Esempio di configurazione di ACS versione 5.2 e WLC per autenticazione WLAN

Sommario

Introduzione

Questo documento offre un esempio di configurazione per limitare l'accesso per utente a una LAN wireless (WLAN) in base all'identificatore del set di servizi (SSID).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione del controller WLC (Wireless LAN Controller) e del Lightweight Access Point (LAP) per un funzionamento di base
- Configurazione di Cisco Secure Access Control Server (ACS)
- Metodi LWAPP (Lightweight Access Point Protocol) e di sicurezza wireless

Componenti usati

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

- Cisco serie 5500 WLC con firmware versione 7.4.110
- Cisco serie 1142 LAP
- Cisco Secure ACS Server versione 5.2.0.26.11

Configurazione

Per configurare i dispositivi per questa installazione, è necessario:

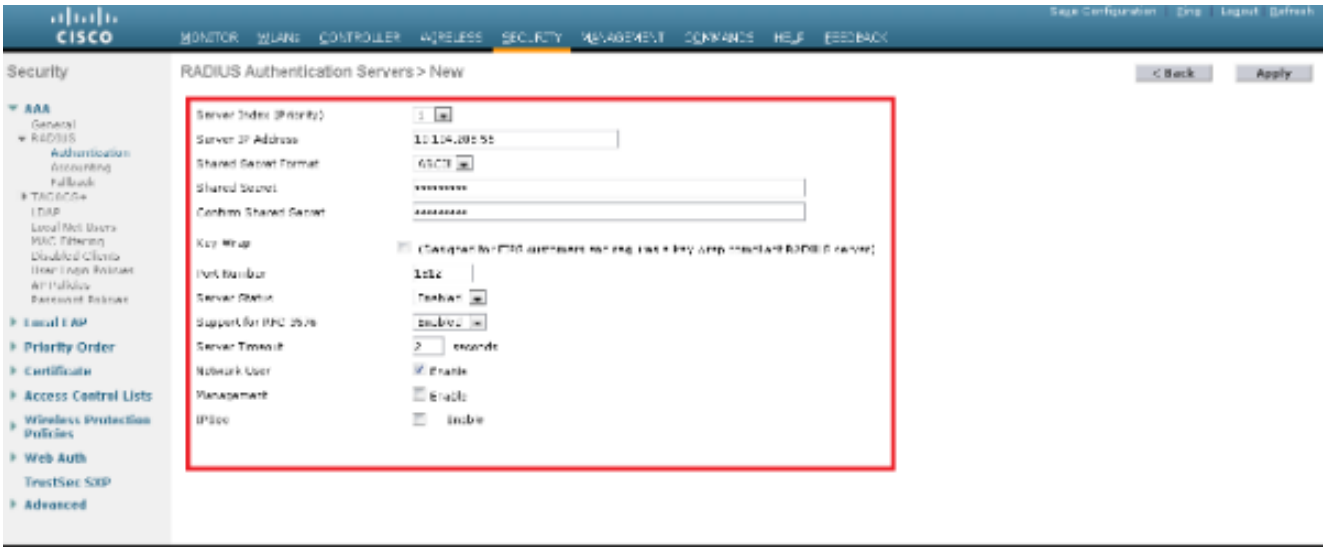
1. Configurare il WLC per le due WLAN e il server RADIUS.
2. Configurare Cisco Secure ACS.
3. Configurare i client wireless e verificare la configurazione.

Configurare il WLC

Completare questa procedura per configurare il WLC per questa configurazione:

1. Configurare il WLC per inoltrare le credenziali dell'utente a un server RADIUS esterno. Il server RADIUS esterno (in questo caso Cisco Secure ACS) convalida quindi le credenziali utente e fornisce l'accesso ai client wireless. Attenersi alla seguente procedura: Selezionare **Sicurezza > Autenticazione RADIUS** dall'interfaccia utente del controller per visualizzare la pagina Server di autenticazione RADIUS.

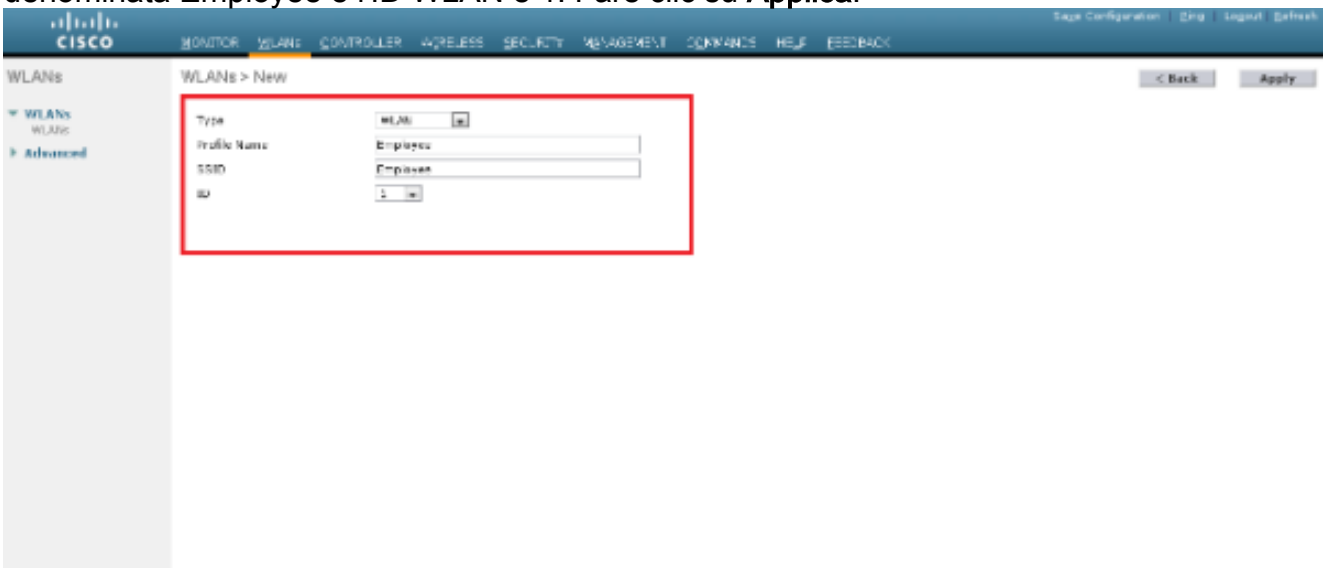
Per definire i parametri del server RADIUS, fare clic su **New** (Nuovo). Questi parametri includono l'indirizzo IP, il segreto condiviso, il numero di porta e lo stato del server RADIUS. Le caselle di controllo Utente di rete e Gestione determinano se l'autenticazione basata su RADIUS è valida per gli utenti di rete e di gestione. In questo esempio viene utilizzato Cisco Secure ACS come server RADIUS con indirizzo IP 10.104.208.56.



Fare clic su **Apply** (Applica).

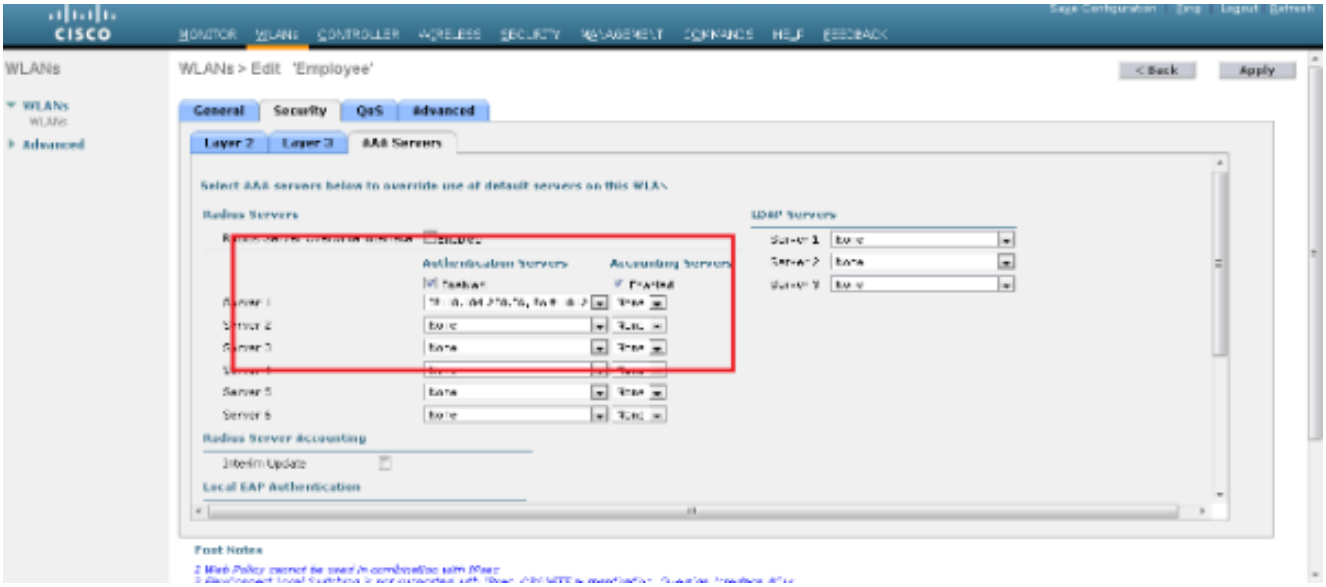
2. Completare questi passaggi per configurare una WLAN per il dipendente con SSID **dipendente** e l'altra WLAN per i collaboratori con SSID **collaboratore esterno**. Per creare una

WLAN, fare clic su **WLAN** dall'interfaccia utente del controller. Viene visualizzata la finestra WLAN. In questa finestra sono elencate le WLAN configurate sul controller.Per configurare una nuova WLAN, fare clic su **New** (Nuovo).In questo esempio viene creata una WLAN denominata Employee e l'ID WLAN è 1. Fare clic su **Applica**.



Selezionare la finestra **WLAN > Modifica** e definire i parametri specifici della WLAN: Dalla scheda Protezione di layer 2, selezionare **802.1x**. Per impostazione predefinita, l'opzione Protezione di livello 2 è 802.1x. Ciò consente l'autenticazione 802.1 x/Extensible Authentication Protocol (EAP) per la WLAN.

Dalla scheda Server AAA, selezionare il server RADIUS appropriato dall'elenco a discesa in Server RADIUS. Gli altri parametri possono essere modificati in base ai requisiti della rete WLAN. Fare clic su **Apply** (Applica).



Analogamente, per creare una WLAN per i collaboratori esterni, ripetere i passaggi da b a d.

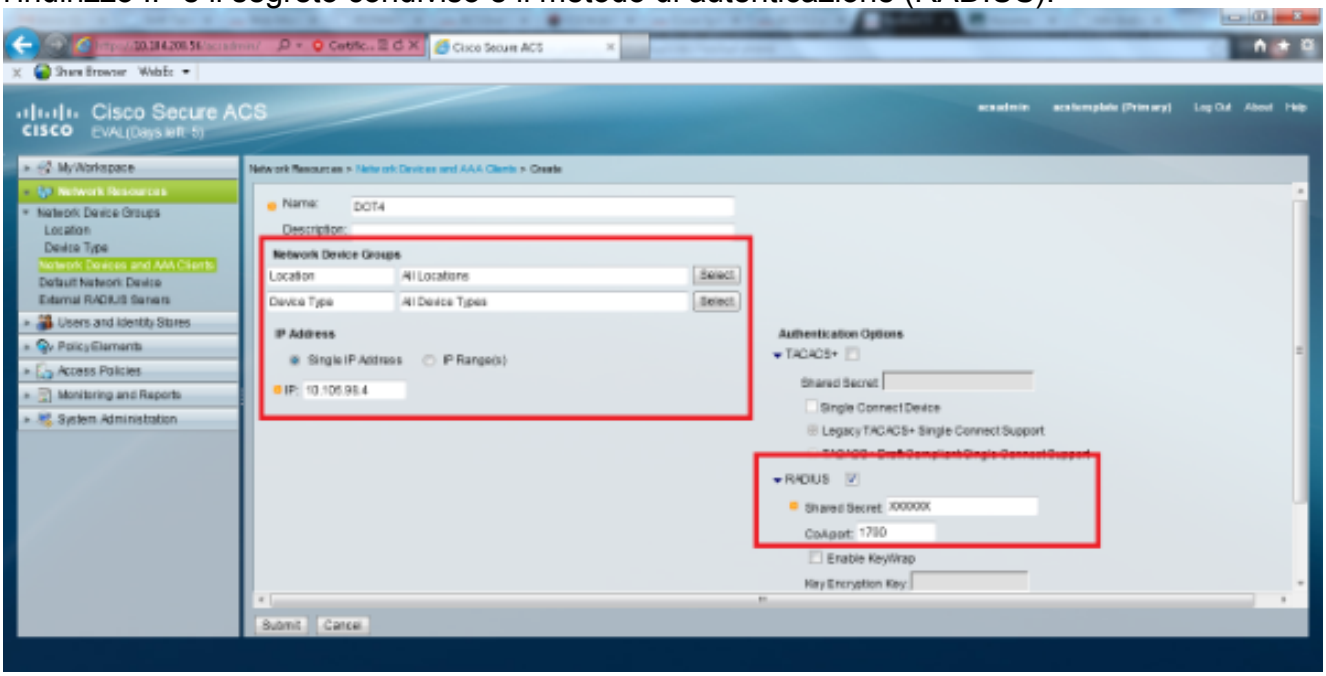
Configurazione di Cisco Secure ACS

Sul server Cisco Secure ACS è necessario:

1. Configurare il WLC come client AAA.
2. Creare il database utenti (credenziali) per l'autenticazione basata su SSID.
3. Abilitare l'autenticazione EAP.

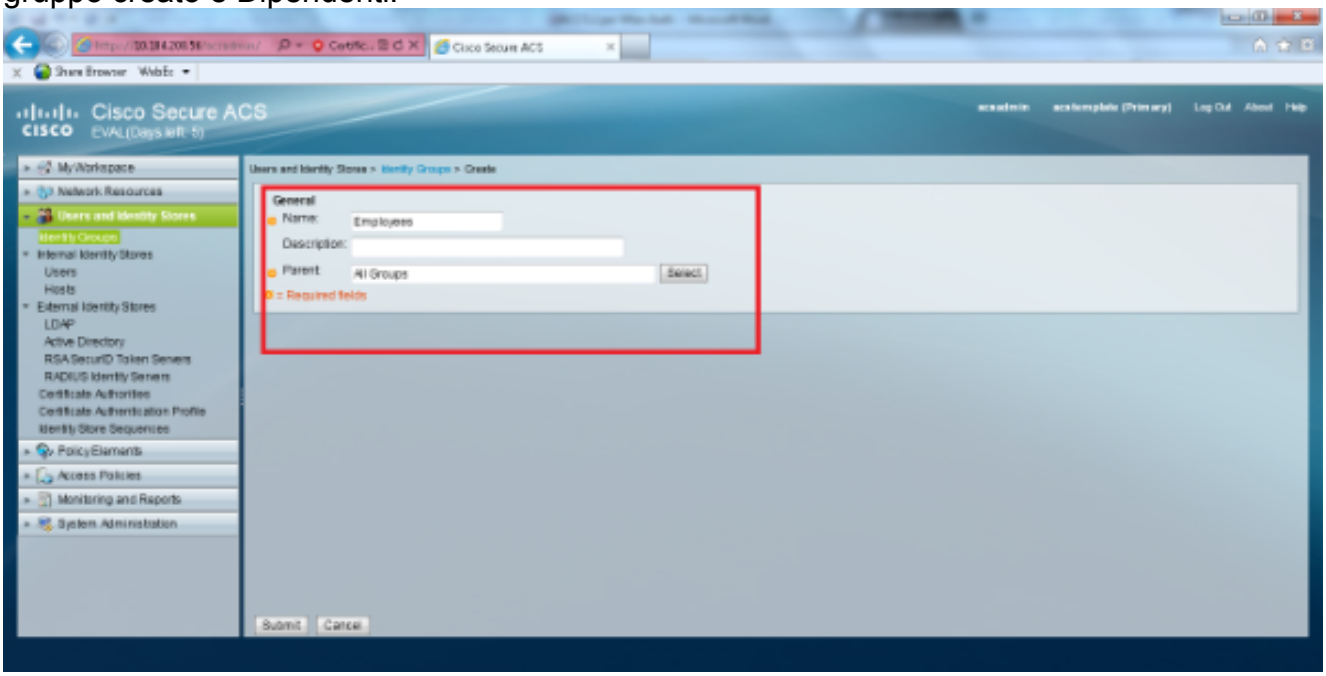
Completare questi passaggi su Cisco Secure ACS:

1. Per definire il controller come client AAA sul server ACS, selezionare **Risorse di rete > Dispositivi di rete e client AAA** dall'interfaccia utente di ACS. In Dispositivi di rete e client AAA, fare clic su **Crea.**
2. Quando viene visualizzata la pagina Configurazione di rete, definire il nome del WLC, l'indirizzo IP e il segreto condiviso e il metodo di autenticazione (RADIUS).

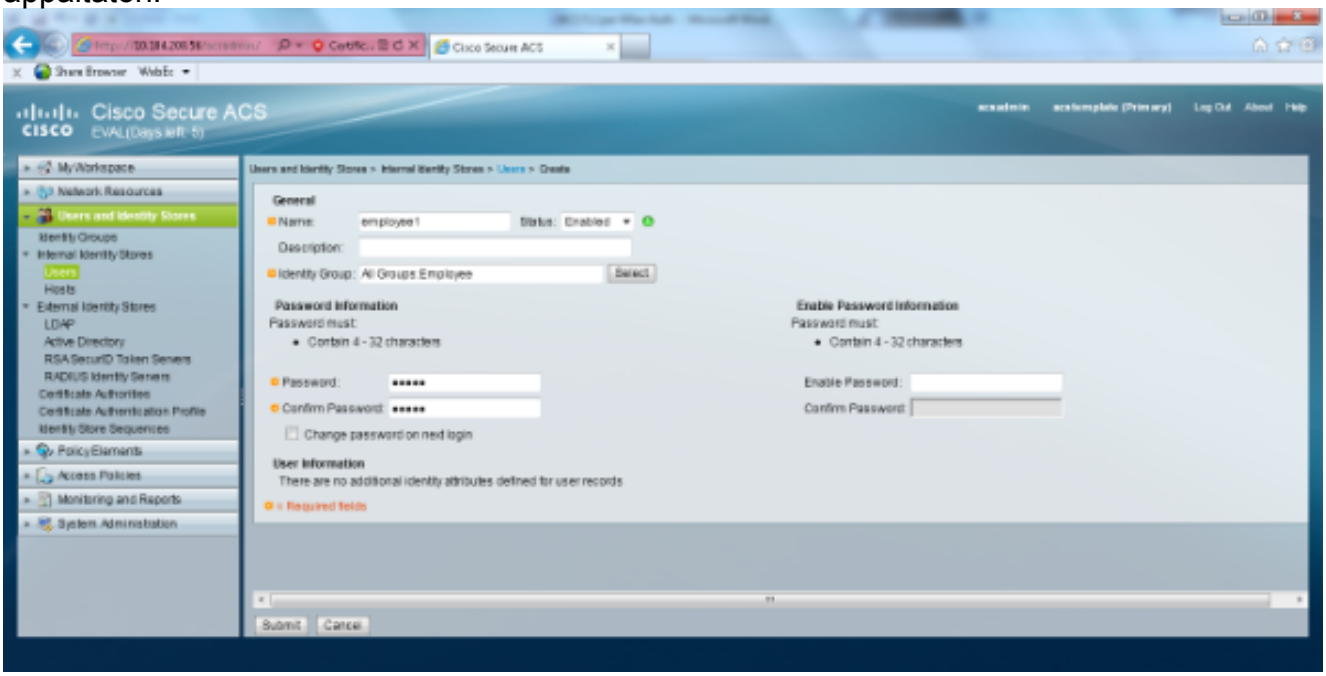


3. Selezionare **Utenti e archivi identità > Gruppi di identità** dalla GUI di ACS. Creare i rispettivi gruppi per dipendente e appaltatore e fare clic su **Crea**. In questo esempio il nome del

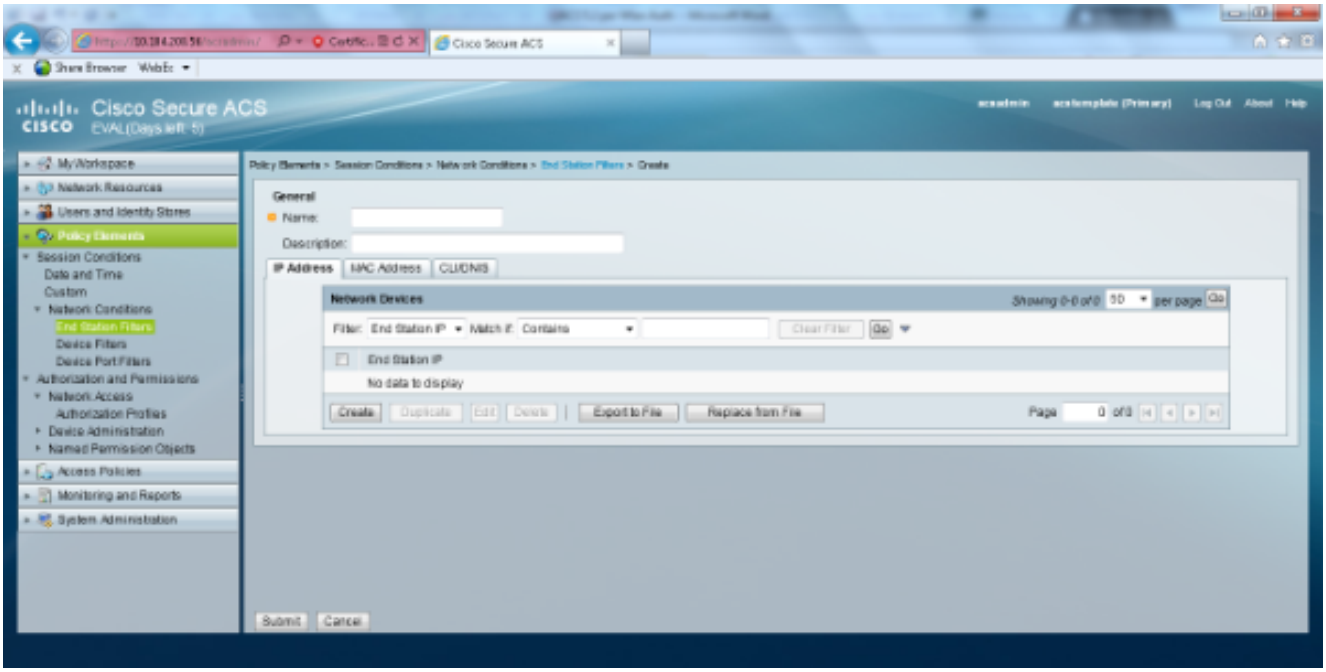
gruppo creato è Dipendenti.



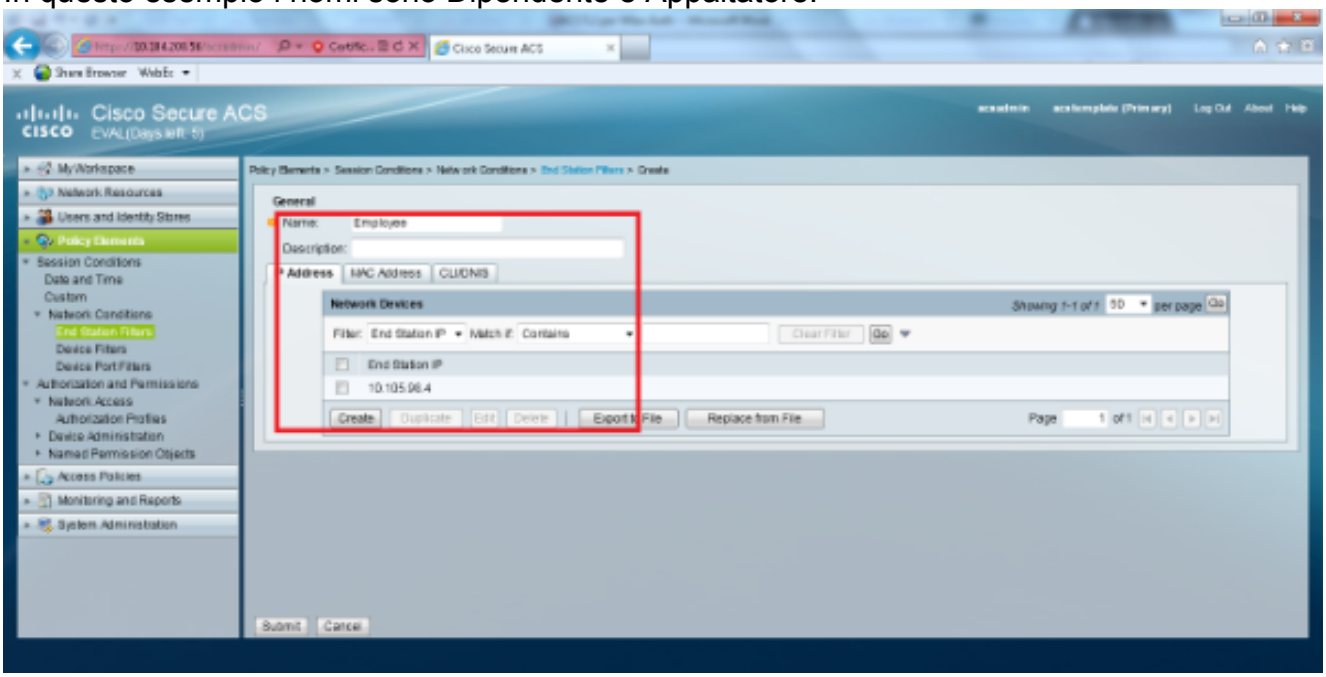
4. Selezionare **Utenti e archivi identità > Archivi identità interni**. Fare clic su **Create** (Crea) e immettere il nome utente. Inserirli nel gruppo corretto, definirne la password e fare clic su **Invia**.In questo esempio viene creato un utente denominato employee1 nel gruppo Employee. Analogamente, creare un utente denominato appaltatore1 nel gruppo appaltatori.



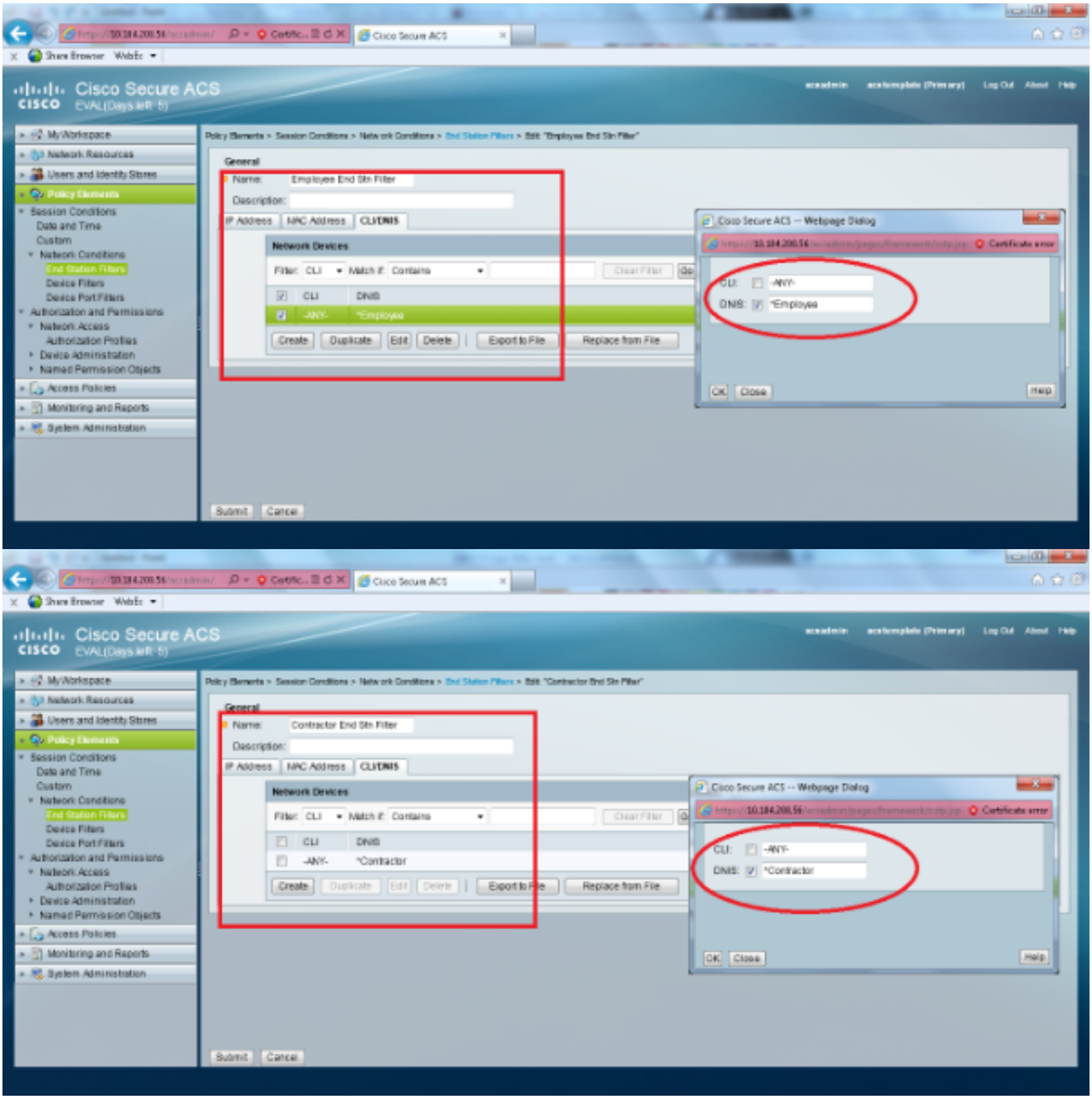
5. Selezionare **Elementi dei criteri > Condizioni di rete > Filtri stazioni finali**. Fare clic su **Crea**.



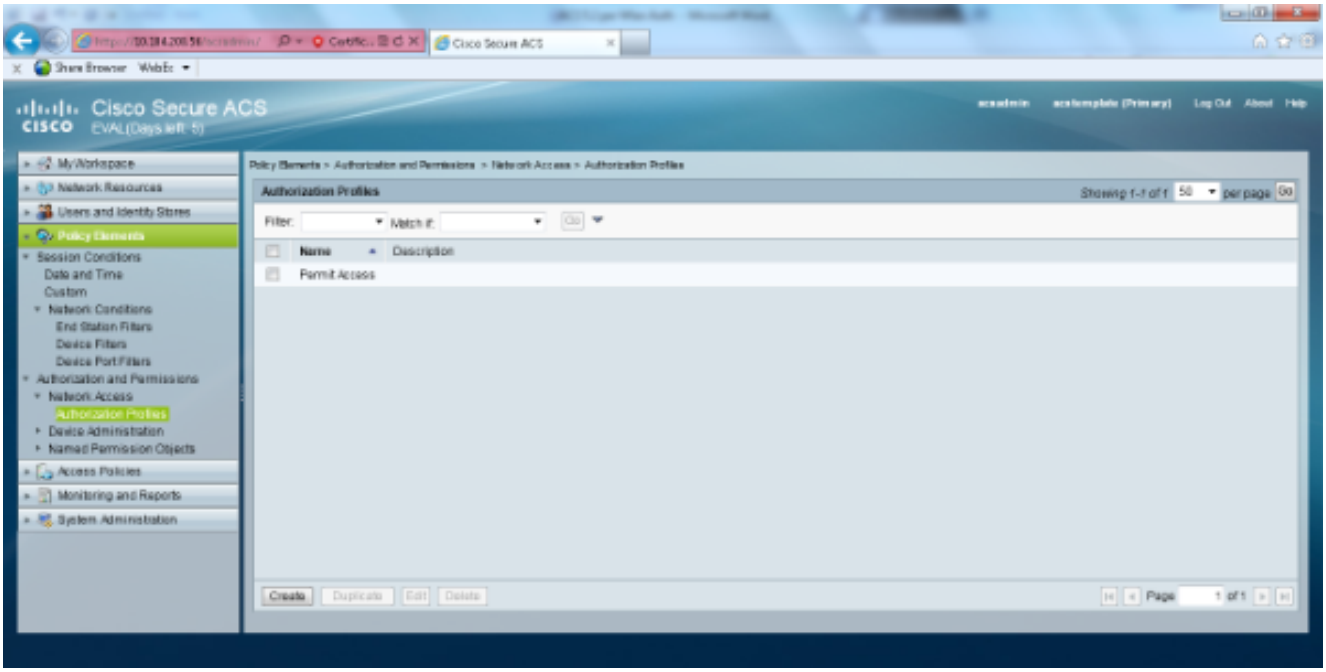
Immettere un nome significativo e nella scheda **Indirizzo IP** immettere l'indirizzo IP del WLC. In questo esempio i nomi sono Dipendente e Appaltatore.



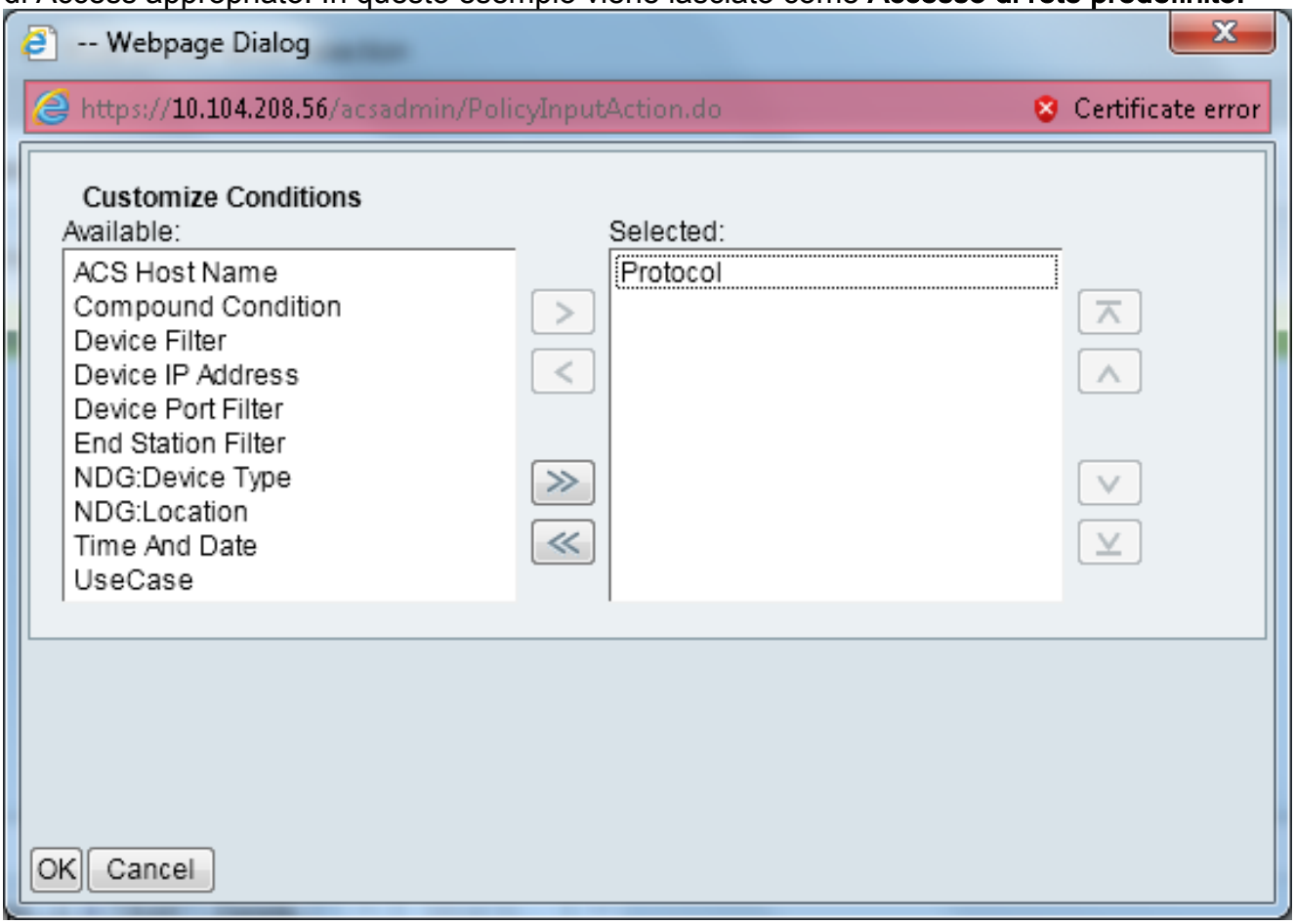
Nella scheda CLI/DNIS, lasciare CLI come -ANY- e immettere DNIS come *<SSID>. In questo esempio, il campo DNIS viene immesso come *Dipendente in quanto questo filtro della stazione terminale viene utilizzato per limitare l'accesso solo alla WLAN del dipendente. L'attributo DNIS definisce l'SSID a cui l'utente può accedere. Il WLC invia l'SSID nell'attributo DNIS al server RADIUS.Ripetere gli stessi passaggi per il filtro Stazione finale terzista.

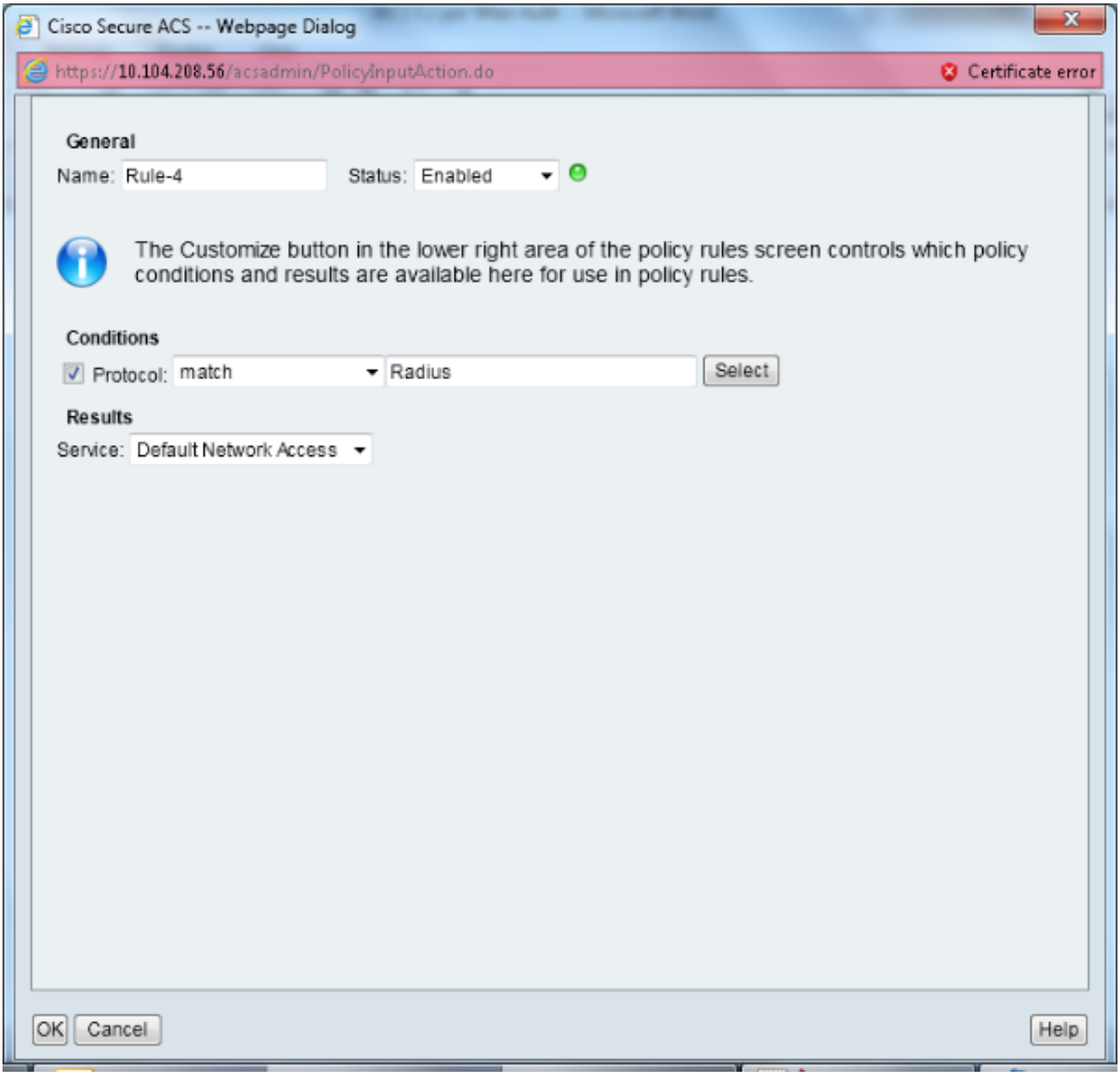


6. Selezionare **Elementi criteri > Autorizzazioni e autorizzazioni > Accesso alla rete > Profili di autorizzazione**. Deve essere presente un profilo predefinito per Permit Access.

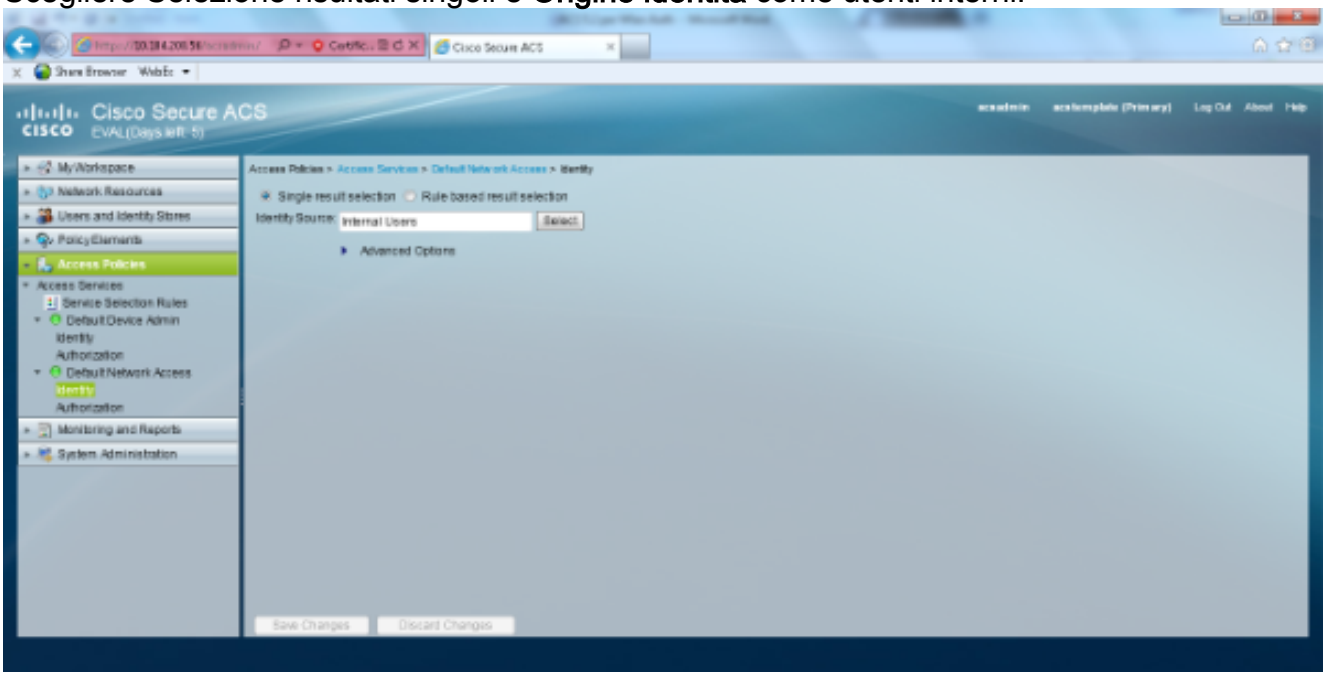


7. Selezionare **Criteri di accesso > Servizi di accesso > Regole selezione servizi**. Fare clic su **Personalizza**. Aggiungere eventuali condizioni appropriate. In questo esempio viene utilizzato il protocollo Radius come condizione di corrispondenza.Fare clic su **Crea**. Denominare la regola. Selezionare **Protocollo**, quindi **Raggio.**In **Risultati** scegliere il servizio di Access appropriato. In questo esempio viene lasciato come **Accesso di rete predefinito.**

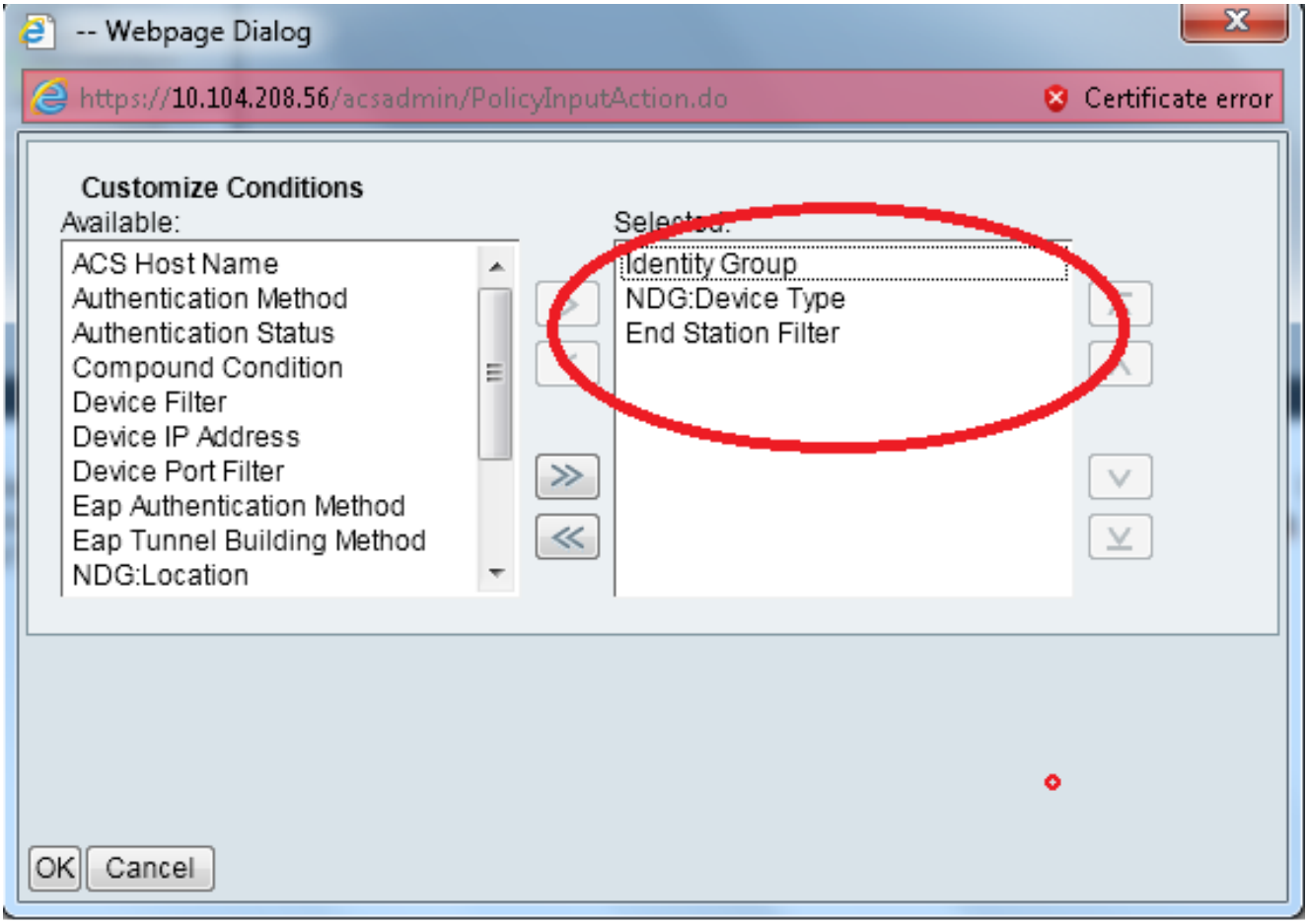




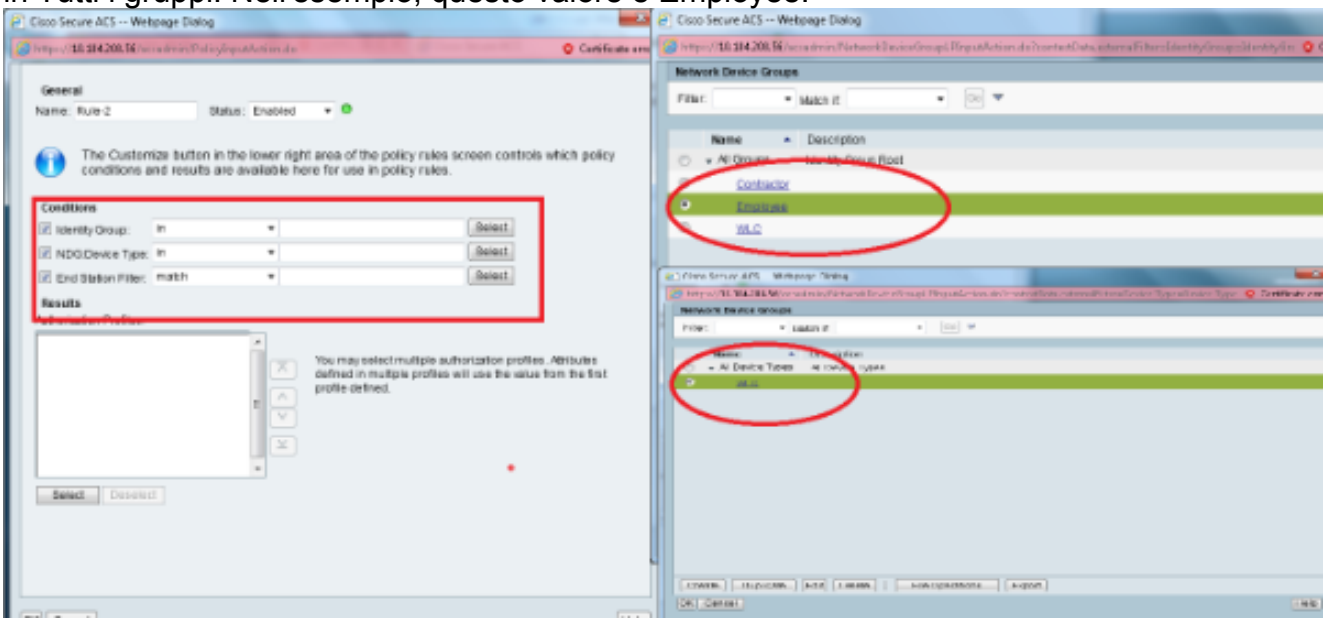
8. Selezionare **Criteri di accesso > Servizi di accesso > Accesso di rete predefinito > Identità**. Scegliere Selezione risultati singoli e **Origine identità** come utenti interni.



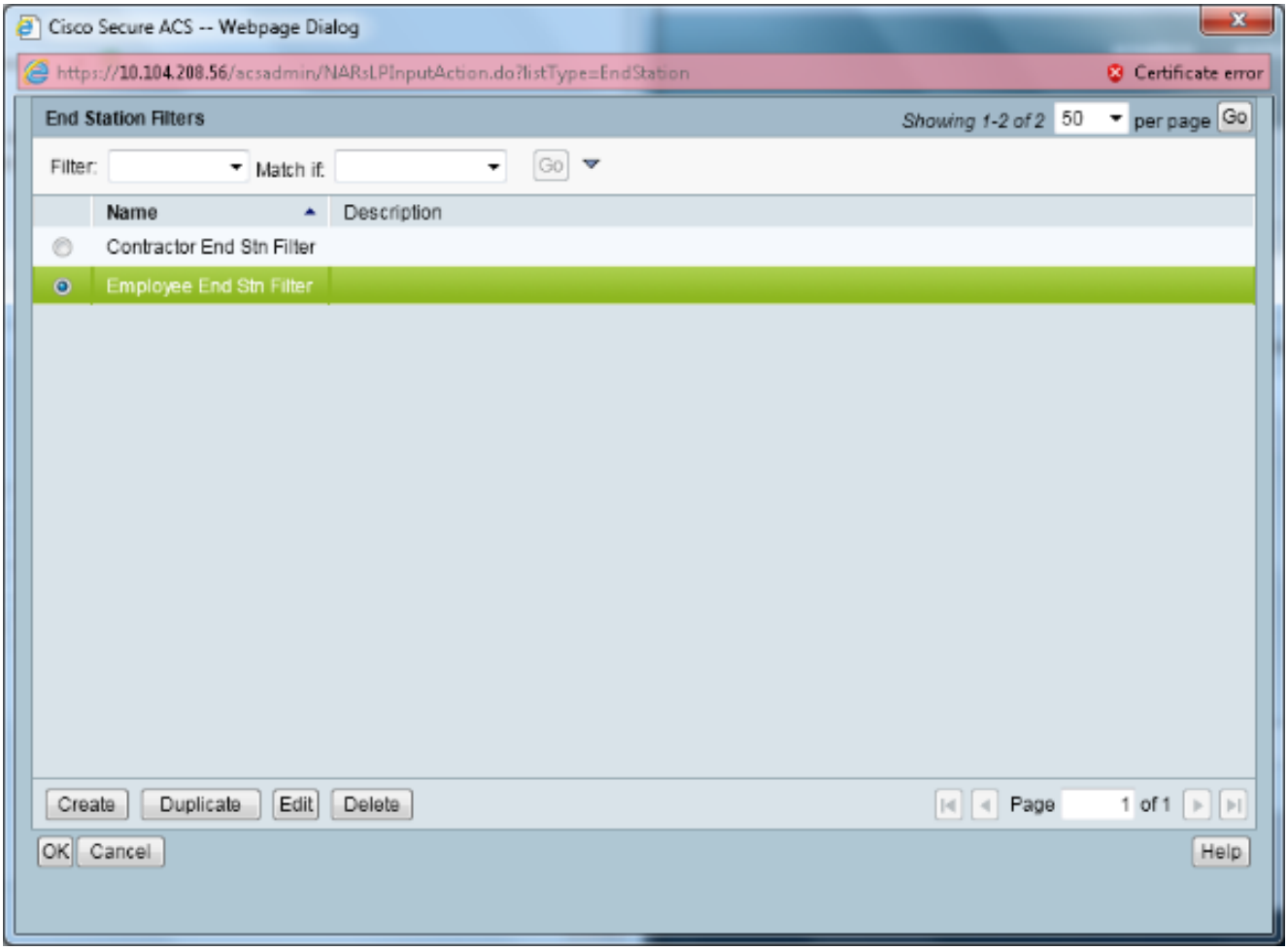
Selezionare **Criteri di accesso > Servizi di accesso > Accesso alla rete predefinito > Autorizzazione.** Fare clic su **Personalizza** e aggiungere le condizioni Personalizzate. In questo esempio vengono utilizzati, nell'ordine, Identity Group, NDG:Device Type e End Station Filter.



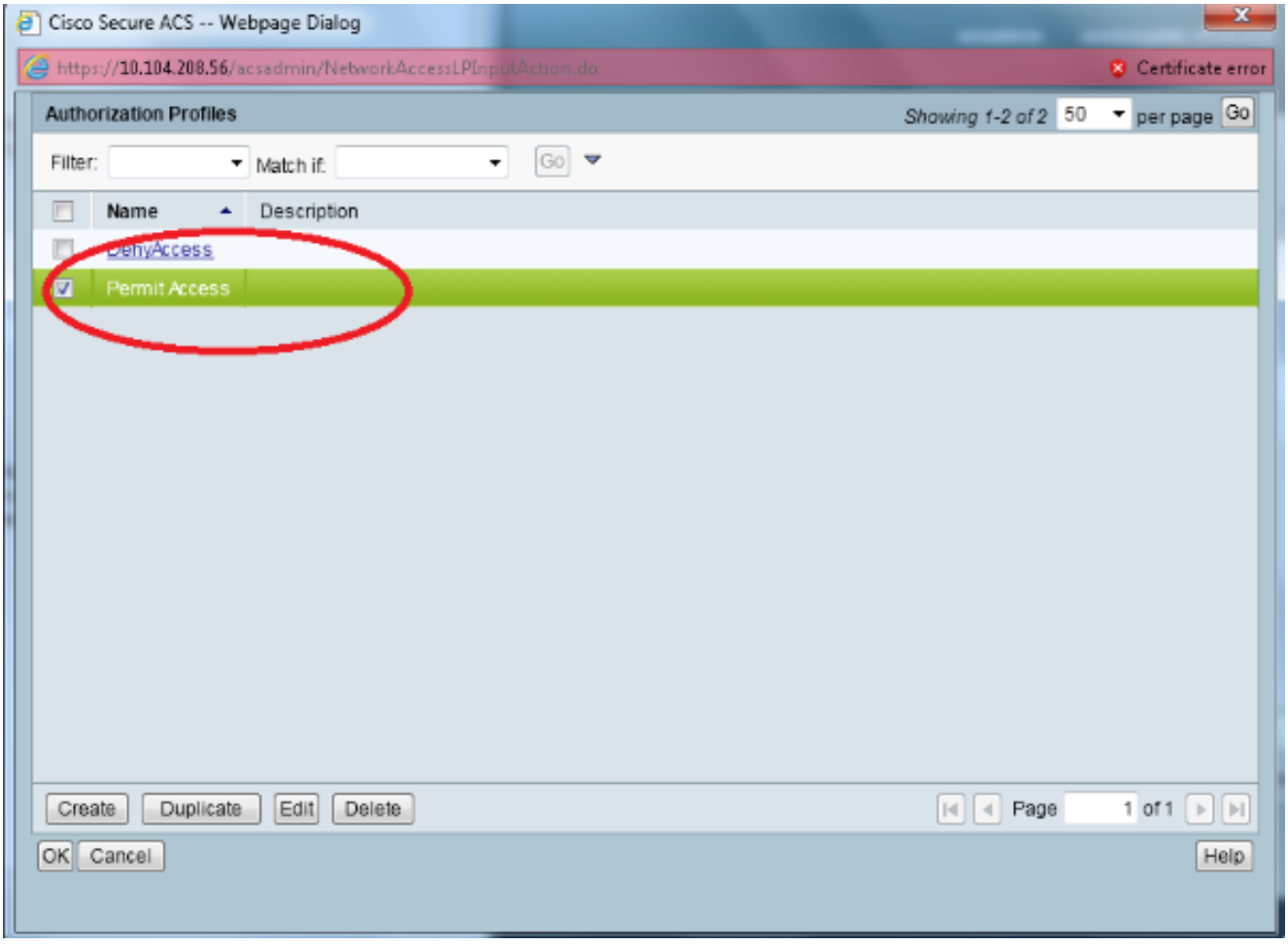
Fare clic su **Crea**. Assegnare un nome alla regola e scegliere il gruppo di identità appropriato in Tutti i gruppi. Nell'esempio, questo valore è Employee.



Fare clic sul pulsante di opzione **Employee End Stn Filter** o immettere il nome immesso al punto 1b nella sezione "Configurazione del WLC".

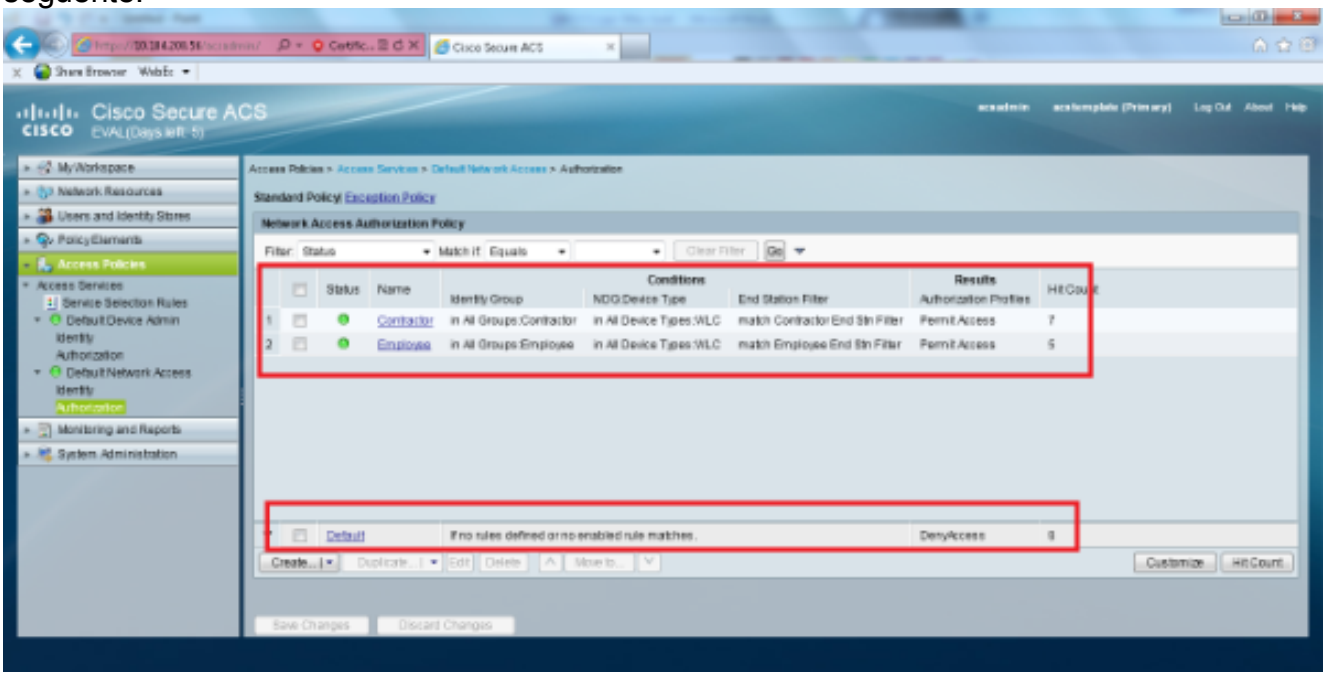


Selezionare la casella di controllo **Consenti accesso**.



Ripetere gli stessi passaggi descritti in precedenza anche per le regole collaboratori esterni.

Assicurarsi che l'azione predefinita sia **Nega accesso**. Dopo aver completato il passaggio e, le regole dovrebbero essere simili a quelle riportate nell'esempio seguente:



La configurazione è terminata. Dopo questa sezione, il client deve essere configurato di conseguenza con l'SSID e i parametri di sicurezza per potersi connettere.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

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