Externe TACACS-servers configureren en probleemoplossing op ISE

Inhoud

Inleiding

Dit document beschrijft de functie om de externe TACACS+ server te gebruiken in een implementatie met behulp van Identity Services Engine (ISE) als een proxy.

Voorwaarden

Vereisten

- Basisbegrip van apparaattoediening op ISE.
- Dit document is gebaseerd op versie 2.0 van de Identity Services Engine, van toepassing op elke versie van Identity Services Engine die hoger is dan 2.0.

Gebruikte componenten

> Opmerking: Elke verwijzing naar ACS in dit document kan worden geïnterpreteerd als een verwijzing naar een externe TACACS+ server. De configuratie op de ACS- en de configuratie op een andere TACACS-server kan echter verschillen.

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

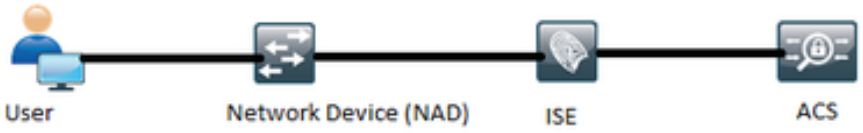
- Identity Services Engine 2.0
- Access Control System (ACS) 5.7

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg ervoor dat u de potentiële impact van elke configuratie verandering begrijpt.

Configureren

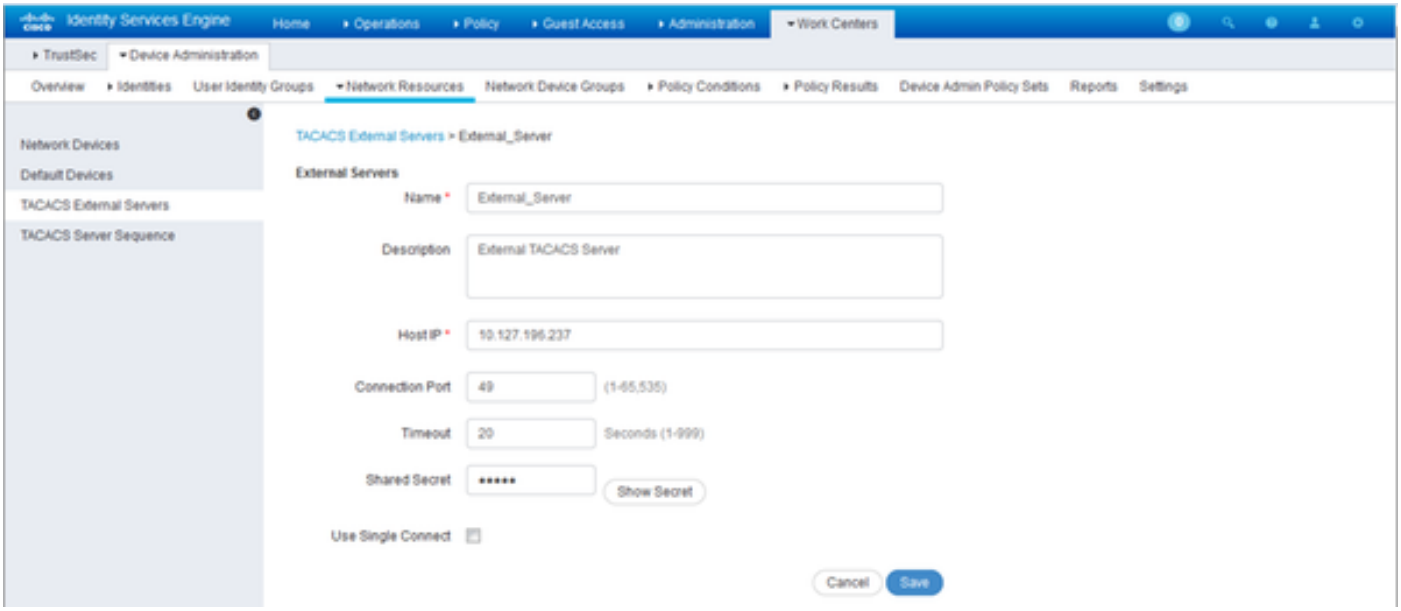
Deze sectie helpt om ISE aan volmacht TACACS+ verzoeken aan ACS te vormen.

Netwerkdiagram



ISE configureren

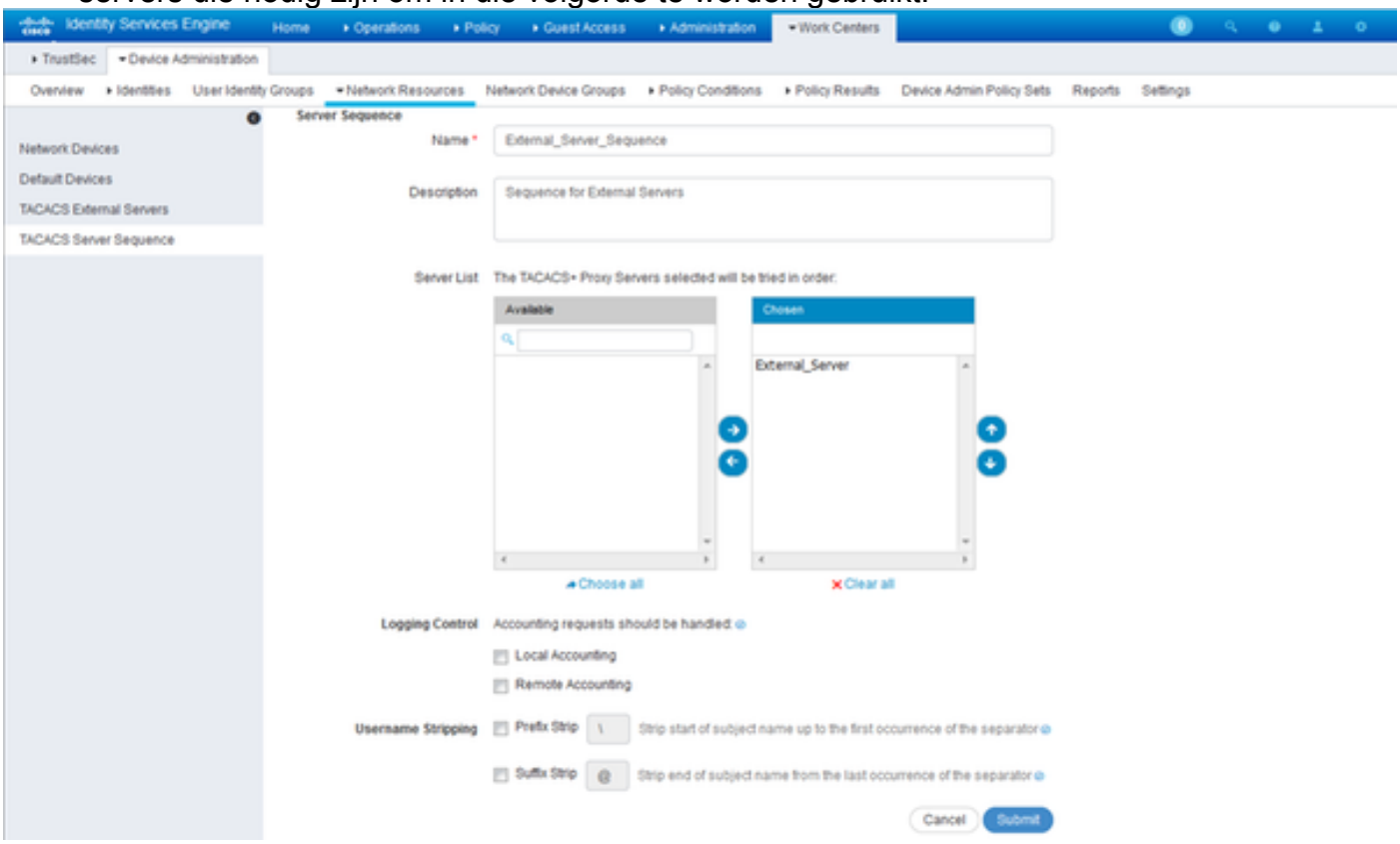
1. Meerdere externe TACACS-servers kunnen op ISE worden geconfigureerd en kunnen worden gebruikt om de gebruikers voor de authenticatie te zorgen. Om externe TACACS+ server op ISE te configureren **navigeer** naar **werkcentra > Apparaatbeheer > Netwerkbronnen > TACACS externe servers.** Klik op **Add** en vul de details van de Externe Server in.



Het gedeelde geheim dat in deze afdeling wordt verstrekt, moet hetzelfde geheim zijn dat in het ACS wordt gebruikt.

2. Om de geconfigureerd externe TACACS-server te kunnen gebruiken, moet deze in een TACACS-serverreeks worden toegevoegd om in de beleidssets te worden gebruikt. Om de reeks TACACS Server te configureren navigeer naar **werkcentra > Apparaatbeheer > Netwerkbronnen > TACACS Server sequentie.** Klik op **Add,** vul de details in en kies de

servers die nodig zijn om in die volgorde te worden gebruikt.

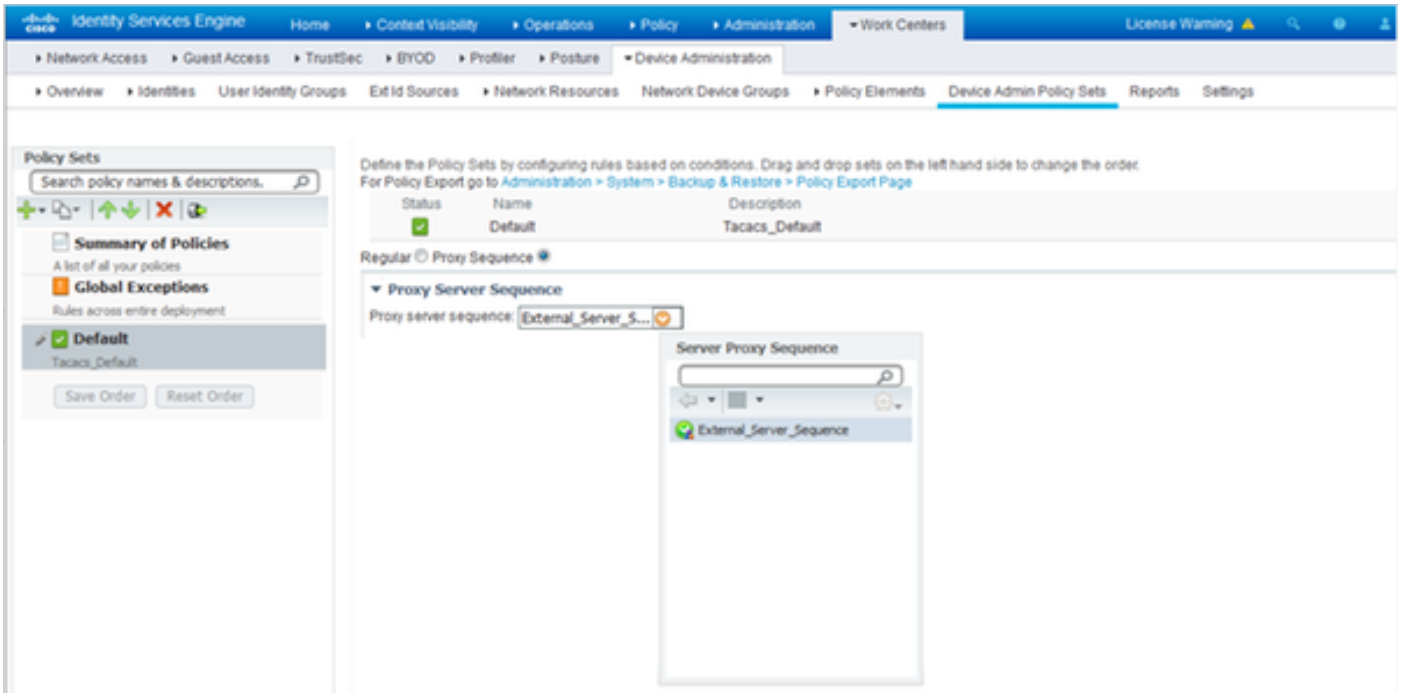


Naast de serverreeks zijn er nog twee andere opties geboden. Loging Control en Username Stripping.

Logging Control biedt de mogelijkheid om de boekhoudkundige verzoeken lokaal te registreren op ISE of de boekhoudkundige verzoeken te registreren bij de externe server die ook de verificatie verwerkt.

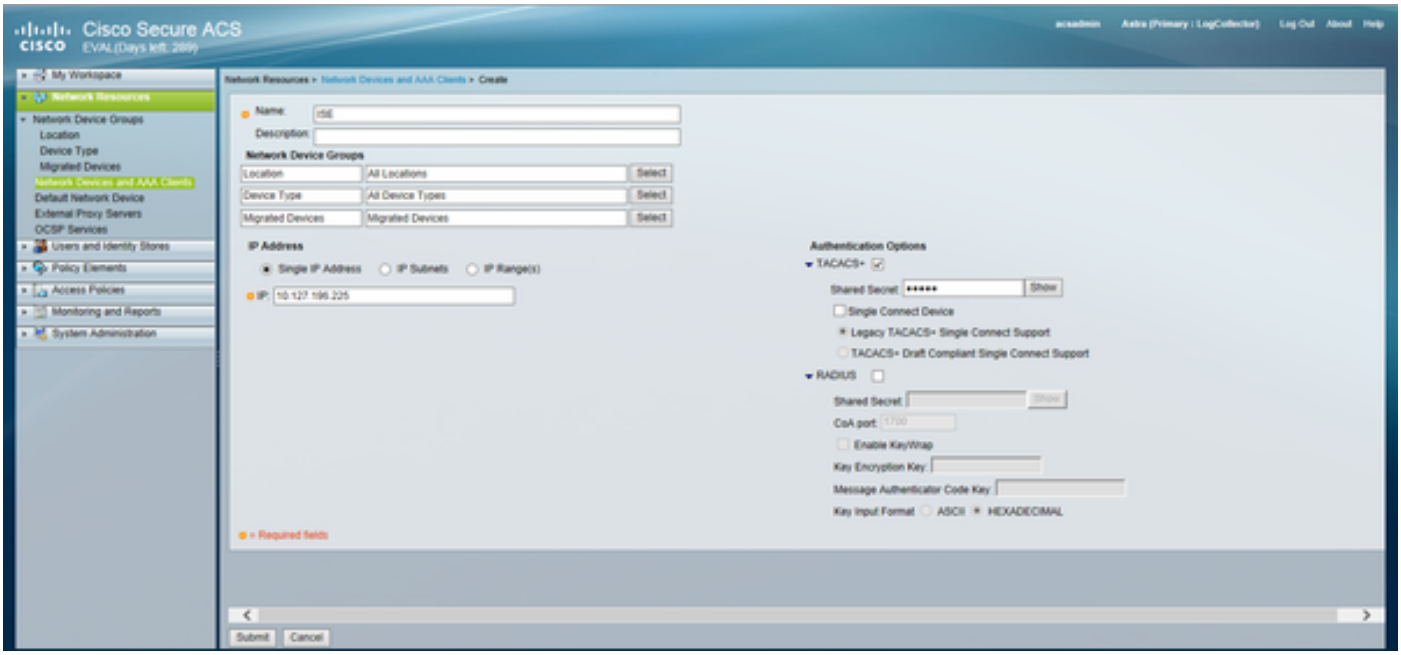
Gebruikersnaam Stripping wordt gebruikt om hetzij de prefixeerwaarde of de suffix te verwijderen door een afbakening te specificeren voordat het verzoek naar een externe TACACS-server wordt verzonden.

3. Om de geconfigureerde externe TACACS-servervolgorde te gebruiken, moeten de beleidssets worden geconfigureerd om de gecreëerde volgorde te gebruiken. Om de beleidssets te configureren die u wilt gebruiken de externe servervolgorde, navigeer dan naar **werkcentra > Apparaatbeheer > Apparaatbeheerset > [selecteer de beleidsset].** radioknop omdraaien die **Proxy sequentie** zegt. Kies de externe servervolgorde die is gemaakt.

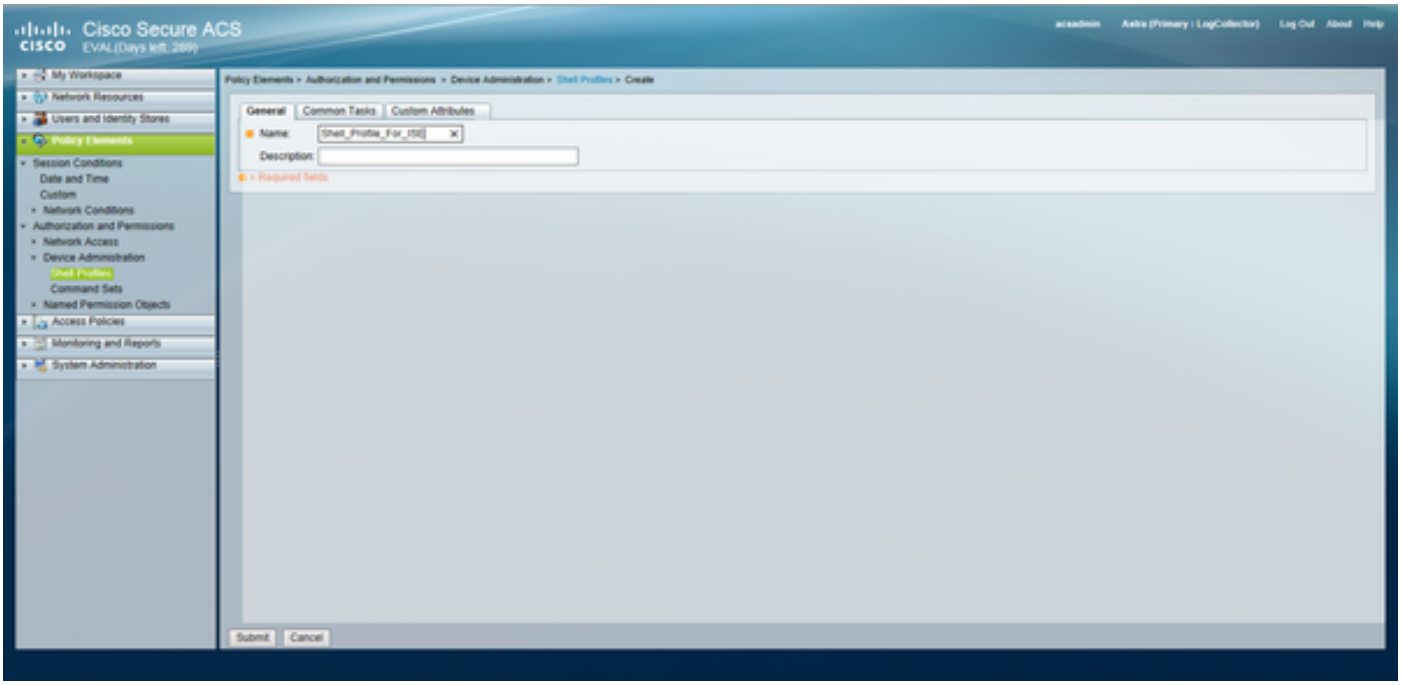


ACS configureren

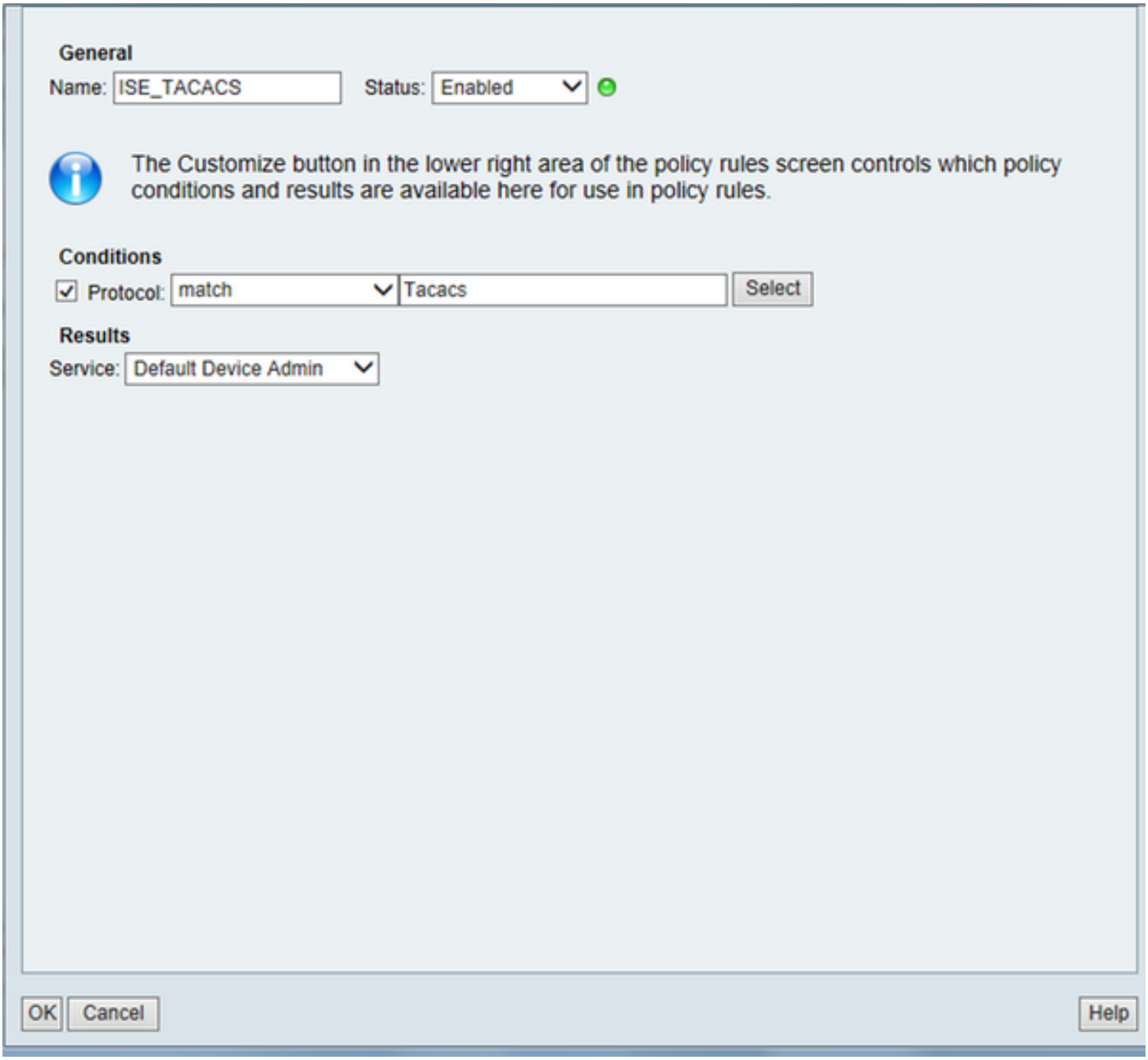
Voor ACS is ISE gewoon een ander netwerkapparaat dat een TACACS-aanvraag zal verzenden. Om ISE als een netwerkapparaat in ACS te configureren kunt u navigeren naar **Netwerkbronnen > Netwerkapparaten en AAA-clients.** Klik op **Maken** en vul de details van de ISE Server in met behulp van het zelfde gedeelde geheim dat op ISE is ingesteld.



Configureer apparaatbeheerparameters op ACS die, de shell profielen en de opdrachtsets zijn. Om Shell profielen te configureren navigeer naar **elementen van het beleid > autorisatie en toegangsrechten > profielen van Shell (Apparaatbeheer).** Klik op **Maken** en stel de naam, Gemeenschappelijke Taken en Aangepaste Toekeningszaken in zoals in de vereiste.



Om de reeks Opdrachten te configureren **navigeer** naar **elementen van het beleid > Vergunning en Toestemmingen > Stadsbeheer > Opdrachtsets.** Klik op **Maken** en vul de details in zoals vereist.



Configureer de toegangsservice die is geselecteerd in de Service Selection Rule zoals vereist.Om de regels voor toegangsservices te configureren kunt u **navigeren** naar **toegangsbeleid > Toegangsservices >** Standaard **Apparaatbeheer > Identity Services** die gebruikt moet worden geselecteerd voor verificatie. De vergunningsregels kunnen worden ingesteld door in te **navigeren** naar **toegangsbeleid > Toegangsservices >Standaard apparaatbeheer > autorisatie.**

> Opmerking: De configuratie van het vergunningenbeleid en de shell-profielen van specifieke hulpmiddelen kan variëren en dat valt buiten het toepassingsgebied van dit document.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Verificatie kan zowel op de ISE als op de ACS worden verricht. Elke fout in de configuratie van de ISE of de ACS zal leiden tot een echtheidsfout. ACS is de primaire server die de authenticatie en de vergunningsverzoeken zal behandelen, ISE draagt de verantwoordelijkheid van en naar de ACS-server en fungeert als een volmacht voor de verzoeken. Aangezien de pakketreizen door

beide servers lopen, kan de verificatie van de verificatie of het vergunningsverzoek op beide servers worden uitgevoerd.

Netwerkapparaten zijn geconfigureerd met ISE als TACACS-server en niet de ACS. Daarom bereikt het verzoek eerst ISE en op basis van de geconfigureerde regels besluit ISE of het verzoek naar een externe server moet worden doorgestuurd. Dit kan worden geverifieerd in de TACACS Live-logbestanden op de ISE.

Om de bewegende logbestanden op ISE te bekijken, navigeer naar **bewerkingen > TACACS > Live Logs.** Live rapporten kunnen op deze pagina worden bekeken en de details van een specifiek verzoek kunnen worden gecontroleerd door te klikken op het pictogram van vergroot glas met betrekking tot dat specifieke verzoek dat van belang is.

Om de verificatierapporten over het ACS te kunnen bekijken, moet u naar **bewaking en rapporten > Monitoring and Report Viewer > Monitoring and Reports > Rapporten > AAA Protocol > TACACS-verificatie** navigeren**.** Net als ISE kunnen de details van een bepaald verzoek worden

gecontroleerd door te klikken op het pictogram van vergroot glas met betrekking tot dat specifieke verzoek dat van belang is

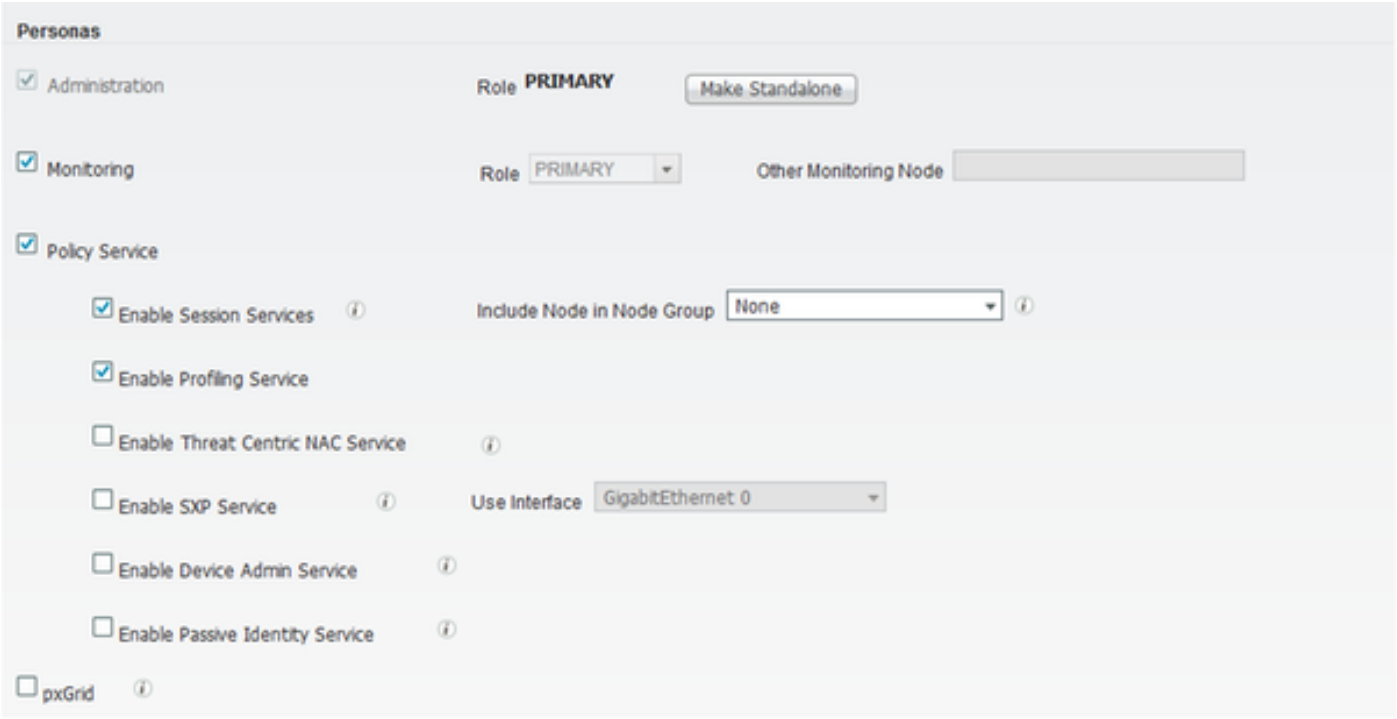
Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen

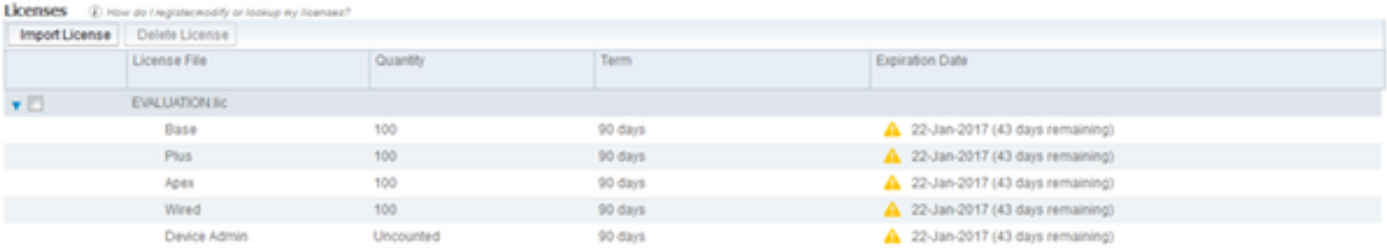
1. Als de details van het rapport op ISE de foutmelding tonen die in de afbeelding wordt weergegeven, dan duidt dit op een ongeldig gedeeld geheim dat is ingesteld op ofwel de ISE ofwel het Netwerkapparaat (NAD).

2. Indien er geen verificatierapport voor een verzoek op de ISE is, maar de toegang aan de eindgebruiker wordt geweigerd, wijst dit meestal op verschillende dingen.

- Het verzoek zelf heeft de ISE-server niet bereikt.
- Als de wastafel van het apparaat op ISE wordt uitgeschakeld, wordt een TACACS+ verzoek aan ISE stilletjes ingetrokken. In de rapporten of in de Live Logs worden geen registers weergegeven waarin hetzelfde wordt aangegeven. Om dit te verifiëren, navigeer naar **Administratie > Systeem > Plaatsing > [selecteer het knooppunt].** Klik op **Bewerken** en merk het vakje "**Apparaatbeheerder inschakelen**" in het tabblad **Algemene instellingen** zoals in het afbeelding. Dat selectieteken moet worden gecontroleerd zodat de Apparaatbeheerder aan ISE kan werken.



- Als er geen licentie voor apparaatbeheer aanwezig is van verlopen, worden alle TACACS+ aanvragen stilletjes ingetrokken. In de GUI worden voor hetzelfde programma geen logbestanden weergegeven. Navigeer naar **Administratie > Systeem > Licentie** om de licentie voor apparaatbeheer te controleren.

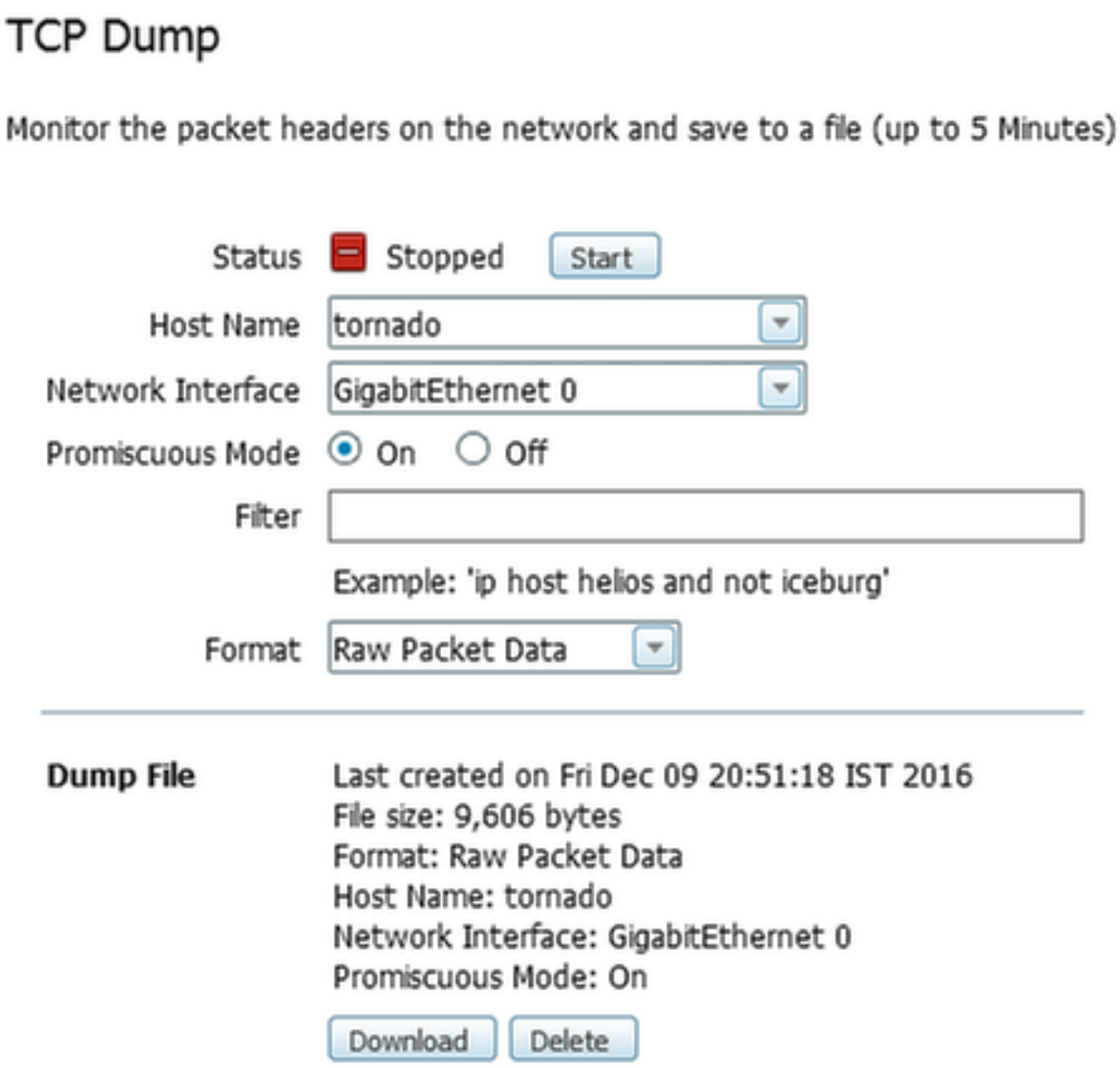


- Als het netwerkapparaat niet is geconfigureerd of als een fout netwerkapparaat in IP is ingesteld op ISE, dan laat ISE in stilte het pakket vallen. Er wordt geen antwoord naar de cliënt teruggestuurd en in de GUI worden geen logbestanden getoond. Dit is een verandering van gedrag in ISE voor TACACS+ in vergelijking met die van ACS die aangeeft dat het verzoek van een onbekend netwerkapparaat of AAA-client is binnengekomen.

- Het verzoek bereikte het ACS-EG-Verdrag, maar het antwoord kwam niet terug op de ISE. Dit scenario kan worden gecontroleerd aan de hand van de verslagen over de ACS-landen, zoals in het cijfer weergegeven. Meestal is dit te wijten aan een ongeldig gedeeld geheim, hetzij op de ACS die voor ISE is ingesteld, hetzij op de ISE die voor de ACS is ingesteld.

- De respons wordt niet verstuurd, zelfs als ISE niet is geconfigureerd of het IP-adres van de Management-interface van ISE niet is ingesteld in het ACS-netwerk in de configuratie van het netwerkapparaat. In een dergelijk geval kan de boodschap in de figuur op de ACS worden waargenomen.

- Als er een succesvol verificatieverslag op de ACS wordt gezien, maar er geen rapporten op de ISE worden gezien en de gebruiker wordt verworpen, dan zou dat zeer wel een probleem kunnen zijn in het netwerk. Dit kan worden geverifieerd door een pakketvastlegging op ISE met de benodigde filters. Om een pakketvastlegging op ISE te verzamelen, navigeer naar **Operations > Probleemoplossing > diagnostische tools > Algemene tools > TCP pomp.**



3. Als de rapporten op ISE maar niet op het ACS-systeem kunnen worden gezien, kan dit betekenen dat het verzoek het ACS niet heeft bereikt vanwege een verkeerde configuratie van de beleidsreeksen op ISE die op basis van het gedetailleerde rapport over ISE kunnen worden opgelost, of vanwege een netwerkprobleem dat kan worden geïdentificeerd door een pakketvastlegging op het ACS.

4. Indien de rapporten zowel op ISE als op het ACS-gebied worden gezien, maar de gebruiker nog steeds geen toegang krijgt, dan is het meestal een probleem in de configuratie van het toegangsbeleid voor ACS'en, die op basis van het gedetailleerde verslag over het ACS-gebied kan worden opgelost. Tevens moet het retourverkeer van de ISE naar het netwerkapparaat zijn toegestaan.