Configurazione di ACS 5.2 per l'autenticazione basata sulla porta con un LAP

Sommario

Introduzione

In questo documento viene descritto come configurare un Lightweight Access Point (LAP) come supplicant 802.1x per l'autenticazione su un server RADIUS come Access Control Server (ACS) 5.2.

Prerequisiti

Requisiti

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

- Conoscere a fondo il controller WLC (Wireless LAN Controller) e i LAP.
- Avere una 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
- 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.

Premesse

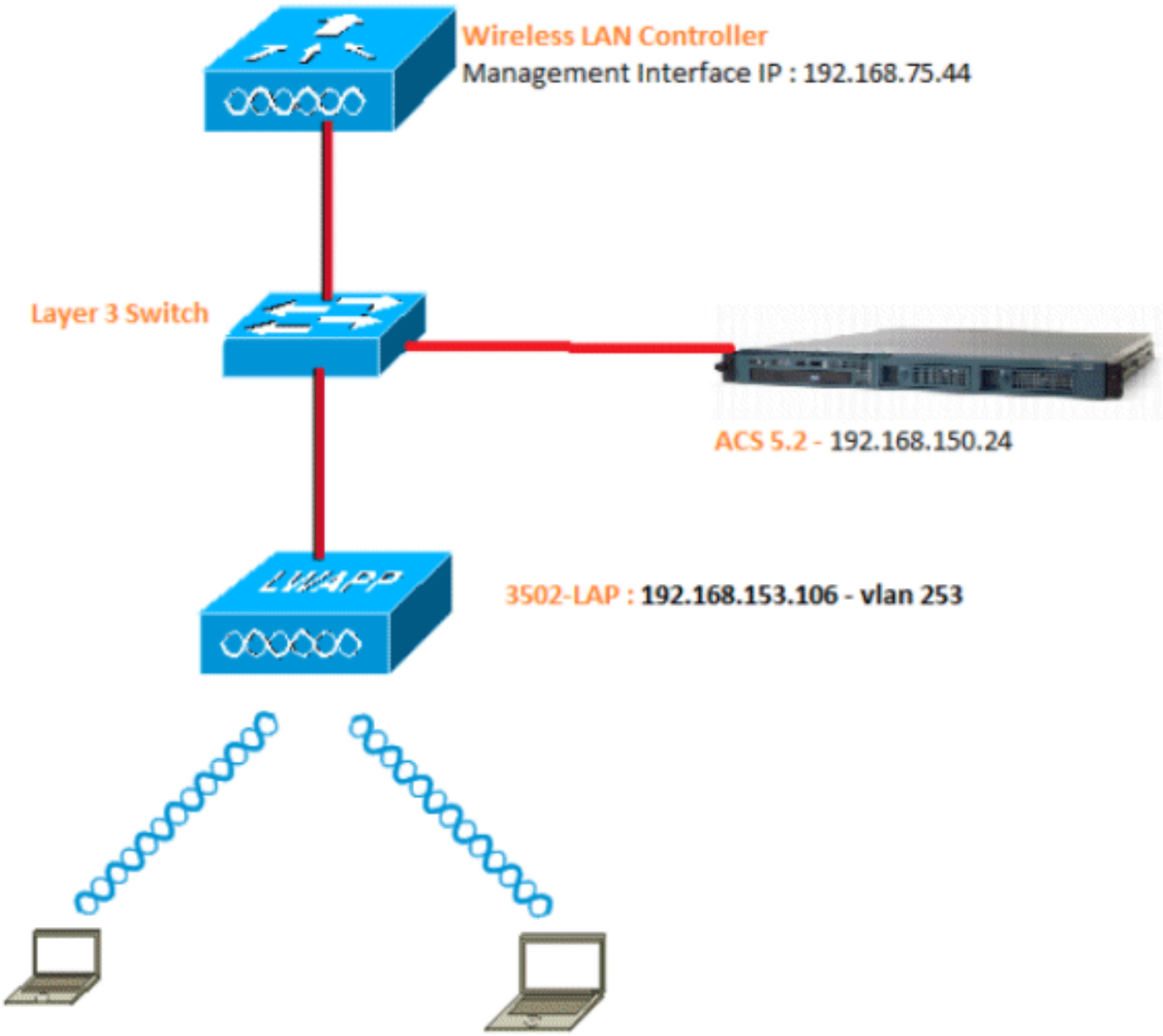
I LAP dispongono di certificati X.509 preinstallati (firmati da una chiave privata) che vengono masterizzati nel dispositivo al momento della produzione. I LAP utilizzano questo certificato per autenticarsi al WLC nel processo di join. Questo metodo descrive un altro modo per autenticare i LAP. Con il software WLC, è possibile configurare l'autenticazione 802.1x tra un Cisco Aironet Access Point (AP) e uno switch Cisco. In questo caso, l'access point agisce come supplicant 802.1x ed è autenticato dallo switch su un server RADIUS (ACS) che usa EAP-FAST con provisioning PAC anonimo. Dopo aver configurato la porta per l'autenticazione 802.1x, lo switch non consente il passaggio di traffico diverso dal traffico 802.1x fino a quando il dispositivo connesso alla porta non esegue correttamente l'autenticazione. Un access point può essere autenticato prima di essere aggiunto a un WLC o dopo essere stato aggiunto a un WLC, nel qual caso è possibile configurare 802.1x sullo switch dopo che il LAP si è unito al WLC.

Configurazione

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

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.
- Il LAP viene inserito nella VLAN 253.
- VLAN 253: 192.168.153.x/24. Gateway: 192.168.153.10
- VLAN 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 categorie:

1. Configurare il LAP.
2. Configurare lo switch.
3. Configurare il server RADIUS.

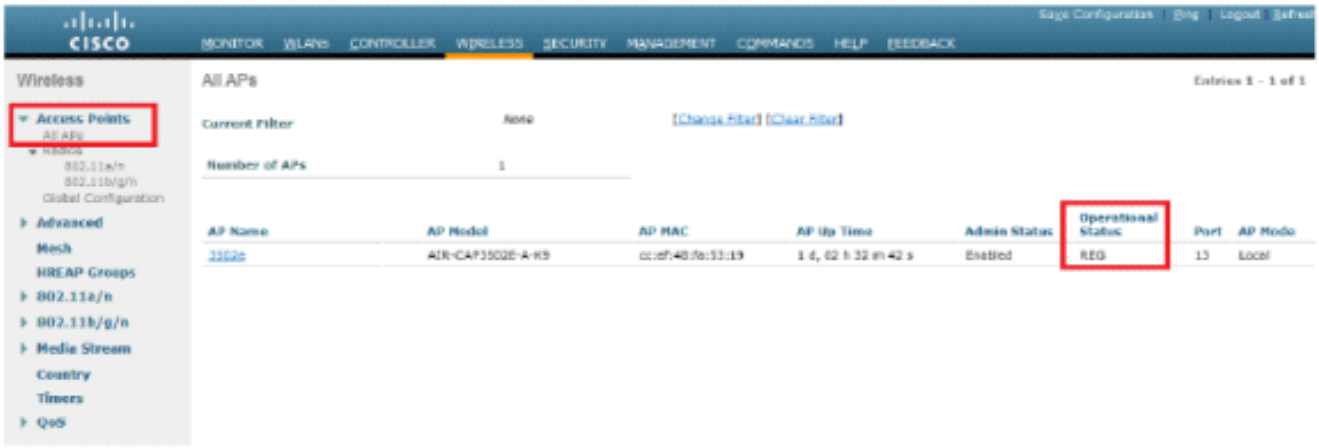
Configurazione LAP

Presupposti:

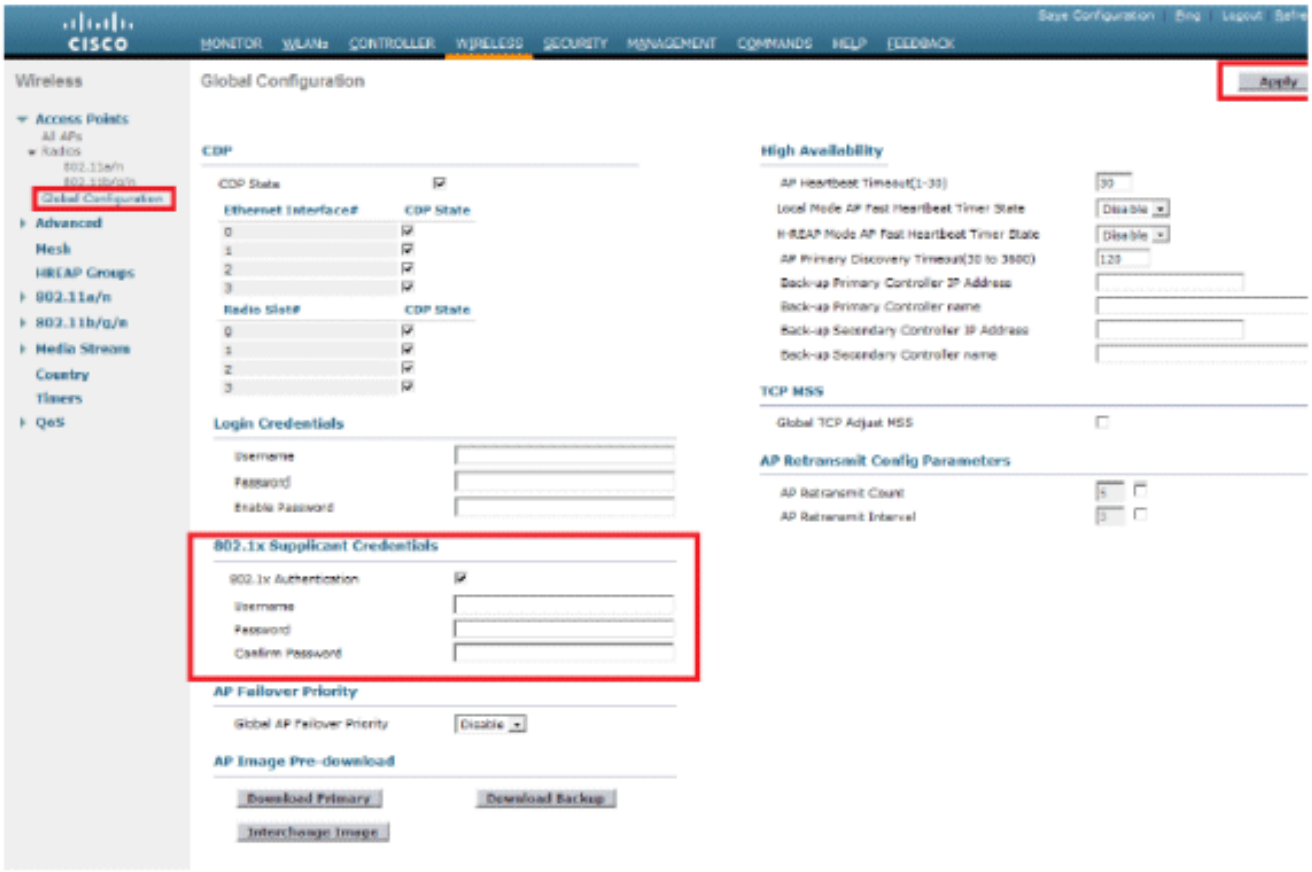
Il LAP è già registrato sul WLC con l'opzione 43, il DNS o l'IP dell'interfaccia di gestione del WLC configurato staticamente.

Attenersi alla seguente procedura:

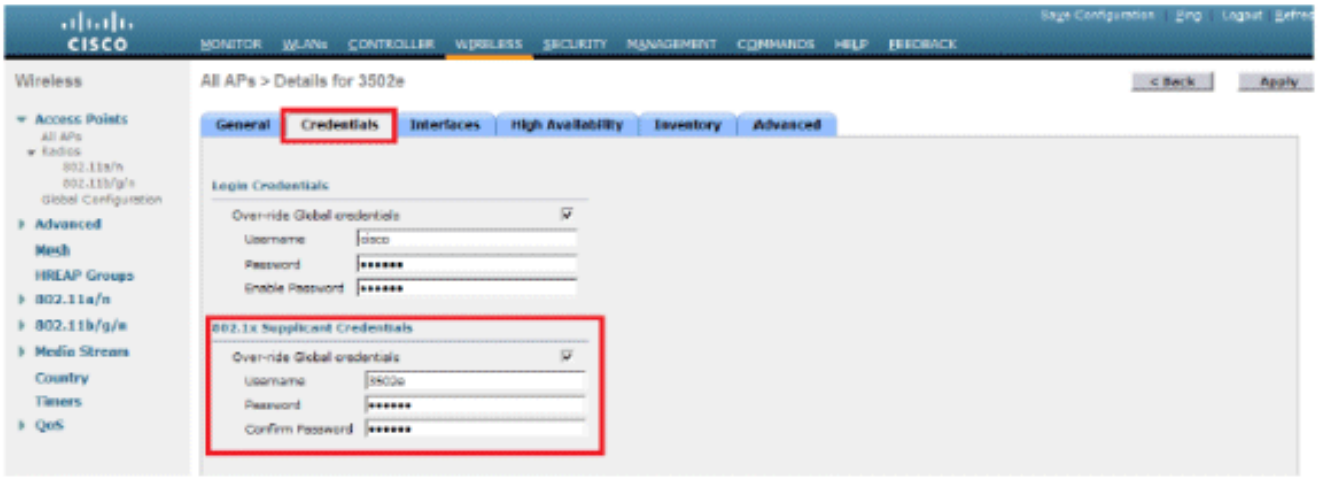
1. Per verificare la registrazione dei LAP sul WLC, selezionare **Wireless > Access Point > Tutti gli AP**.



2. Èpossibile configurare le credenziali 802.1x (nome utente/password) per tutti i LAP in due modi:**Globalmente**Per un LAP già aggiunto, è possibile impostare le credenziali a livello globale in modo che ogni LAP aggiunto al WLC erediti tali credenziali.

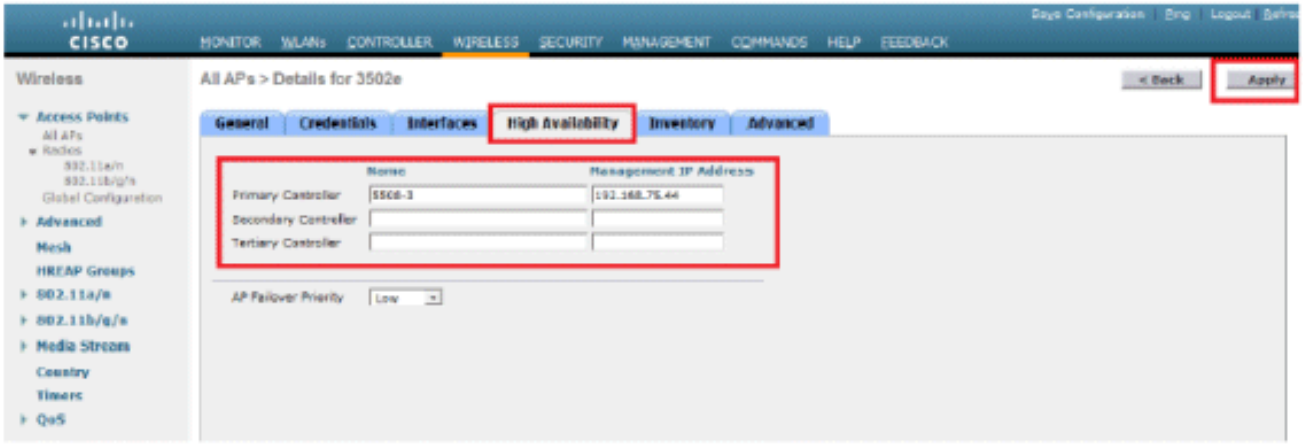


SingolarmenteConfigurare i profili 802.1 x per access point. Nell'esempio riportato sotto, le credenziali verranno configurate per ciascun access point.Selezionare **Wireless > All AP** (Tutti gli access point), quindi selezionare l'access point in questione.Aggiungere il nome utente e la password nei campi **Credenziali richiedente 802.1x**.



Nota: le credenziali di accesso vengono utilizzate per Telnet, SSH o console nell'access point.

3. Configurare la sezione Alta disponibilità e fare clic su **Applica**.



Nota: una volta salvate, queste credenziali vengono conservate nel WLC e l'access point viene riavviato. Le credenziali cambiano solo quando il LAP si unisce a un nuovo WLC. Il LAP presume il nome utente e la password configurati sul nuovo WLC.Se l'access point non è ancora stato aggiunto a un WLC, è necessario eseguire la console nel LAP per impostare le credenziali. Usare questo comando CLI in modalità di abilitazione:**LAP#lwapp ap dot1x nomeutente *<nomeutente>* password *<password>* oLAP#capwap dot1x nomeutente *<nomeutente>* password *<password>* Nota:** questo comando è disponibile solo per i punti di accesso che eseguono l'immagine di ripristino.Il nome utente e la password predefiniti per i LAP sono rispettivamente `cisco` e `Cisco`.

Configura switch

Lo switch funge da autenticatore per il LAP e autentica il LAP su un server RADIUS. Se lo switch non dispone di software compatibile, aggiornarlo. Nella CLI dello switch, usare questi comandi per abilitare l'autenticazione 802.1x su una porta dello switch:

```
switch#configure terminal
switch(config)#dot1x system-auth-control
switch(config)#aaa new-model
!--- Enables 802.1x on the Switch. switch(config)#aaa authentication dot1x default group radius
switch(config)#radius server host 192.168.150.24 key cisco
!--- Configures the RADIUS server with shared secret and enables switch to send !--- 802.1x
information to the RADIUS server for authentication. switch(config)#ip radius source-interface
vlan 253
!--- We are sourcing RADIUS packets from VLAN 253 with NAS IP: 192.168.153.10.
switch(config)interface gigabitEthernet 0/11 switch(config-if)switchport mode access
switch(config-if)switchport access vlan 253 switch(config-if)mls qos trust dscp switch(config-
if)spanning-tree portfast !--- gig0/11 is the port number on which the AP is connected.
switch(config-if)dot1x pae authenticator !--- Configures dot1x authentication. switch(config-
if)dot1x port-control auto !--- With this command, the switch initiates the 802.1x
authentication.
```

Nota: se si hanno altri access point sullo stesso switch e non si desidera che utilizzino 802.1x, è possibile lasciare la porta non configurata per 802.1x o usare questo comando:

```
switch(config-if)authentication port-control force-authorized
```

Configura server RADIUS

LAP è autenticato con EAP-FAST. Se non si utilizza Cisco ACS 5.2, verificare che il server RADIUS in uso supporti questo metodo EAP.

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 ACS basato su regole. In altre parole, 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 di dispositivo e così via.
- **Autorizzazioni** - VLAN o livelli di privilegio 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 le condizioni in base alle quali l'utente può accedere alla rete e anche il livello di autorizzazione consentito quando sono soddisfatte condizioni specifiche.

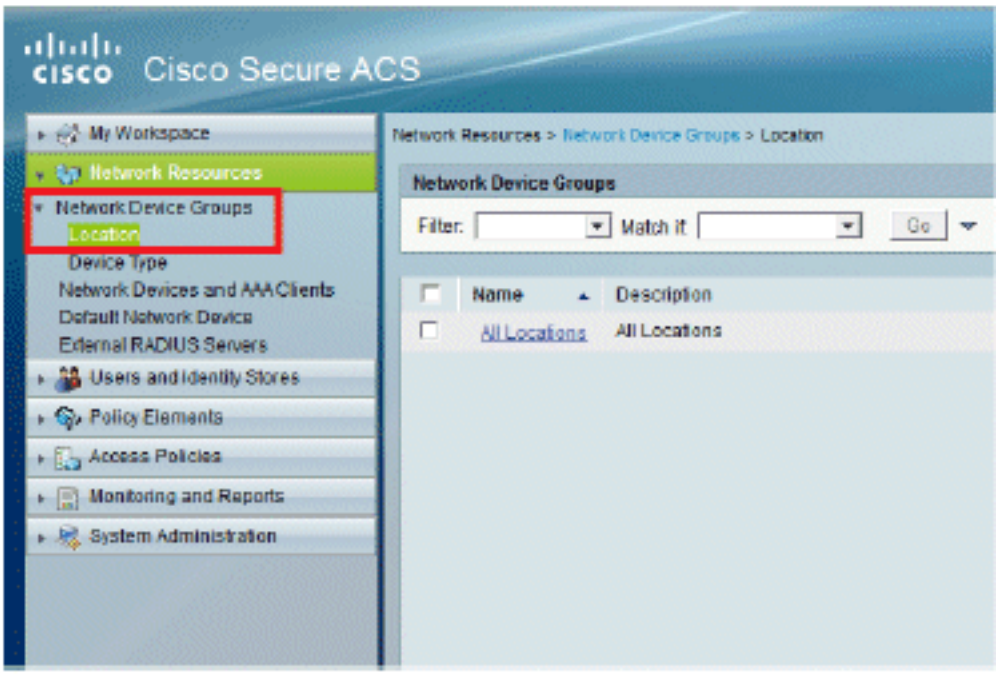
Configura risorse di rete

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

In questa procedura viene illustrato come aggiungere lo switch come client AAA sul server RADIUS in modo che lo switch possa passare le credenziali utente del LAP al server RADIUS.

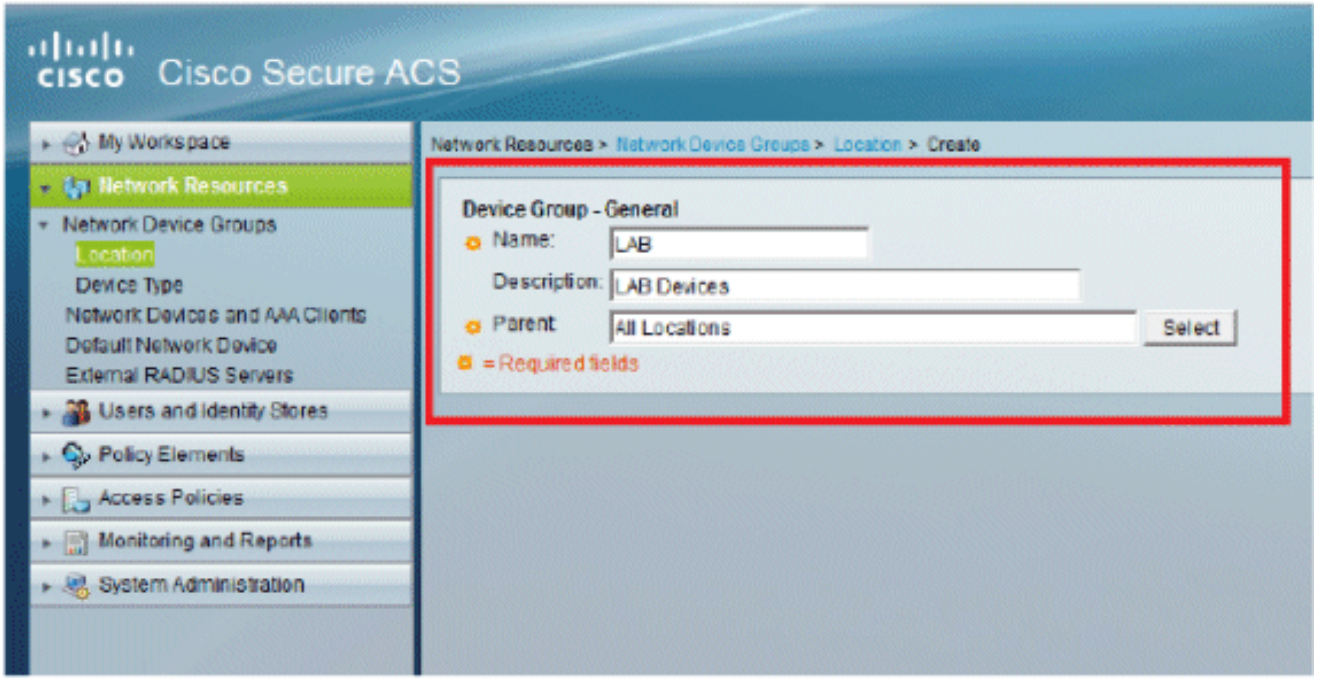
Attenersi alla seguente procedura:

1. Dall'interfaccia utente di ACS, fare clic su **Risorse di rete**.
2. Fare clic su **Gruppi di dispositivi di rete**.
3. Selezionare **Posizione > Crea** (in basso

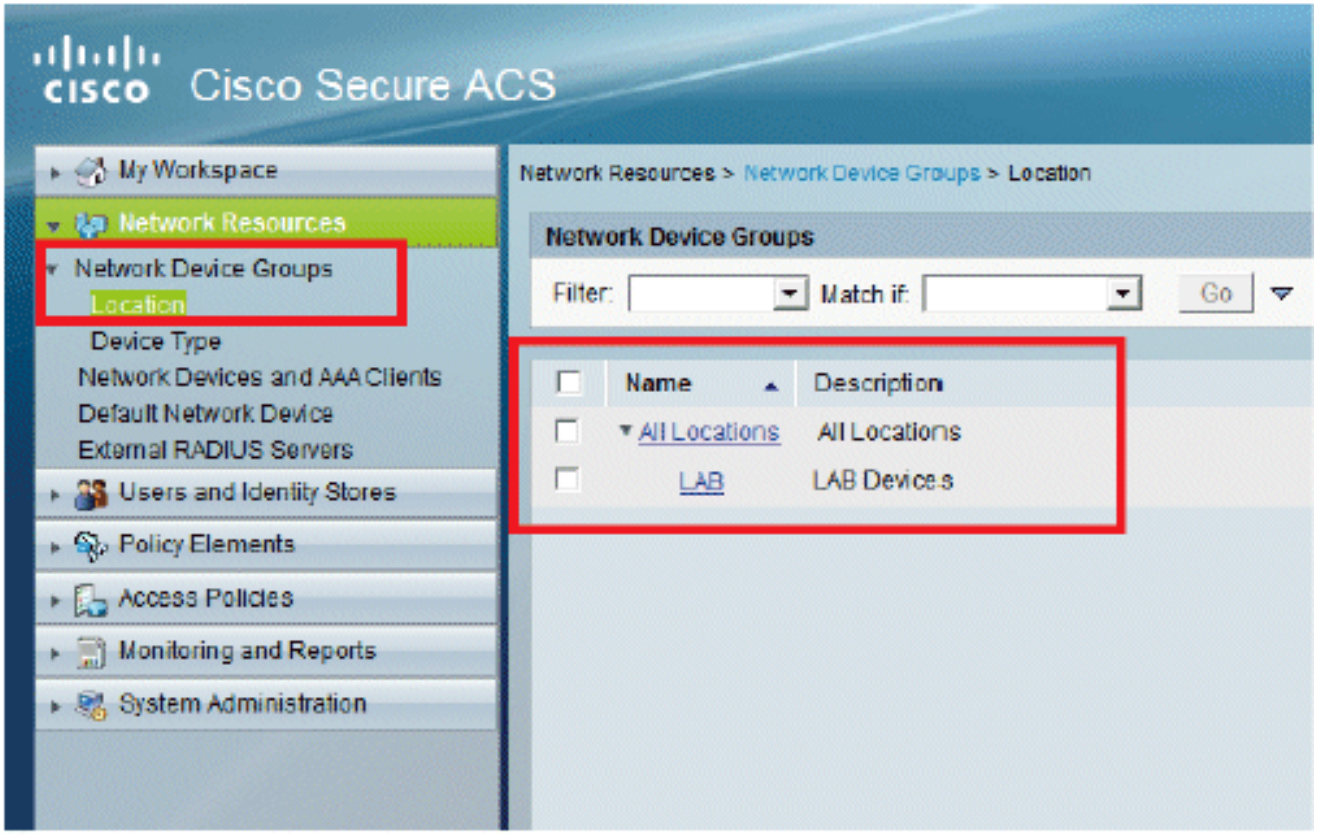


).

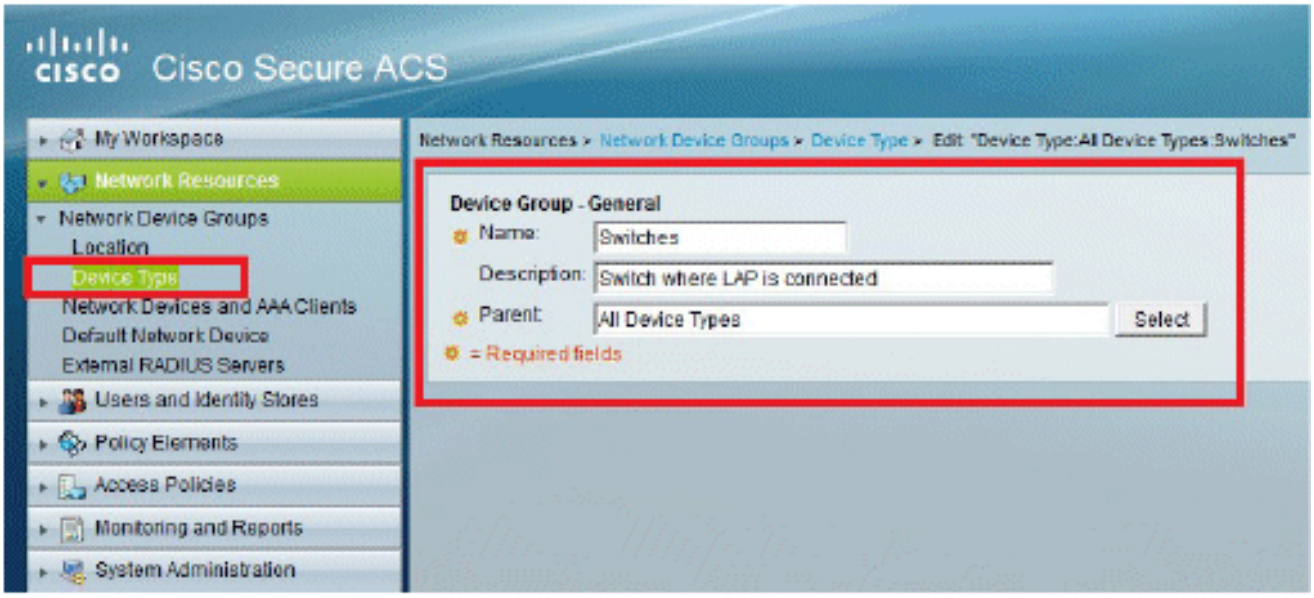
4. Aggiungere i campi obbligatori e fare clic su **Invia**.



5. La finestra viene aggiornata:



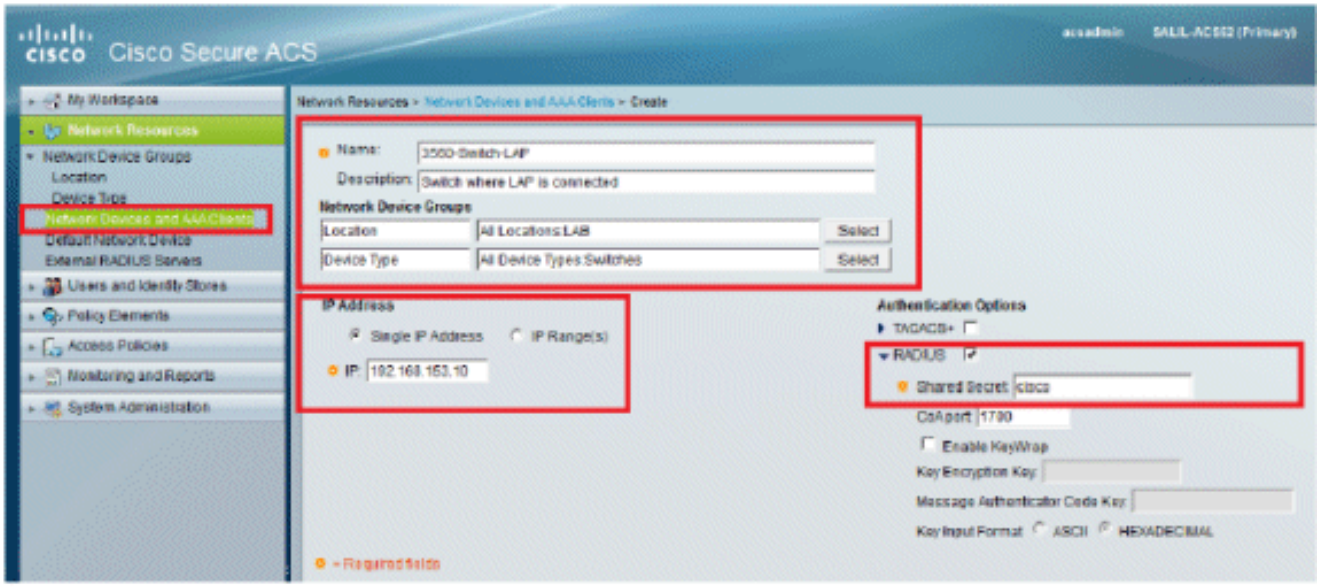
6. Selezionate **Tipo periferica (Device Type) > Crea (Create)**.



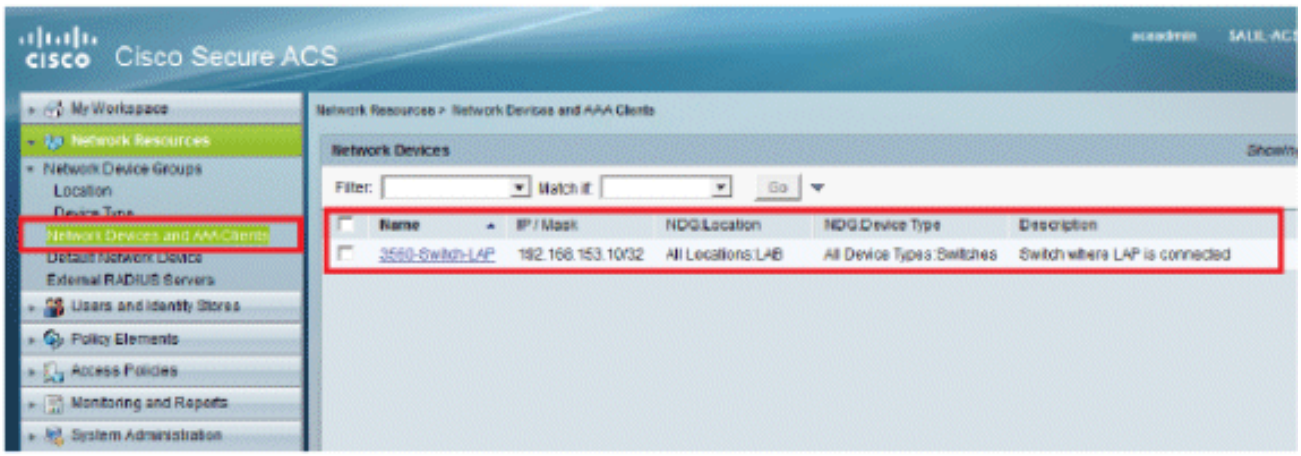
7. Fare clic su **Invia**. Al termine, la finestra viene

aggiornata:

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



10. Fare clic su **Invia**. La finestra viene aggiornata:

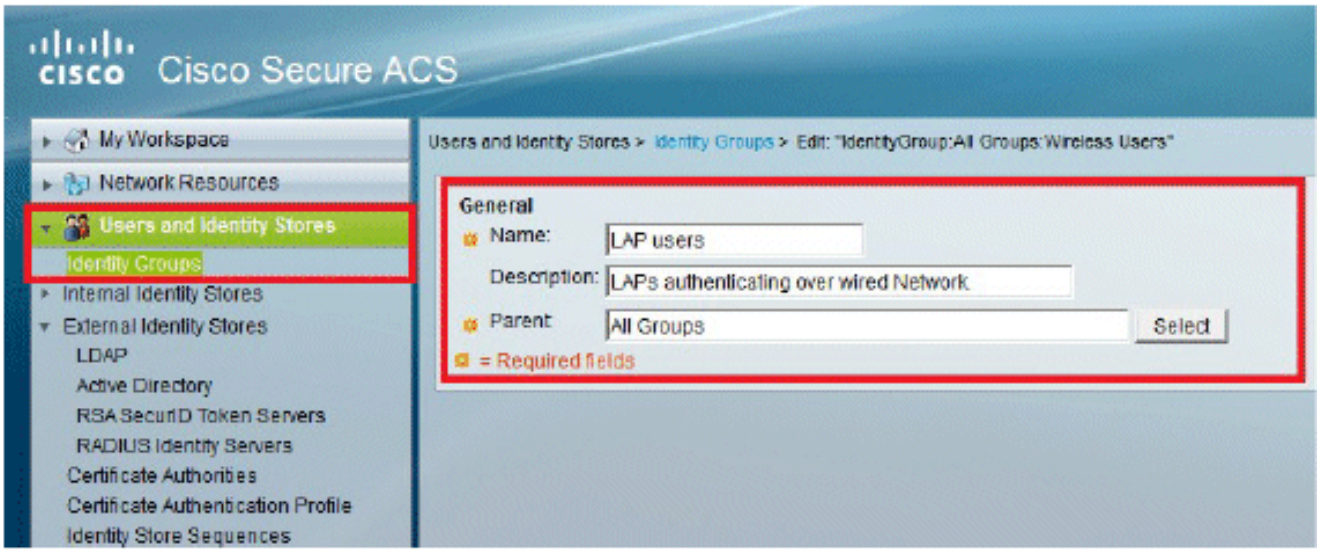


Configura utenti

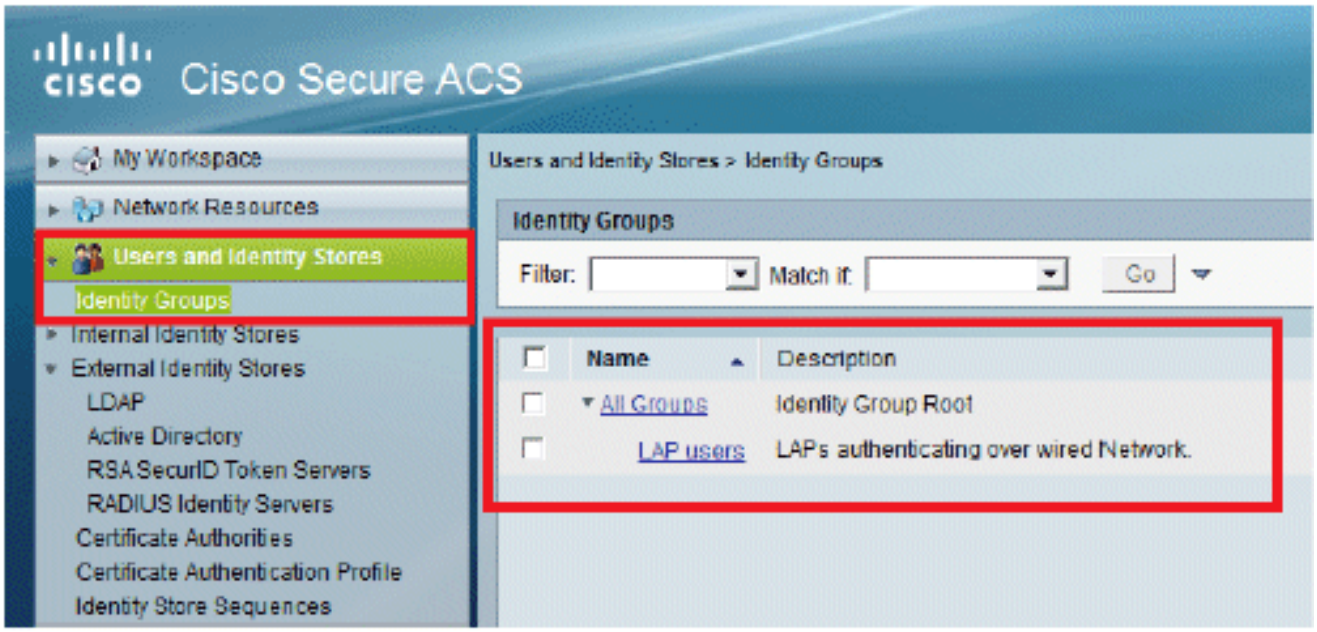
In questa sezione viene illustrato come creare un utente sul server ACS configurato in precedenza. L'utente verrà assegnato a un gruppo denominato "utenti LAP".

Attenersi alla seguente procedura:

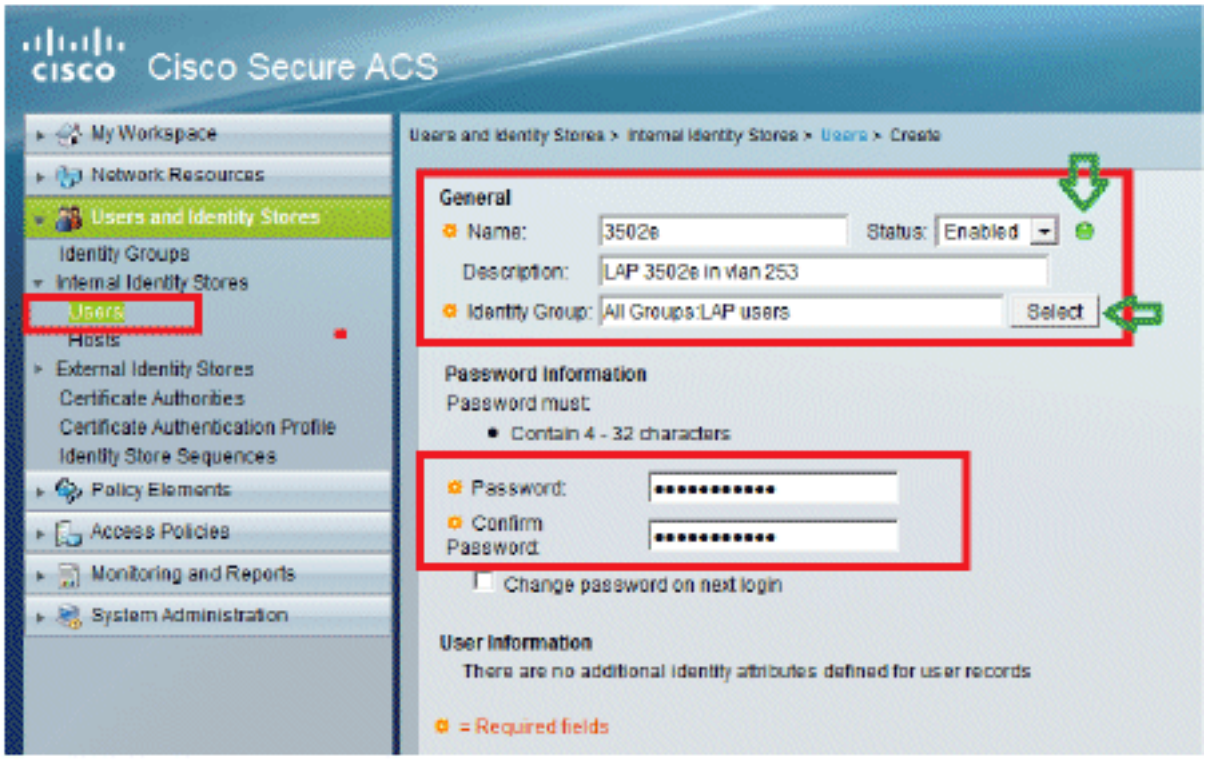
1. Andare a **Utenti e archivi identità > Gruppi di identità > Crea**.



2. Fare clic su Invia.



3. Creare lo switch **3502e** assegnarlo al gruppo "utenti LAP".
4. Andare a **Utenti e archivi identità > Gruppi di identità > Utenti >**

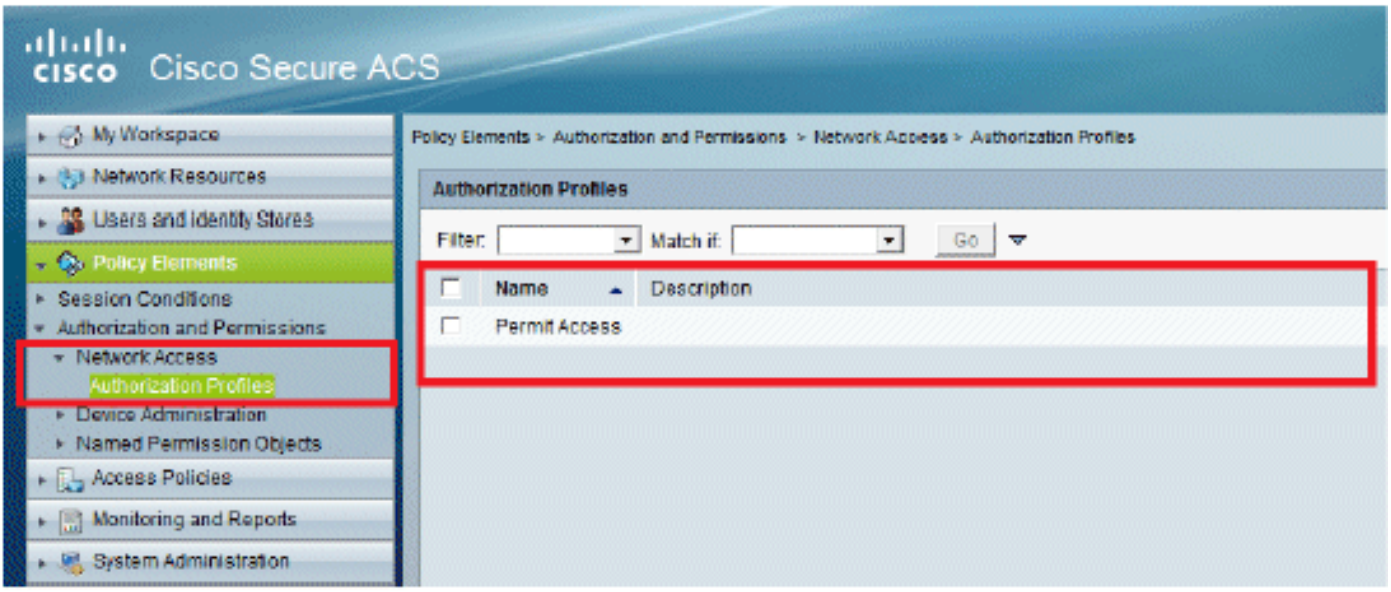


Crea.

5. Verranno visualizzate le informazioni aggiornate:

Definizione degli elementi dei criteri

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

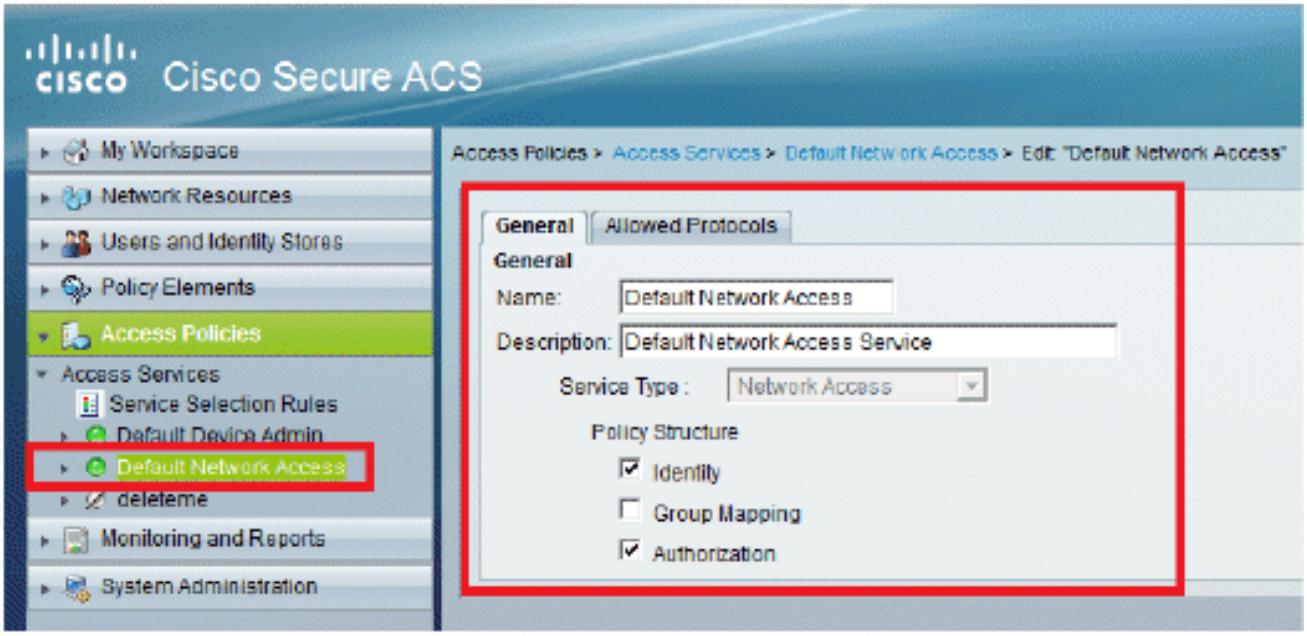


Applica criteri di accesso

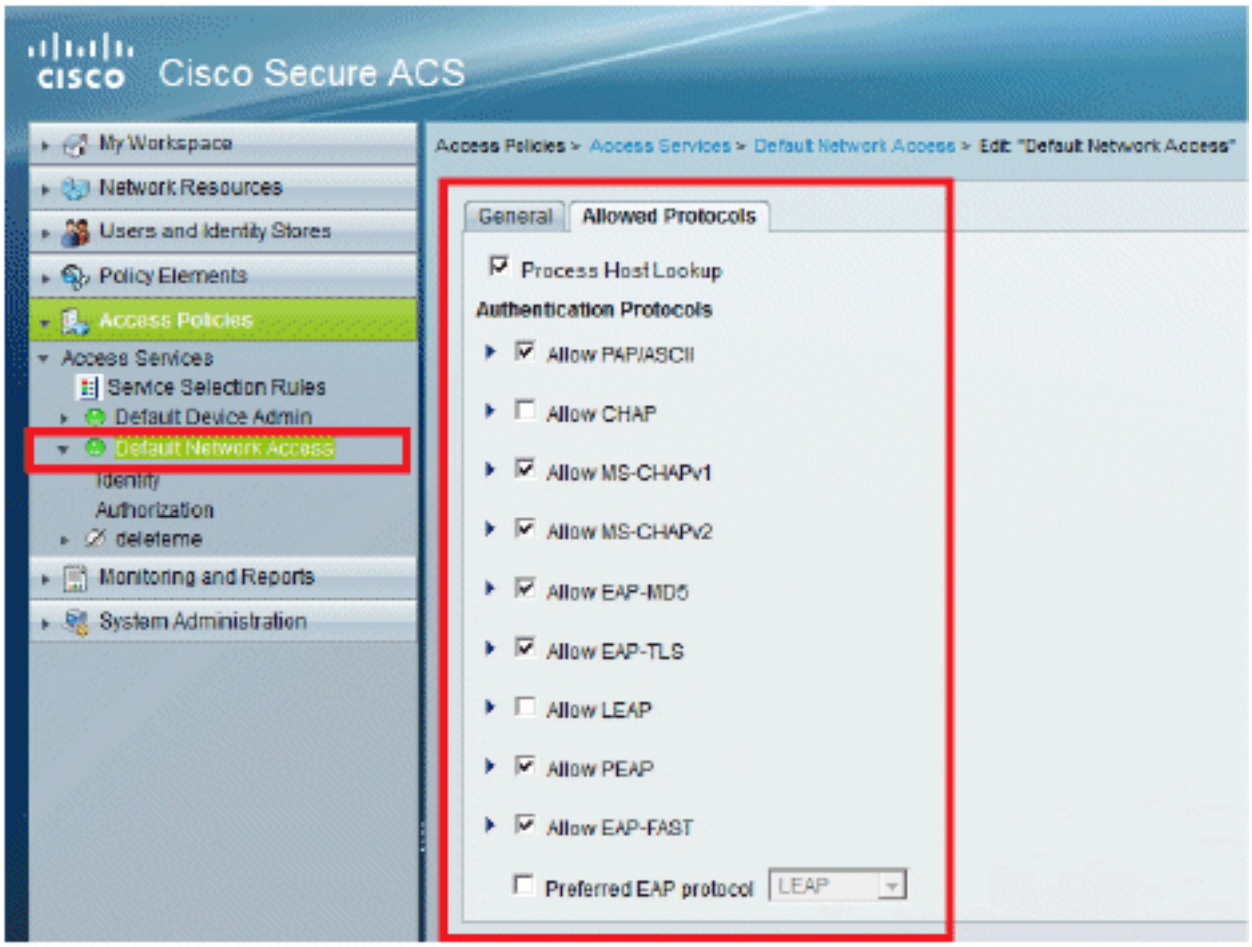
In questa sezione, selezionare EAP-FAST come metodo di autenticazione usato per i LAP per l'autenticazione. Le regole verranno quindi create in base ai passaggi precedenti.

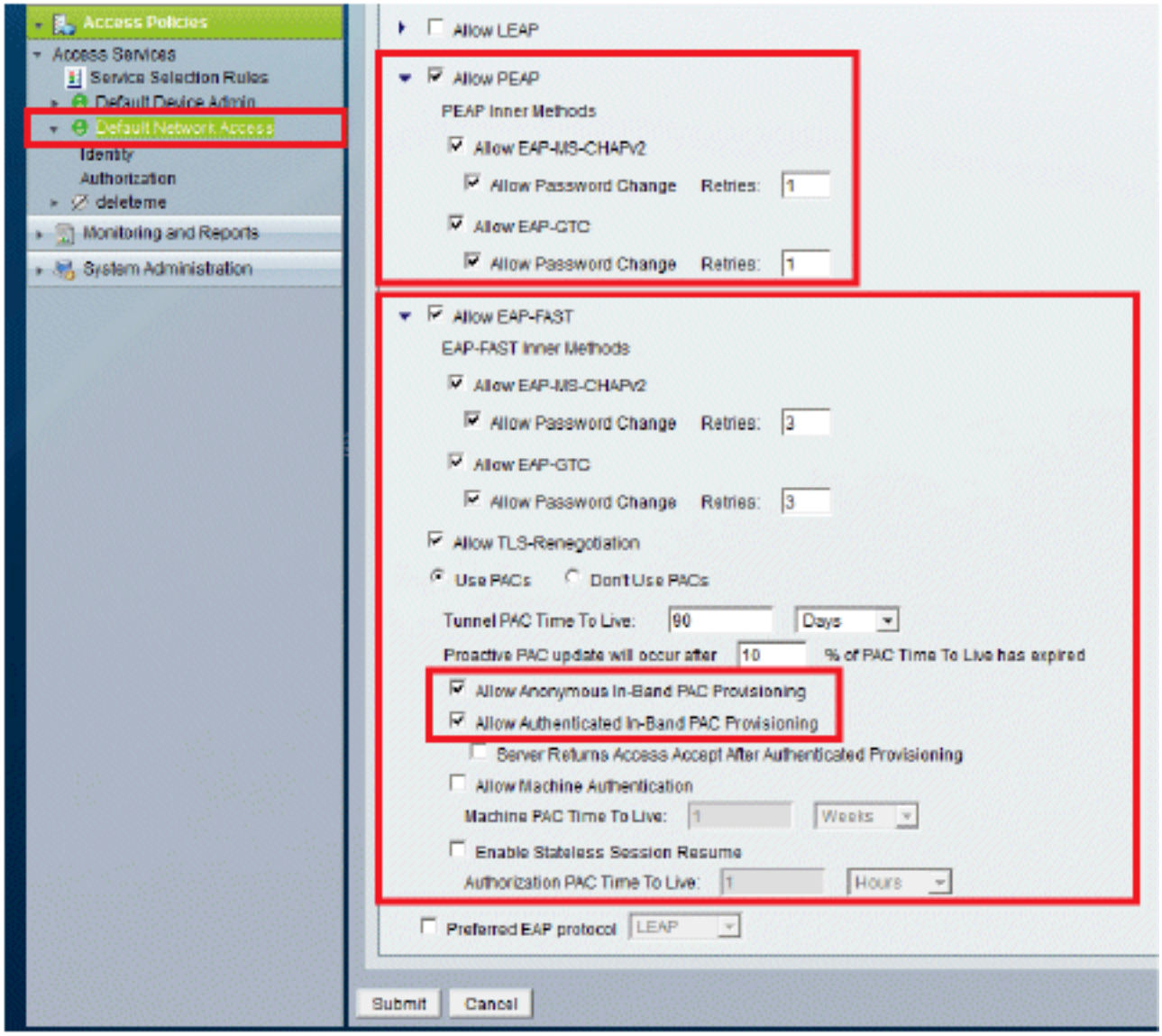
Attenersi alla seguente procedura:

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

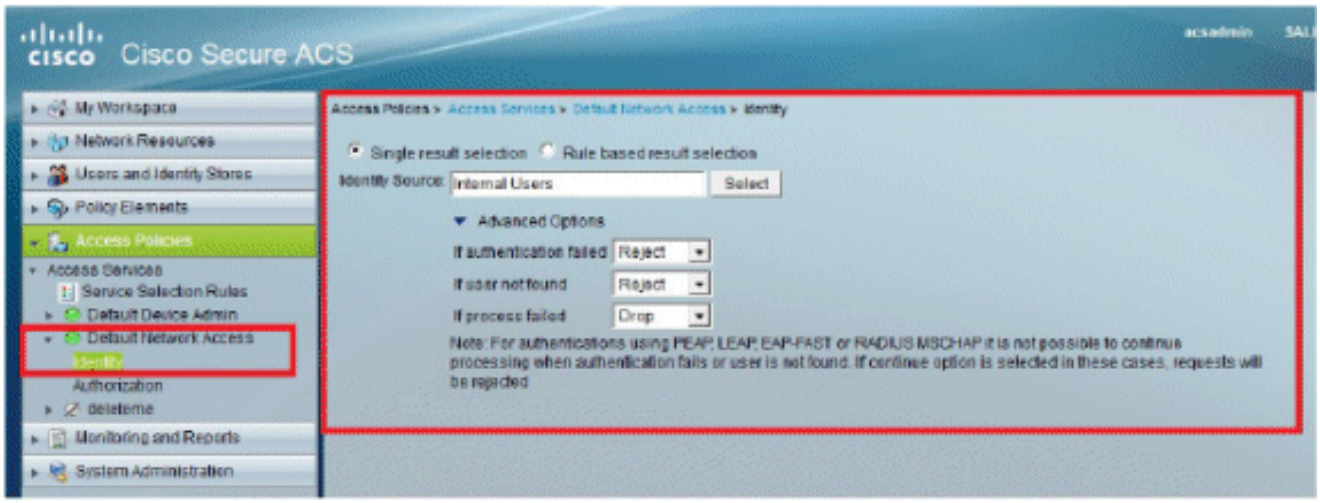


2. Accertarsi di aver abilitato **EAP-FAST** e la **preparazione anonima della PAC in banda**.


Cisco Secure ACS
My Workspace
Network Resources
Users and Identity Stores
Policy Elements
Access Policies
Access Services
Service Selection Rules
Default Device Admin
Default Network Access
Identity
Authorization
deleteme
Monitoring and Reports
System Administration
Access Policies > Access Services > Default Network Access > Edit: "Default Network Access"
General
Allowed Protocols
Process Host Lookup
Authentication Protocols
Allow PAP/ASCII
Allow CHAP
Allow MS-CHAPv1
Allow MS-CHAPv2
Allow EAP-MD5
Allow EAP-TLS
Allow LEAP
Allow PEAP
Allow EAP-FAST
Preferred EAP protocol
LEAP

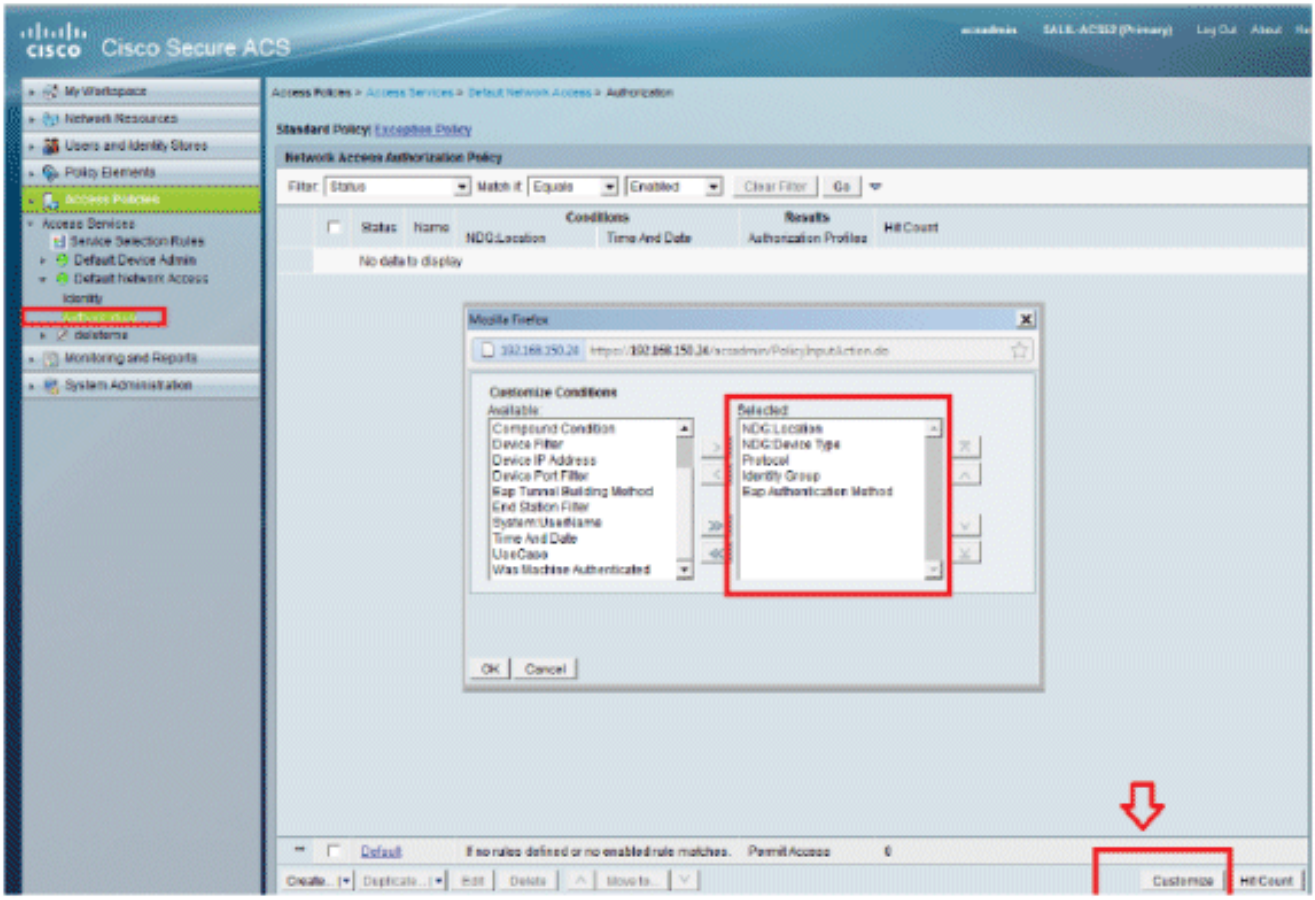


3. Fare clic su **Invia**.
4. Verificare il gruppo di identità selezionato. In questo esempio, utilizzare **Internal Users** (creato su ACS) e salvare le
modifiche.

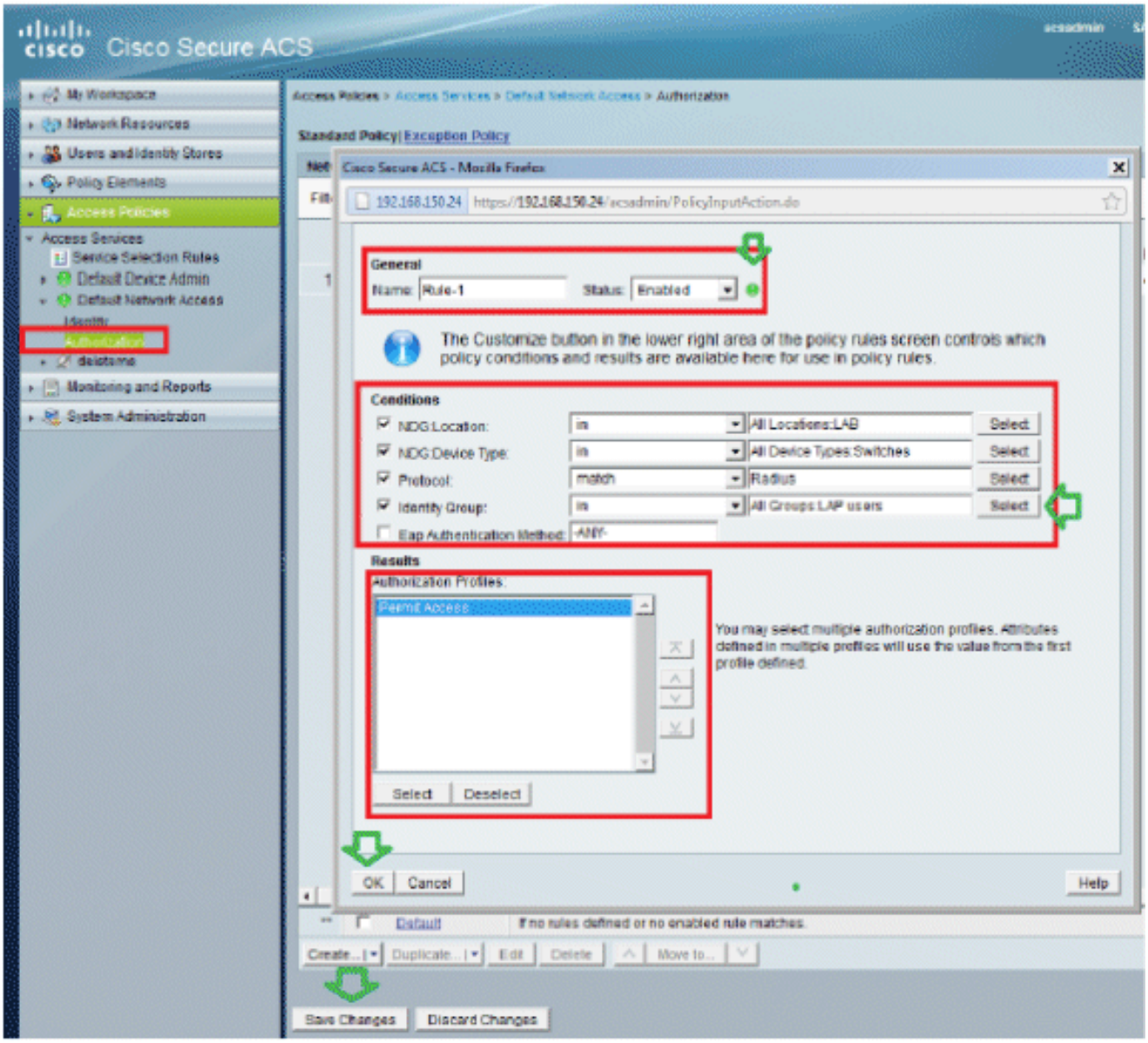


5. Per verificare il profilo di autorizzazione, selezionare **Access Policies > Access Services > Default Network Access > Authorization** (Policy di accesso **> Servizi di accesso > Accesso di rete predefinito > Autorizzazione**).Èpossibile personalizzare in base a quali condizioni si consentirà a un utente l'accesso alla rete e a quali profili di autorizzazione (attributi) si

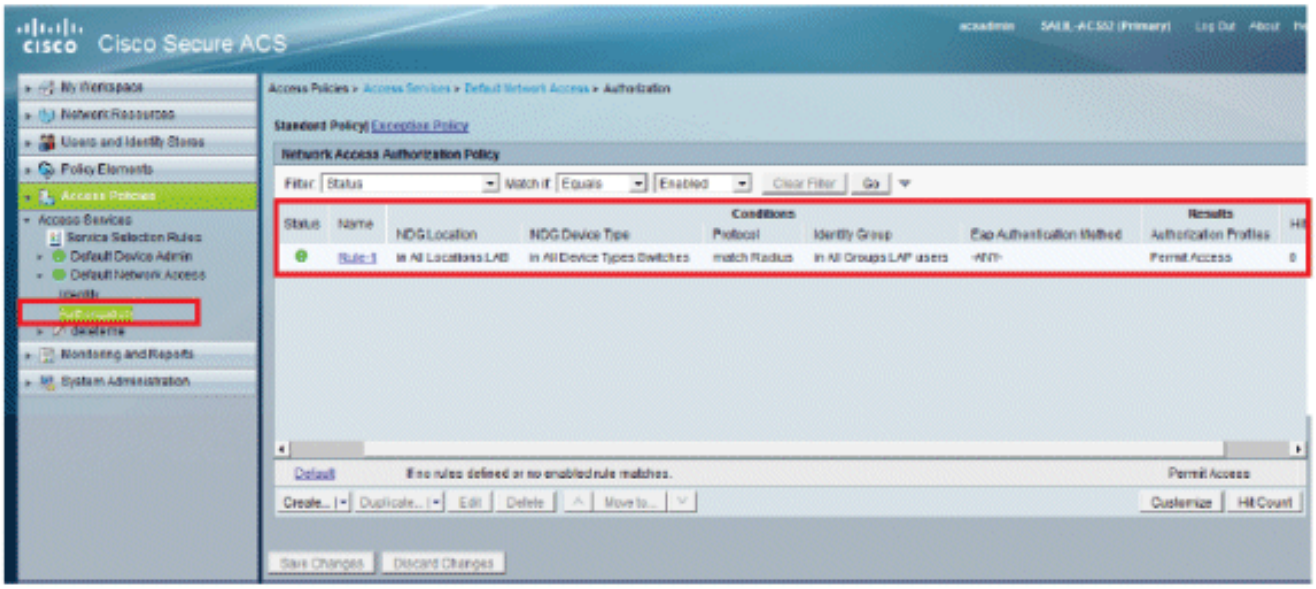
passerà dopo l'autenticazione. Questa granularità è disponibile solo in ACS 5.x. Nell'esempio sono selezionati Location, **Device Type**, **Protocol**, **Identity Group** e **EAP Authentication Method**.



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, è consentito l'accesso LAP senza condizioni.
8. Selezionate **Crea (Create) > Regola-1 (Rule-1)**. Questa regola è destinata agli utenti del gruppo "utenti
LAP".

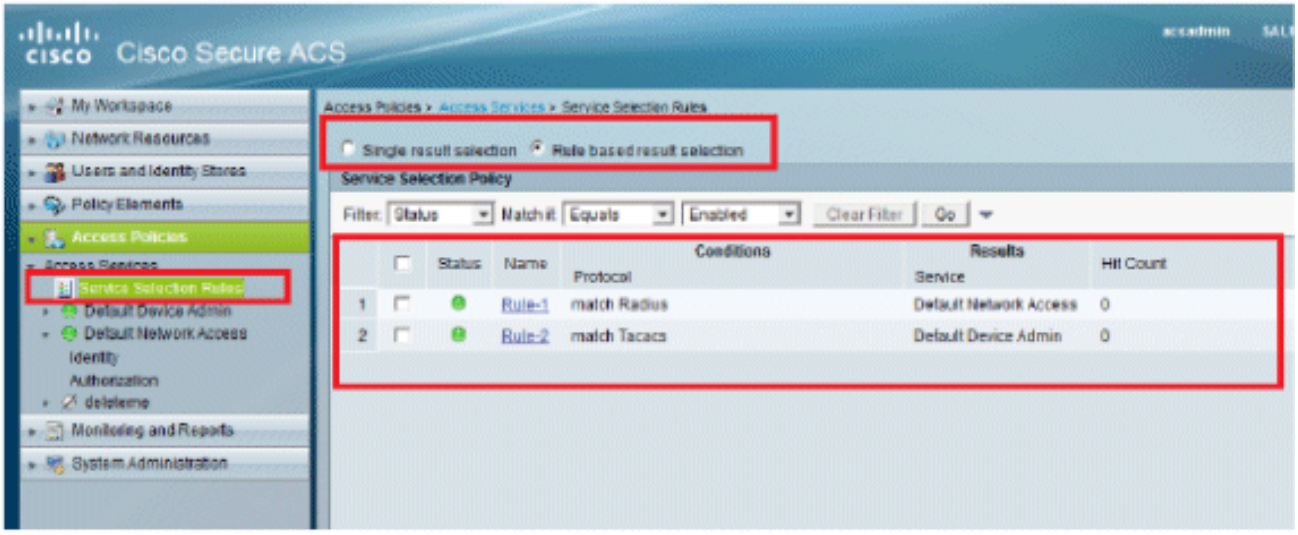


9. Fare clic su **Salva modifiche**. Se si desidera negare agli utenti che non soddisfano le condizioni, modificare la regola predefinita in "Nega accesso".



10. L'ultimo passo consiste nel definire 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. Ad esempio:



Verifica

Dopo aver abilitato 802.1x sulla porta dello switch, tutto il traffico, ad eccezione del traffico 802.1x, viene bloccato tramite la porta. Il LAP, già registrato sul WLC, viene dissociato. Solo dopo un'autenticazione 802.1x riuscita è consentito il passaggio di altro traffico. La corretta registrazione del LAP sul WLC dopo l'abilitazione della versione 802.1x sullo switch indica che l'autenticazione LAP è riuscita.

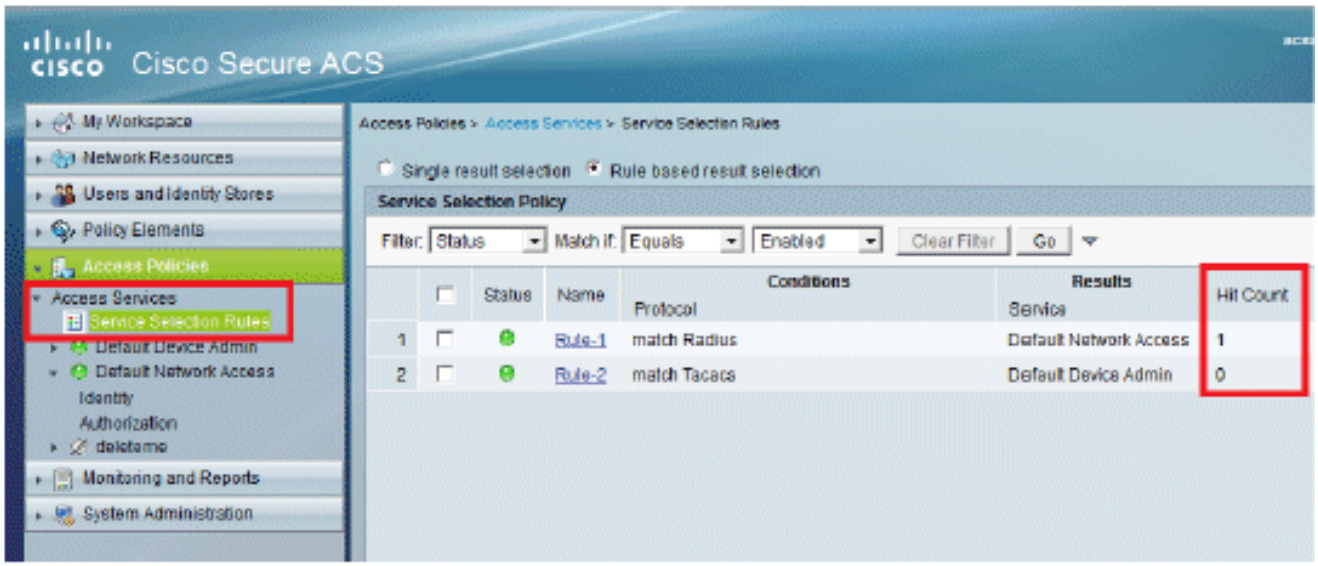
Console AP:

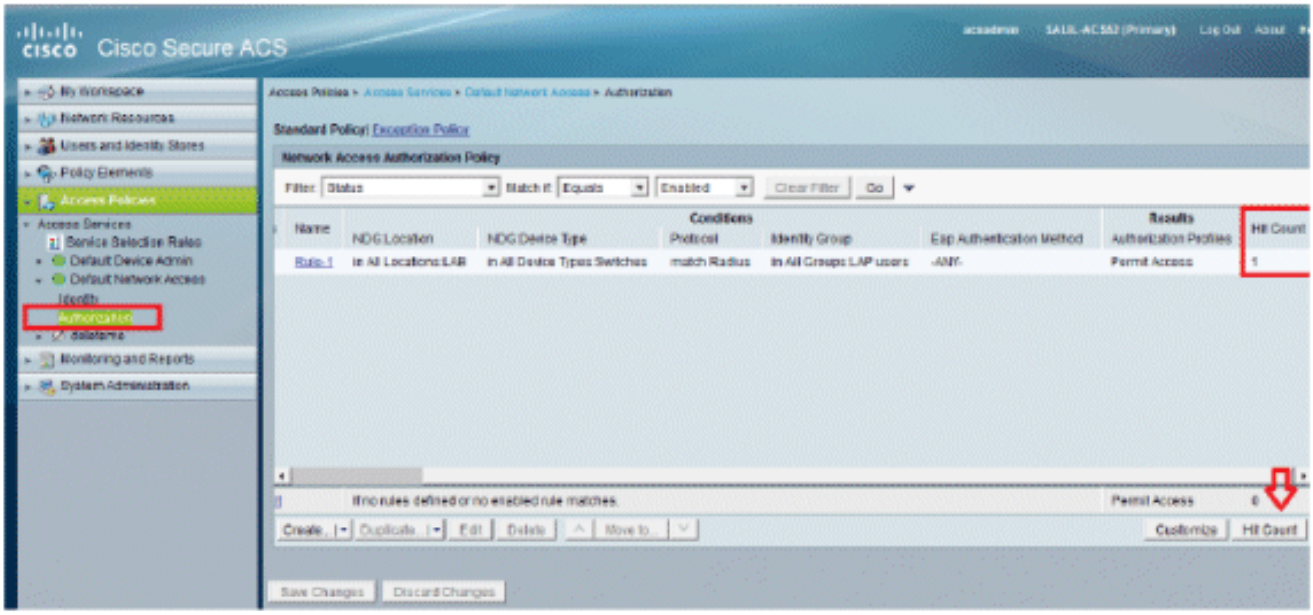
```
*Jan 29 09:10:24.048: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
   192.168.75.44:5246
*Jan 29 09:10:27.049: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
   192.168.75.44:5247
!--- AP disconnects upon adding dot1x information in the gig0/11. *Jan 29 09:10:30.104: %WIDS-5-
DISABLED: IDS Signature is removed and disabled. *Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP
changed state to DISCOVERY *Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP changed state to
DISCOVERY *Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
administratively down *Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dot11Radio1, changed
state to administratively down *Jan 29 09:10:30.186: %LINK-5-CHANGED: Interface Dot11Radio0,
changed state to reset *Jan 29 09:10:30.201: %LINK-3-UPDOWN: Interface Dot11Radio1, changed
state to up *Jan 29 09:10:30.211: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:10:30.220: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to reset Translating
"CISCO-CAPWAP-CONTROLLER"...domain server (192.168.150.25) *Jan 29 09:10:36.203: status of
voice_diag_test from WLC is false
*Jan 29 09:11:05.927: %DOT1X_SHIM-6-AUTH_OK: Interface GigabitEthernet0 authenticated [EAP-FAST]
*Jan 29 09:11:08.947: %DHCP-6-ADDRESS_ASSIGN: Interface GigabitEthernet0 assigned DHCP address
192.168.153.106, mask 255.255.255.0, hostname 3502e
!--- Authentication is successful and the AP gets an IP. Translating "CISCO-CAPWAP-
CONTROLLER.Wlab"...domain server (192.168.150.25) *Jan 29 09:11:37.000: %CAPWAP-5-DTLSREQSEND:
DTLS connection request sent peer_ip: 192.168.75.44 peer_port: 5246 *Jan 29 09:11:37.000:
%CAPWAP-5-CHANGED: CAPWAP changed state to *Jan 29 09:11:37.575: %CAPWAP-5-DTLSREQSUCC: DTLS
connection created successfully peer_ip: 192.168.75.44 peer_port: 5246 *Jan 29 09:11:37.578:
%CAPWAP-5-SENDJOIN: sending Join Request to 192.168.75.44 *Jan 29 09:11:37.578: %CAPWAP-5-
CHANGED: CAPWAP changed state to JOIN

*Jan 29 09:11:37.748: %CAPWAP-5-CHANGED: CAPWAP chan
wmmAC status is FALSEged state to CFG
*Jan 29 09:11:38.890: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to
```

```
   down
*Jan 29 09:11:38.900: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
   reset
*Jan 29 09:11:38.900: %CAPWAP-5-CHANGED: CAPWAP changed state to UP
*Jan 29 09:11:38.956: %CAPWAP-5-JOINEDCONTROLLER: AP has joined controller
   5508-3
*Jan 29 09:11:39.013: %CAPWAP-5-DATA_DTLS_START: Starting Data DTLS handshake.
   Wireless client traffic will be blocked until DTLS tunnel is established.
*Jan 29 09:11:39.013: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:11:39.016: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[0]
*Jan 29 09:11:39.028: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to
   down
*Jan 29 09:11:39.038: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
   reset
*Jan 29 09:11:39.054: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up
*Jan 29 09:11:39.060: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to
   down
*Jan 29 09:11:39.069: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
   reset
*Jan 29 09:11:39.085: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:11:39.135: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[1]DTLS
   keys are plumbed successfully.
*Jan 29 09:11:39.151: %CAPWAP-5-DATA_DTLS_ESTABLISHED: Data DTLS tunnel
   established.
*Jan 29 09:11:39.161: %WIDS-5-ENABLED: IDS Signature is loaded and enabled
!--- AP joins the 5508-3 WLC.
```

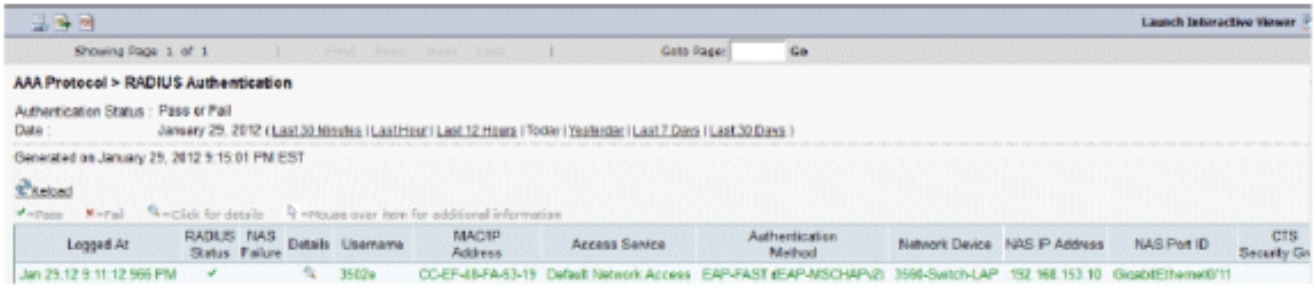
Log ACS:

1. Visualizza il numero di accessi:Se si stanno controllando i registri entro 15 minuti dall'autenticazione, assicurarsi di aggiornare il numero di accessi. Nella stessa pagina, nella parte inferiore è presente la scheda **Conteggio visite**.





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



Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Cisco Secure Access Control System
- 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).