Configurazione dell'autenticazione TACACS Prime 3.1 per ISE 2.x

Sommario

Introduzione

Questo documento descrive come configurare Prime Infrastructure per l'autenticazione tramite TACACS con ISE 2.x.

Requisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

- Identity Services Engine (ISE)
- Prime Infrastructure

Configurazione

Cisco Prime Network Control System 3.1

Cisco Identity Service Engine 2.0 o versione successiva.

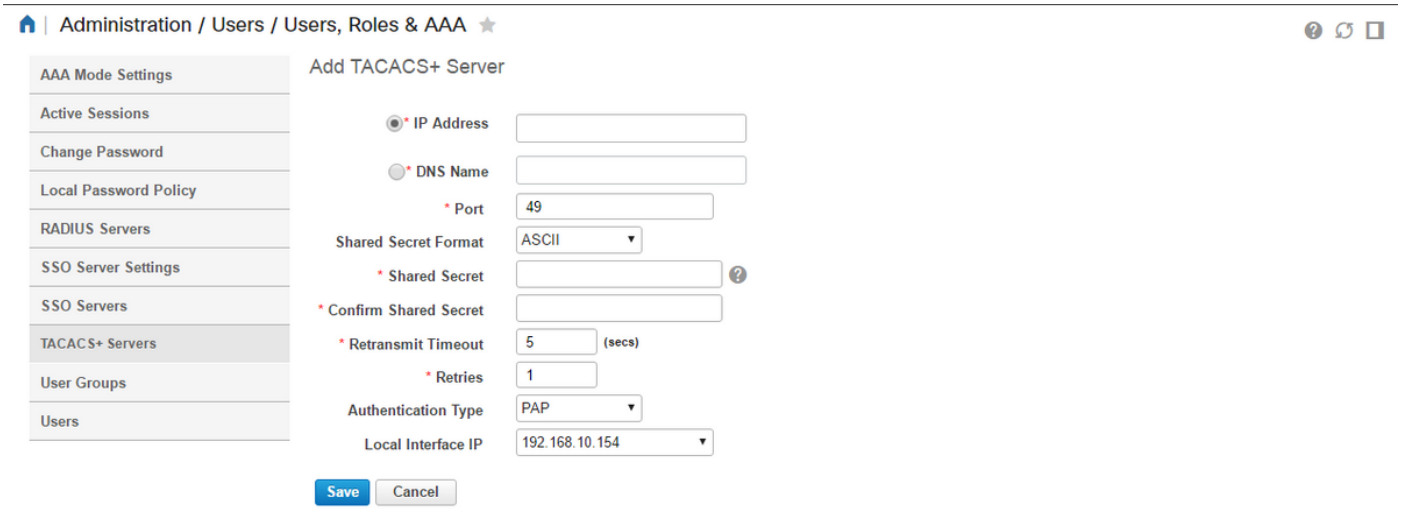
(Nota: ISE supporta solo TACACS a partire dalla versione 2.0, ma è possibile configurare Prime per l'utilizzo di Radius. Prime include l'elenco degli attributi Radius oltre a TACACS se si preferisce utilizzare Radius, con una versione precedente di ISE o una soluzione di terze parti.)

Prime Configuration

Passare alla schermata seguente: Amministrazione / Utenti/ Utenti, Ruoli & AAA come mostrato di seguito.

Quindi, selezionare la scheda TACACS+ Server, selezionare l'opzione Add TACACS+ Server (Aggiungi server TACACS+) nell'angolo in alto a destra e selezionare go (Vai).

Nella schermata successiva è disponibile la configurazione della voce relativa al server TACACS (questa operazione deve essere eseguita per ciascun server TACACS).



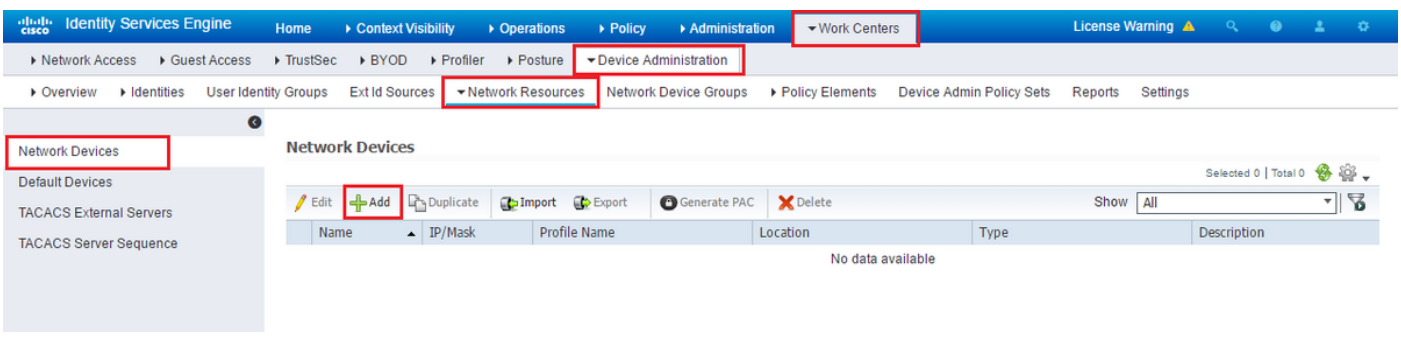
Immettere l'indirizzo IP o l'indirizzo DNS del server, nonché la chiave privata condivisa. Notare anche l'indirizzo IP dell'interfaccia locale che si desidera usare, poiché questo stesso indirizzo IP deve essere usato per il client AAA ad ISE.

Per completare la configurazione su Prime. È necessario abilitare TACACS in Amministrazione / Utenti / Utenti, Ruoli & AAA nella scheda Impostazioni modalità AAA.

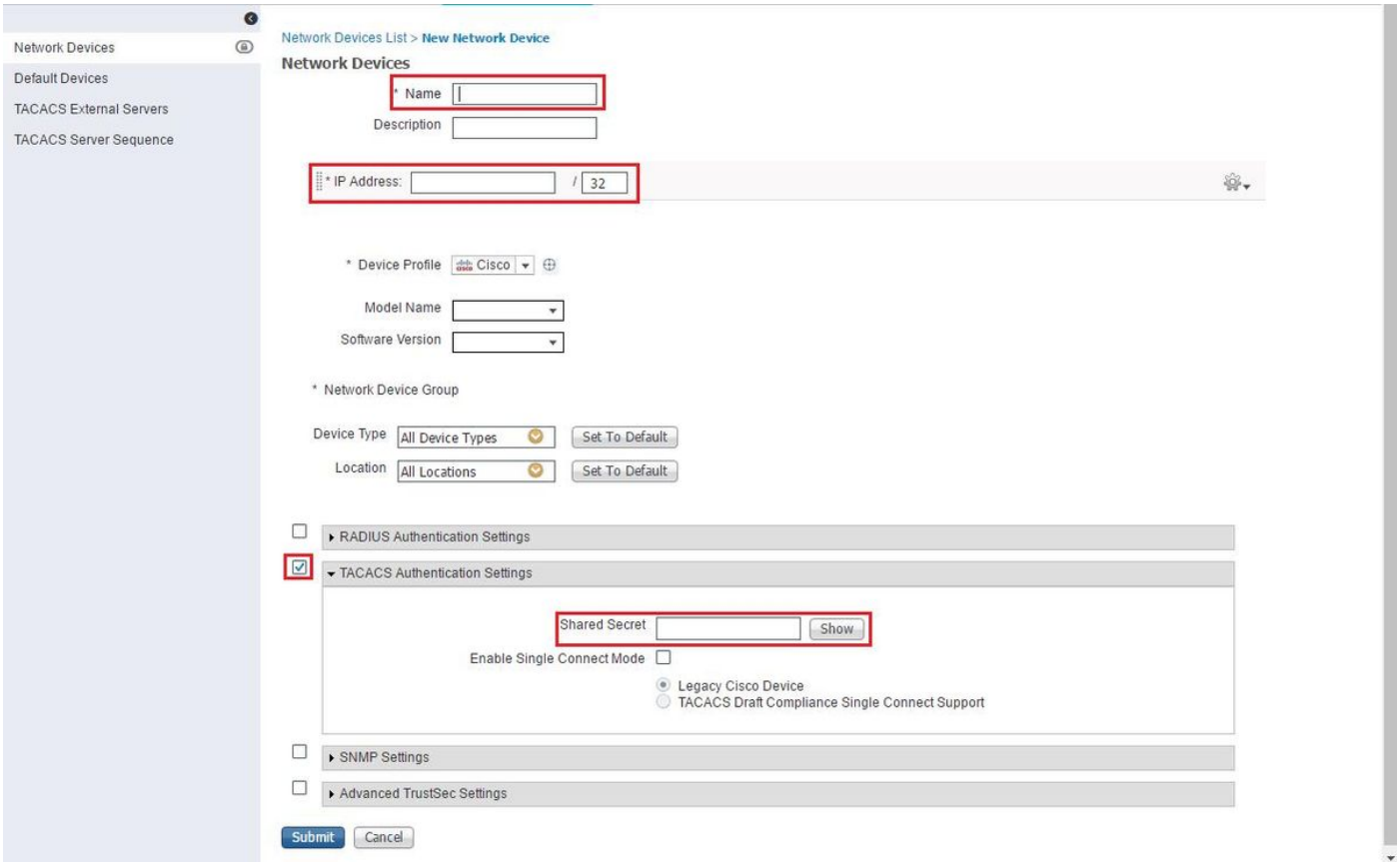
(Nota: Si consiglia di selezionare l'opzione Abilita fallback su locale, con l'opzione SOLO su nessuna risposta del server o L'opzione Su nessuna risposta o errore, in particolare durante il test della configurazione.

Configurazione di ISE

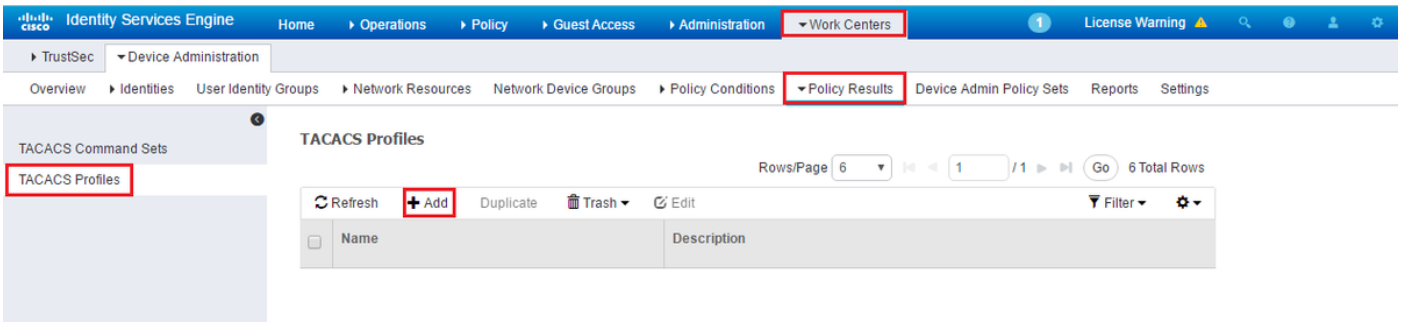
Configurazione di Prime come client AAA su ISE, centri di lavoro / amministrazione dispositivi / risorse di rete / dispositivi di rete / aggiunta



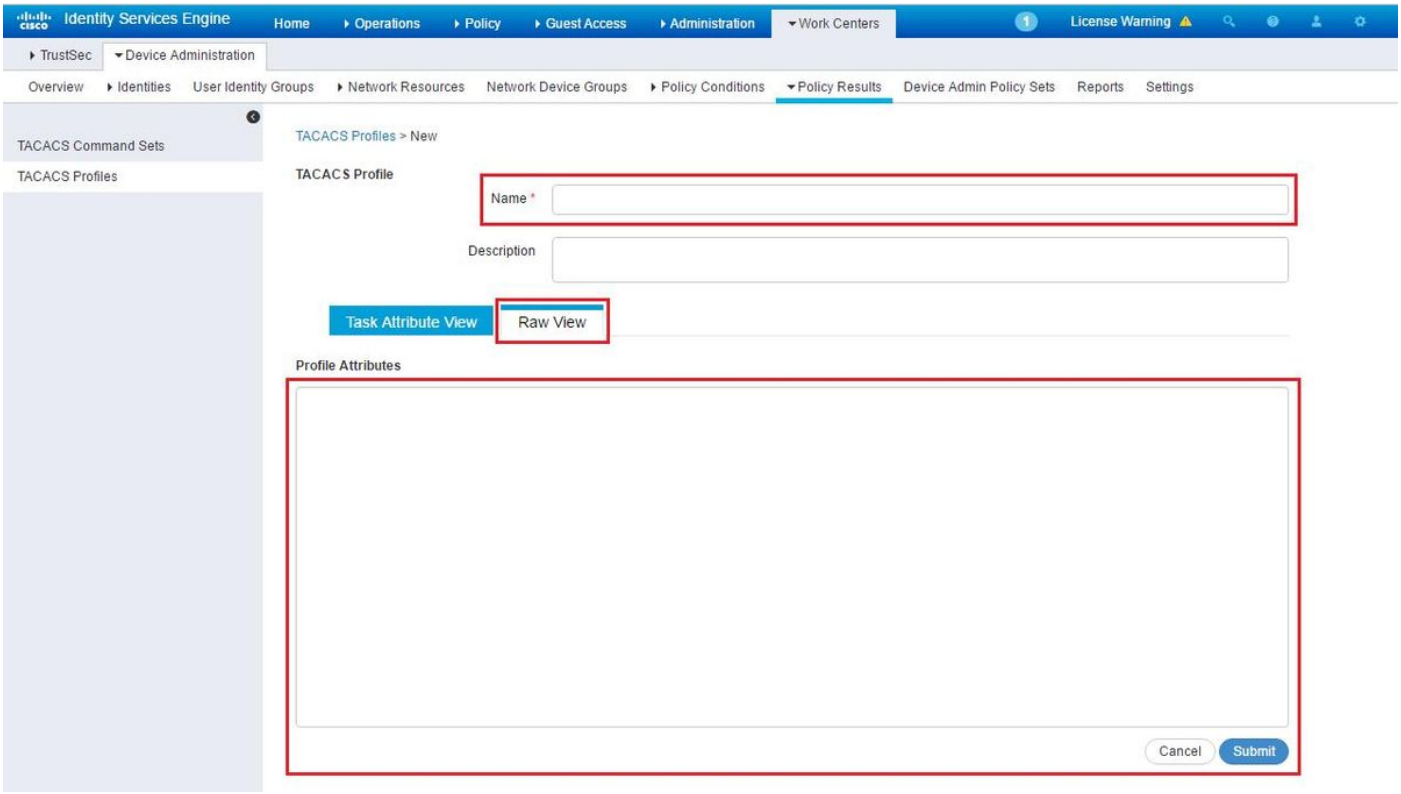
Immettere le informazioni per il server Prime. Gli attributi obbligatori da includere sono Nome, Indirizzo IP, selezionare l'opzione per TACACS e il segreto condiviso. È inoltre possibile aggiungere un Tipo di dispositivo, specificatamente per Prime, da utilizzare successivamente come Condizione per la Regola di autorizzazione o altre informazioni, anche se questa operazione è facoltativa.



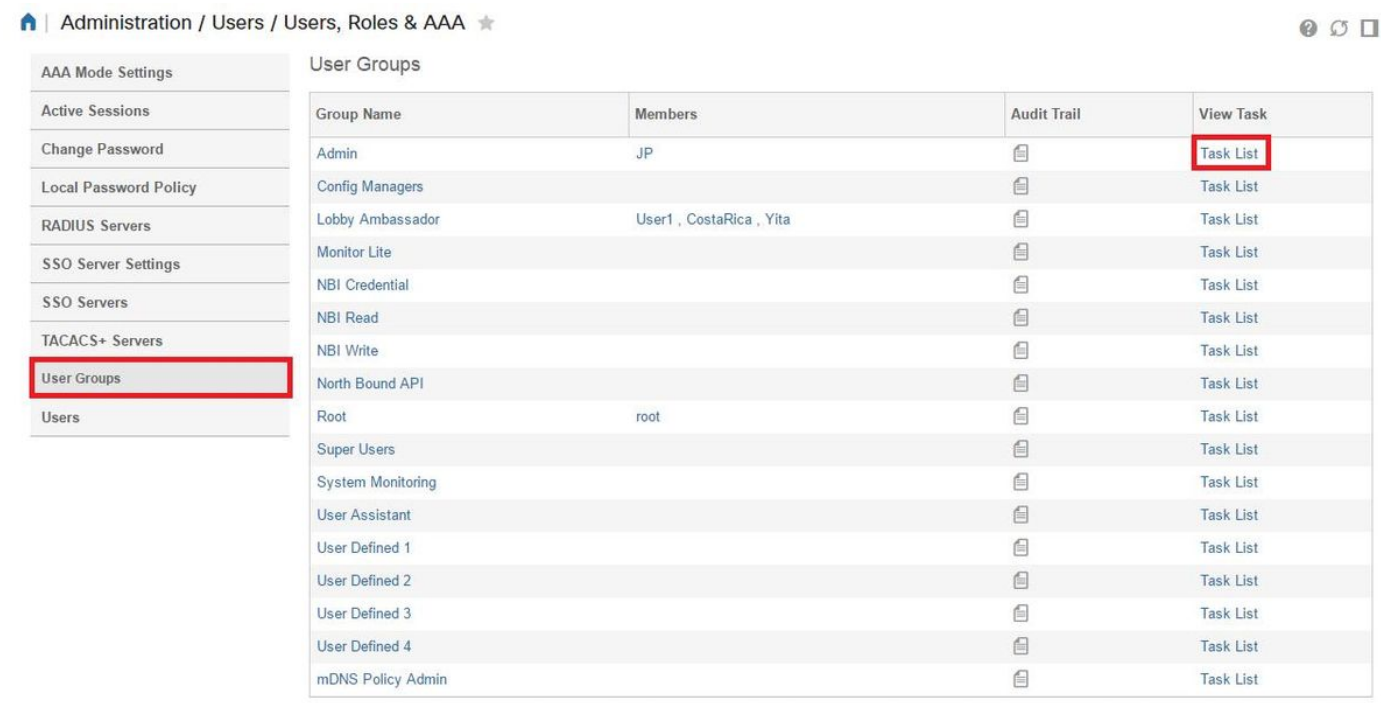
Quindi creare un risultato del profilo TACACS per inviare gli attributi richiesti da ISE a Prime, in modo da fornire il corretto livello di accesso. Passare a Centri di lavoro / Risultati criteri / Profili TACACS e selezionare l'opzione Aggiungi.



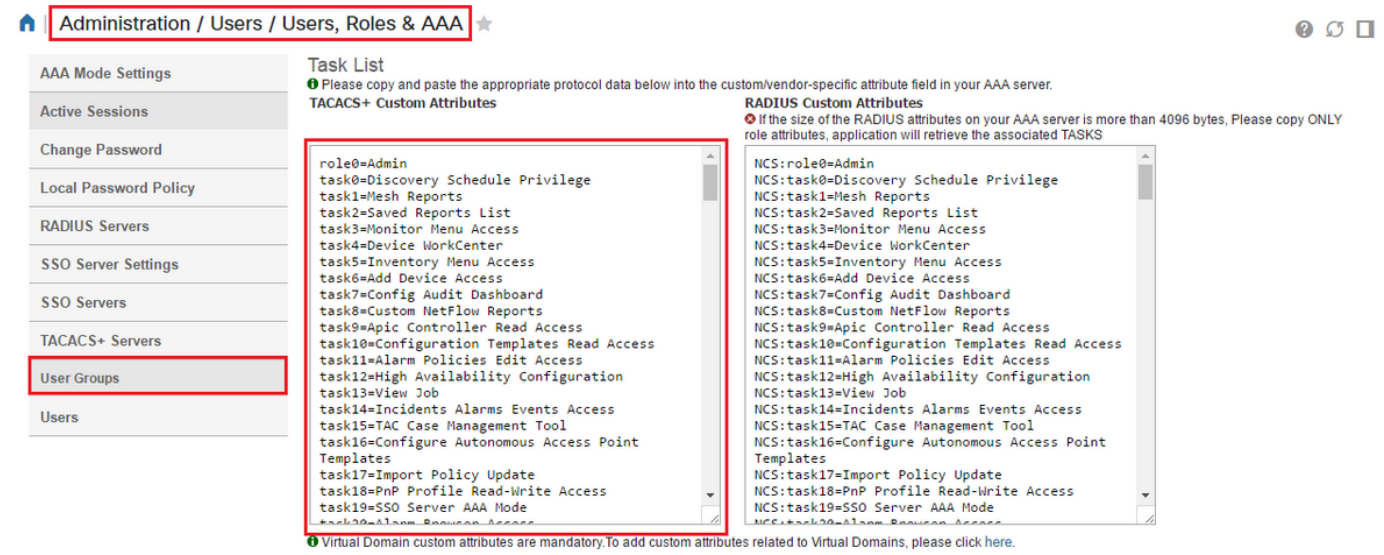
Configurare il nome e utilizzare l'opzione Visualizzazione non elaborata per immettere gli attributi nella casella Attributi profilo. Gli attributi provengono dal server di base stesso.



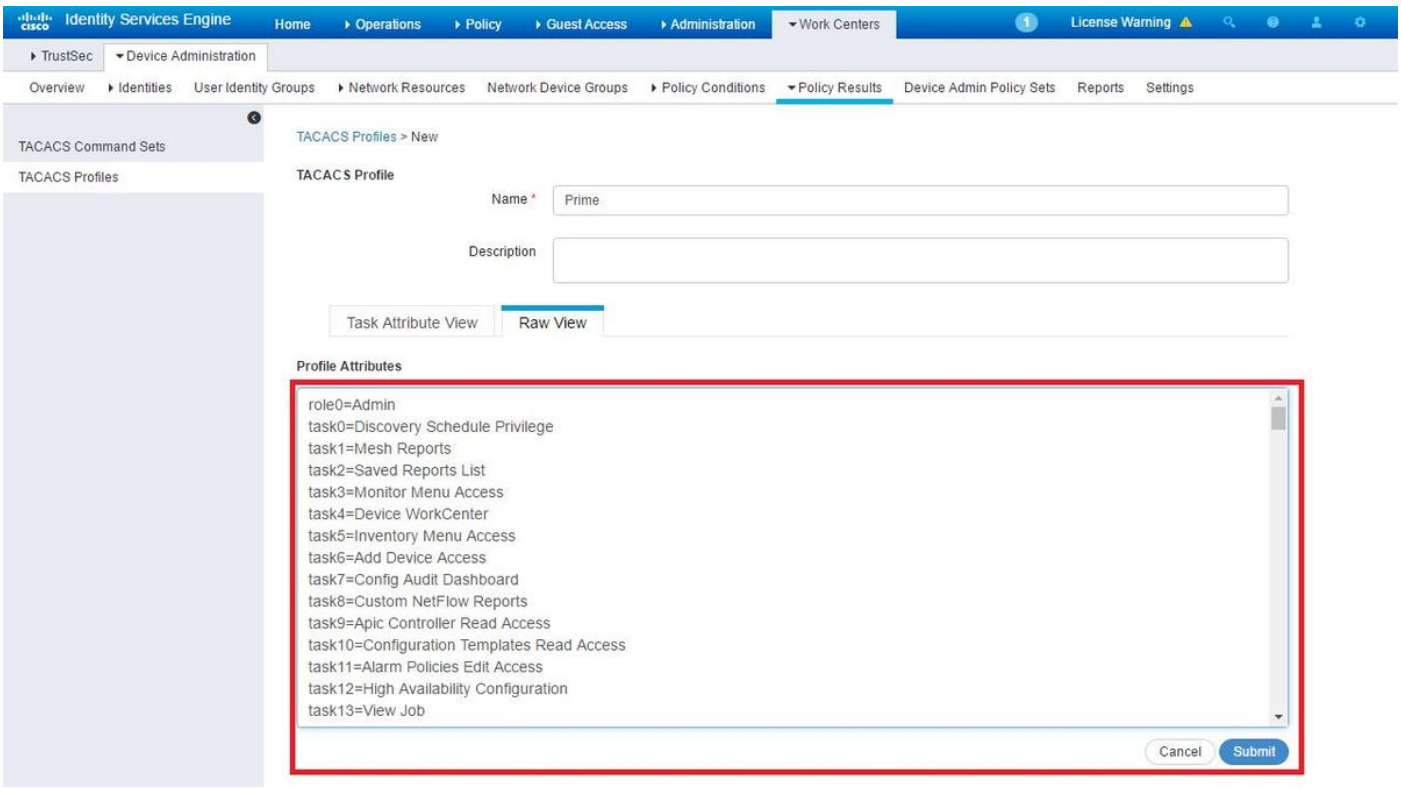
Ottenere gli attributi nella schermata Amministrazione / Utenti/ Utenti, Ruoli & AAA e selezionare la scheda Gruppi di utenti. Selezionare il livello di accesso Gruppo che si desidera fornire. In questo esempio l'accesso come amministratore viene fornito selezionando l'elenco di task appropriato sul lato sinistro.



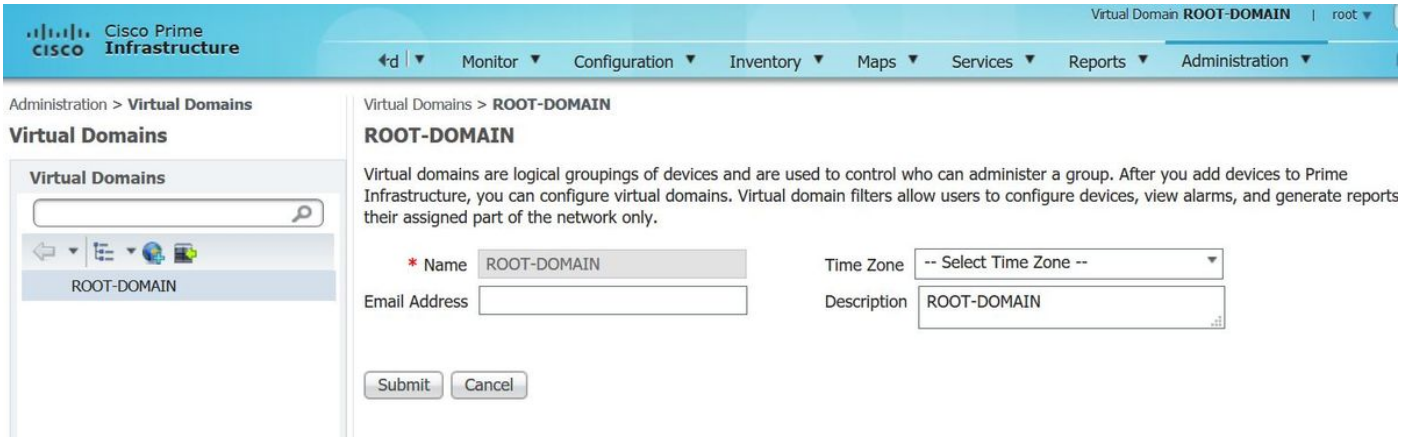
Copiare tutti gli attributi personalizzati TACACS.



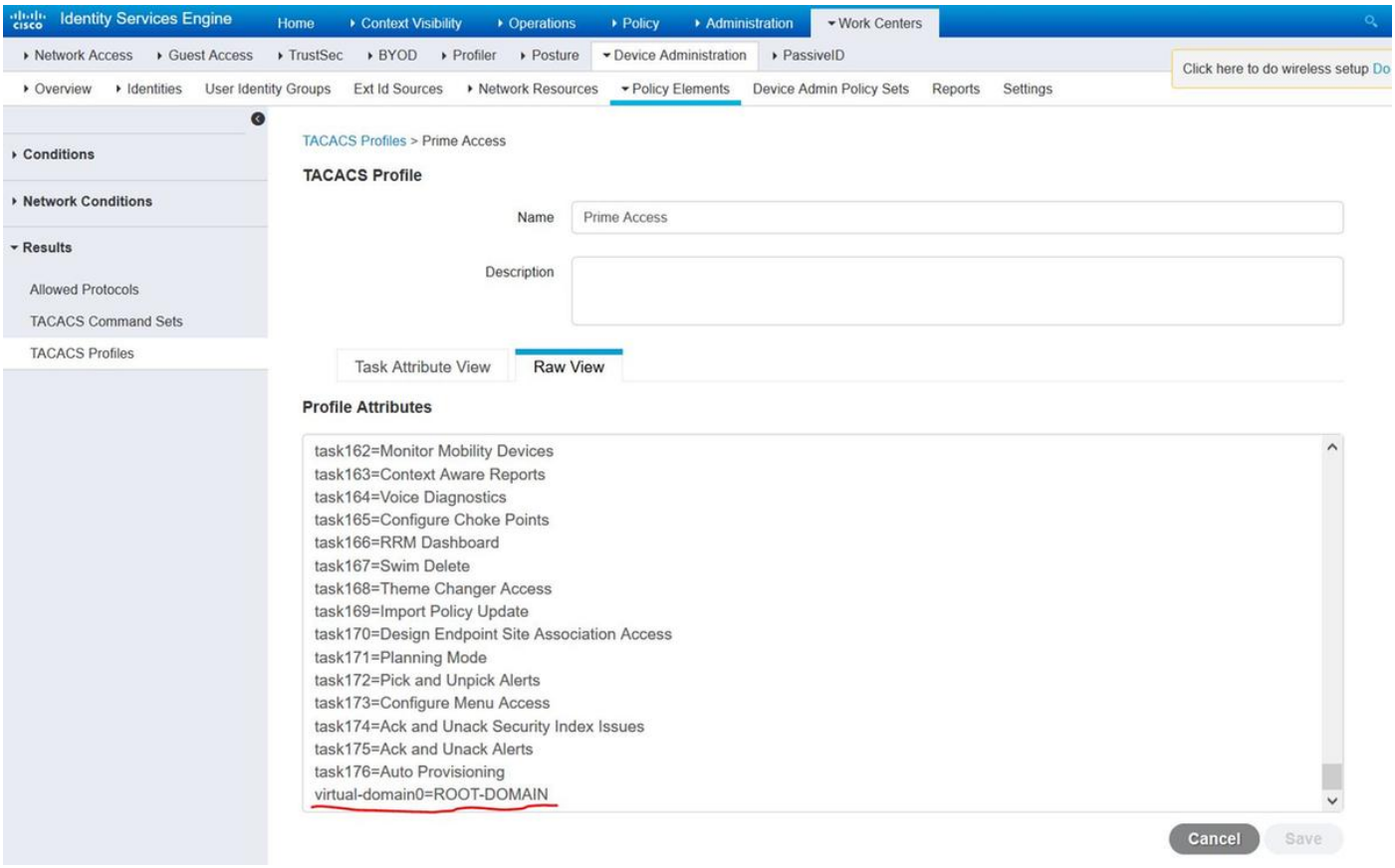
Quindi incollale nella sezione "Visualizzazione raw" del Profilo su ISE.



Gli attributi personalizzati del dominio virtuale sono obbligatori. Le informazioni sul dominio principale sono disponibili in Amministrazione principale -> Domini virtuali.

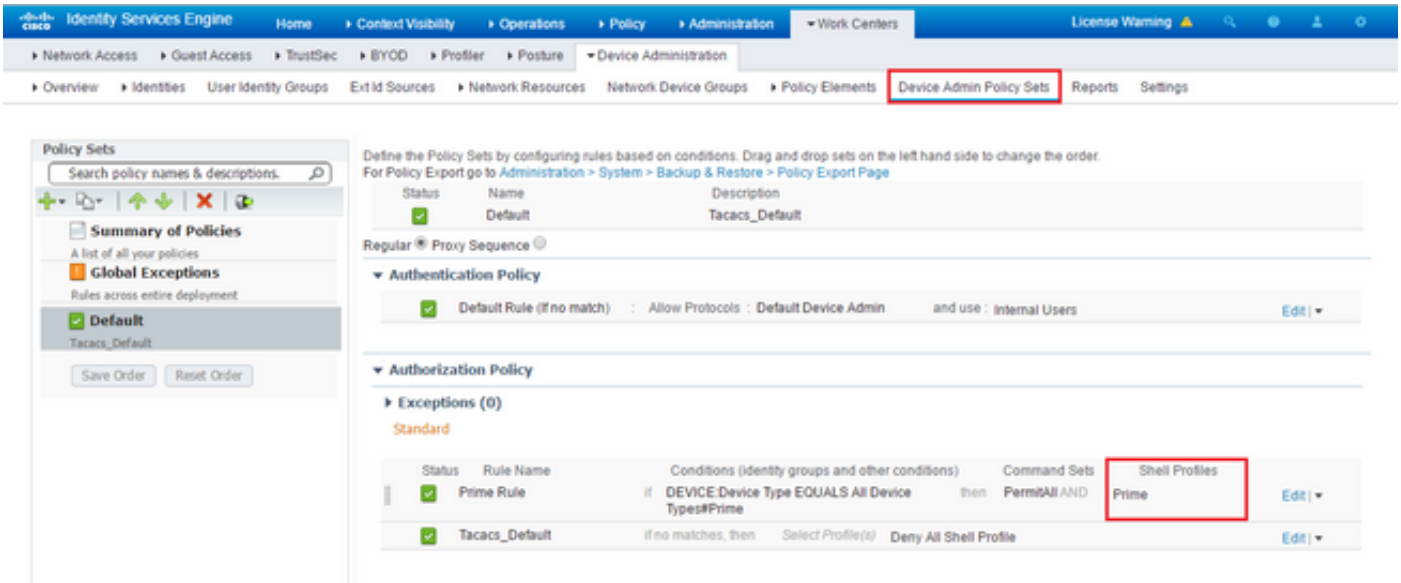


Il nome del dominio virtuale principale deve essere aggiunto come attributo **virtual-domain0=**"nome dominio virtuale"



Al termine, è sufficiente creare una regola per assegnare il profilo di shell creato nel passaggio precedente, in Centri di lavoro / Amministrazione dispositivi / Set di criteri di amministrazione dispositivi

(Nota: Le "Condizioni" variano a seconda della distribuzione, tuttavia è possibile utilizzare "Tipo di dispositivo" specificatamente per Prime o un altro tipo di filtro, ad esempio l'indirizzo IP di Prime, come una delle "Condizioni" in modo che questa regola filtri correttamente le richieste)



A questo punto la configurazione deve essere completa.

Risoluzione dei problemi

Se questa configurazione non ha esito positivo e l'opzione di fallback locale è stata abilitata su Prime, è possibile forzare il failover da ISE, rimuovendo l'indirizzo IP di Prime. In questo modo ISE non risponderà e verrà forzato l'uso delle credenziali locali. Se il fallback locale è configurato per essere eseguito su un rifiuto, gli account locali continueranno a funzionare e forniranno l'accesso al cliente.

Se ISE ha completato l'autenticazione e soddisfa la regola corretta, ma Prime rifiuta comunque la richiesta. Verificare che gli attributi siano configurati correttamente nel profilo e che non siano stati inviati attributi aggiuntivi.