

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

Inhalt

[Einführung](#)

[Anforderungen](#)

[Konfigurieren](#)

[Prime-Konfiguration](#)

[ISE-Konfiguration](#)

[Fehlerbehebung](#)

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).

Administration / Users / Users, Roles & AAA ★

AAA Mode Settings

Active Sessions

Change Password

Local Password Policy

RADIUS Servers

SSO Server Settings

SSO Servers

TACACS+ Servers

User Groups

Users

Add TACACS+ Server

IP Address

DNS Name

* Port 49

Shared Secret Format ASCII

* Shared Secret

* Confirm Shared Secret

* Retransmit Timeout 5 (secs)

* Retries 1

Authentication Type PAP

Local Interface IP 192.168.10.154

Save Cancel

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.

Administration / Users / Users, Roles & AAA ★

AAA Mode Settings

Active Sessions

Change Password

Local Password Policy

RADIUS Servers

SSO Server Settings

SSO Servers

TACACS+ Servers

User Groups

Users

AAA Mode

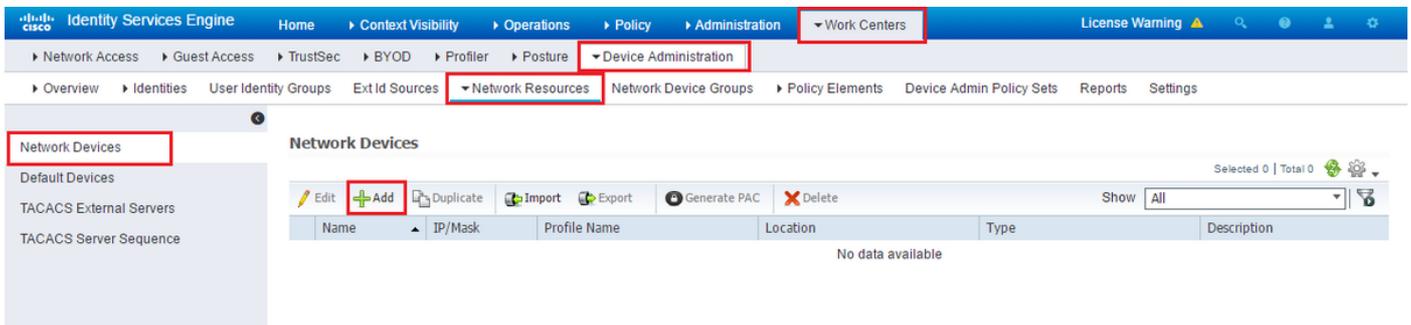
Local RADIUS TACACS+ SSO

Enable fallback to Local ONLY on no server respon:

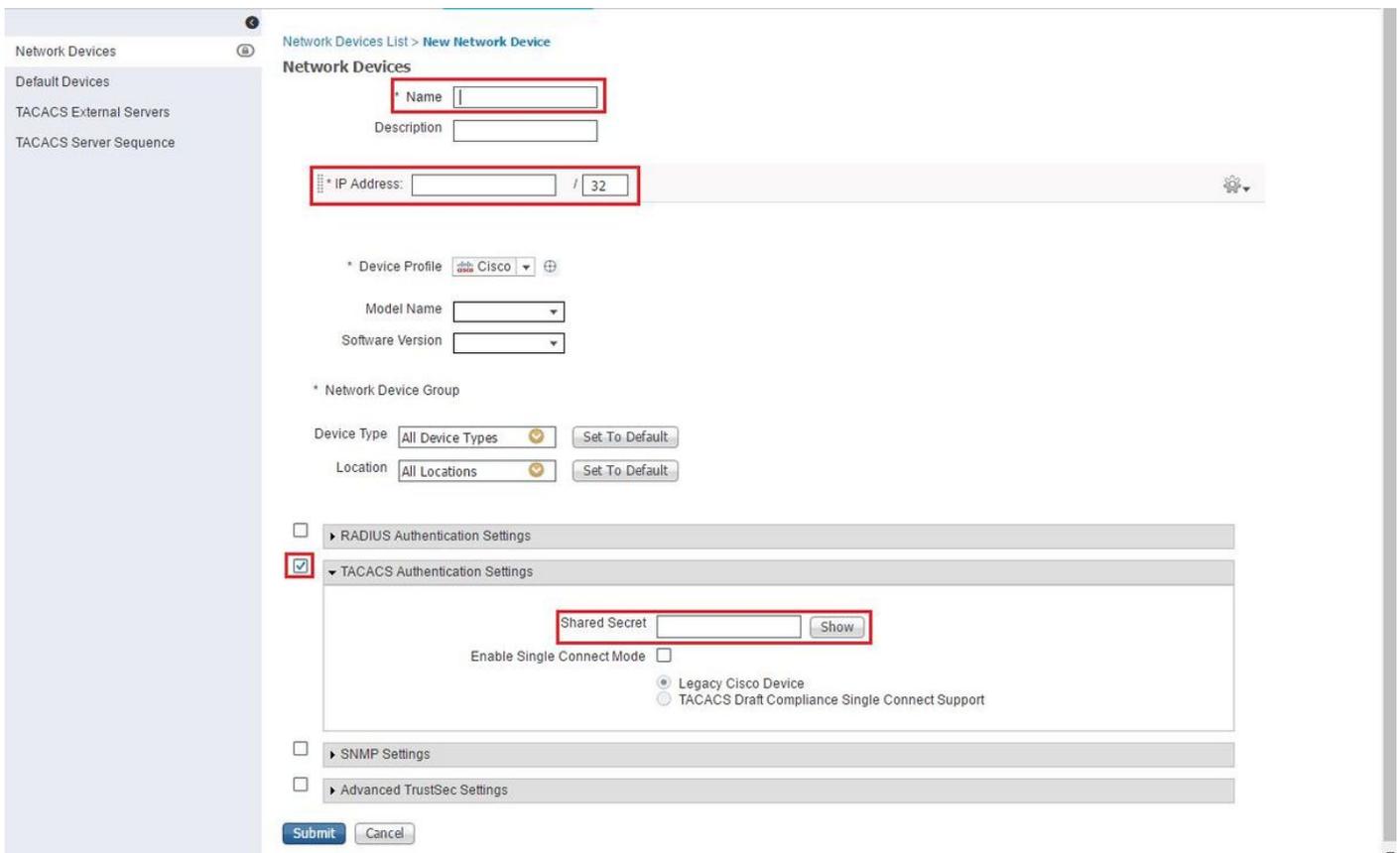
Save

ISE-Konfiguration

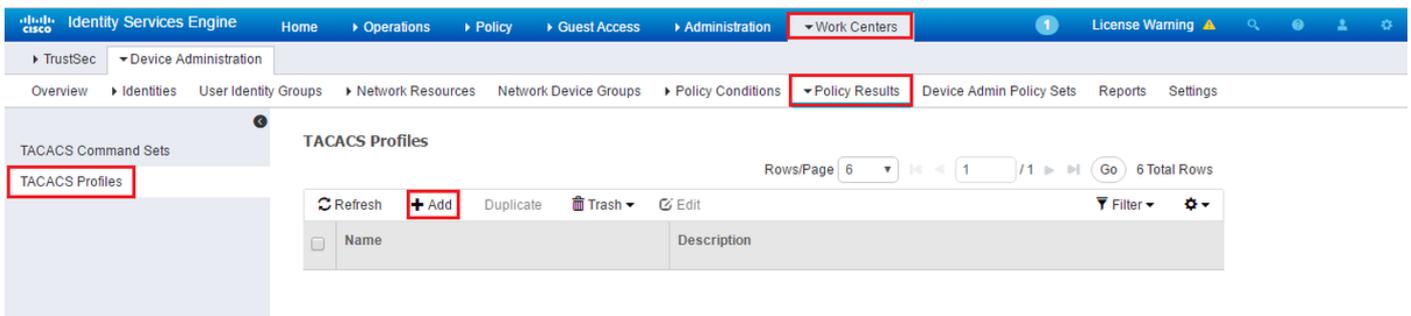
Konfigurieren Sie Prime als AAA-Client auf der ISE in Work Centers/Device Administration/Network Resources/Network Devices/Add



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.

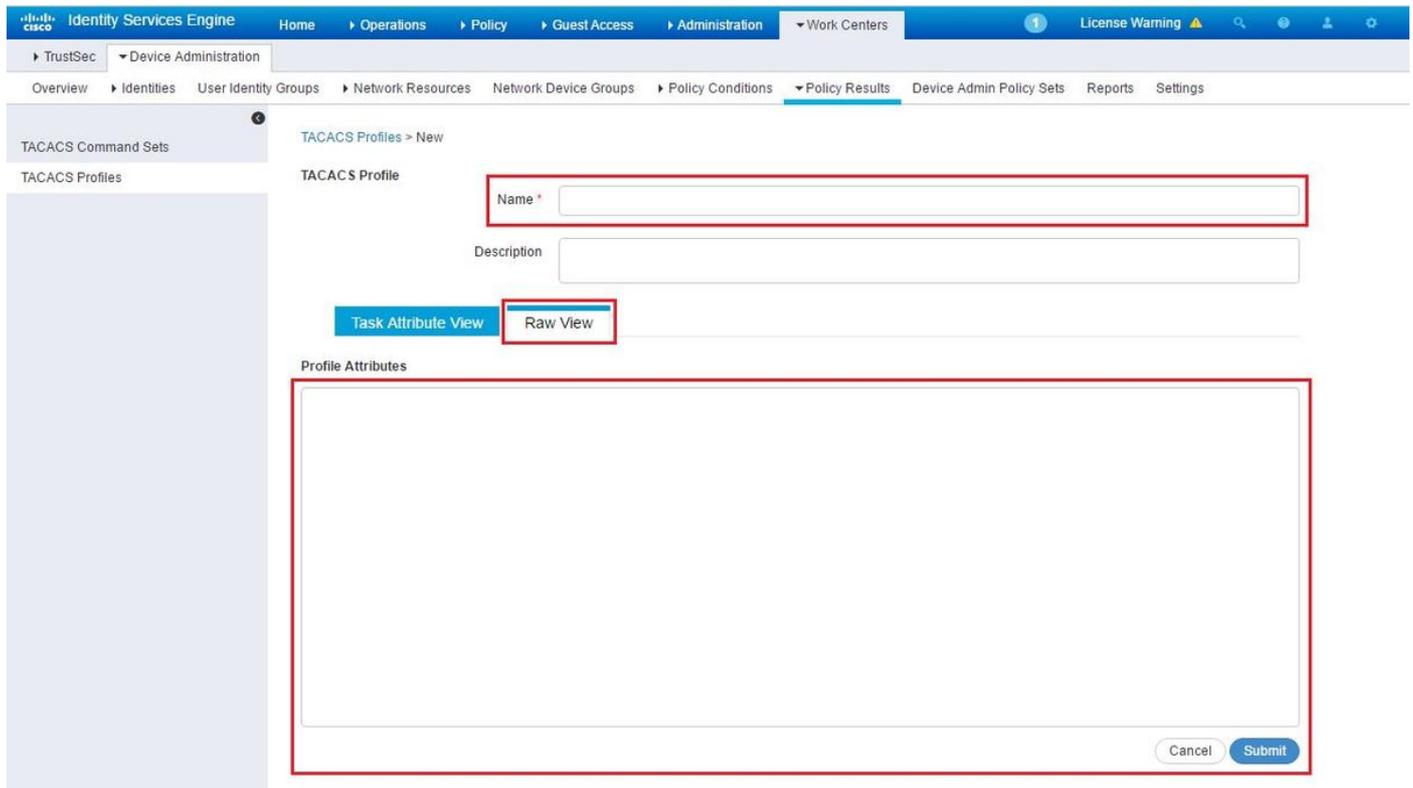


Erstellen Sie anschließend ein TACACS-Profilergebnis, um die erforderlichen Attribute von der ISE an Prime zu senden, um die richtige Zugriffsebene bereitzustellen. Navigieren Sie zu Work Center/Policy Results/Tacacs Profiles, und wählen Sie die Option Add (Hinzufügen) aus.



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.

Administration / Users / Users, Roles & AAA

Group Name	Members	Audit Trail	View Task
Admin	JP		Task List
Config Managers			Task List
Lobby Ambassador	User1 , CostaRica , Yita		Task List
Monitor Lite			Task List
NBI Credential			Task List
NBI Read			Task List
NBI Write			Task List
North Bound API			Task List
Root	root		Task List
Super Users			Task List
System Monitoring			Task List
User Assistant			Task List
User Defined 1			Task List
User Defined 2			Task List
User Defined 3			Task List
User Defined 4			Task List
mDNS Policy Admin			Task List

Kopieren Sie alle benutzerdefinierten TACACS-Attribute.

Administration / Users / Roles & AAA

Task List
Please copy and paste the appropriate protocol data below into the custom/vendor-specific attribute field in your AAA server.

TACACS+ Custom Attributes

```
role0=Admin
task0=Discovery Schedule Privilege
task1=Mesh Reports
task2=Saved Reports List
task3=Monitor Menu Access
task4=Device WorkCenter
task5=Inventory Menu Access
task6=Add Device Access
task7=Config Audit Dashboard
task8=Custom NetFlow Reports
task9=Apic Controller Read Access
task10=Configuration Templates Read Access
task11=Alarm Policies Edit Access
task12=High Availability Configuration
task13=View Job
task14=Incidents Alarms Events Access
task15=TAC Case Management Tool
task16=Configure Autonomous Access Point
Templates
task17=Import Policy Update
task18=PnP Profile Read-Write Access
task19=SSO Server AAA Mode
```

RADIUS Custom Attributes

If the size of the RADIUS attributes on your AAA server is more than 4096 bytes, Please copy ONLY role attributes, application will retrieve the associated TASKS

```
NCS:role0=Admin
NCS:task0=Discovery Schedule Privilege
NCS:task1=Mesh Reports
NCS:task2=Saved Reports List
NCS:task3=Monitor Menu Access
NCS:task4=Device WorkCenter
NCS:task5=Inventory Menu Access
NCS:task6=Add Device Access
NCS:task7=Config Audit Dashboard
NCS:task8=Custom NetFlow Reports
NCS:task9=Apic Controller Read Access
NCS:task10=Configuration Templates Read Access
NCS:task11=Alarm Policies Edit Access
NCS:task12=High Availability Configuration
NCS:task13=View Job
NCS:task14=Incidents Alarms Events Access
NCS:task15=TAC Case Management Tool
NCS:task16=Configure Autonomous Access Point
Templates
NCS:task17=Import Policy Update
NCS:task18=PnP Profile Read-Write Access
NCS:task19=SSO Server AAA Mode
```

Virtual Domain custom attributes are mandatory. To add custom attributes related to Virtual Domains, please click here.

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

Identity Services Engine

TrustSec > Device Administration

TACACS Profiles > New

TACACS Profile

Name * Prime

Description

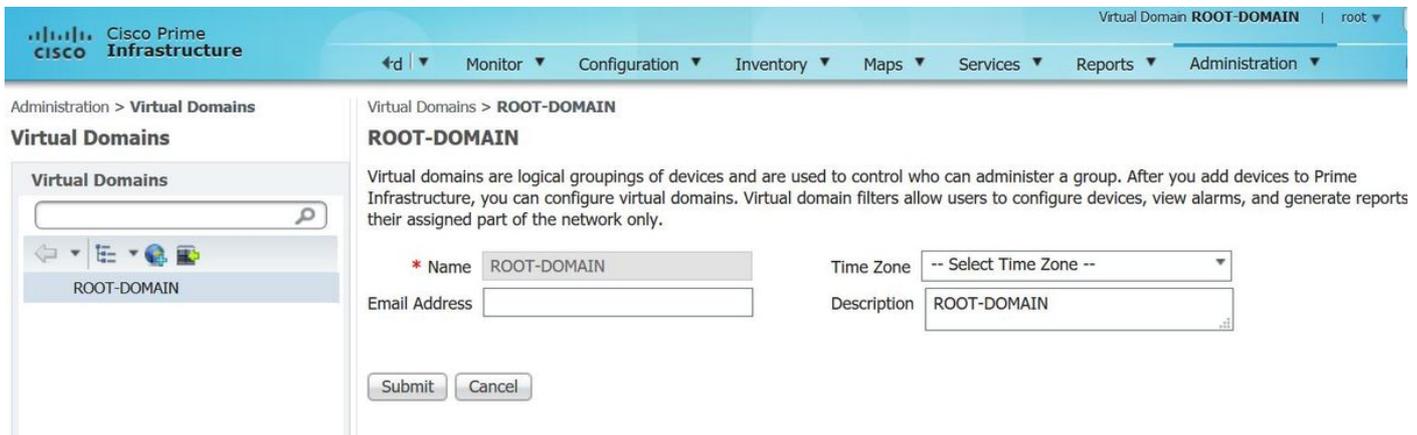
Task Attribute View | **Raw View**

Profile Attributes

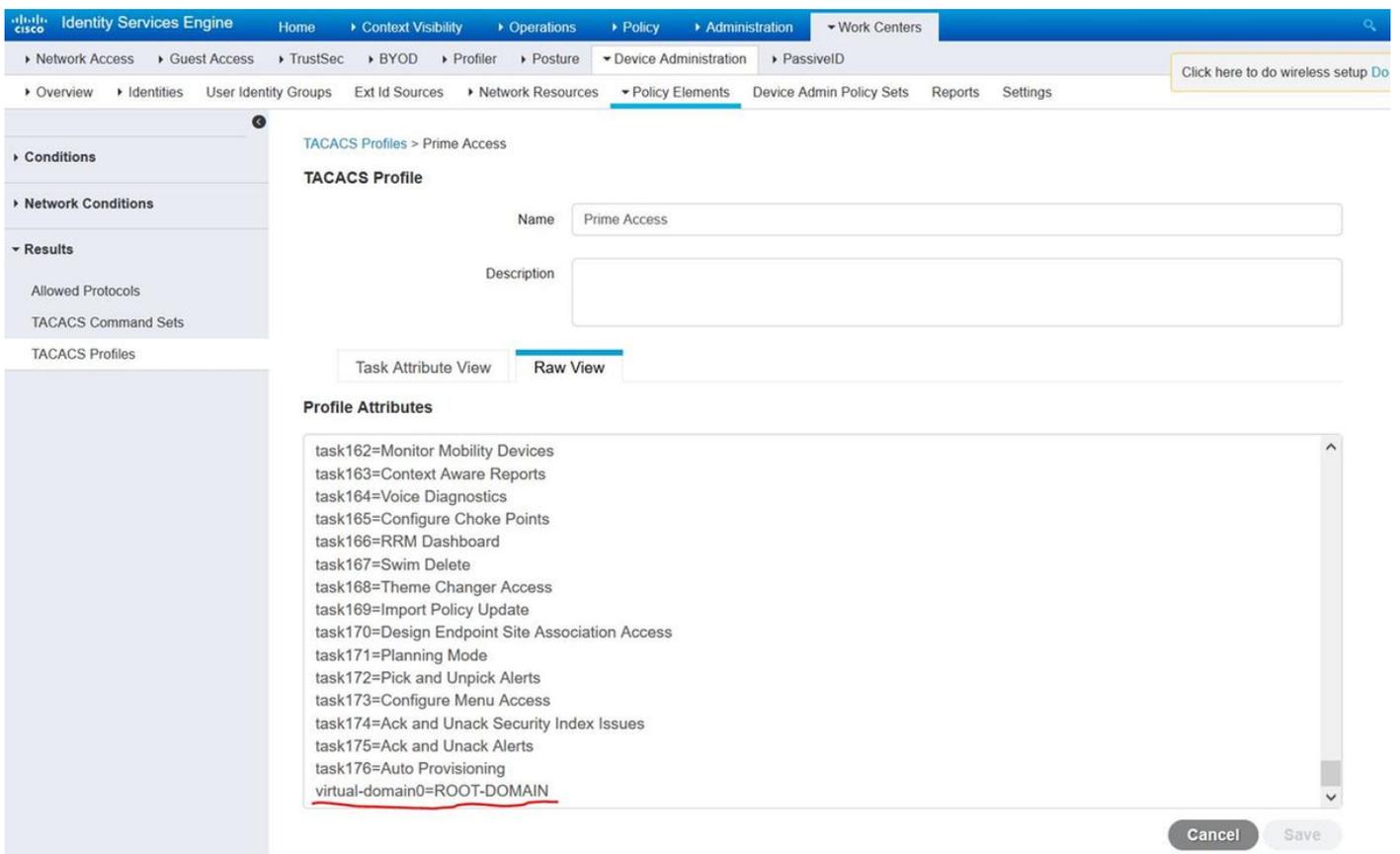
```
role0=Admin
task0=Discovery Schedule Privilege
task1=Mesh Reports
task2=Saved Reports List
task3=Monitor Menu Access
task4=Device WorkCenter
task5=Inventory Menu Access
task6=Add Device Access
task7=Config Audit Dashboard
task8=Custom NetFlow Reports
task9=Apic Controller Read Access
task10=Configuration Templates Read Access
task11=Alarm Policies Edit Access
task12=High Availability Configuration
task13=View Job
```

Cancel Submit

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.

Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Status	Name	Description
<input checked="" type="checkbox"/>	Default	Tacacs_Default

Regular Proxy Sequence

▼ Authentication Policy

<input checked="" type="checkbox"/>	Default Rule (if no match)	Allow Protocols : Default Device Admin and use : Internal Users	Edit
-------------------------------------	----------------------------	---	------

▼ Authorization Policy

► Exceptions (0)

Standard

Status	Rule Name	Conditions (Identity groups and other conditions)	Command Sets	Shell Profiles	Edit
<input checked="" type="checkbox"/>	Prime Rule	if DEVICE Device Type EQUALS All Device Types#Prime	then PermAll AND	Prime	Edit
<input checked="" type="checkbox"/>	Tacacs_Default	if no matches, then Select Profile(s)	Deny All Shell Profile		Edit

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.