Amministrazione di dispositivi di Cisco WLC con TACACS+

Sommario

Introduzione

Questo documento descrive come configurare TACACS+ per l'amministrazione dei dispositivi di Cisco Wireless LAN Controller (WLC) con Identity Service Engine (ISE).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di Identity Service Engine (ISE)
- Conoscenze base di Cisco Wireless LAN Controller (WLC)

Componenti usati

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

- Cisco Identity Service Engine 2.4
- Cisco Wireless LAN Controller 8.5.135

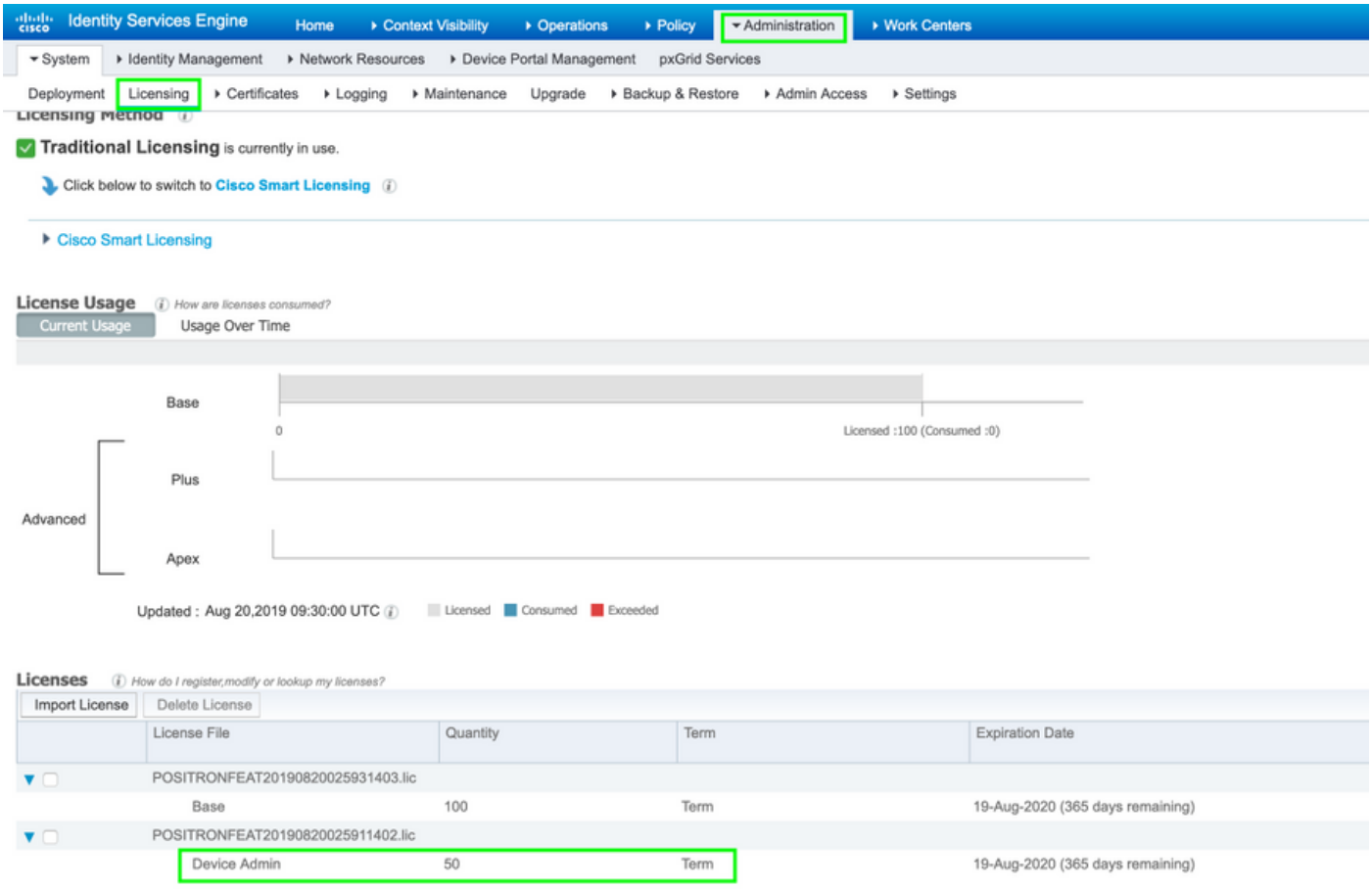
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Passaggio 1. Controllare la licenza di amministrazione del dispositivo.

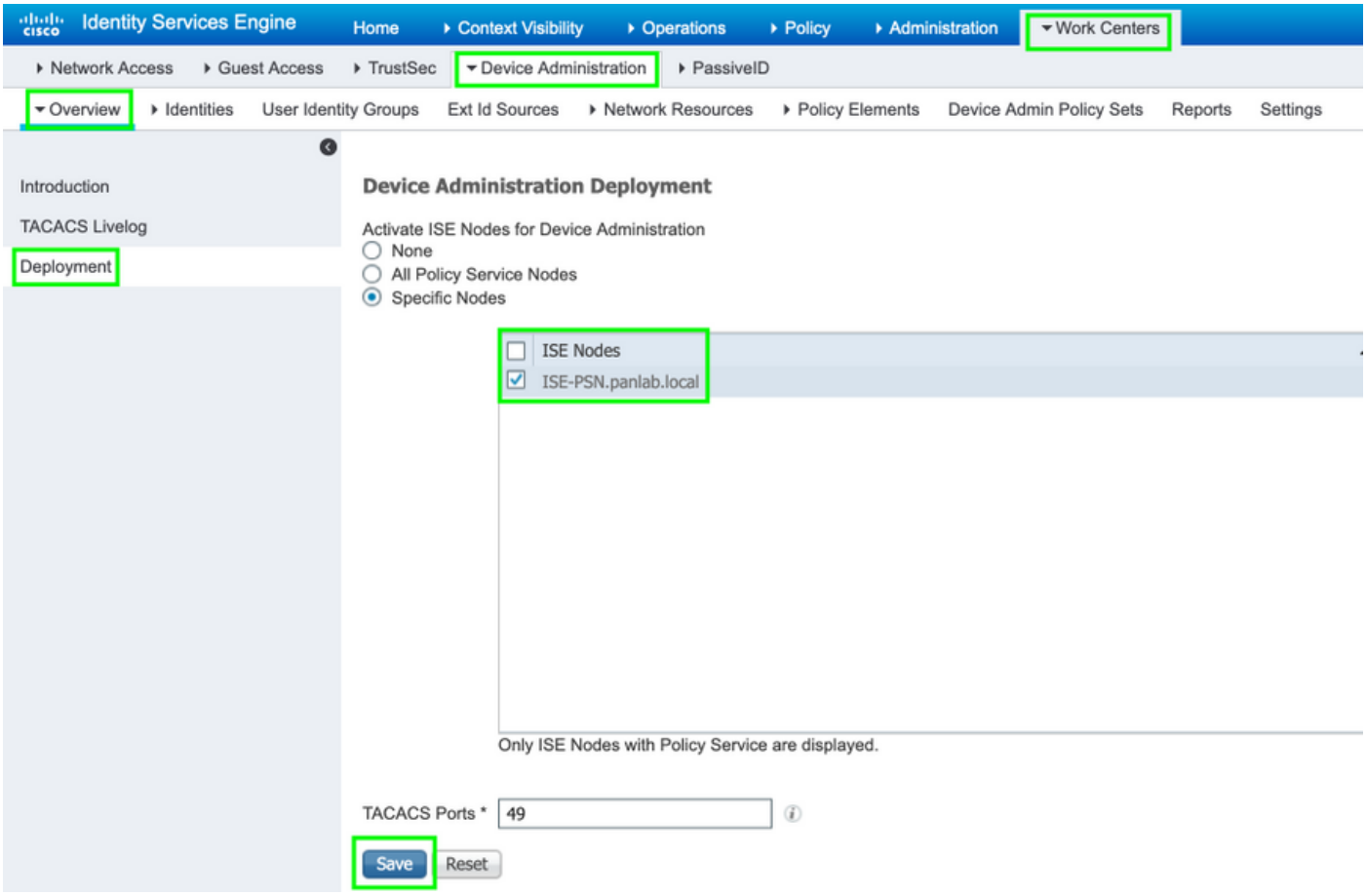
Passare a **Amministrazione > Sistema >** scheda **Licenze** e verificare che la licenza di **Device Admin** sia installata, come mostrato nell'immagine.



> **Nota:** Per usare la funzionalità TACACS+ su ISE, è necessaria una licenza di amministratore del dispositivo.

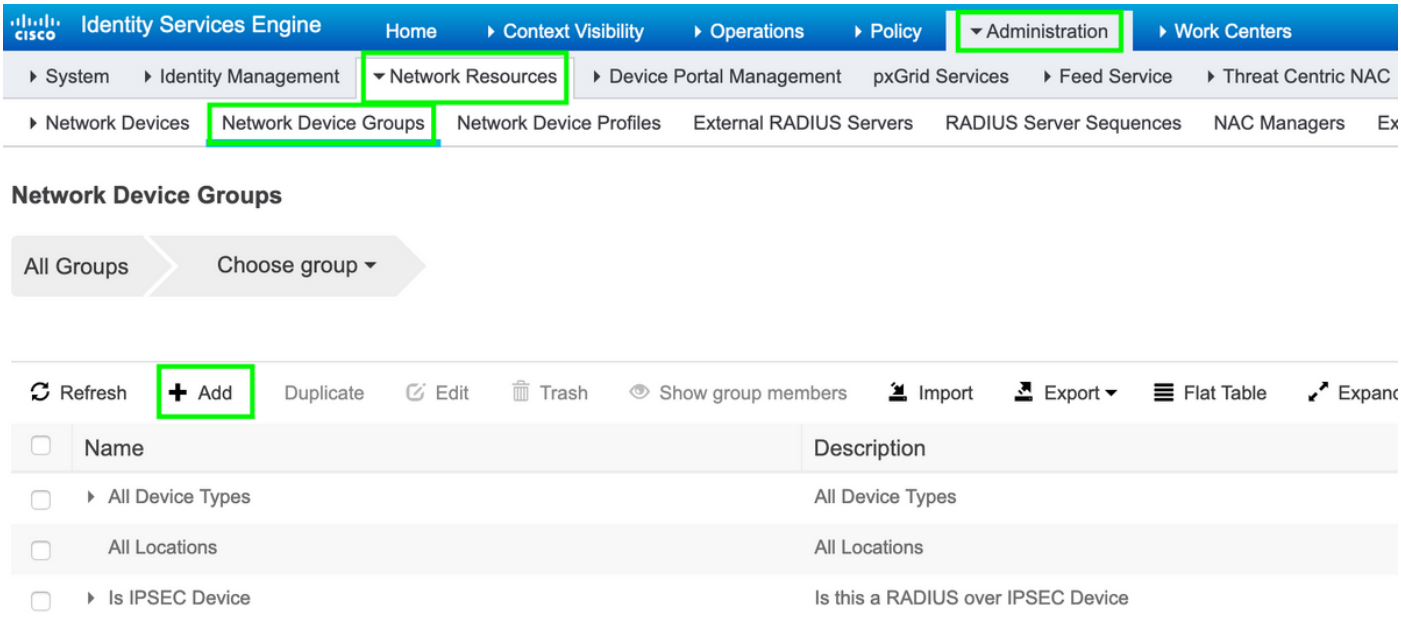
Passaggio 2. Abilitare l'amministrazione dei dispositivi sui nodi PSN ISE.

Passare a **Centri di lavoro > Amministrazione dispositivi > Panoramica**, fare clic su **Distribuzione** scheda**, Selezionare** il pulsante di scelta Nodo PSN specifico**. Abilitare** Device Administration sul nodo ISE selezionando la **casella di controllo** e facendo clic su **save**, come mostrato nell'immagine:



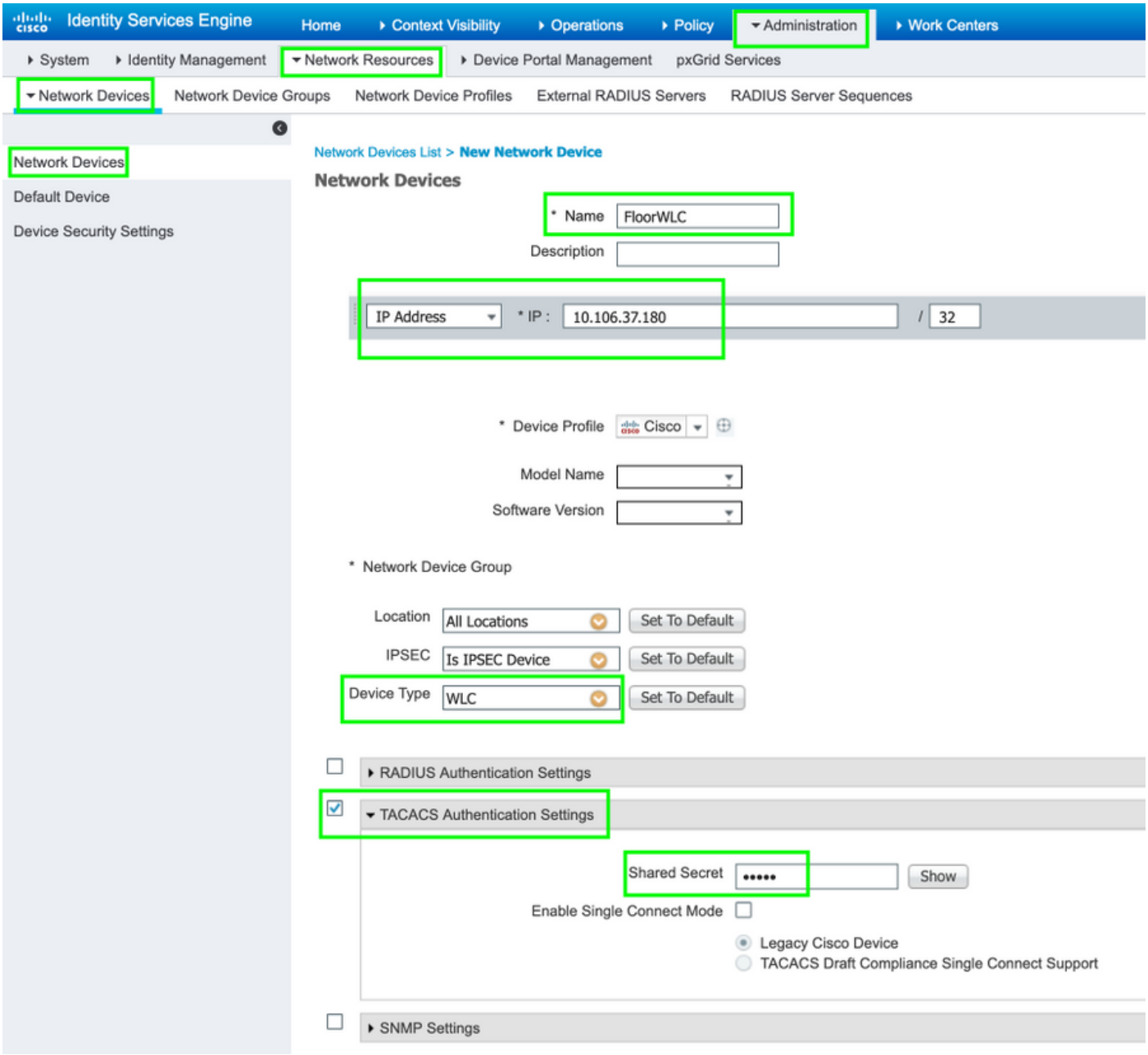
Passaggio 3. Creare un gruppo di dispositivi di rete.

Per aggiungere il WLC come dispositivo di rete sull'ISE, selezionare **Amministrazione > Risorse di rete > Gruppi di dispositivi di rete > Tutti i tipi di dispositivo**, quindi creare un **nuovo gruppo** per il WLC, come mostrato nell'immagine:



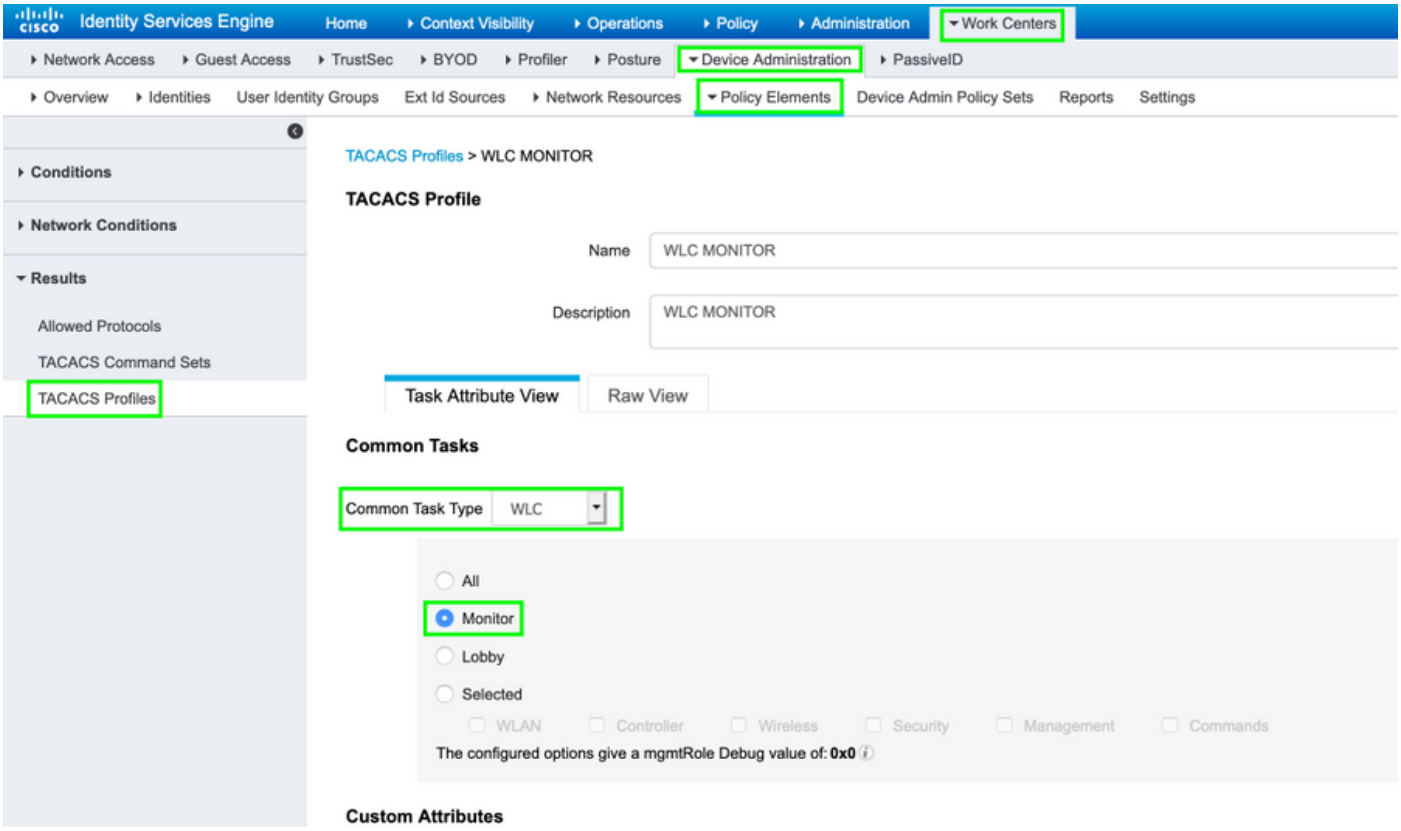
Passaggio 4. Aggiungere WLC come dispositivo di rete.

Passare a **Centri di lavoro > Amministrazione dispositivi > Risorse di rete > Dispositivi di rete**. Fare clic su Add, fornire Name, IP Address e selezionare il tipo di dispositivo come **WLC**, selezionare la casella di controllo **TACACS+Authentication Settings** e fornire la **chiave Shared Secret**, come mostrato nell'immagine:

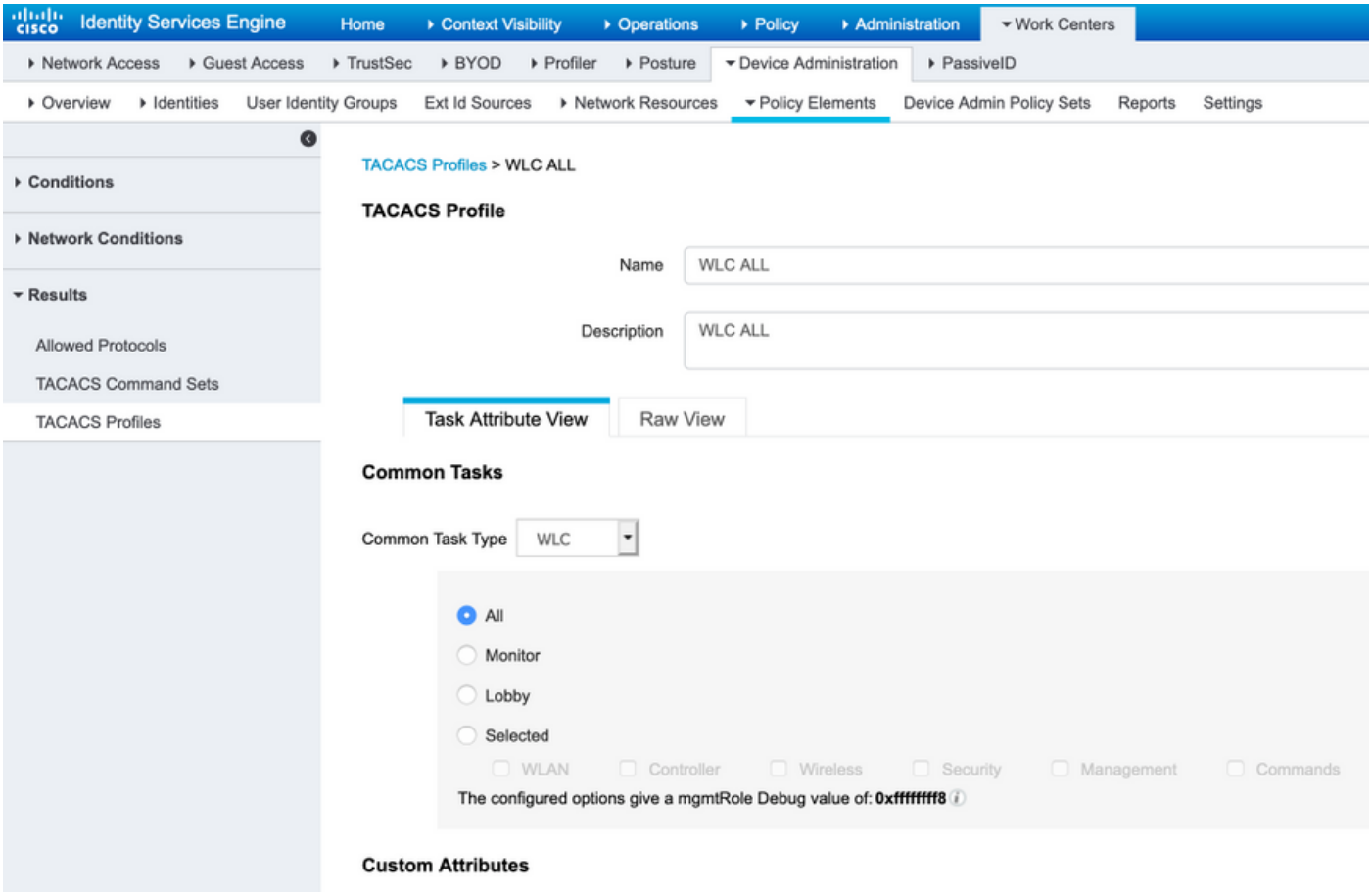


Passaggio 5. Creare un profilo TACACS per WLC.

Passare a **Centri di lavoro > Amministrazione dispositivi > Elementi della policy > Risultati > Profili TACACS.** Fare clic su **Add (Aggiungi) e** specificare un **nome. Nella scheda Visualizzazione attributi task**, selezionare **WLC** per **Tipo di task comune.** Sono presenti profili predefiniti dai quali selezionare **Controlla** per consentire un accesso limitato agli utenti, come mostrato nell'immagine.

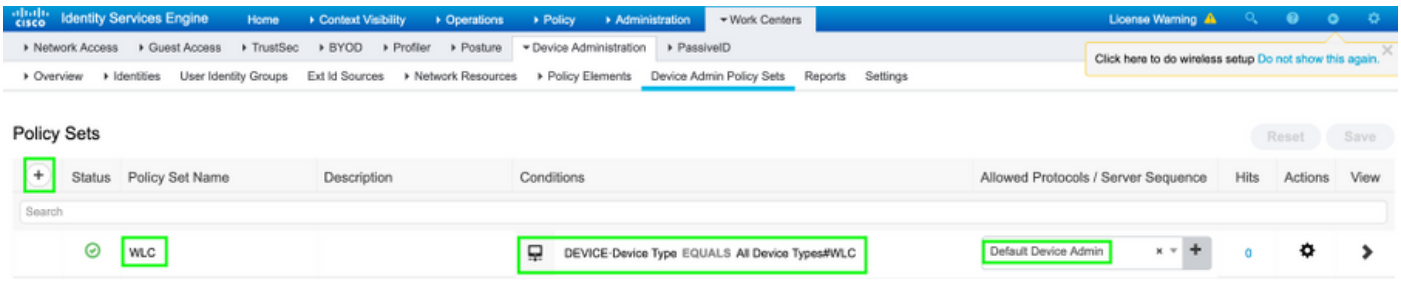


Esiste un altro profilo predefinito **All** che consente l'accesso completo all'utente, come mostrato nell'immagine.



Passaggio 6. Creare un set di criteri.

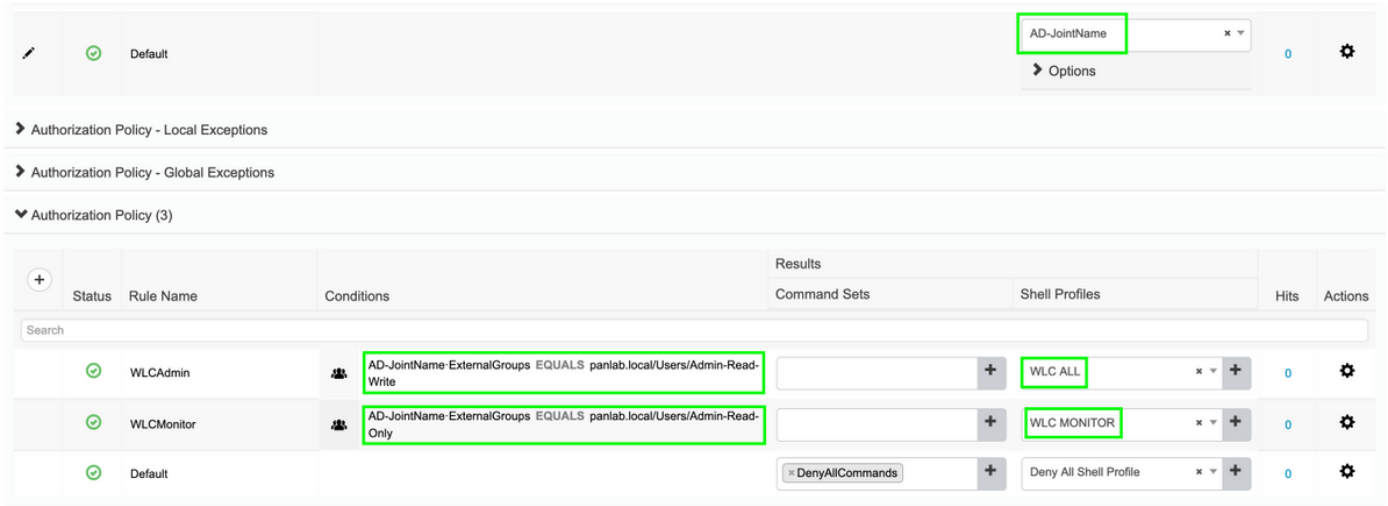
Passare a **Centri di lavoro > Amministrazione dispositivi > Set di criteri di amministrazione dispositivi.** Fare clic su **(+)** e assegnare un nome al set di criteri. Nella condizione del criterio selezionare **Device Type** as WLC, Allowed protocols can be **Default Device Admin**, come mostrato nell'immagine.



Passaggio 7. Creazione di criteri di autenticazione e autorizzazione.

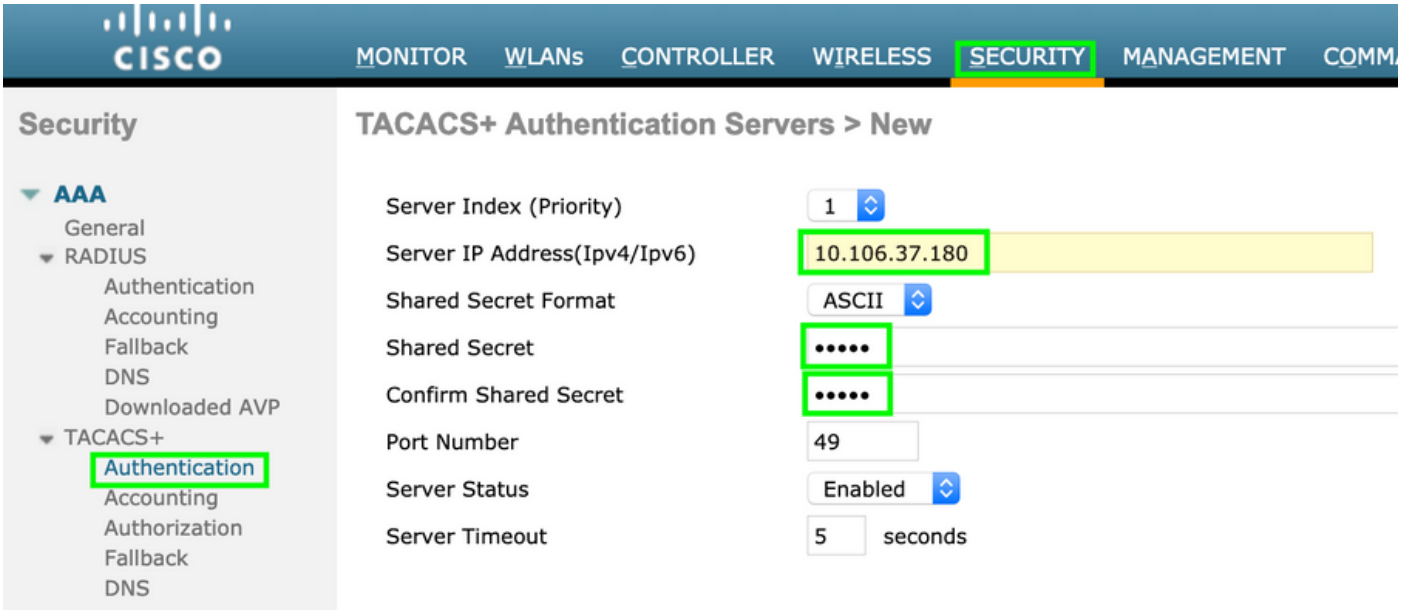
In questo documento, due gruppi di esempio, **Admin-Read-Write** e **Admin-Read-Only** sono configurati su Active Directory e un utente all'interno di ogni gruppo **admin1**, **admin2** rispettivamente. Active Directory è integrato con ISE tramite un punto di unione denominato **AD-JointName.**

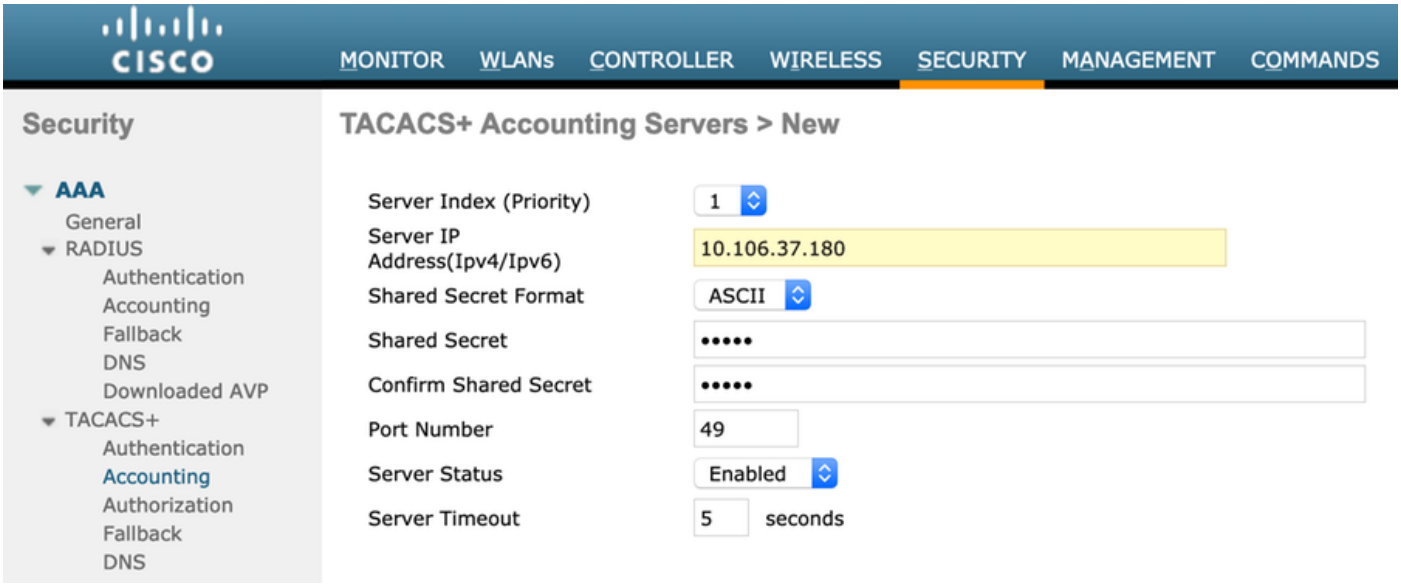
Creare due criteri di autorizzazione, come illustrato nell'immagine:



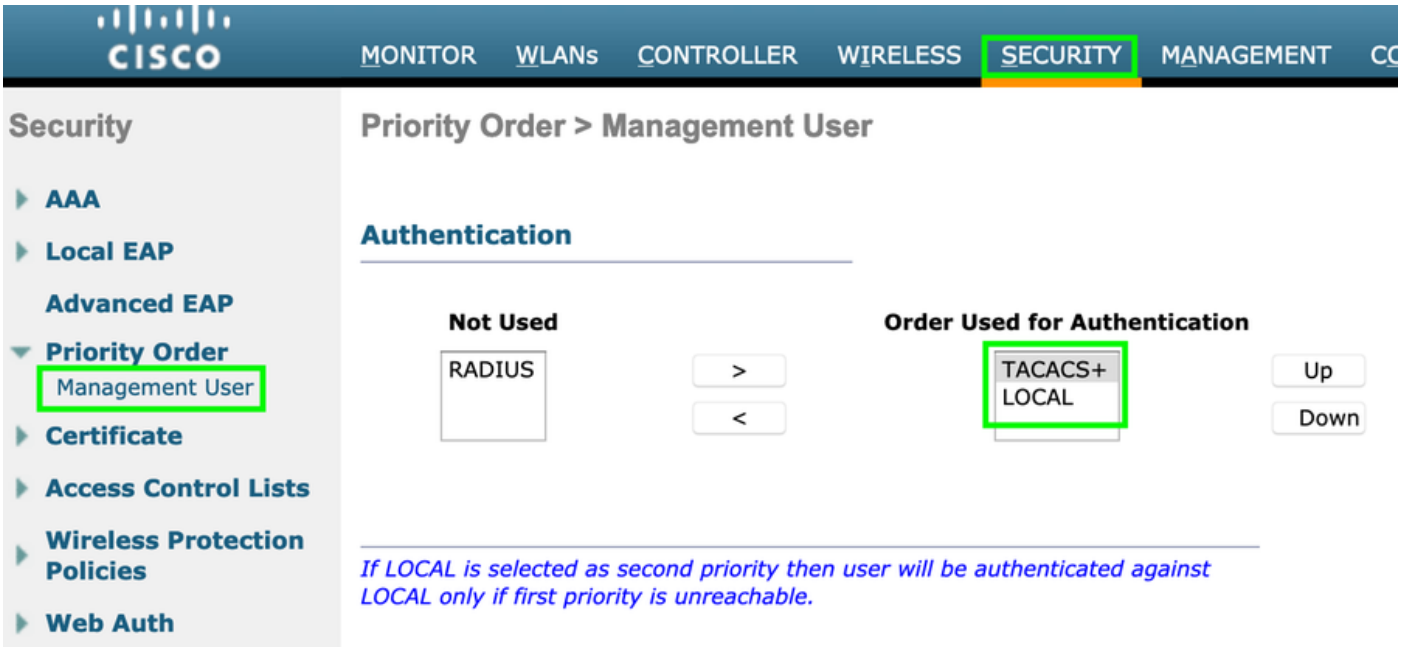
Passaggio 8. Configurare WLC per Device Administration.

Selezionare **Security > AAA > TACACS+** fare clic su **New** (Nuova) e aggiungere Authentication (Autenticazione), Accounting server, come mostrato nell'immagine.





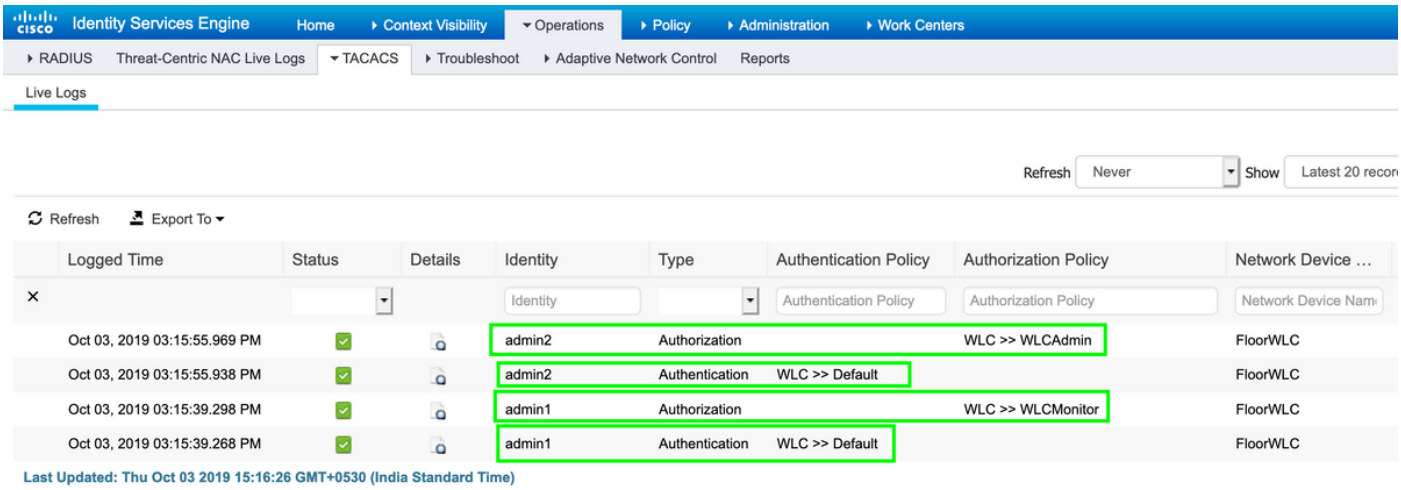
Modificare l'ordine di priorità e impostare TACACS+ in alto e Local in basso, come mostrato nell'immagine:



Attenzione: Non chiudere la sessione GUI WLC corrente. Si consiglia di aprire la GUI del WLC in un browser Web diverso e verificare se l'accesso con le credenziali TACACS+ funziona o meno. In caso contrario, verificare la configurazione e la connettività al nodo ISE sulla porta TCP 49.

Verifica

Passare a **Operazioni > TACACS > Live Log** e monitorare i **Live Log**. Aprire l'interfaccia utente WLC e accedere con le credenziali utente di Active Directory, come mostrato nell'immagine



Risoluzione dei problemi

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