Konfigurieren der Prime 3.1 TACACS-Authentifizierung für ISE 2.x

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Prime-Infrastruktur für die Authentifizierung über TACACS mit ISE 2.x konfiguriert wird.

Anforderungen

Cisco empfiehlt, dass Sie über grundlegende Kenntnisse in folgenden Bereichen verfügen:

- Identity Services Engine (ISE)
- Prime-Infrastruktur

Konfigurieren

Cisco Prime Network Control System 3.1

Cisco Identity Service Engine 2.0 oder höher

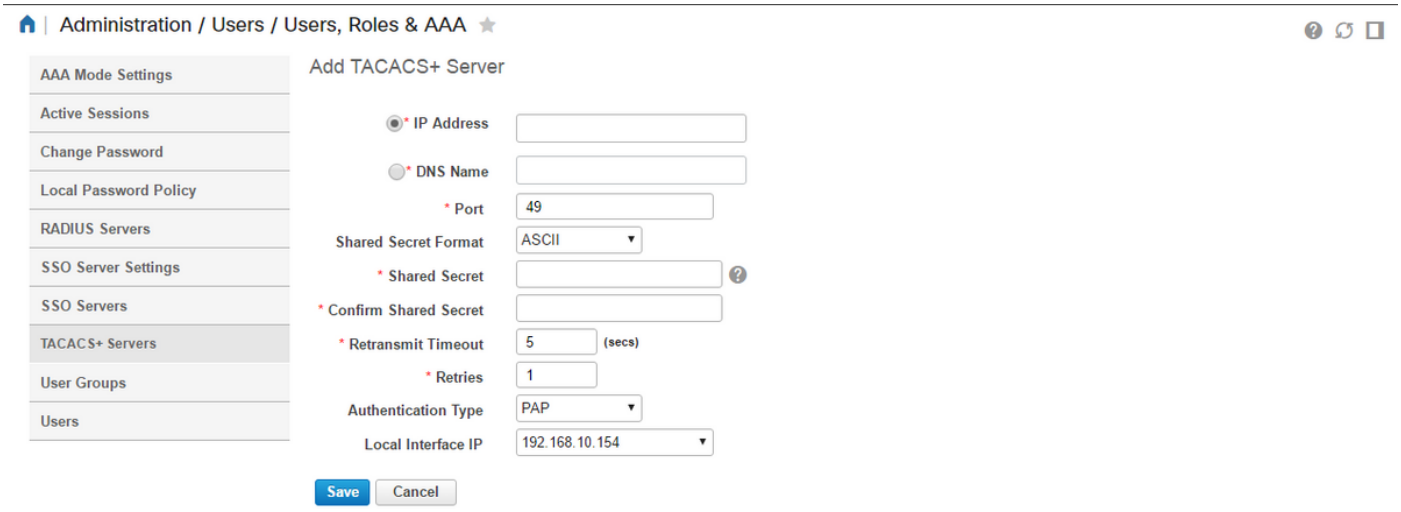
(Hinweis: Die ISE unterstützt nur TACACS ab Version 2.0. Es ist jedoch möglich, Prime für die Verwendung von Radius zu konfigurieren. Prime enthält zusätzlich zu TACACS eine Liste mit Radius-Attributen, wenn Sie Radius verwenden möchten. Dies gilt auch für eine ältere Version der ISE oder einer Drittanbieterlösung.)

Prime-Konfiguration

Navigieren Sie zum folgenden Bildschirm: Administration/Benutzer/Benutzer, Rollen und AAA wie unten dargestellt.

Wählen Sie dort die Registerkarte TACACS+ Servers (TACACS+-Server) aus, wählen Sie anschließend in der rechten oberen Ecke die Option Add TACACS+ Server (TACACS+-Server hinzufügen) aus, und wählen Sie Go (Los) aus.

Auf dem nächsten Bildschirm ist die Konfiguration des TACACS-Servereintrags verfügbar (dies muss für jeden einzelnen TACACS-Server erfolgen).



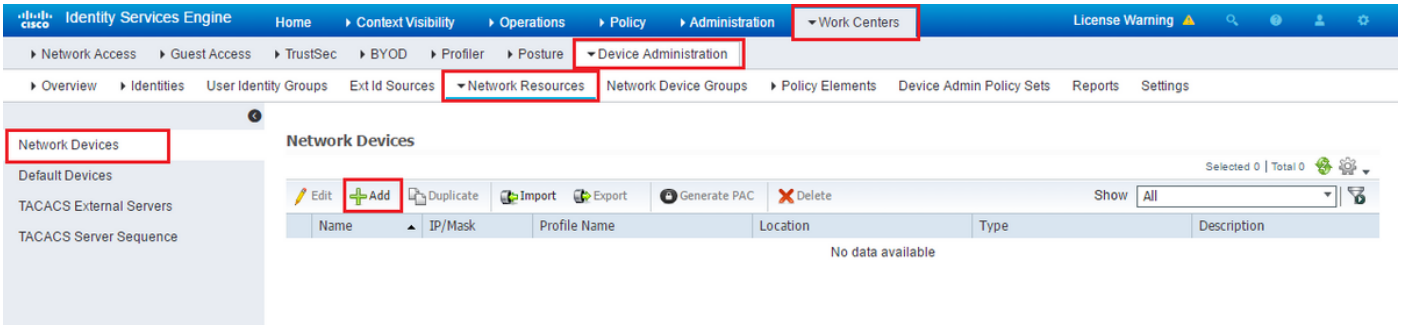
Hier müssen Sie entweder die IP-Adresse oder die DNS-Adresse des Servers sowie den gemeinsamen geheimen Schlüssel eingeben. Bitte beachten Sie auch die IP-Adresse der lokalen Schnittstelle, die Sie verwenden möchten, da diese IP-Adresse später für den AAA-Client in der ISE verwendet werden muss.

Um die Konfiguration auf Prime abzuschließen. Sie müssen TACACS unter Administration / Users / Users, Roles & AAA unter der Registerkarte AAA Mode settings (AAA-Modus-Einstellungen) aktivieren.

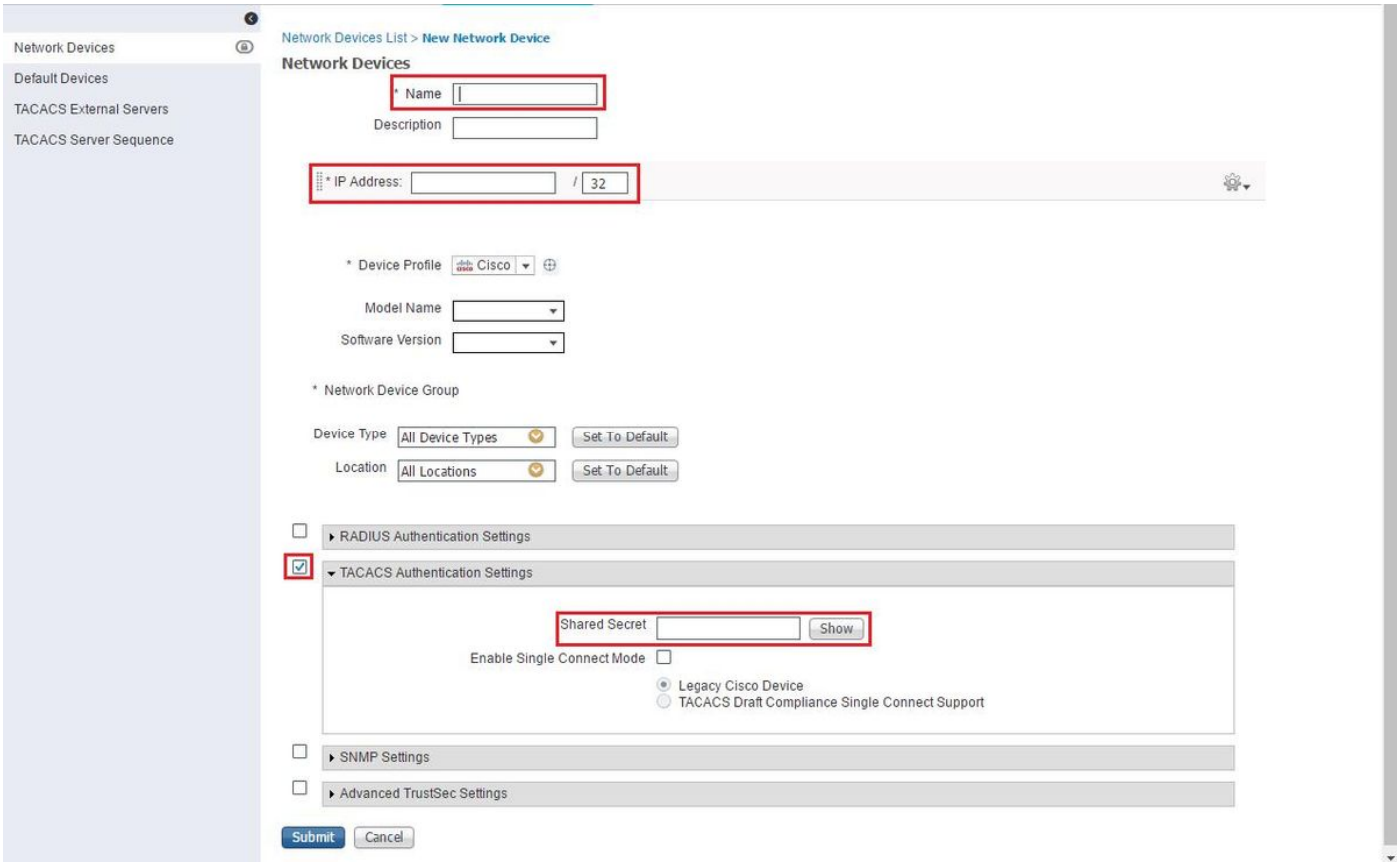
(Hinweis: Es wird empfohlen, die Option Enable fallback to Local (Fallback auf Lokal aktivieren) zu aktivieren, wobei entweder NUR auf Keine Serverantwort oder die Option On no response (Keine Antwort oder Fehler), insbesondere beim Testen der Konfiguration, verwendet werden sollte.

ISE-Konfiguration

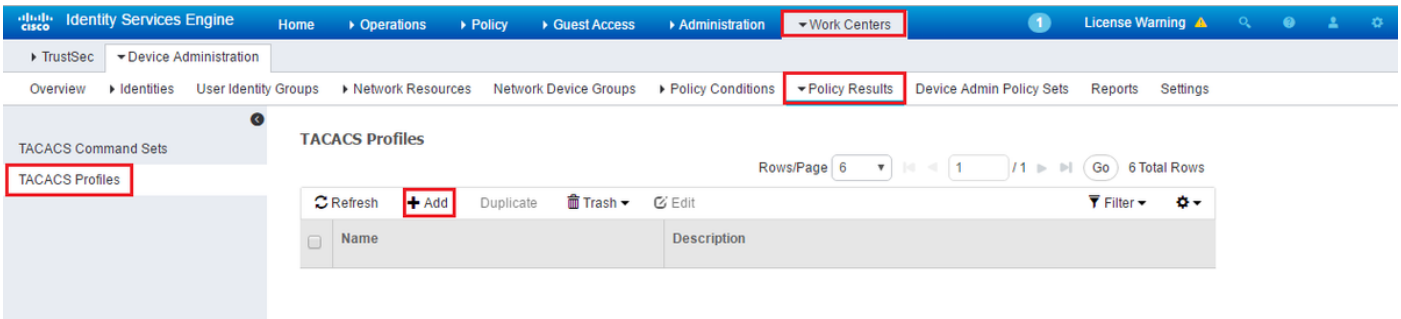
Konfigurieren Sie Prime als AAA-Client auf der ISE in Work Centers/Device Administration/Network Resources/Network Devices/Add



Geben Sie die Informationen für den Prime-Server ein. Die erforderlichen Attribute, die Sie einschließen müssen, sind Name, IP-Adresse, wählen Sie die Option für TACACS und den Shared Secret aus. Sie können zusätzlich einen Gerätetyp, speziell für Prime, hinzufügen, um später als Bedingung für die Autorisierungsregel oder andere Informationen verwendet zu werden. Dies ist jedoch optional.

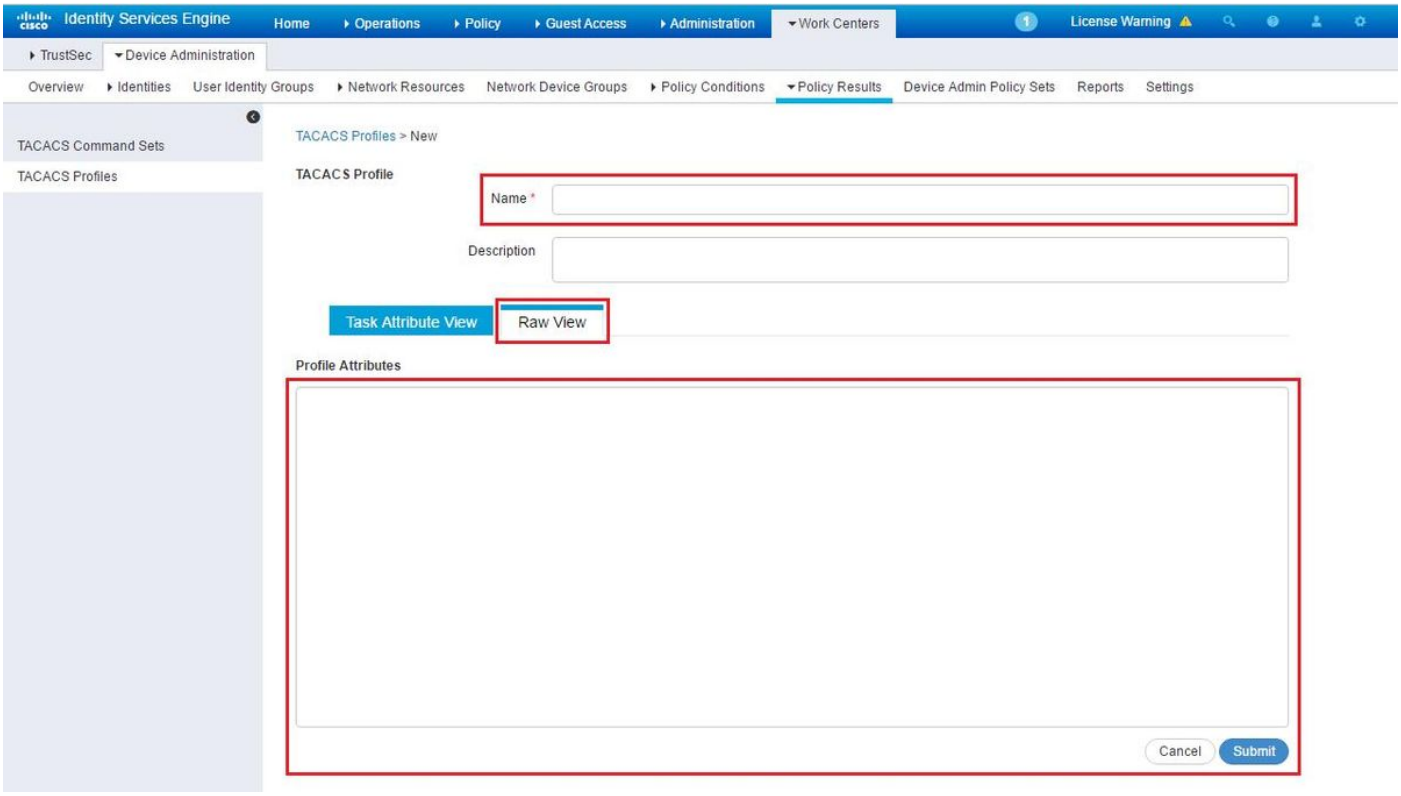


Erstellen Sie anschließend ein TACACS-Profilergebnis, um die erforderlichen Attribute von der ISE an Prime zu senden, um die richtige Zugriffsebene bereitzustellen. Navigieren Sie zu Work Center/Policy Results/Tacacs Profiles, und wählen Sie die Option Add (Hinzufügen) aus.

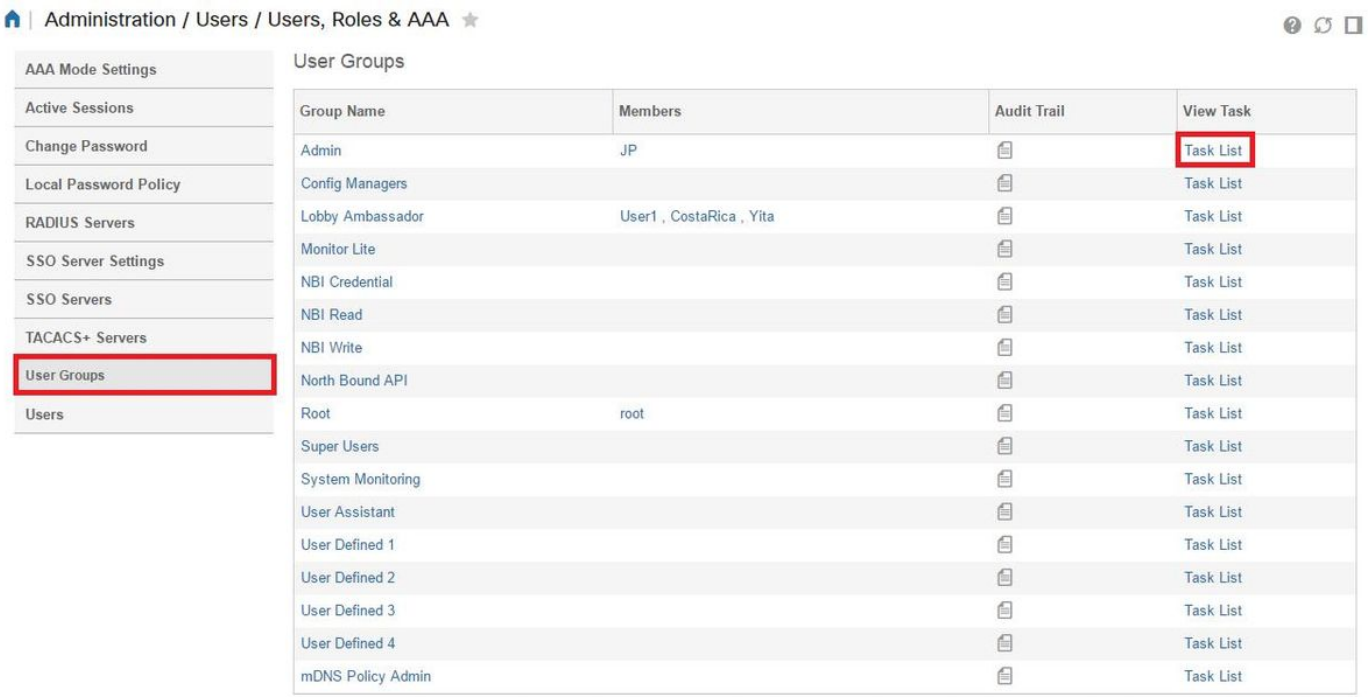


Konfigurieren Sie den Namen, und geben Sie die Attribute unter dem Feld Profile attribute (Profile-Attribute) mithilfe der Option Raw View (Raw-Ansicht) ein. Die Attribute werden vom Primärserver

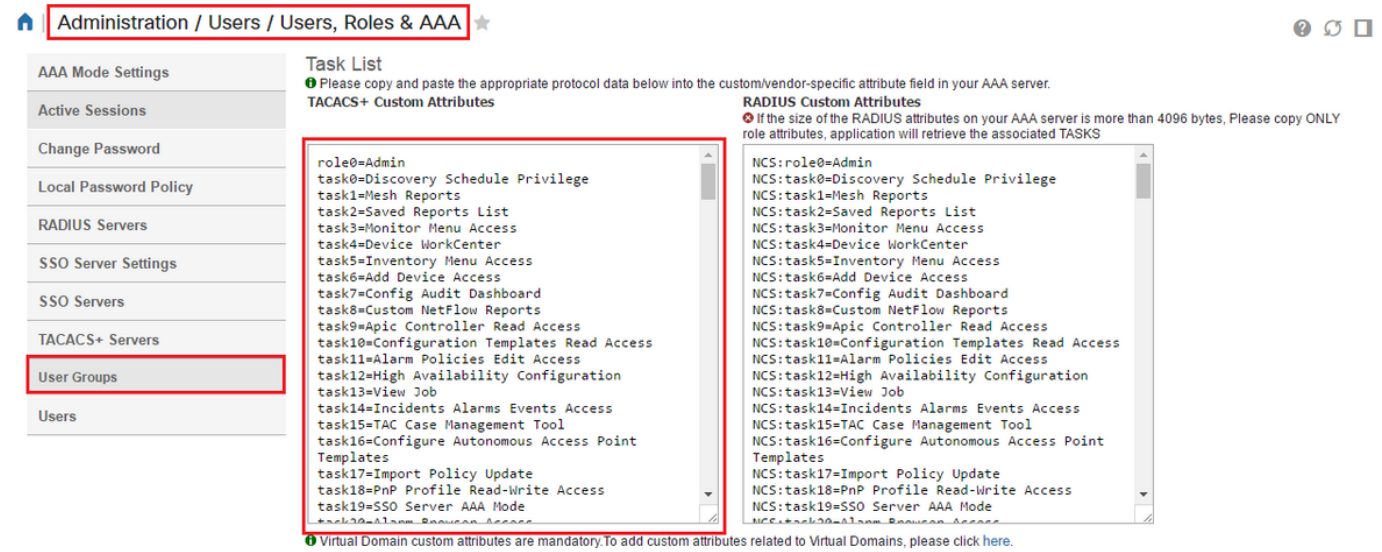
selbst übernommen.



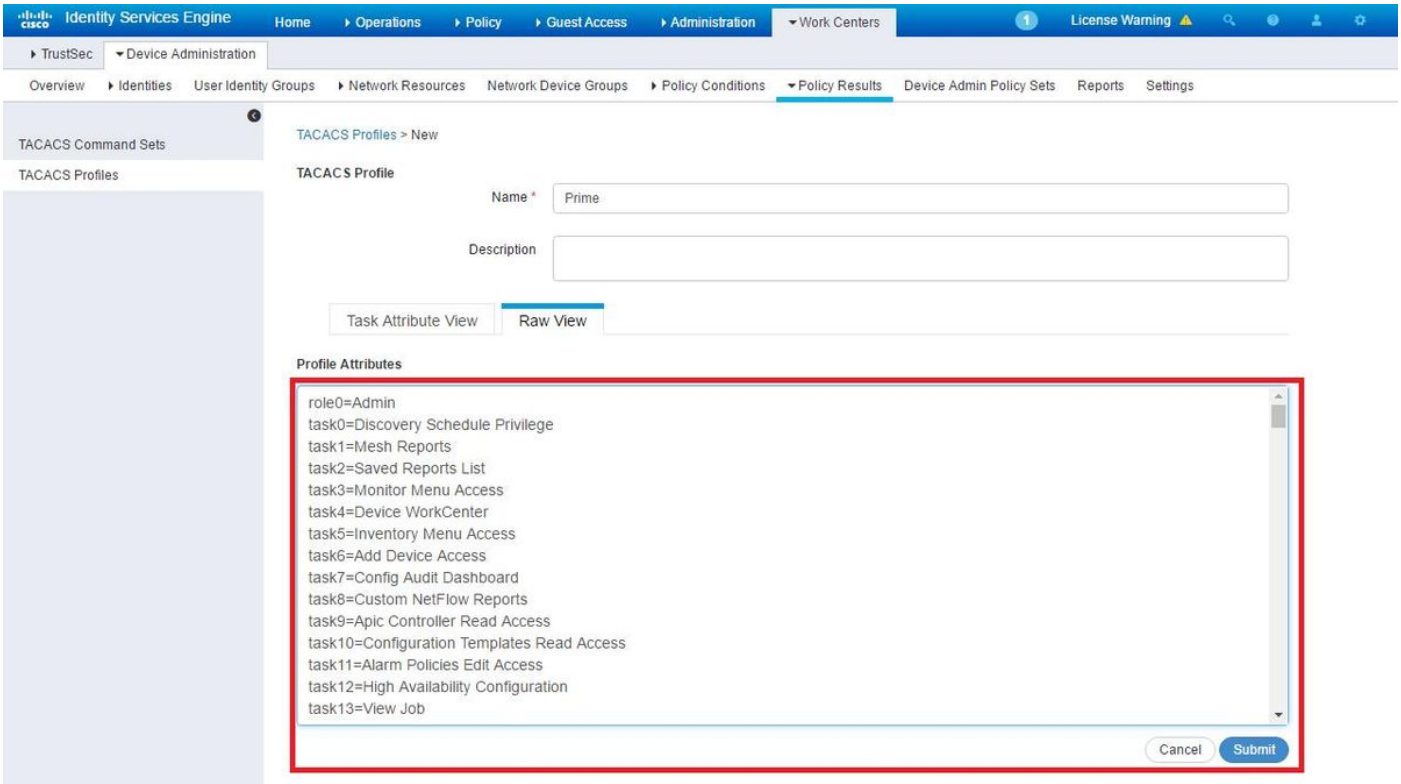
Rufen Sie die Attribute im Bildschirm Administration / Users / Users, Roles & AAA ab, und wählen Sie die Registerkarte User Groups (Benutzergruppen) aus. Hier wählen Sie die Zugriffsebene Gruppe aus, die Sie bereitstellen möchten. In diesem Beispiel wird der Administratorzugriff durch Auswahl der entsprechenden Aufgabenliste auf der linken Seite gewährt.



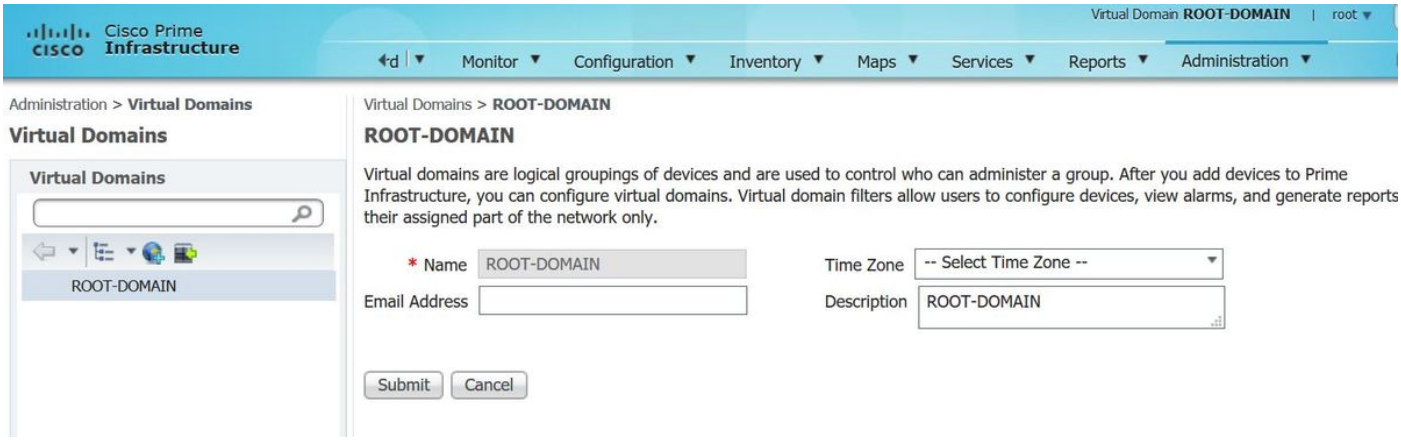
Kopieren Sie alle benutzerdefinierten TACACS-Attribute.



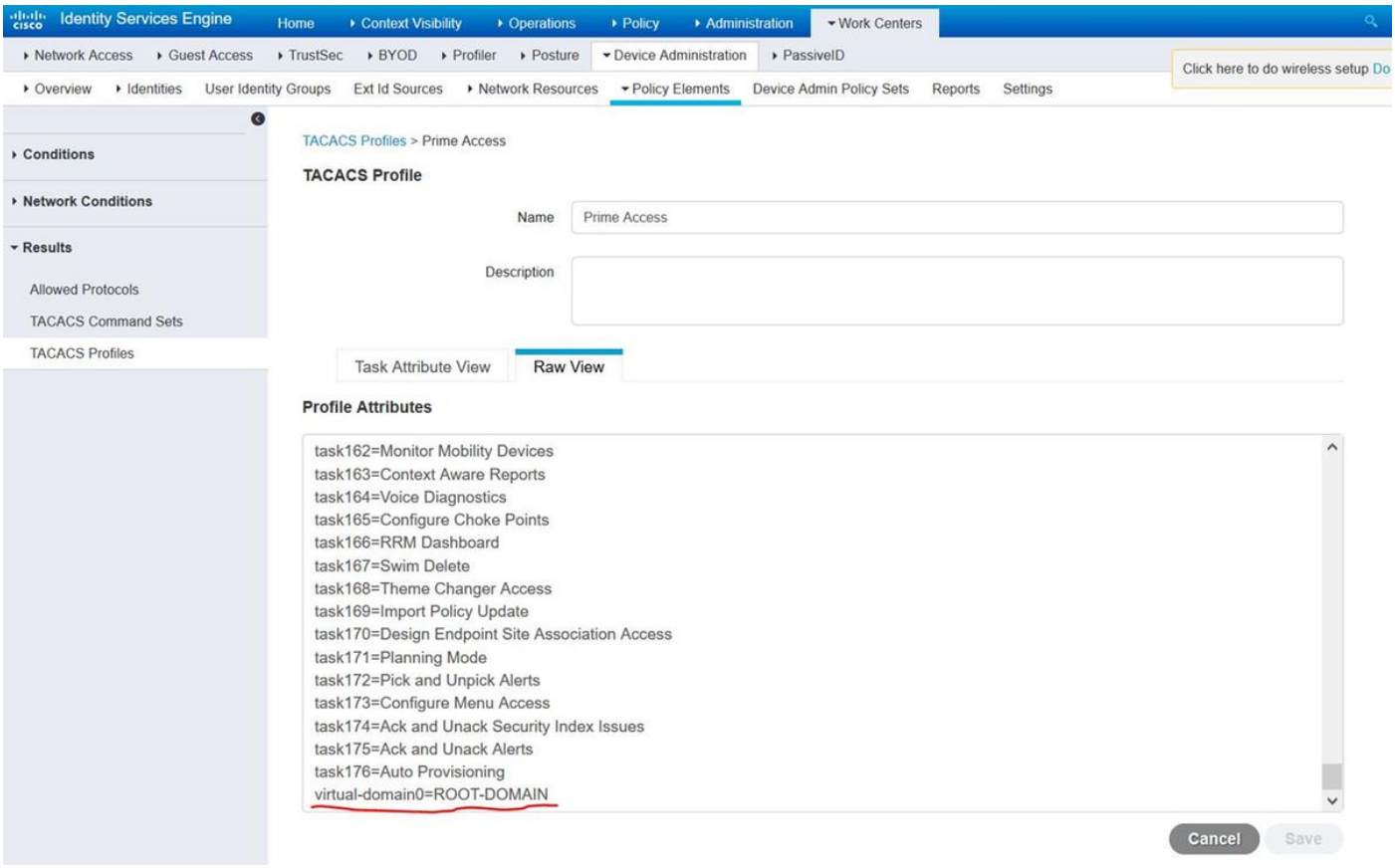
Fügen Sie sie dann im Abschnitt "Raw View" des Profils auf der ISE ein.



Benutzerdefinierte Attribute virtueller Domänen sind obligatorisch. Informationen zur Root-Domain finden Sie unter Prime Administration -> Virtual Domains (Prime-Verwaltung -> virtuelle Domänen).

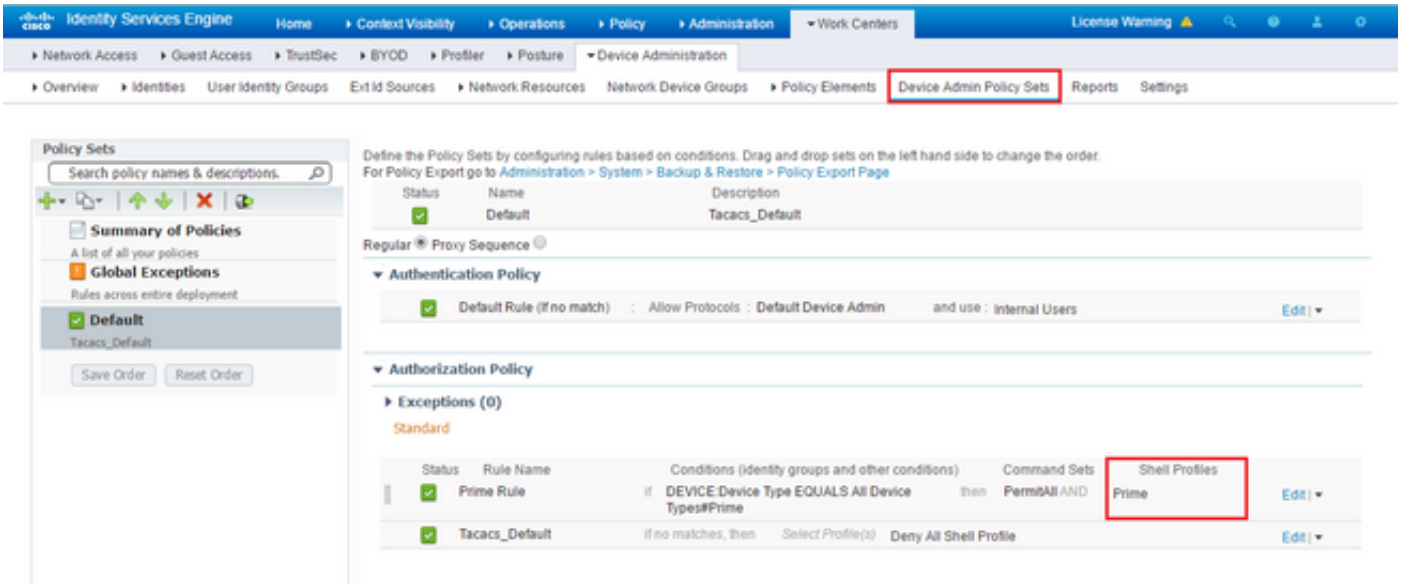


Der Name der Prime Virtual Domain muss als Attribut **virtual-domain0=**"virtual domain name" hinzugefügt werden.



Danach müssen Sie nur noch eine Regel erstellen, um das im vorherigen Schritt erstellte Shell-Profil unter Work Center/Device Administration/Device Admin Policy Sets (Work Center/Device Administration/Device Admin-Richtliniensätze) zuzuweisen.

(Hinweis: "Bedingungen" variieren je nach Bereitstellung. Sie können jedoch "Gerätetyp" speziell für Prime oder einen anderen Filtertyp wie die IP-Adresse von Prime verwenden, um Anfragen entsprechend zu filtern.



Zu diesem Zeitpunkt sollte die Konfiguration abgeschlossen sein.

Fehlerbehebung

Wenn diese Konfiguration nicht erfolgreich ist und die lokale Rückfalloption auf Prime aktiviert wurde, können Sie einen Failover von der ISE erzwingen, indem Sie die IP-Adresse von Prime entfernen. Dies führt dazu, dass die ISE nicht reagiert und die Verwendung lokaler Anmeldeinformationen erzwingt. Wenn für eine Ablehnung ein lokaler Fallback konfiguriert ist, funktionieren die lokalen Konten weiterhin und ermöglichen dem Kunden Zugriff.

Wenn die ISE eine erfolgreiche Authentifizierung anzeigt und mit der richtigen Regel übereinstimmt, Prime jedoch die Anforderung noch ablehnt, können Sie überprüfen, ob die Attribute im Profil korrekt konfiguriert sind und keine weiteren Attribute gesendet werden.