Externe RADIUS-servers configureren op ISE

Inhoud

Inleiding

In dit document wordt de configuratie van een RADIUS-server op ISE beschreven als een proxy- en autorisatieserver. Hier worden twee ISE-servers gebruikt en één fungeert als een externe server. Maar elke RFC-conforme RADIUS-server kan worden gebruikt.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van het RADIUS-protocol
- Expertise in beleidsconfiguratie Identity Services Engine (ISE)

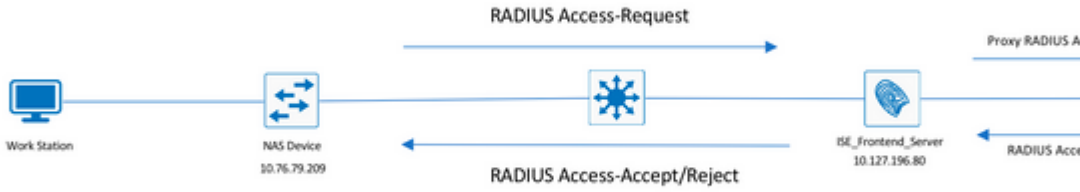
Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco ISE-versies 2.2 en 2.4.

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 live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

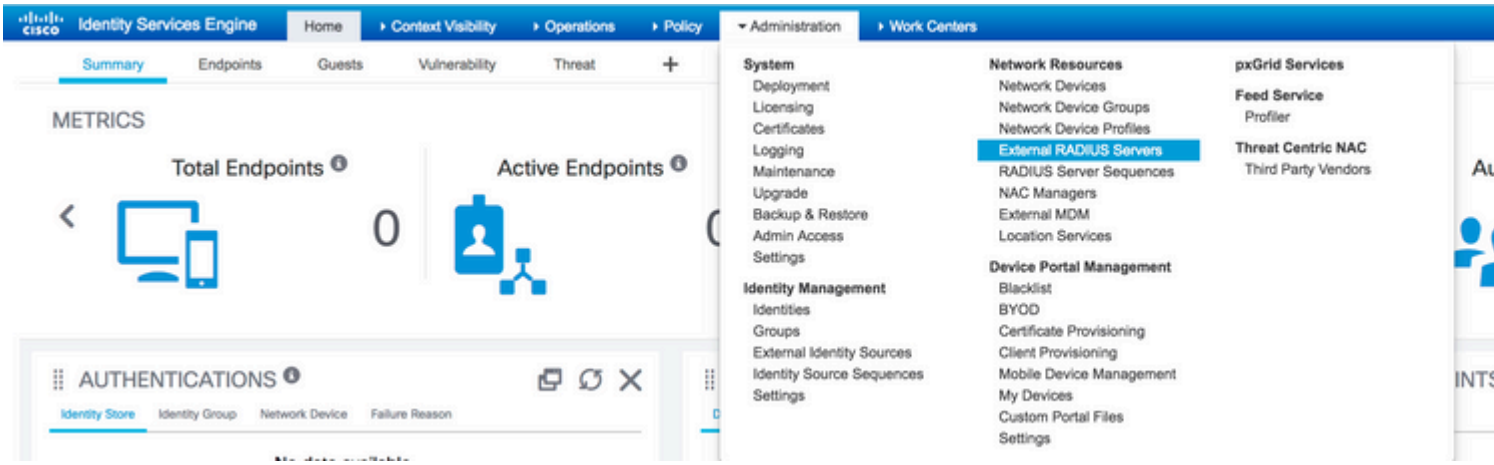
Configureren

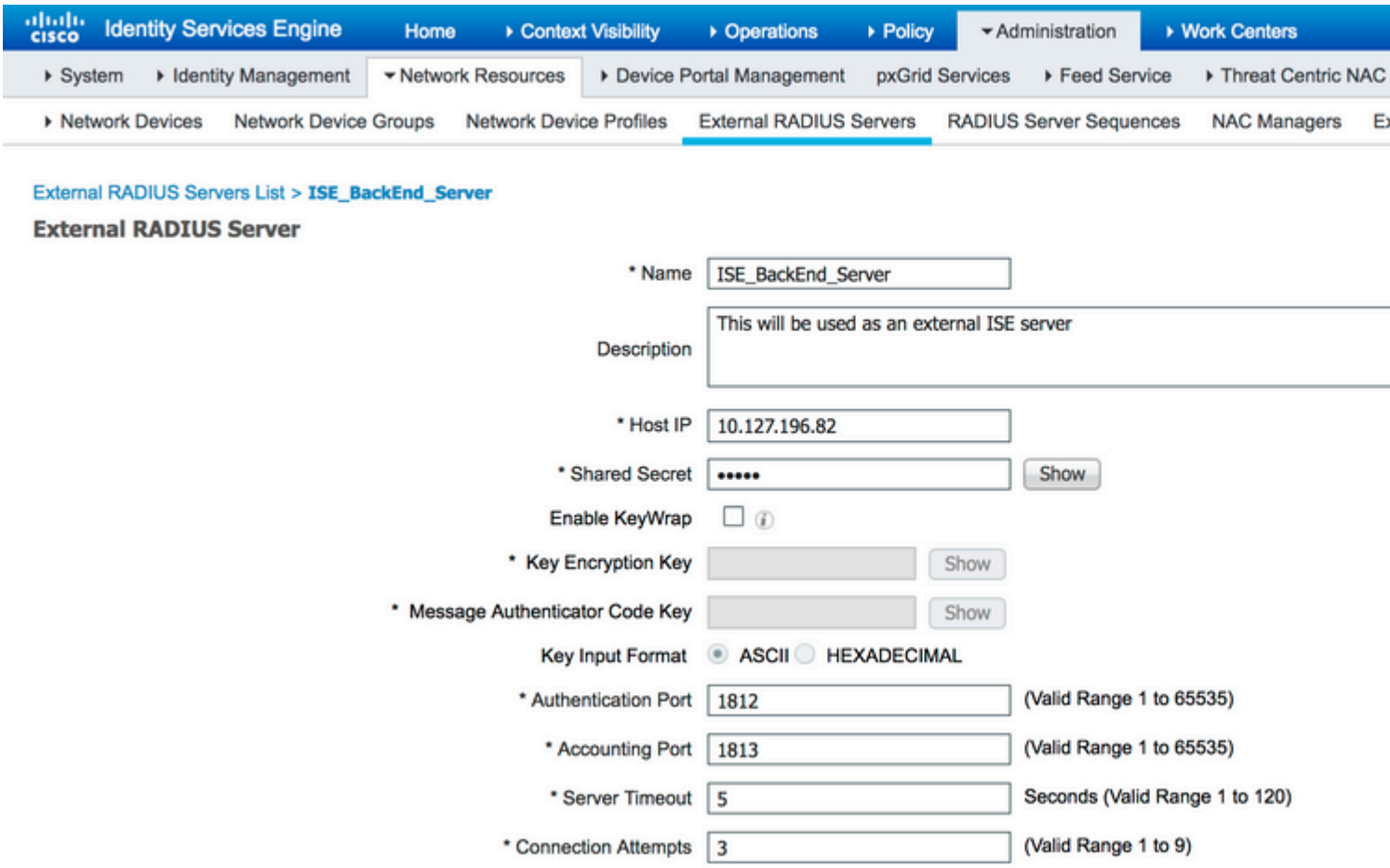
Netwerkdiagram



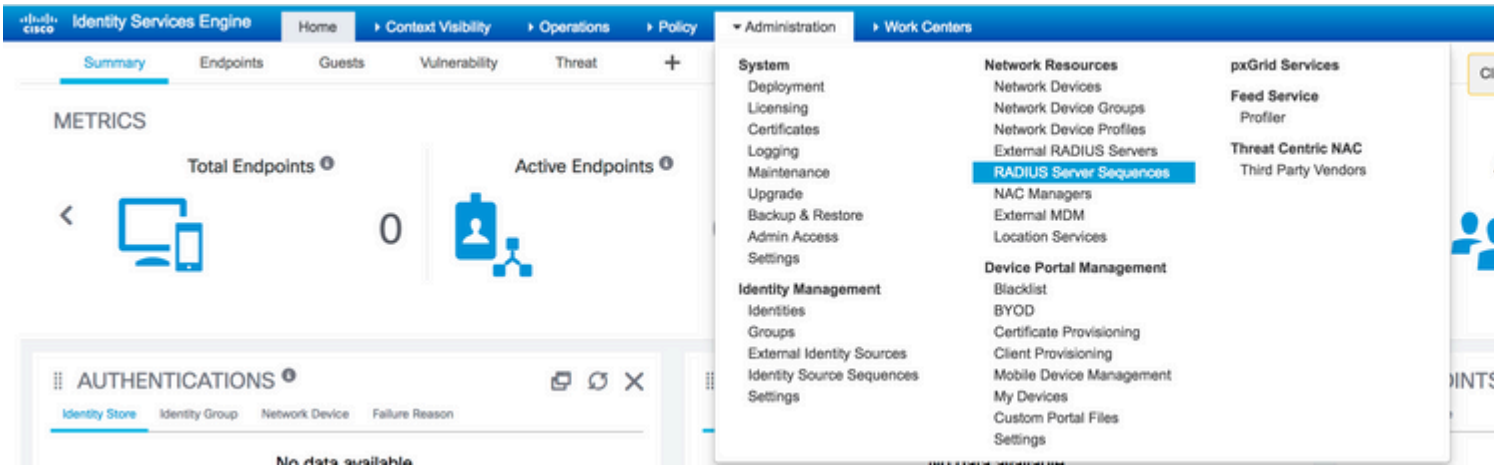
ISE configureren (Frontend Server)

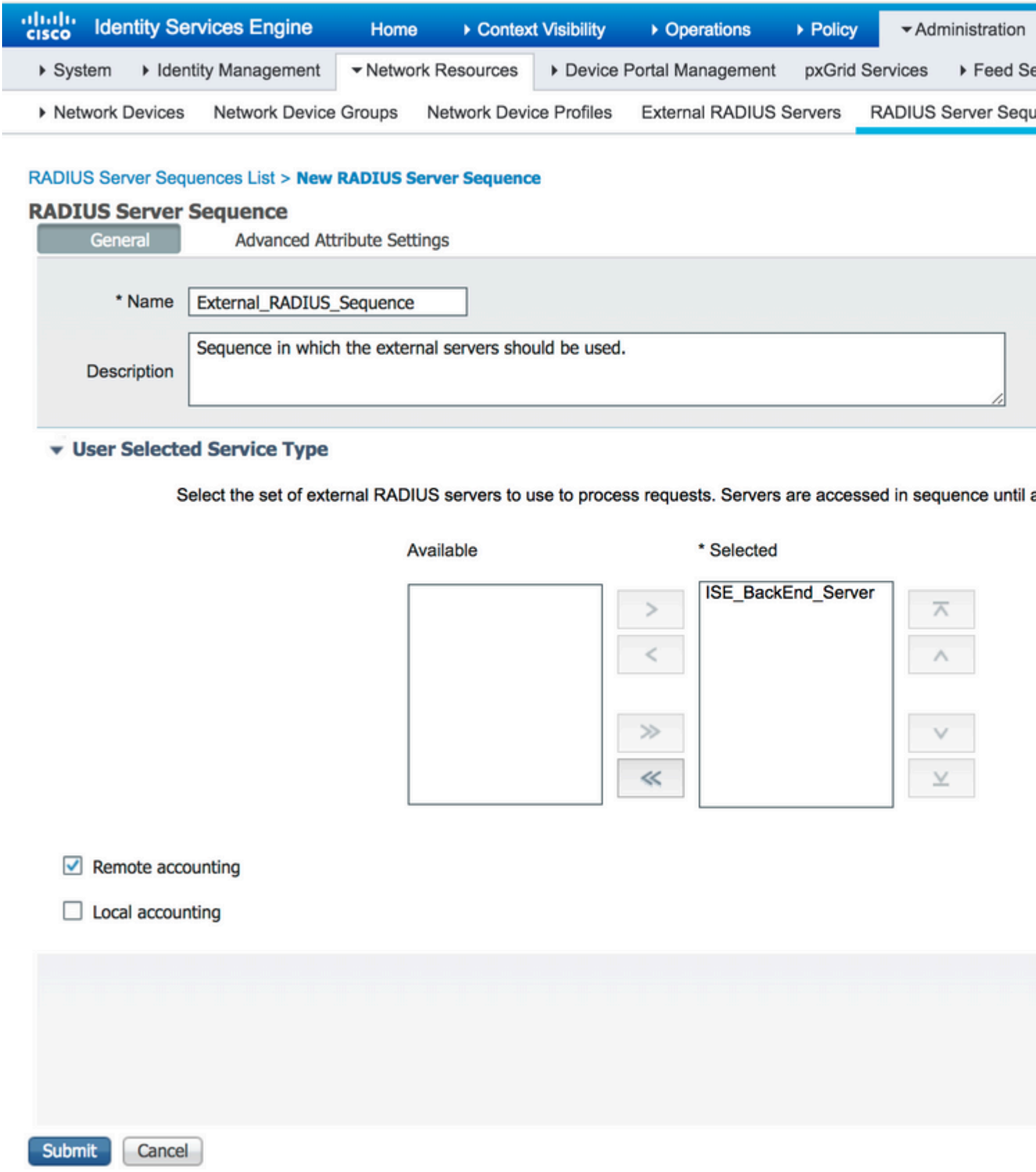
Stap 1. Er kunnen meerdere externe RADIUS-servers worden geconfigureerd en gebruikt om gebruikers op de ISE te verifiëren. Om externe RADIUS-servers te configureren, navigeer u naar Administration > Network Resources > External RADIUS Servers > Add, zoals aangegeven op de afbeelding:





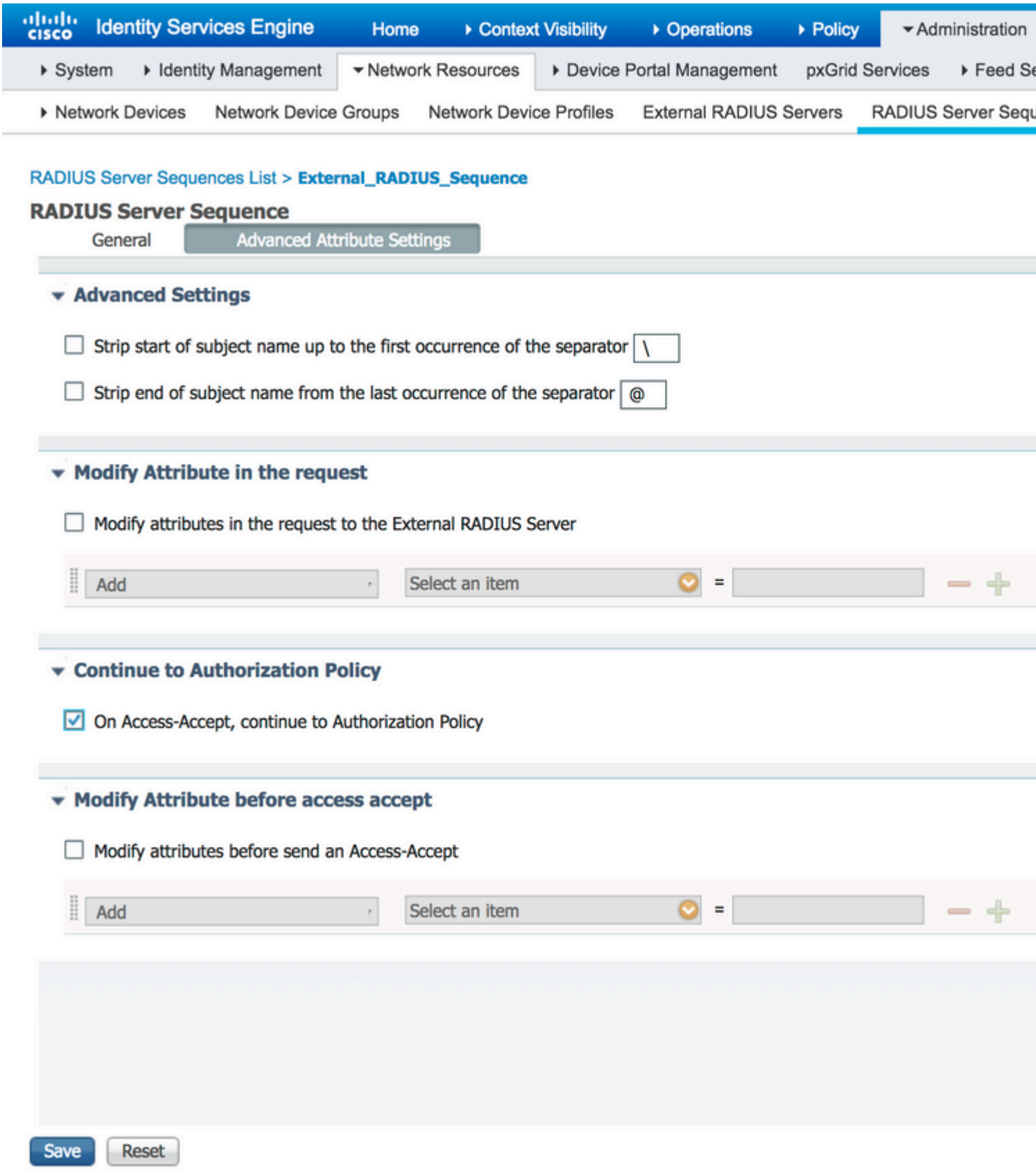
Stap 2. Om de geconfigureerde externe RADIUS-server te kunnen gebruiken, moet een RADIUS-serverreeks worden geconfigureerd die vergelijkbaar is met de reeks van identiteitsbronnen. Om hetzelfde te configureren navigeer u naar Administration > Network Resources > RADIUS Server Sequences > Add, zoals aangegeven in de afbeelding.





Opmerking: een van de opties die beschikbaar zijn wanneer de serverreeks wordt gemaakt, is om te kiezen of de accounting lokaal moet worden uitgevoerd op de ISE of op de externe RADIUS-server. Gebaseerd op de hier gekozen optie, beslist ISE of de accountingverzoeken worden benaderd of deze logbestanden lokaal worden opgeslagen.

Stap 3. Er is een extra sectie die meer flexibiliteit geeft over hoe ISE zich moet gedragen wanneer het verzoeken aan externe RADIUS-servers proxies. Het is te vinden onder Advance Attribute Settings, zoals aangegeven in de afbeelding.



- Geavanceerde instellingen: Hier vindt u opties voor het verwijderen van het begin of het einde van de gebruikersnaam in RADIUS-verzoeken met een scheidingsteken.

- Kenmerk wijzigen in het verzoek: Biedt de optie om een RADIUS-kenmerk aan te passen in de RADIUS-verzoeken. De lijst toont hier de eigenschappen die kunnen worden toegevoegd/verwijderd/bijgewerkt:

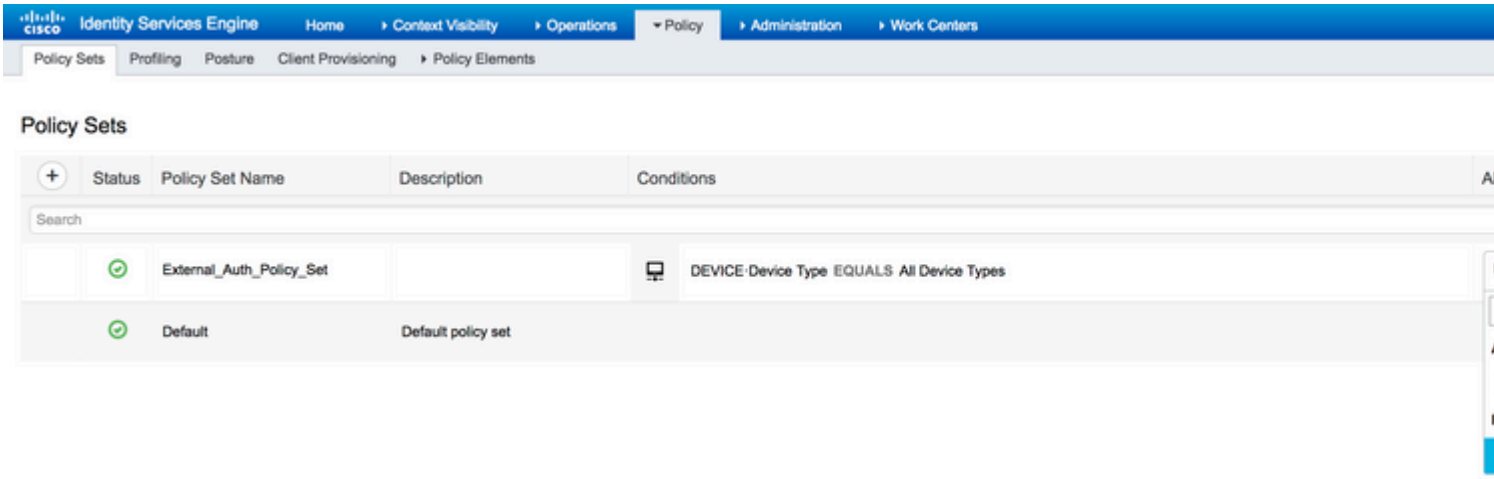
```
User-Name--[1]
NAS-IP-Address--[4]
NAS-Port--[5]
Service-Type--[6]
Framed-Protocol--[7]
Framed-IP-Address--[8]
Framed-IP-Netmask--[9]
Filter-ID--[11]
Framed-Compression--[13]
Login-IP-Host--[14]
Callback-Number--[19]
State--[24]
VendorSpecific--[26]
Called-Station-ID--[30]
Calling-Station-ID--[31]
NAS-Identifier--[32]
Login-LAT-Service--[34]
Login-LAT-Node--[35]
Login-LAT-Group--[36]
Event-Timestamp--[55]
Egress-VLANID--[56]
Ingress-Filters--[57]
Egress-VLAN-Name--[58]
User-Priority-Table--[59]
NAS-Port-Type--[61]
Port-Limit--[62]
Login-LAT-Port--[63]
Password-Retry--[75]
Connect-Info--[77]
NAS-Port-Id--[87]
Framed-Pool--[88]
NAS-Filter-Rule--[92]
NAS-IPv6-Address--[95]
Framed-Interface-Id--[96]
Framed-IPv6-Prefix--[97]
Login-IPv6-Host--[98]
Error-Cause--[101]
Delegated-IPv6-Prefix--[123]
Framed-IPv6-Address--[168]
DNS-Server-IPv6-Address--[169]
Route-IPv6-Information--[170]
Delegated-IPv6-Prefix-Pool--[171]
Stateful-IPv6-Address-Pool--[172]
```

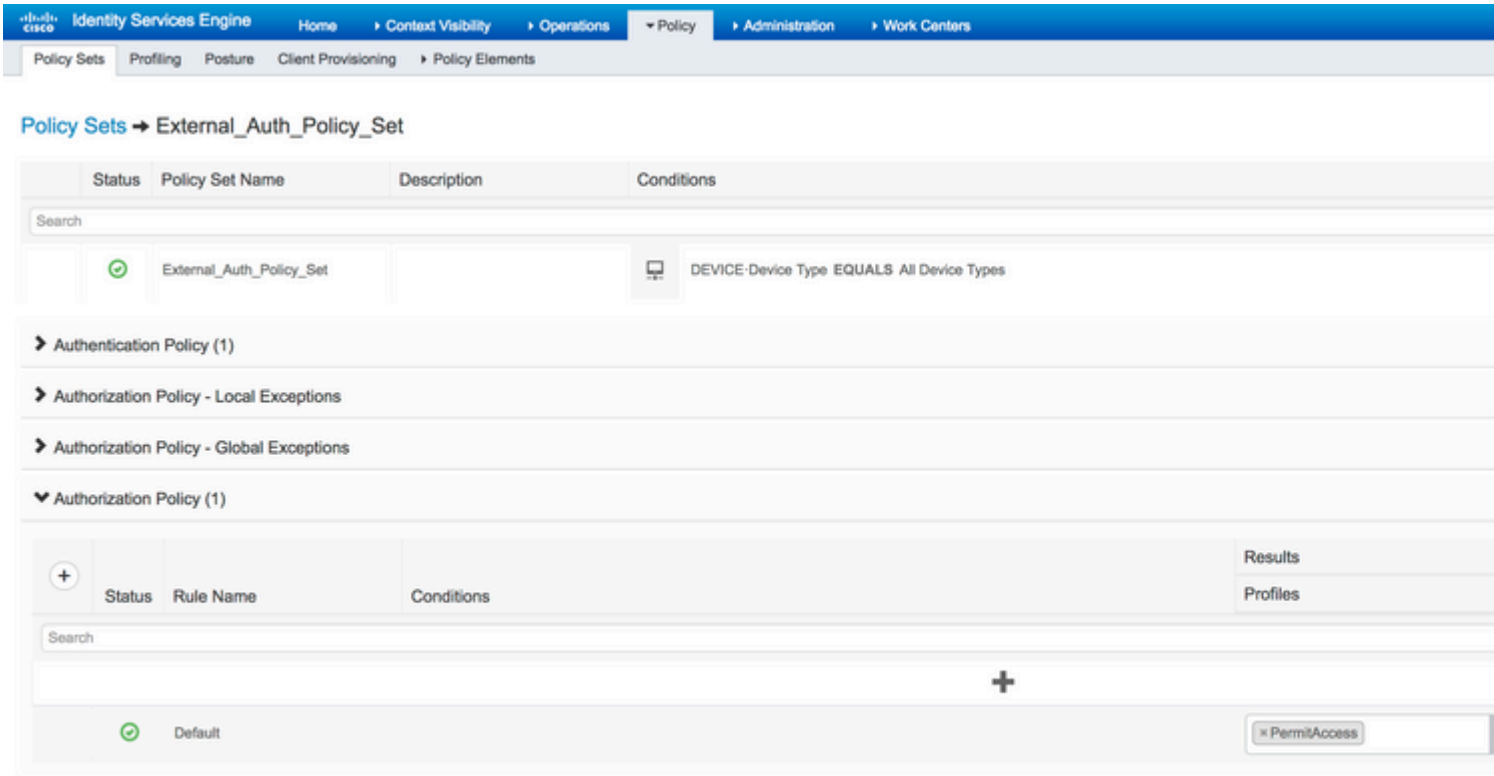
- Ga verder met het autorisatiebeleid voor toegangsacceptatie: biedt een optie om te kiezen of ISE het toegangsacceptatiebeleid gewoon moet verzenden zoals het is of moet doorgaan om toegang te bieden op basis van het autorisatiebeleid dat op de ISE is geconfigureerd in plaats van de autorisatie die door de externe RADIUS-server wordt geboden. Als deze optie geselecteerd is, wordt de door de externe RADIUS-server verstrekte autorisatie overschreven met de door ISE verstrekte autorisatie.

> **Opmerking**: deze optie werkt alleen als er een Access-Accept in antwoord op het geproxileerde RADIUS-toegangsverzoek.

- Kenmerk wijzigen vóór toegangsgoedkeuring: vergelijkbaar met Modify Attribute in the request, kunnen de eerder genoemde attributen worden toegevoegd/verwijderd/bijgewerkt heden in de Access-Accept verzonden door de externe RADIUS-server voordat het wordt verzonden naar het netwerkapparaat.

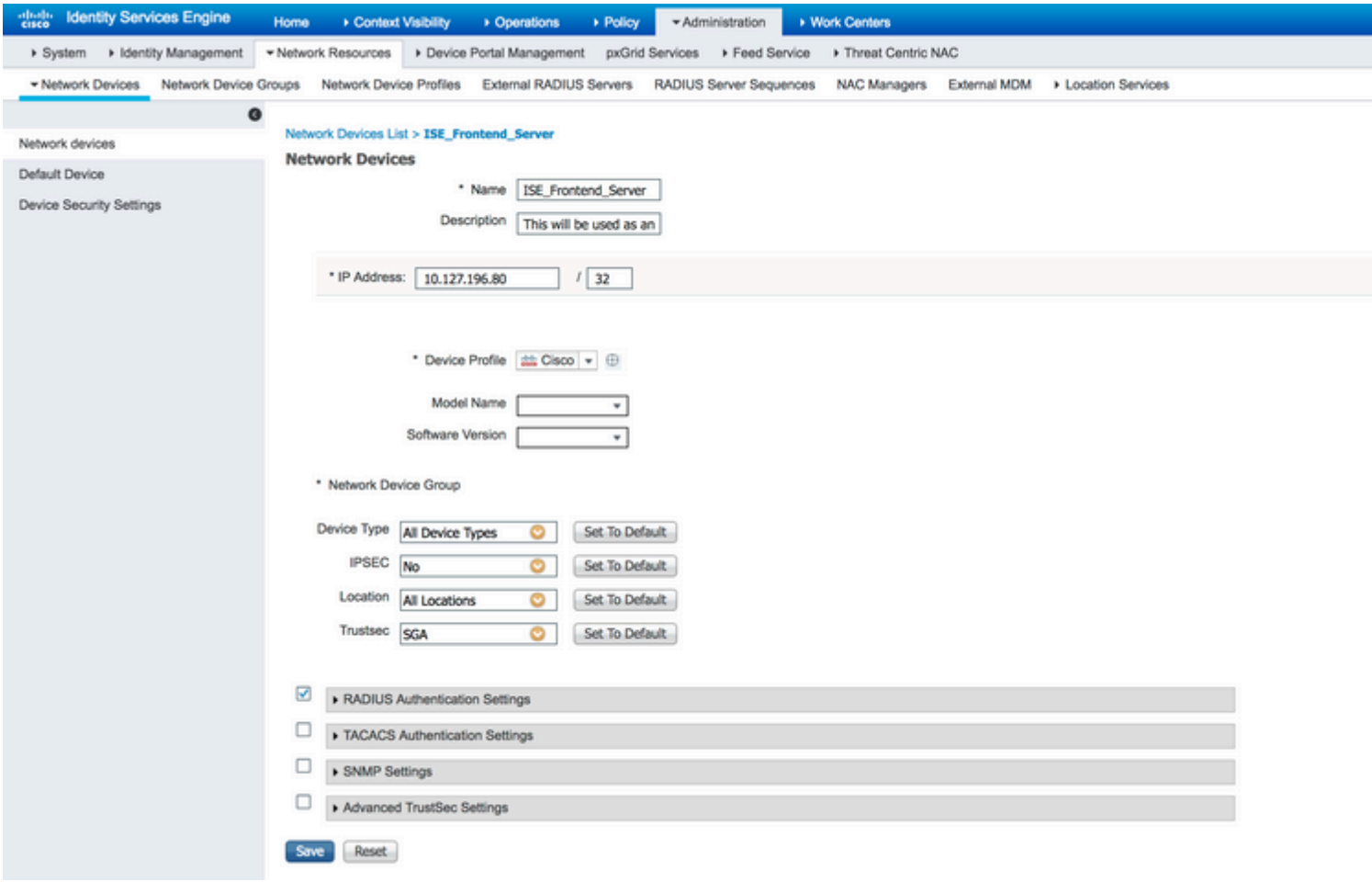
Stap 4. Het volgende deel is dat u de Policy Sets moet configureren om de RADIUS-serverreeks te gebruiken in plaats van de Toegestane Protocollen, zodat de aanvragen naar de externe RADIUS-server worden verzonden. Het kan worden geconfigureerd onder Policy > Policy Sets. Autorisatiebeleid kan worden geconfigureerd onder de Policy Set maar pas in werking treden als de Continue to Authorization Policy on Access-Accept wordt gekozen. Als dit niet het geval is, fungeert ISE gewoon als een proxy voor de RADIUS-verzoeken om de voorwaarden te matchen die voor deze Policy Set zijn geconfigureerd.



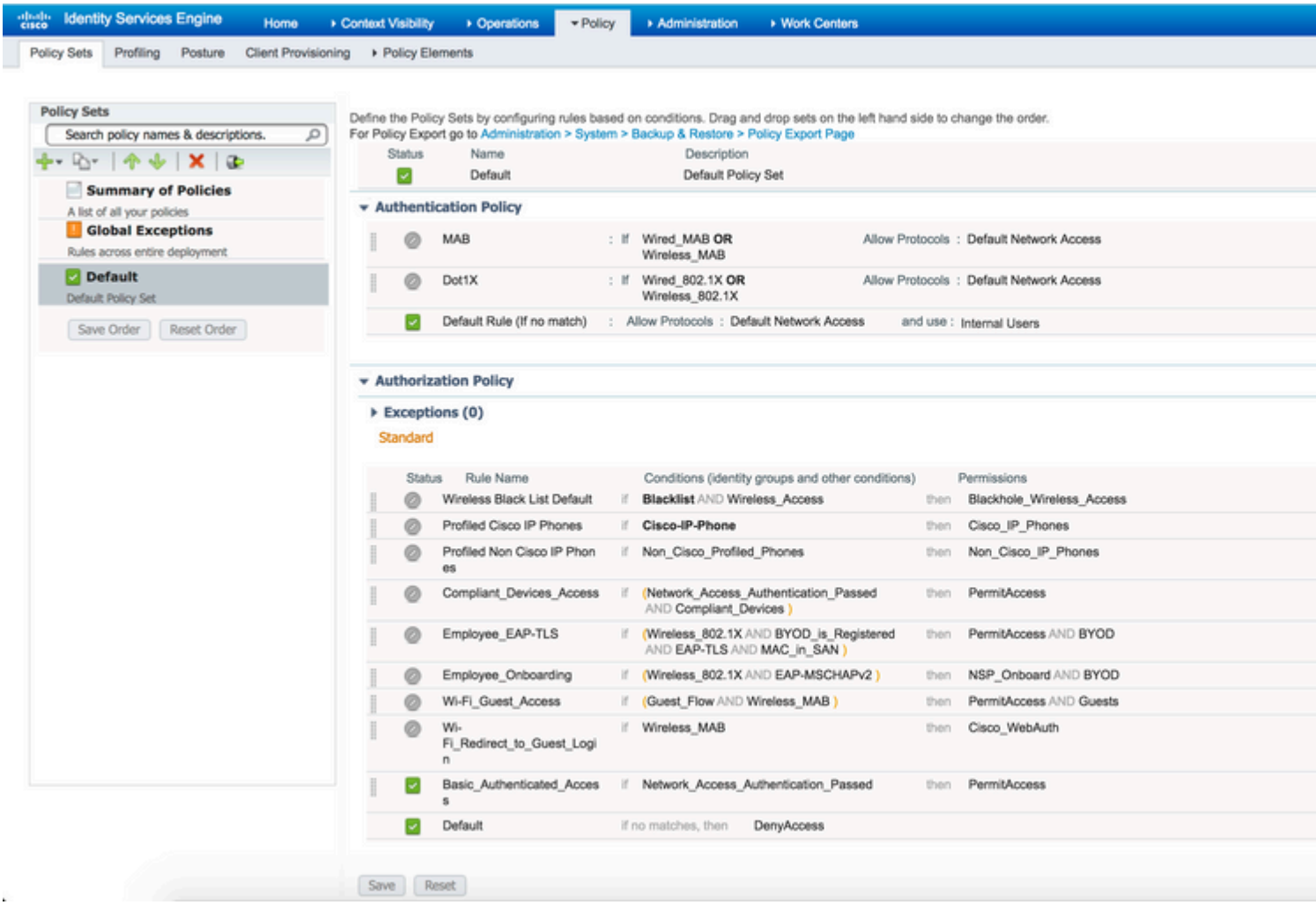


De externe RADIUS-server configureren

Stap 1. In dit voorbeeld wordt een andere ISE-server (versie 2.2) gebruikt als een externe RADIUS-server met de naam ISE_Backend_Server. De ISE (ISE_Frontend_Server) moet worden geconfigureerd als netwerkapparaat of traditioneel NAS worden genoemd in de externe RADIUS-server (ISE_Backend_Server in dit voorbeeld), aangezien de NAS-IP-Address het kenmerk in het toegangsverzoek dat naar de externe RADIUS-server is doorgestuurd, wordt vervangen door het IP-adres van hetISE_Frontend_Server. Het gedeelde geheim dat moet worden geconfigureerd is hetzelfde als dat voor de externe RADIUS-server op de ISE_Frontend_Server.



Stap 2. De externe RADIUS-server kan worden geconfigureerd met zijn eigen authenticatie- en autorisatiebeleid om de verzoeken die door de ISE worden benaderd, te ondersteunen. In dit voorbeeld, wordt een eenvoudig beleid gevormd om de gebruiker in de interne gebruikers te controleren en dan toegang te verlenen indien voor authentiek verklaard.



Verifiëren

Stap 1. Controleer de live-logbestanden van ISE als het verzoek is ontvangen, zoals in de afbeelding.

Stap 2. Controleer of de juiste beleidsset is geselecteerd, zoals in de afbeelding.

Overview

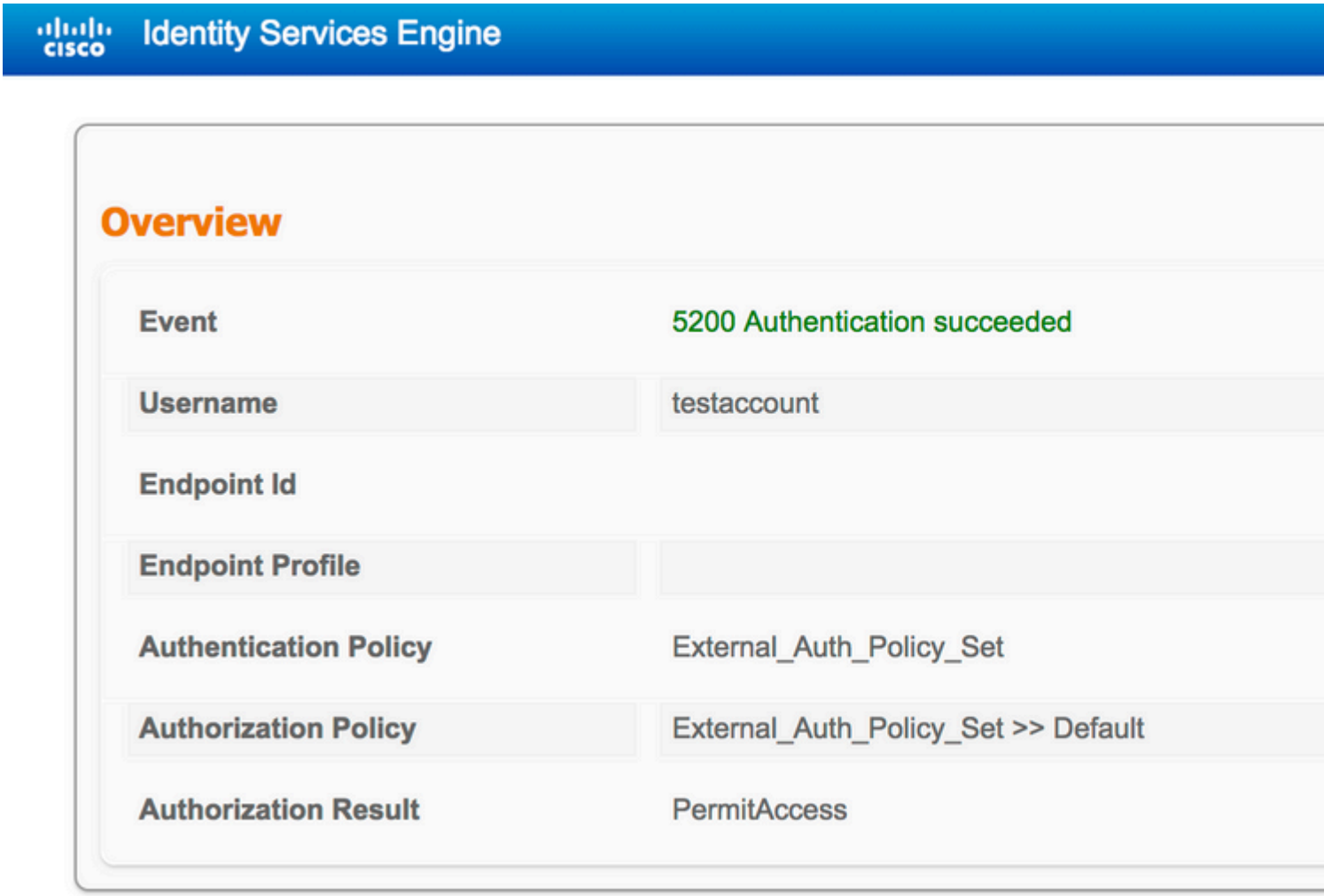
Event	5200 Authentication succeeded
Username	testaccount
Endpoint Id	
Endpoint Profile	
Authentication Policy	External_Auth_Policy_Set
Authorization Policy	External_Auth_Policy_Set
Authorization Result	

Stap 3. Controleer of het verzoek naar de externe RADIUS-server is doorgestuurd.

Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
11049	Settings of RADIUS default network device will be used
11117	Generated a new session ID
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15048	Queried PIP - DEVICE.Device Type
11358	Received request for RADIUS server sequence.
11361	Valid incoming authentication request
11355	Start forwarding request to remote RADIUS server
11365	Modify attributes before sending request to external radius server
11100	RADIUS-Client about to send request - (port = 1812)
11101	RADIUS-Client received response
11357	Successfully forwarded request to current remote RADIUS server
11002	Returned RADIUS Access-Accept

4. Indien de Continue to Authorization Policy on Access-Accept wordt gekozen, controleert u of het toelatingsbeleid wordt geëvalueerd.



Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
11049	Settings of RADIUS default network device will be used
11117	Generated a new session ID
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15048	Queried PIP - DEVICE.Device Type
11358	Received request for RADIUS server sequence.
11361	Valid incoming authentication request
11355	Start forwarding request to remote RADIUS server
11365	Modify attributes before sending request to external radius server
11100	RADIUS-Client about to send request - (port = 1812)
11101	RADIUS-Client received response
11357	Successfully forwarded request to current remote RADIUS server
15036	Evaluating Authorization Policy
15016	Selected Authorization Profile - PermitAccess
22081	Max sessions policy passed
22080	New accounting session created in Session cache
11002	Returned RADIUS Access-Accept

Problemen oplossen

Scenario 1. Event - 5405 RADIUS-aanvraag gedaald

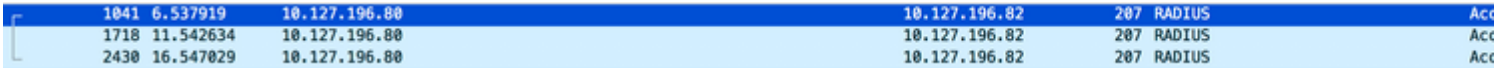
- Het belangrijkste dat moet worden geverifieerd zijn de stappen in het gedetailleerde verificatierapport. Als de stappen de RADIUS-Client request timeout expired, dan betekent het dat de ISE geen enkele reactie van de geconfigureerde externe RADIUS-server heeft ontvangen. Dit kan gebeuren wanneer:

1. Er is een connectiviteitsprobleem met de externe RADIUS-server. ISE kan de externe RADIUS-server niet bereiken op de poorten die daarvoor zijn geconfigureerd.
2. ISE is niet geconfigureerd als een netwerkapparaat of NAS op de externe RADIUS-server.
3. De pakketten worden door de externe RADIUS-server gedropt, hetzij door configuratie, hetzij door een probleem op de externe RADIUS-server.

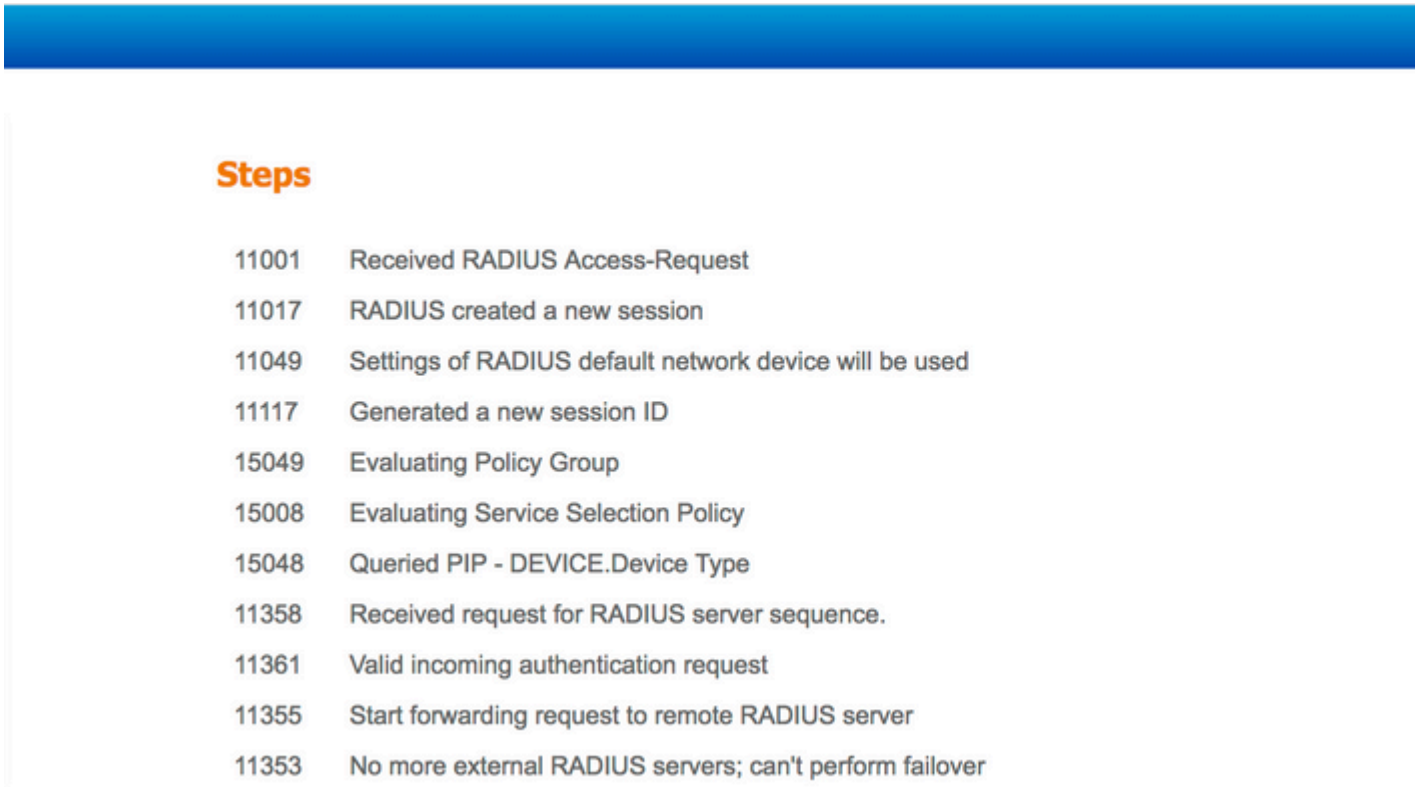
Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
11049	Settings of RADIUS default network device will be used
11117	Generated a new session ID
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15048	Queried PIP - DEVICE.Device Type
11358	Received request for RADIUS server sequence.
11361	Valid incoming authentication request
11355	Start forwarding request to remote RADIUS server
11365	Modify attributes before sending request to external radius server
11100	RADIUS-Client about to send request - (port = 1812)
11104	RADIUS-Client request timeout expired (⏰ Step latency=15011 ms)
11356	Failed to forward request to current remote RADIUS server
11353	No more external RADIUS servers; can't perform failover

Controleer pakketopnamen ook om te zien of het geen vals bericht is, dat wil zeggen, ISE ontvangt het pakket terug van de server, maar meldt nog steeds dat het verzoek is uitgezet.



- Als de stappen Start forwarding request to remote RADIUS server en de onmiddellijke stap is No more external RADIUS servers; can't perform failover, dan betekent het dat alle geconfigureerde externe RADIUS-servers momenteel **dood** zijn gemarkeerd en de verzoeken alleen worden verzonden nadat de dode timer is verlopen.



Opmerking: de standaard **dode tijd** voor externe RADIUS-servers in ISE is **5 minuten**. Deze waarde is hardcoded en kan niet vanaf deze versie worden gewijzigd.

- Als de stappen RADIUS-Client encountered error during processing flow en worden gevolgd door Failed to forward request to current remote RADIUS server; an invalid response was received,dan betekent het dat ISE een probleem is tegengekomen tijdens het doorsturen van het verzoek naar de externe RADIUS-server. Dit wordt gewoonlijk waargenomen wanneer het RADIUS-verzoek dat van het netwerkapparaat/NAS naar de ISE wordt verzonden, niet de juiste NAS-IP-Address als een van de eigenschappen. Als er geen NAS-IP-Address kenmerken en als er geen externe RADIUS-servers worden gebruikt, vult ISE de NAS-IP-Address veld met de IP-bron van het pakket. Dit is echter niet van toepassing wanneer een externe RADIUS-server in gebruik is.

Scenario 2. Event - 5400 verificatie mislukt

- In dit geval, als de stappen zeggen 11368 Please review logs on the External RADIUS Server to determine the precise failure reasonDan betekent het dat de verificatie op de externe RADIUS-server zelf is mislukt en dat er een Access-Reject is verzonden.

Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
11049	Settings of RADIUS default network device will be used
11117	Generated a new session ID
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15048	Queried PIP - DEVICE.Device Type
11358	Received request for RADIUS server sequence.
11361	Valid incoming authentication request
11355	Start forwarding request to remote RADIUS server
11365	Modify attributes before sending request to external radius server
11100	RADIUS-Client about to send request - (port = 1812)
11101	RADIUS-Client received response
11368	Please review logs on the External RADIUS Server to determine the precise failure reason.
11357	Successfully forwarded request to current remote RADIUS server
11003	Returned RADIUS Access-Reject

- Als de stappen 15039 Rejected per authorization profileDit betekent echter dat ISE een Access-Accept heeft ontvangen van de externe RADIUS-server, maar ISE wijst de autorisatie af op basis van het ingestelde autorisatiebeleid.

Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
11049	Settings of RADIUS default network device will be used
11117	Generated a new session ID
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15048	Queried PIP - DEVICE.Device Type
11358	Received request for RADIUS server sequence.
11361	Valid incoming authentication request
11355	Start forwarding request to remote RADIUS server
11365	Modify attributes before sending request to external radius server
11100	RADIUS-Client about to send request - (port = 1812)
11101	RADIUS-Client received response
11357	Successfully forwarded request to current remote RADIUS server
15036	Evaluating Authorization Policy
15016	Selected Authorization Profile - DenyAccess
15039	Rejected per authorization profile
11003	Returned RADIUS Access-Reject

- Indien de Failure Reason op de ISE nog iets anders is dan de hier genoemde in geval van een authenticatiefout, dan kan het een potentieel probleem betekenen met de configuratie of met de ISE zelf. U wordt aangeraden om op dit punt een TAC-case te openen.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.