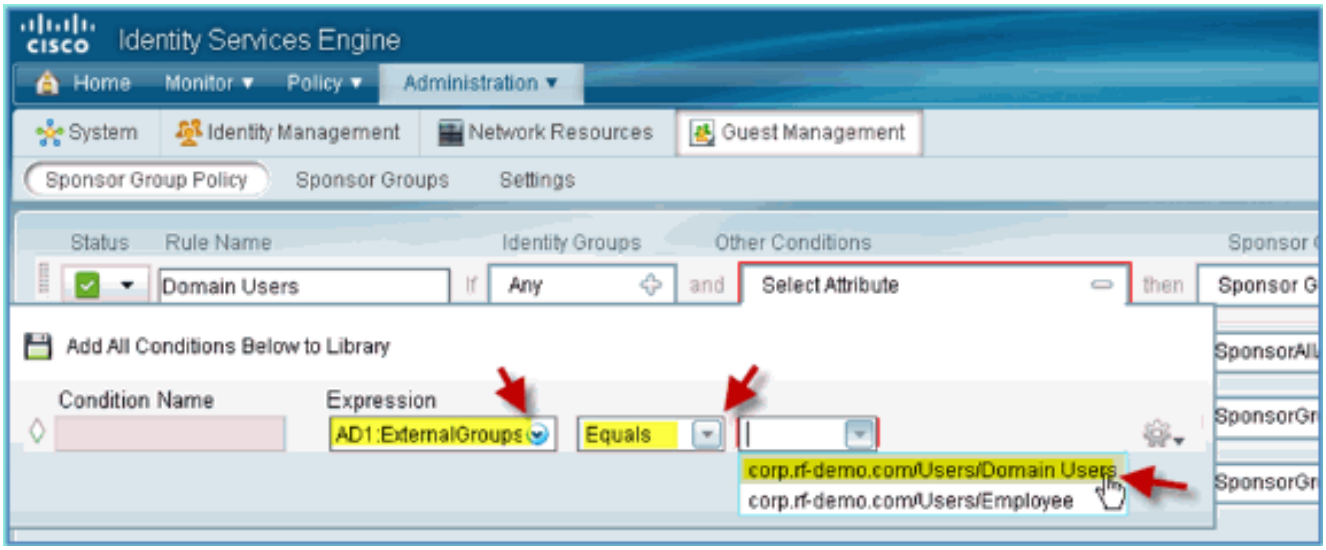
6. Per i nuovi Criteri di gruppo per gli sponsor, creare quanto segue:Nome regola: Utenti dominioGruppi di identità: qualsiasiAltre condizioni: (Crea nuovo/Avanzate) > AD1



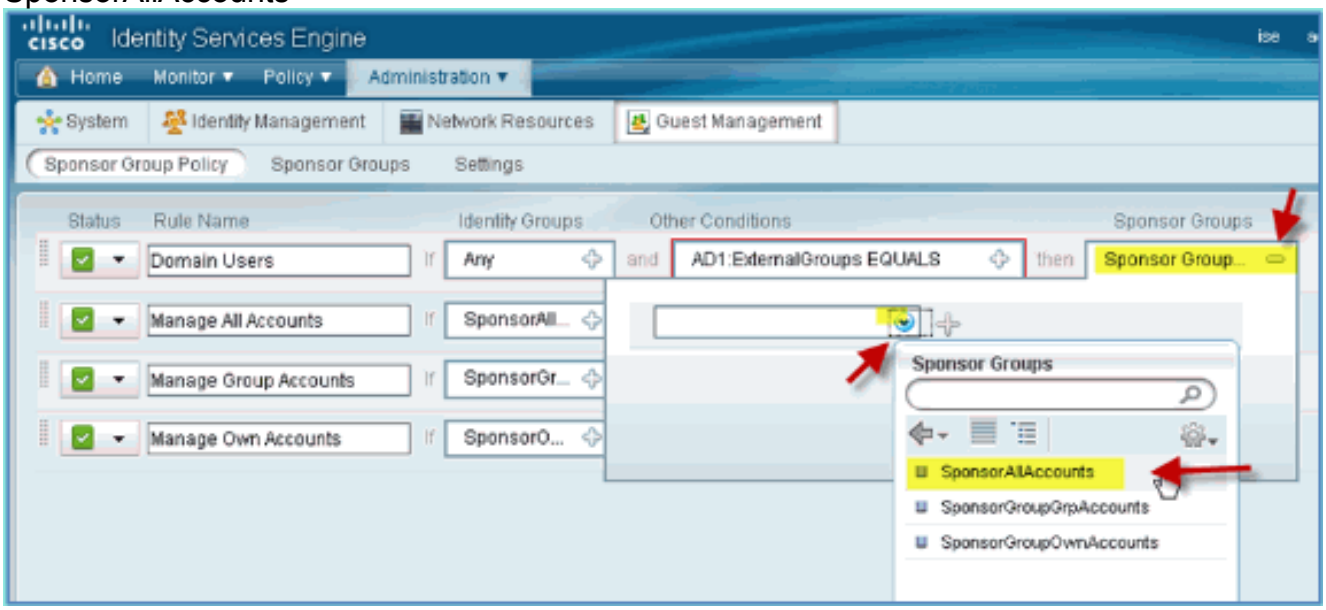
AD1: Gruppi esterni



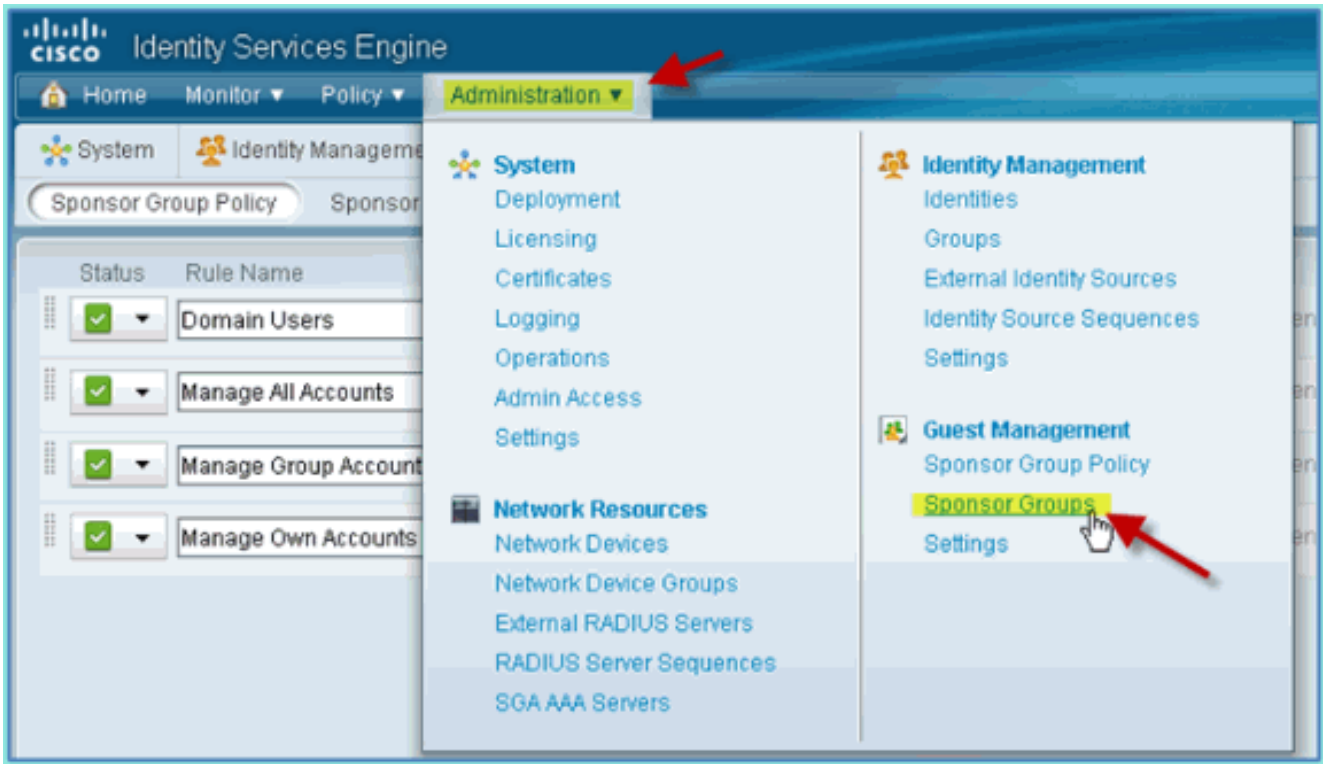
Gruppi esterni AD1 > Uguale a > corp.rf-demo.com/Users/Domain Utenti



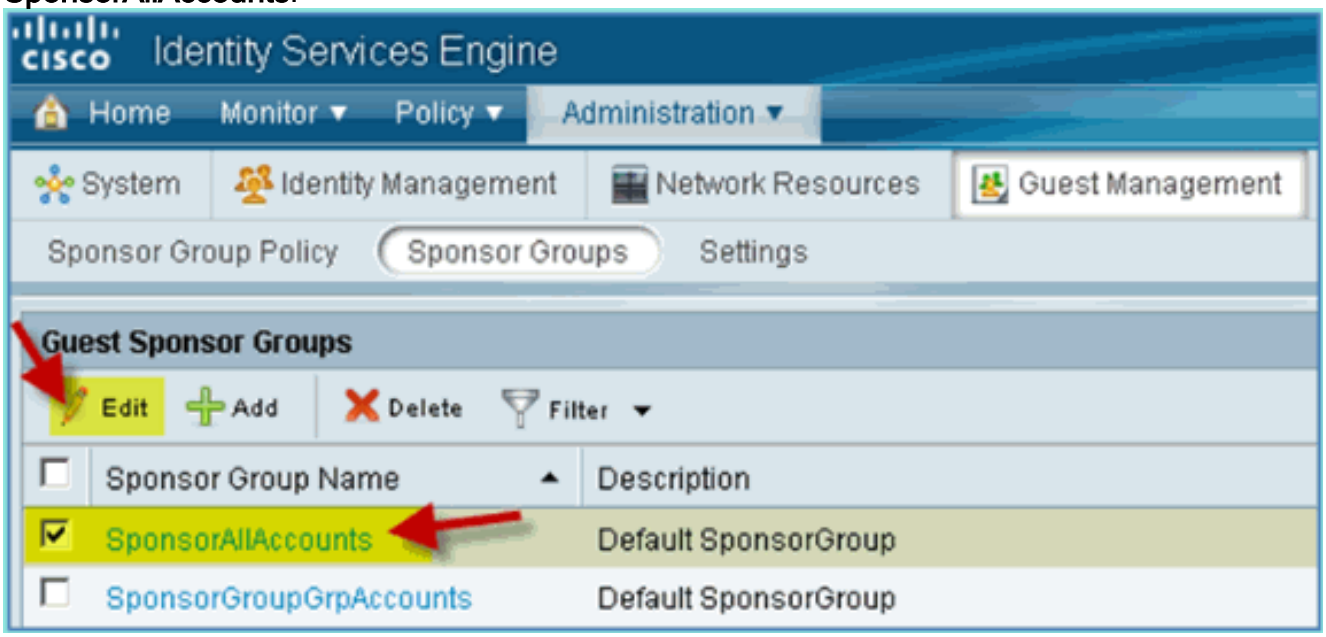
7. In Gruppi di sponsor, impostare quanto segue:Gruppi di sponsor: SponsorAllAccounts



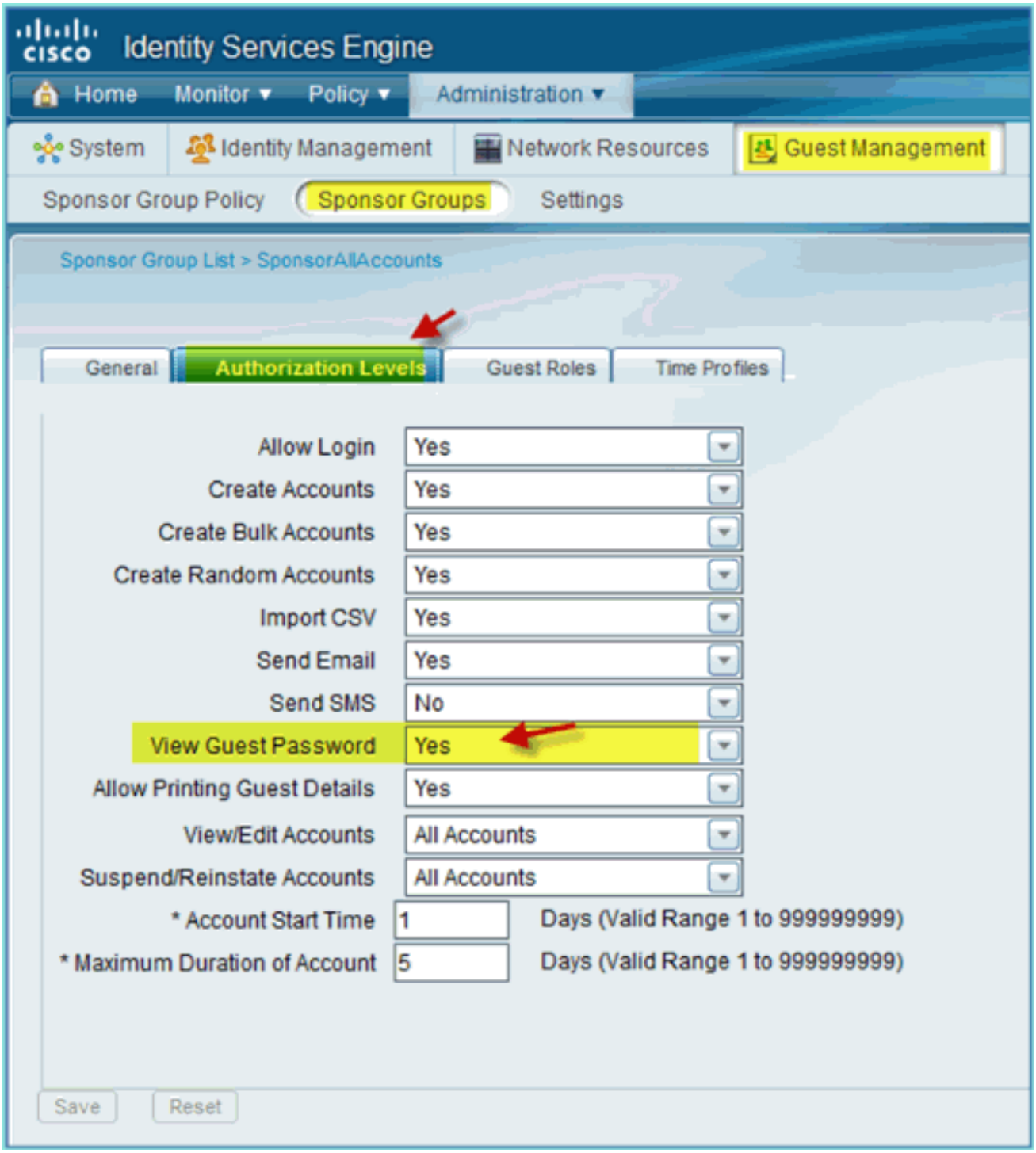
8. Passare a **Amministrazione > Gestione guest > Gruppi sponsor**.



9. Selezionare Modifica > SponsorAllAccounts.



10. Selezionare Livelli di autorizzazione e impostare quanto segue:Visualizza password guest: Sì



Configurazione di SPAN sullo switch

Configure SPAN - L'interfaccia di gestione/probe ISE è l2 adiacente all'interfaccia di gestione WLC. Lo switch può essere configurato su SPAN e su altre interfacce, ad esempio VLAN di interfaccia per dipendenti e ospiti.

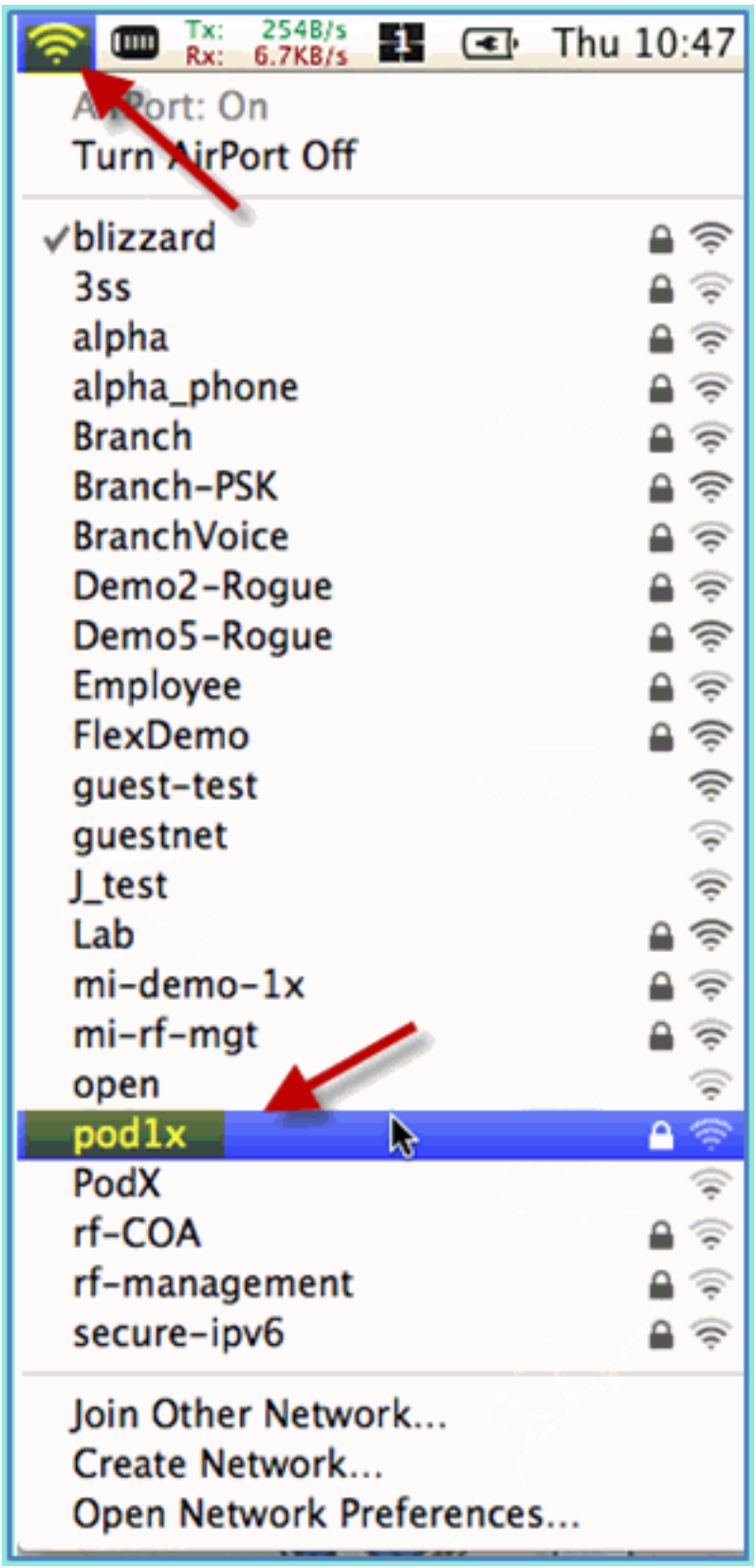
```
Podswitch(config)#monitor session 1 source vlan10 , 11 , 12
Podswitch(config)#monitor session 1 destination interface Fa0/8
ISE virtual probe interface.
```

Riferimento: Autenticazione wireless per Apple MAC OS X

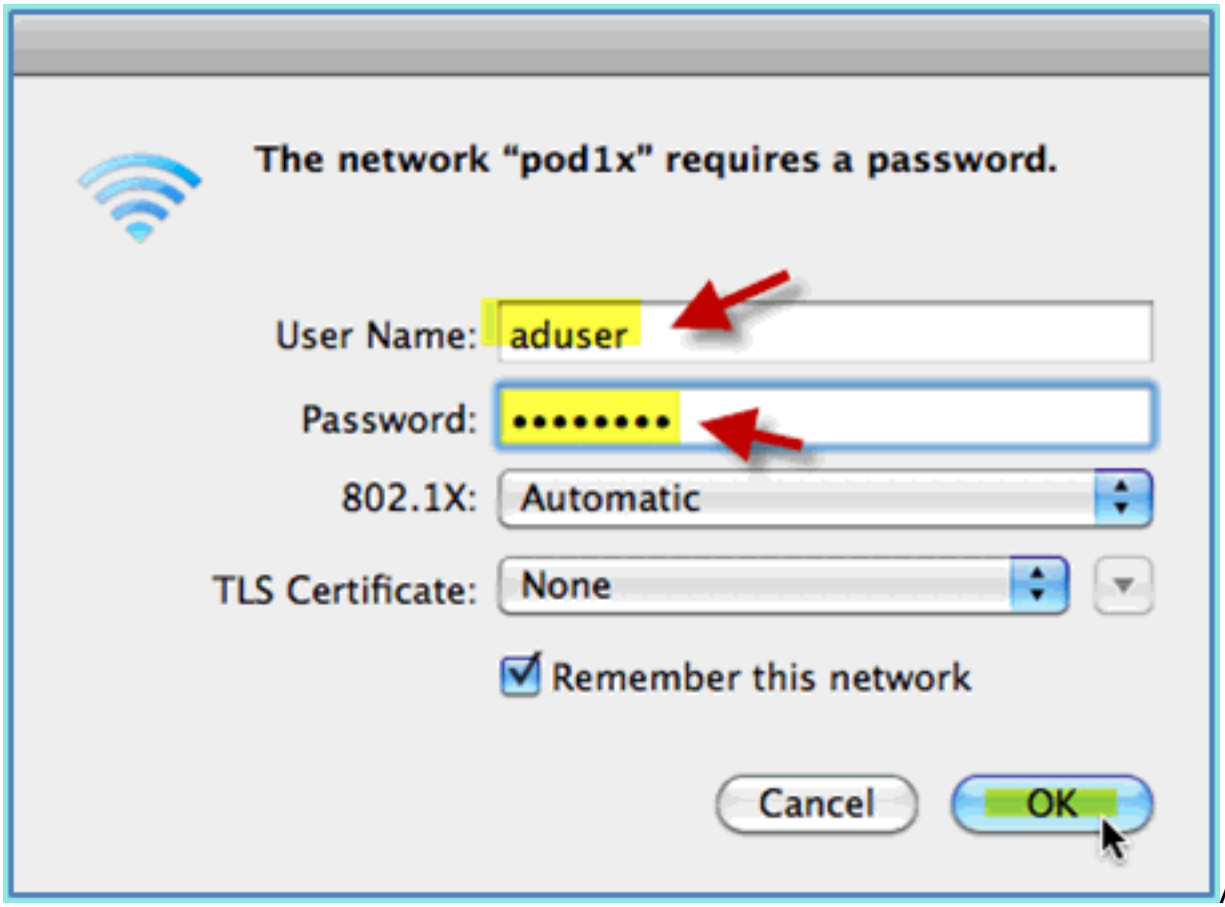
Associarsi al WLC tramite un SSID autenticato come utente INTERNO (o utente AD integrato)

utilizzando un laptop wireless Apple Mac OS X. Ignorare se non applicabile.

1. Su un Mac, vai alle impostazioni WLAN. Attivare WIFI, quindi selezionare e connettersi all'SSID POD 802.1X attivato creato nell'esercizio precedente.



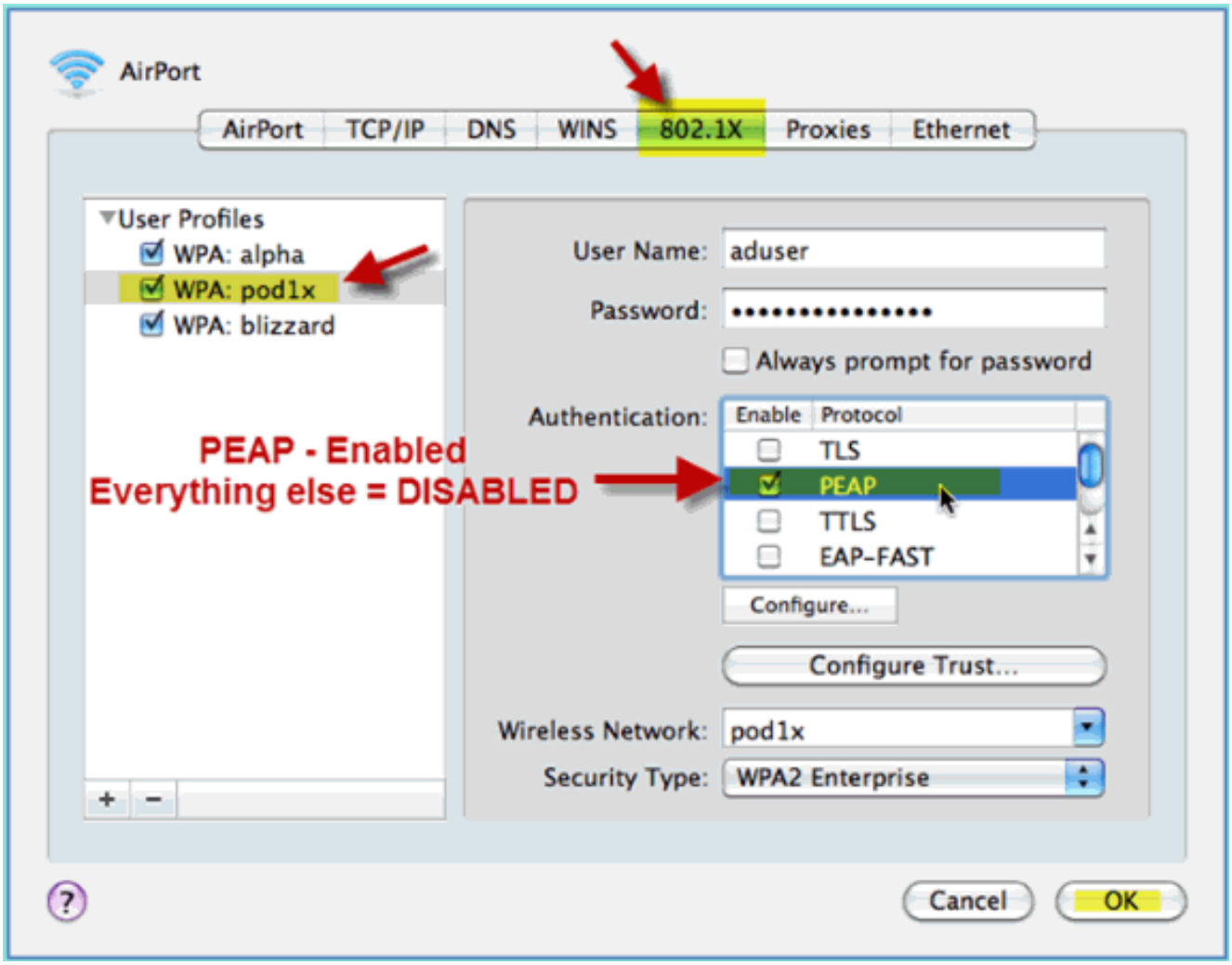
2. Fornire le seguenti informazioni per la connessione:Nome utente: aduser (se si utilizza AD), dipendente (interno - dipendente), terzista (interno - terzista)Password: XXXX802.1X: AutomaticoCertificato TLS:
nessuno



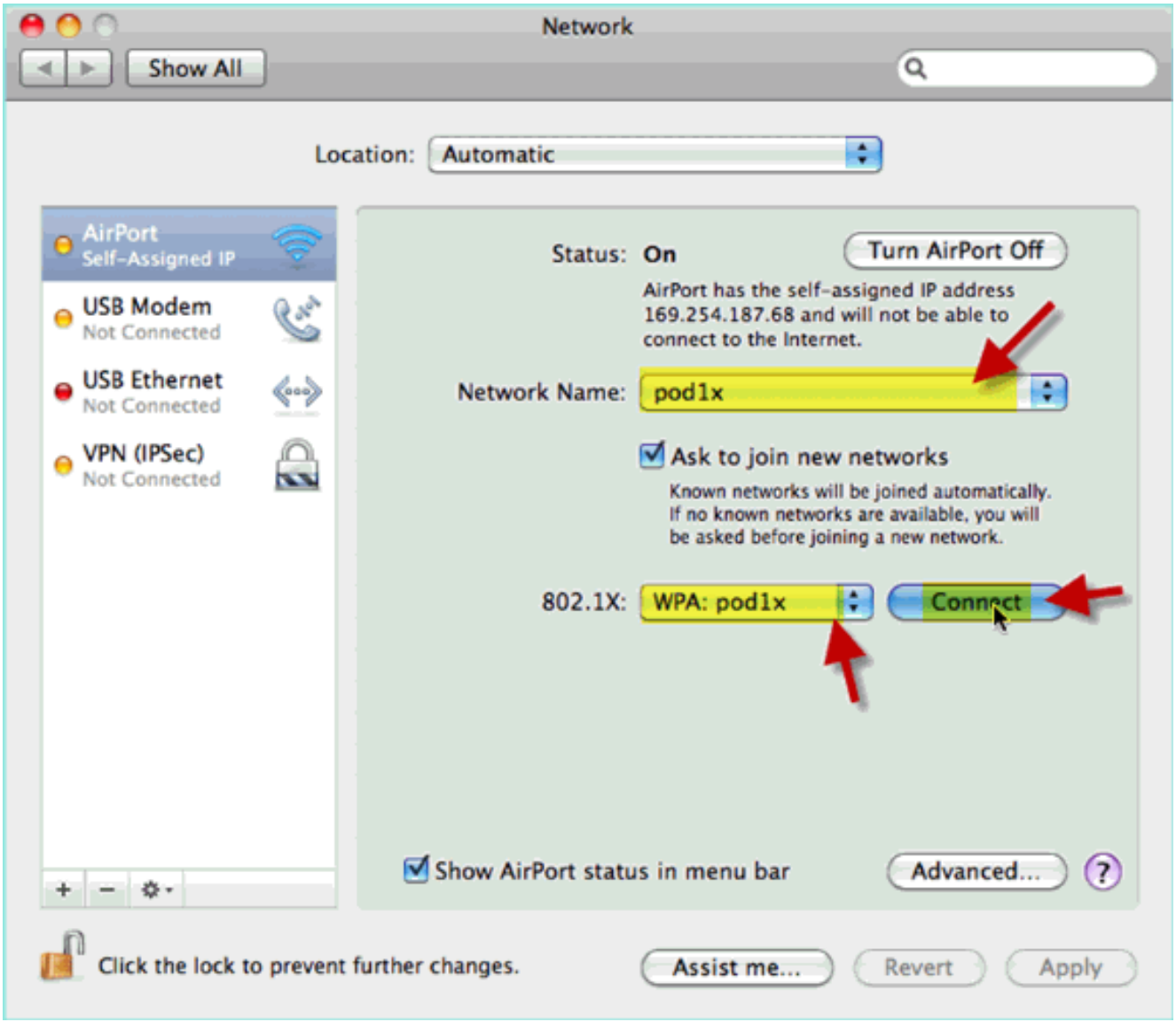
Al momento, il laptop potrebbe non connettersi. Inoltre, ISE può generare un evento di errore come segue:

```
Authentication failed :12514 EAP-TLS failed SSL/TLS handshake because of
an unknown CA in the client certificates chain
```

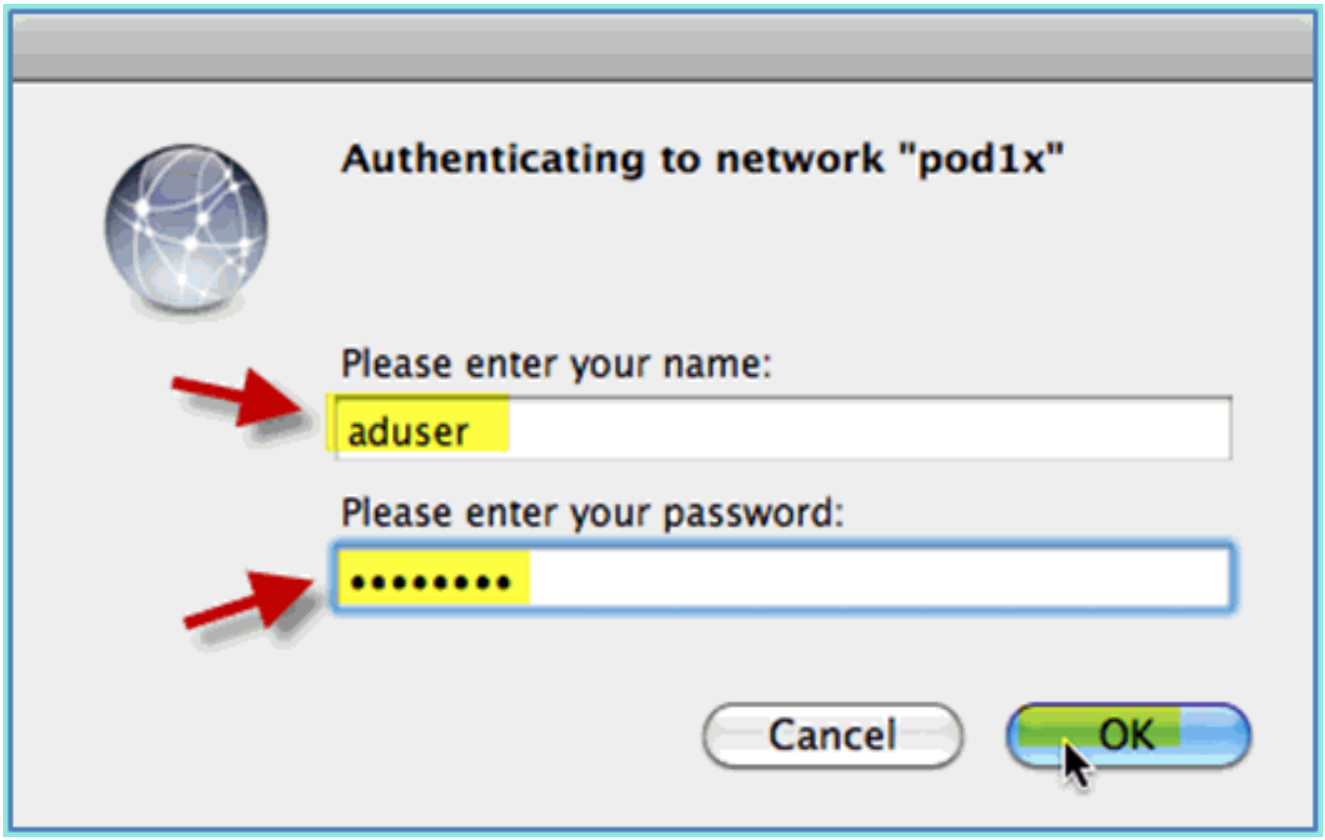
3. Selezionare **Preferenza** di **sistema > Rete > Aeroporto >** Impostazione **802.1X** e impostare la nuova autenticazione POD SSID/WPA come:TLS: disattivatoPEAP: abilitatoTTLS: disattivatoEAP-FAST:
disattivato



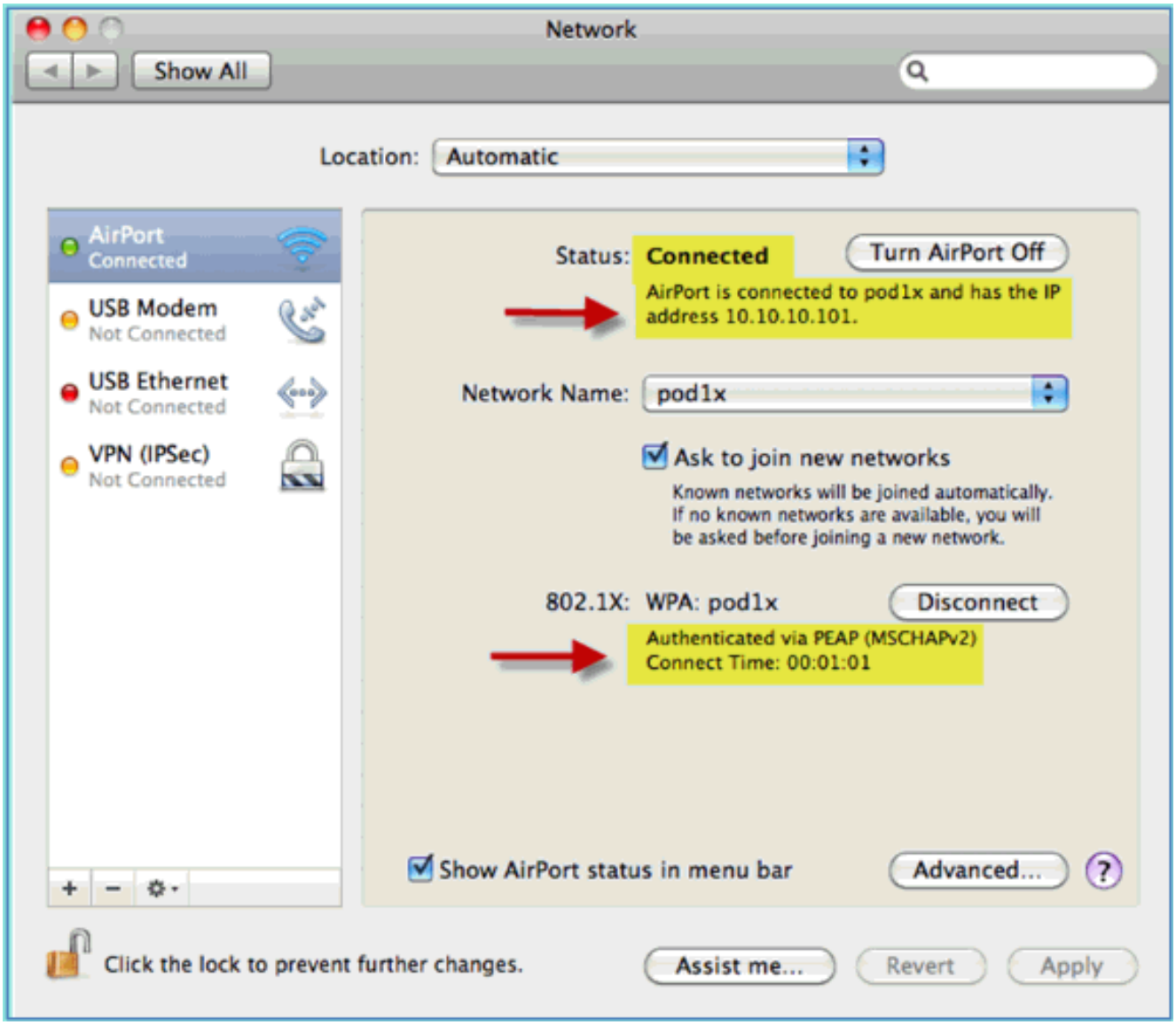
4. Fare clic su **OK** per continuare e salvare l'impostazione.
5. Nella schermata Network (Rete), selezionare il profilo SSID + 802.1X WPA appropriato e fare clic su **Connect**
   (Connetti).



6. Il sistema potrebbe richiedere un nome utente e una password. Immettere l'utente e la password di AD (aduser/XXXX), quindi fare clic su
OK.



Il client deve visualizzare **Connesso** tramite PEAP con un indirizzo IP valido.

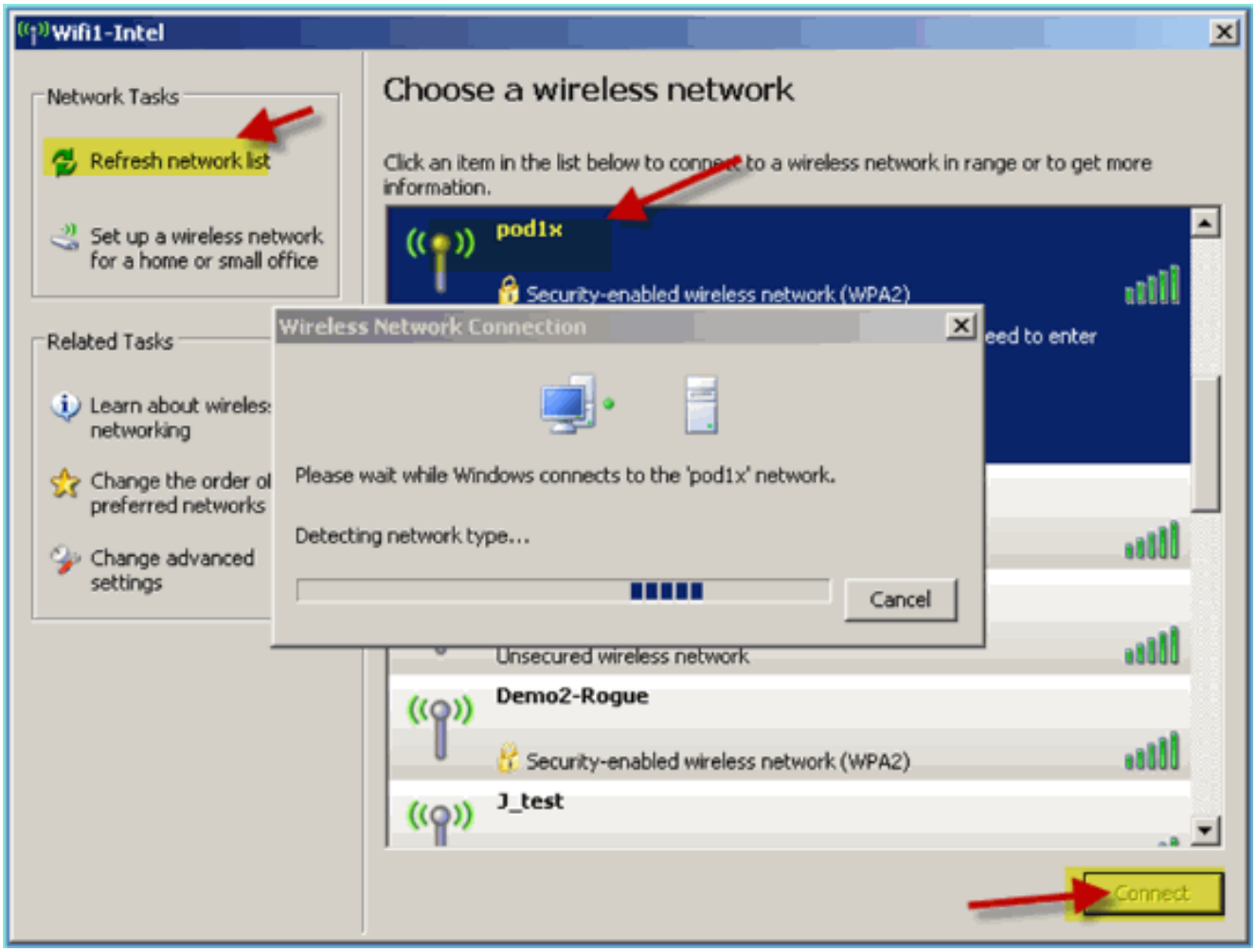


Riferimento: Autenticazione wireless per Microsoft Windows XP

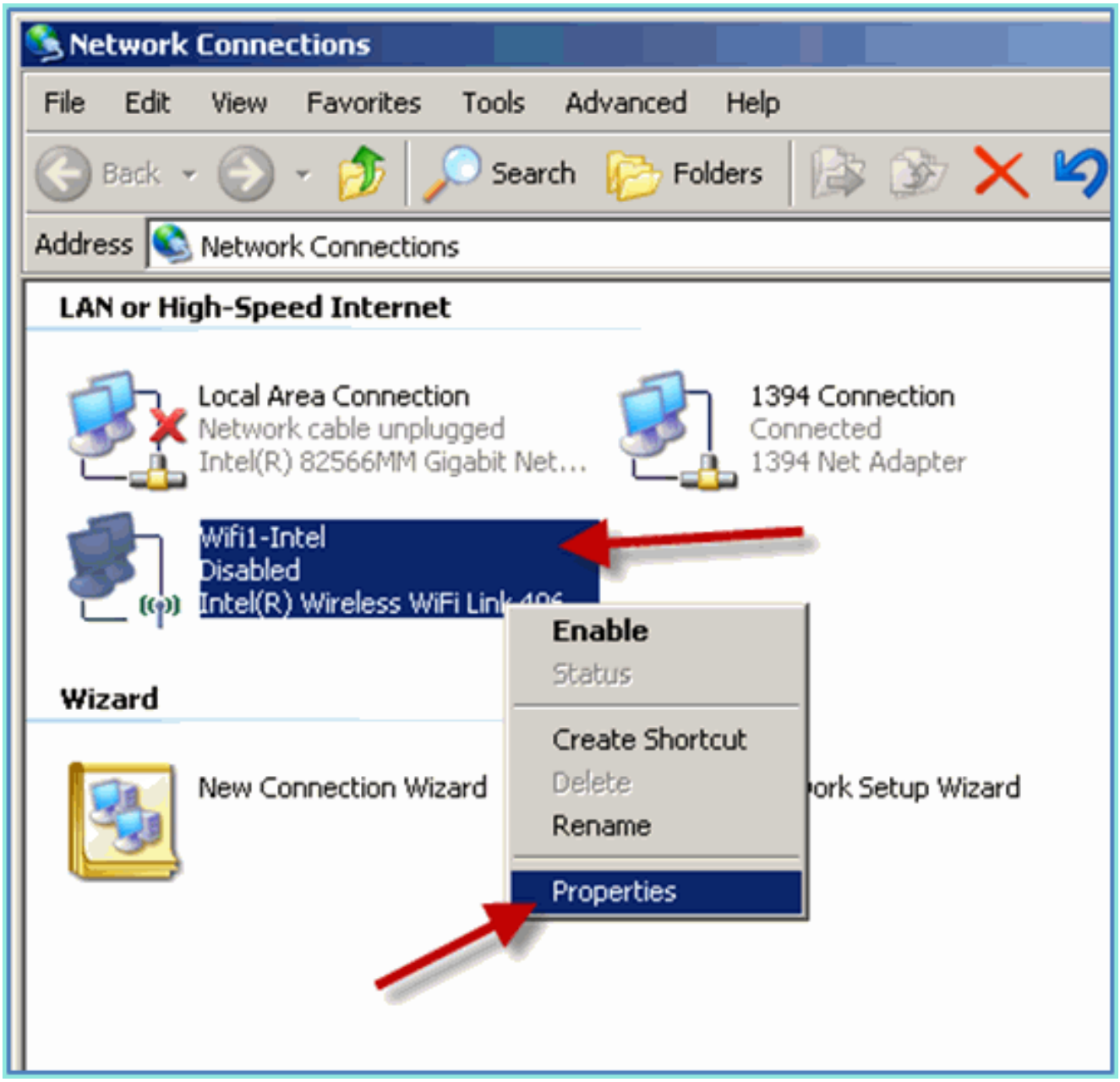
Associarsi al WLC tramite un SSID autenticato come utente INTERNO (o utente AD integrato) utilizzando un laptop wireless di Windows XP. Ignorare se non applicabile.

Attenersi alla seguente procedura:

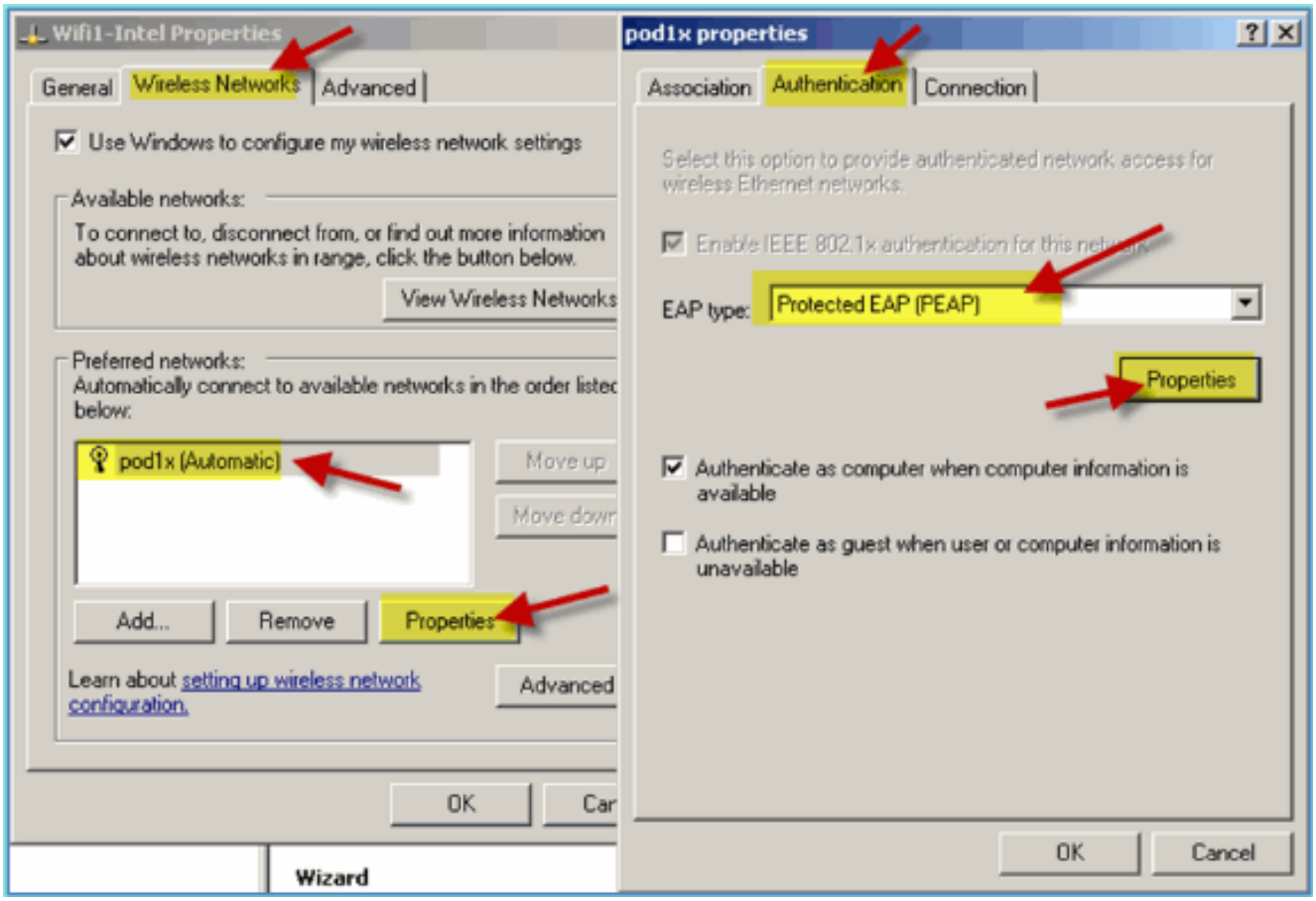
1. Sul laptop, passare alle impostazioni WLAN. Attivare WIFI e connettersi all'SSID POD 802.1X attivato creato nell'esercizio precedente.



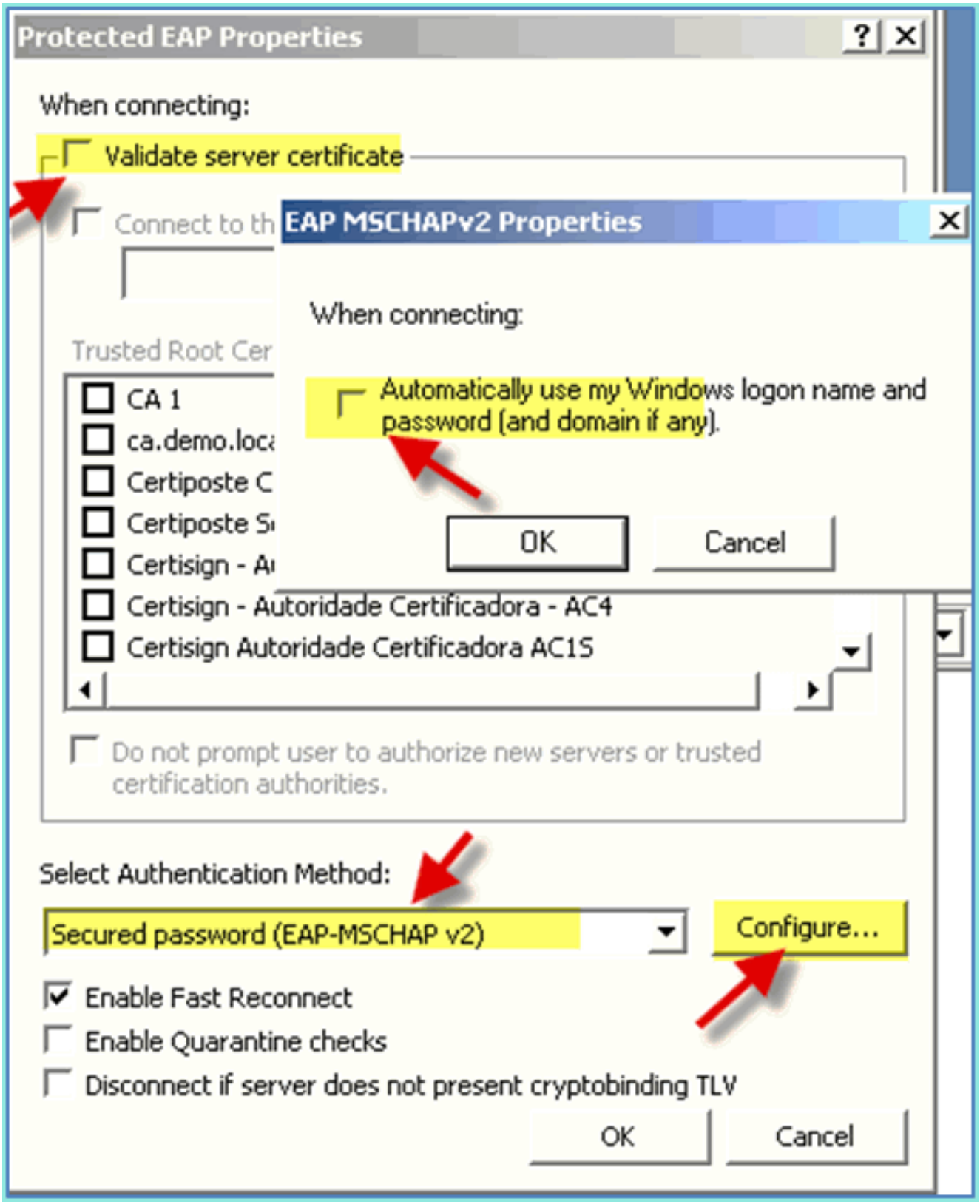
2. Accedere alle proprietà di rete per l'interfaccia WIFI.



3. Passare alla scheda **Reti wireless**. Selezionare il pod SSID network properties > Authentication tab > EAP type = Protected EAP (PEAP).



4. Fare clic su Proprietà EAP.
5. Impostare quanto segue:Convalida certificato server: disattivatoMetodo di autenticazione: password protetta (EAP-MSCHAP
   v2)

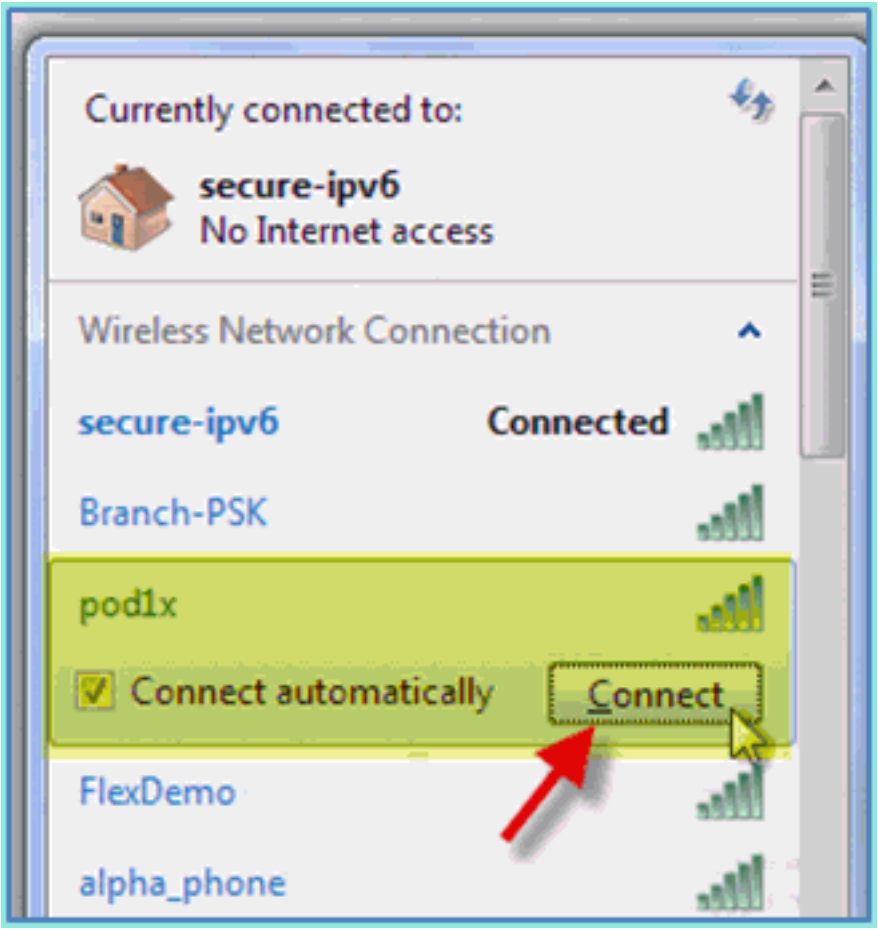


6. Fare clic su **OK** in tutte le finestre per completare questa attività di configurazione.
7. Il client Windows XP richiede il nome utente e la password. In questo esempio, è aduser/XXXX.
8. Confermare la connettività di rete, l'indirizzamento IP (v4).

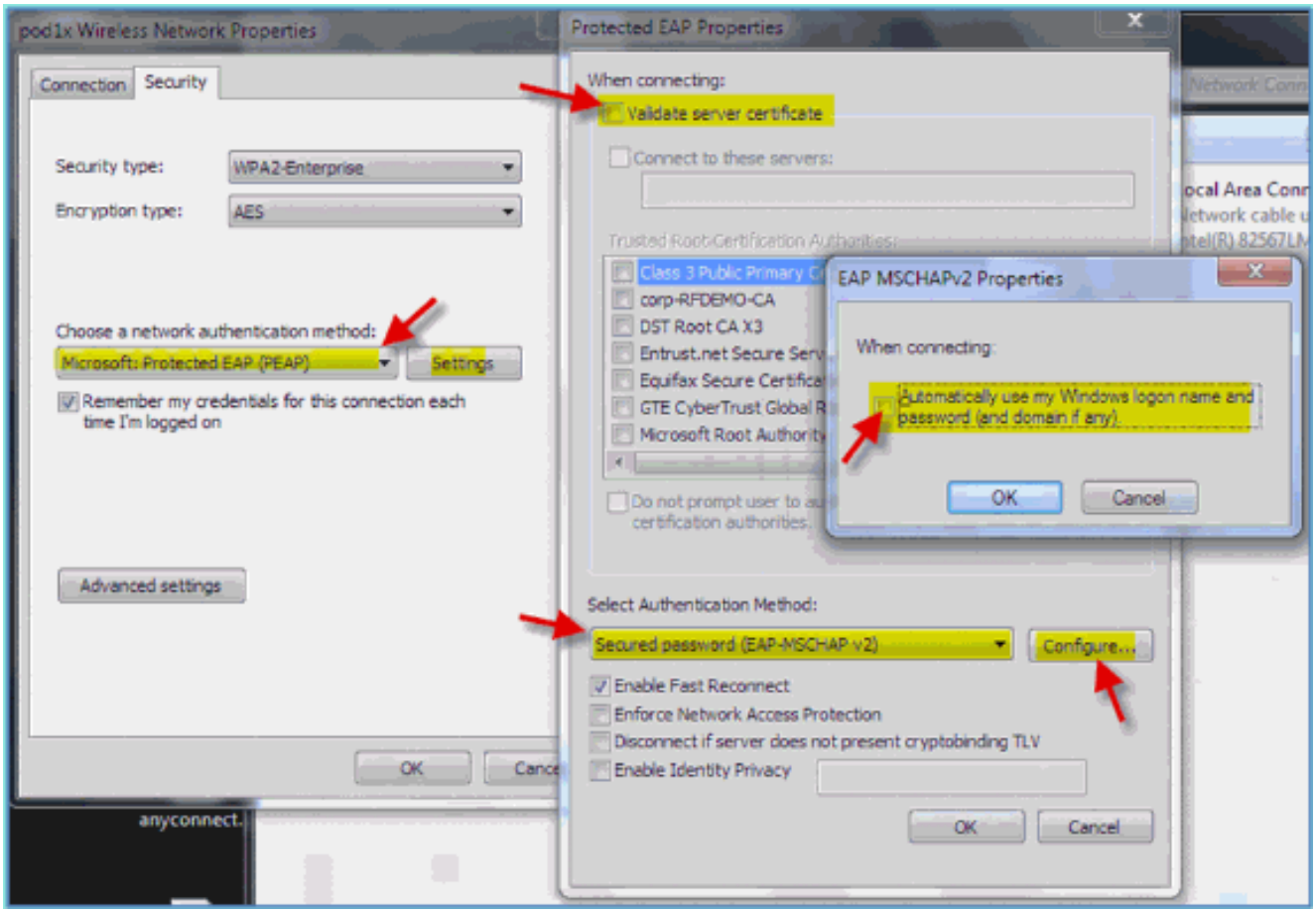
Riferimento: Autenticazione wireless per Microsoft Windows 7

Associarsi al WLC tramite un SSID autenticato come utente INTERNO (o utente AD integrato) utilizzando un laptop wireless di Windows 7.

1. Sul laptop, passare alle impostazioni WLAN. Attivare WIFI e connettersi all'SSID POD 802.1X attivato creato nell'esercizio precedente.



2. Accedere a Wireless Manager e modificare il nuovo profilo POD wireless.
3. Impostare quanto segue:Metodo di autenticazione: PEAPMemorizza credenziali...: disattivatoConvalida certificato server (impostazione avanzata): disattivatoMetodo di autenticazione (impostazione avanzata): EAP-MSCHAP v2Usa automaticamente accesso Windows:
   disattivato



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).