Konfigurieren externer RADIUS-Server auf der ISE

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration eines RADIUS-Servers auf der ISE als Proxy- und Autorisierungsserver beschrieben. Hier werden zwei ISE-Server eingesetzt, einer davon fungiert als externer Server. Es kann jedoch jeder RFC-kompatible RADIUS-Server verwendet werden.

Voraussetzungen

Anforderungen

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

- Grundkenntnisse des RADIUS-Protokolls
- Umfassende Expertise bei der Konfiguration von Identity Services Engine (ISE)-Richtlinien

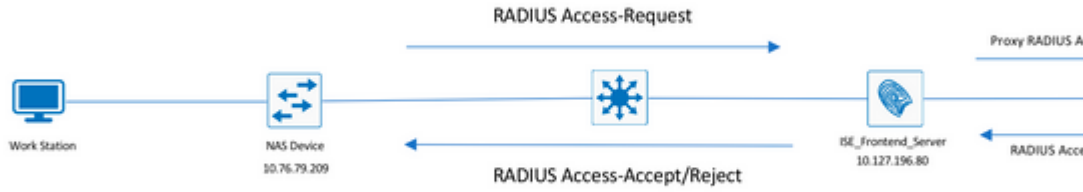
Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco ISE-Versionen 2.2 und 2.4.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

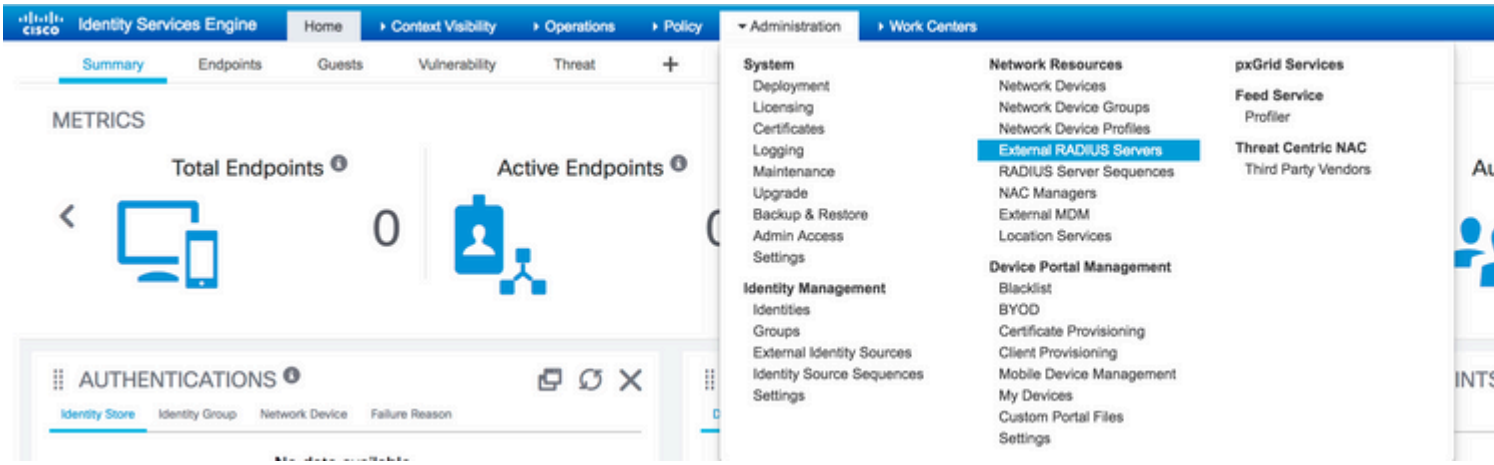
Konfigurieren

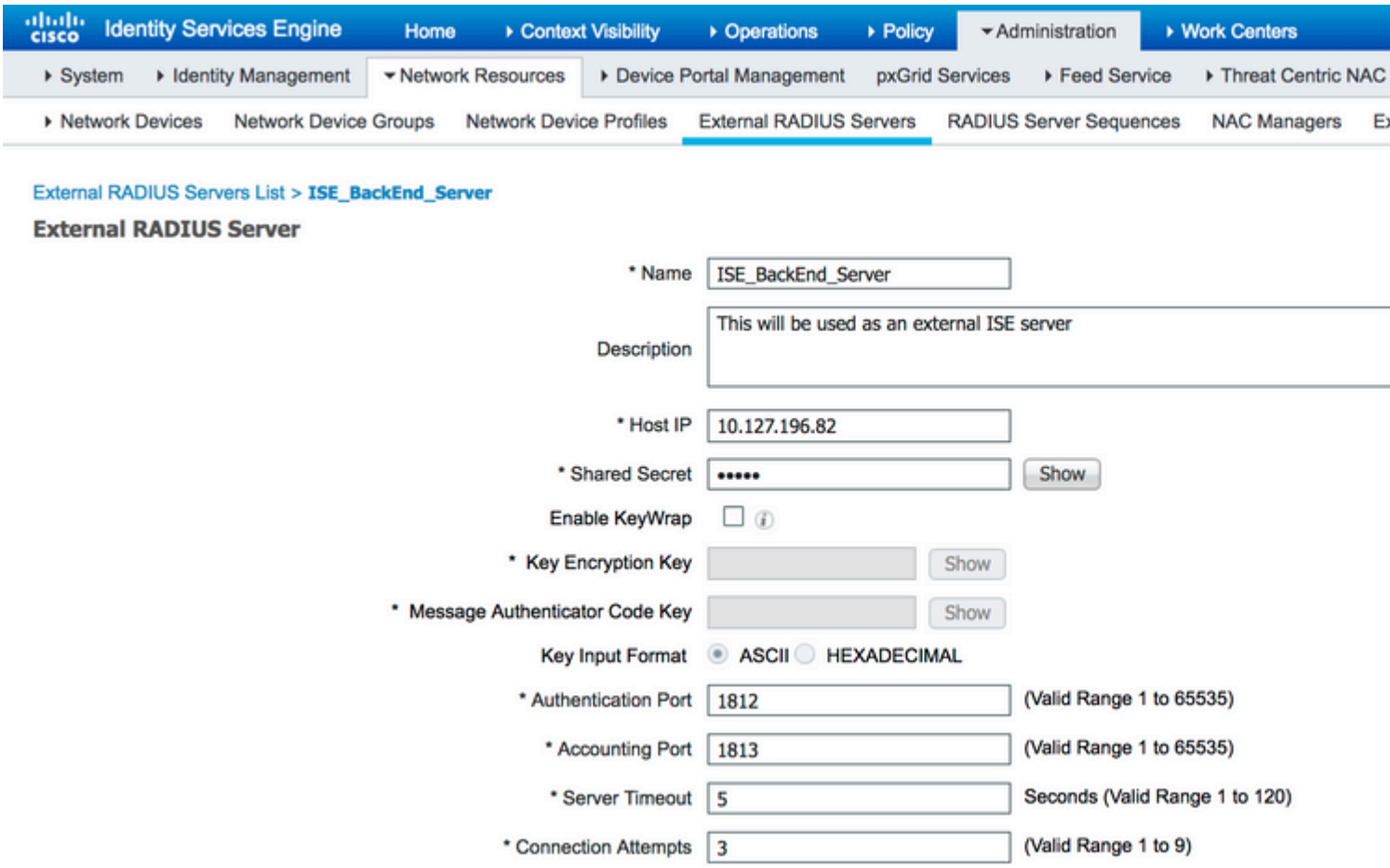
Netzwerkdiagramm



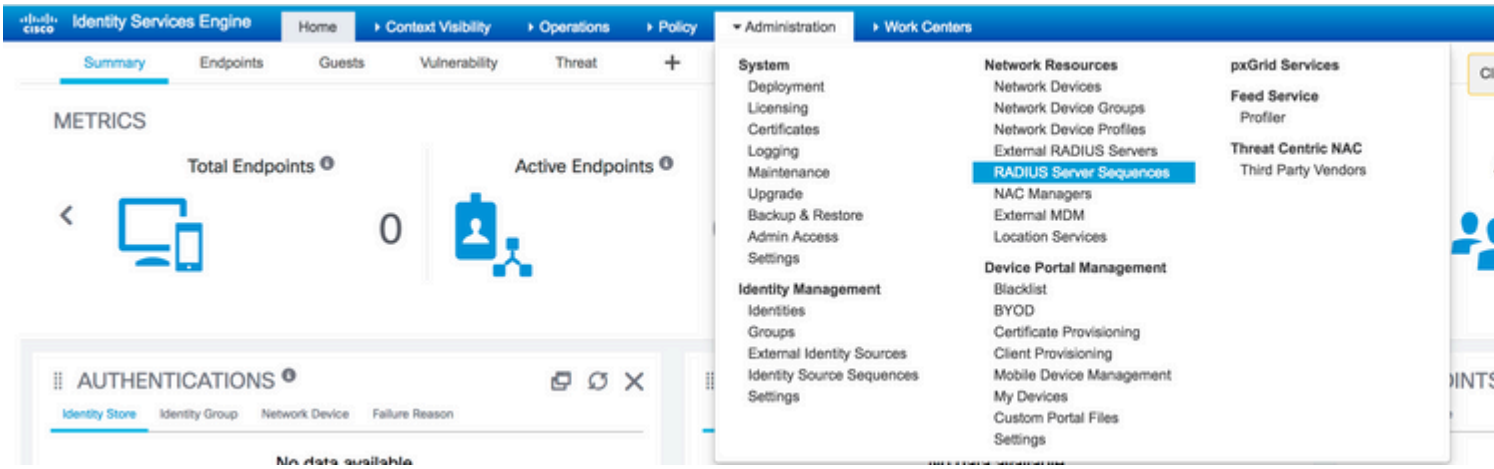
Konfigurieren der ISE (Frontend-Server)

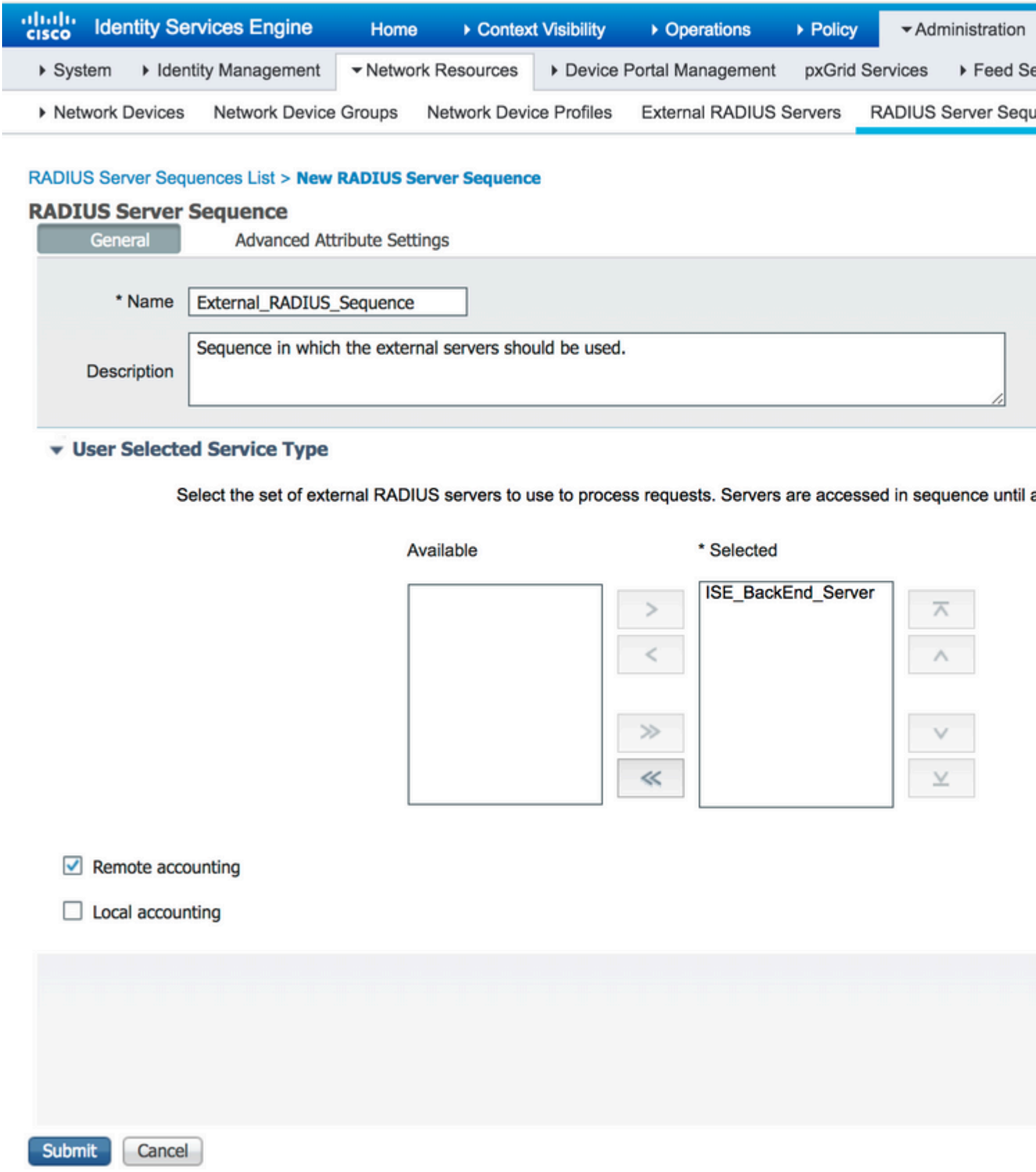
Schritt 1: Mehrere externe RADIUS-Server können konfiguriert und verwendet werden, um Benutzer auf der ISE zu authentifizieren. Um externe RADIUS-Server zu konfigurieren, navigieren Sie zu Administration > Network Resources > External RADIUS Servers > Add, wie in der Abbildung dargestellt:





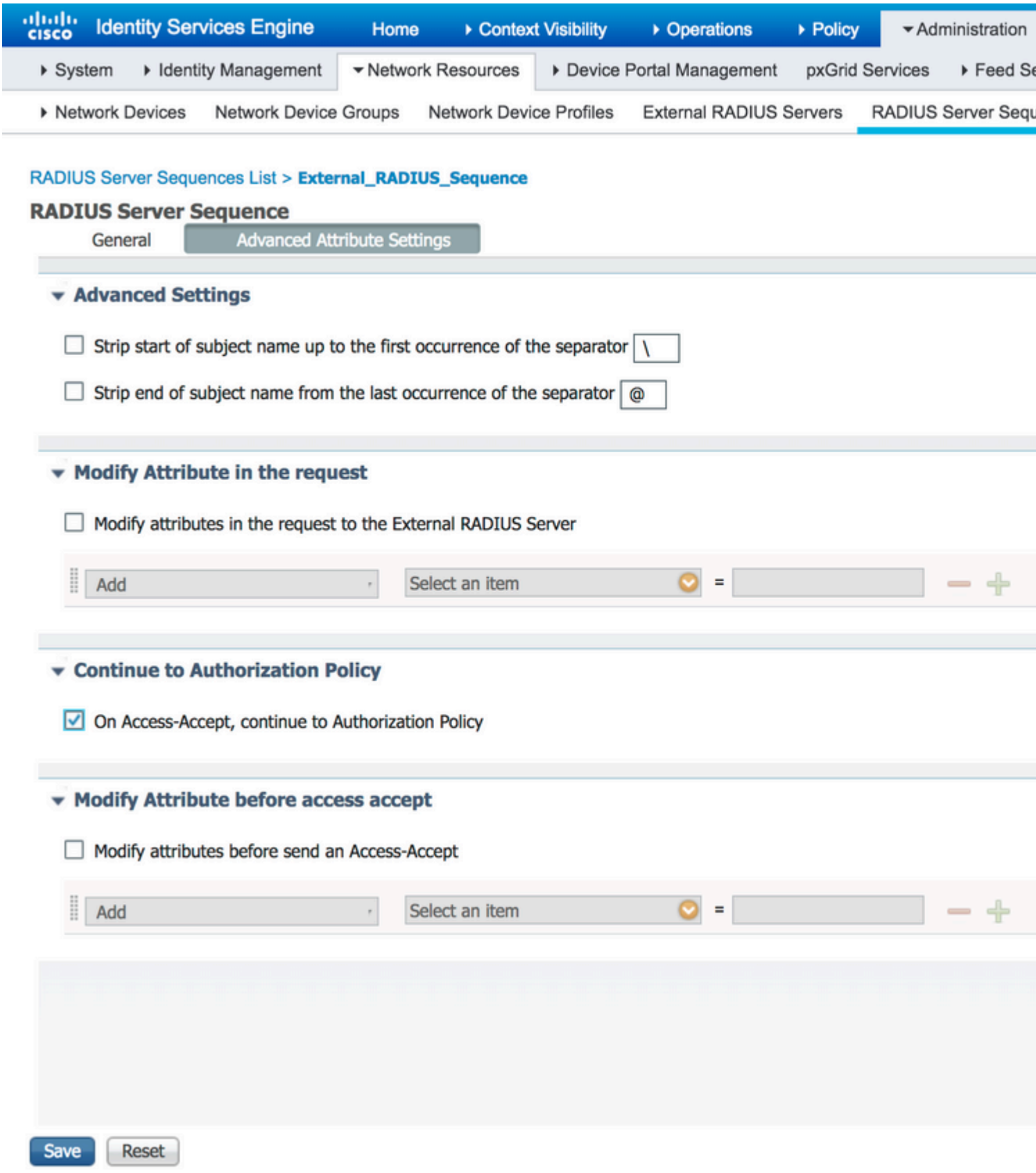
Schritt 2: Um den konfigurierten externen RADIUS-Server verwenden zu können, muss eine RADIUS-Serversequenz konfiguriert werden, die der Identity-Quellsequenz ähnelt. Um diese zu konfigurieren, navigieren Sie zu Administration > Network Resources > RADIUS Server Sequences > Add, wie im Bild dargestellt.





Hinweis: Bei der Erstellung der Serversequenz können Sie unter anderem wählen, ob die Abrechnung lokal auf der ISE oder auf dem externen RADIUS-Server erfolgen soll. Basierend auf der hier gewählten Option entscheidet die ISE, ob ein Proxy für die Buchhaltungsanforderungen verwendet oder diese Protokolle lokal gespeichert werden.

Schritt 3: In einem weiteren Abschnitt wird das Verhalten der ISE bei der Proxyweiterleitung von Anfragen an externe RADIUS-Server flexibler beschrieben. Sie finden es unter Advance Attribute Settings, wie im Bild dargestellt.



- Erweiterte Einstellungen: Bietet Optionen zum Entfernen des Anfangs oder Endes des Benutzernamens in RADIUS-Anforderungen mit einem Trennzeichen.

- Modify Attribute in the request: Stellt die Option bereit, ein beliebiges RADIUS-Attribut in den RADIUS-Anforderungen zu ändern. Die Liste hier zeigt die Attribute, die hinzugefügt/entfernt/aktualisiert werden können:

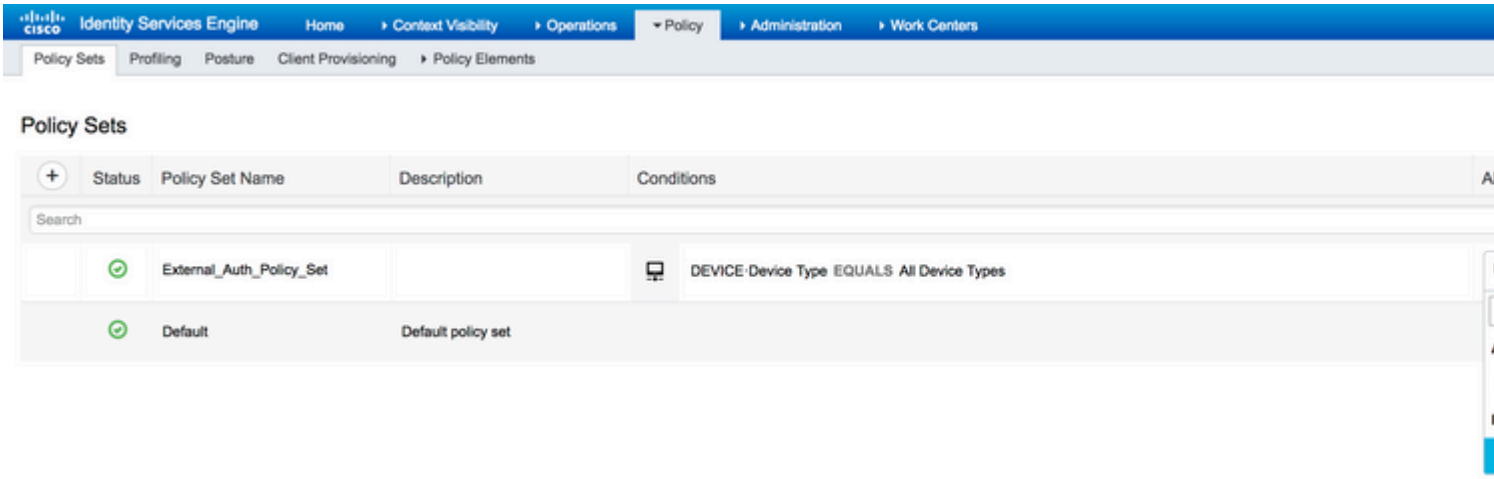
```
User-Name--[1]
NAS-IP-Address--[4]
NAS-Port--[5]
Service-Type--[6]
Framed-Protocol--[7]
Framed-IP-Address--[8]
Framed-IP-Netmask--[9]
Filter-ID--[11]
Framed-Compression--[13]
Login-IP-Host--[14]
Callback-Number--[19]
State--[24]
VendorSpecific--[26]
Called-Station-ID--[30]
Calling-Station-ID--[31]
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]
```

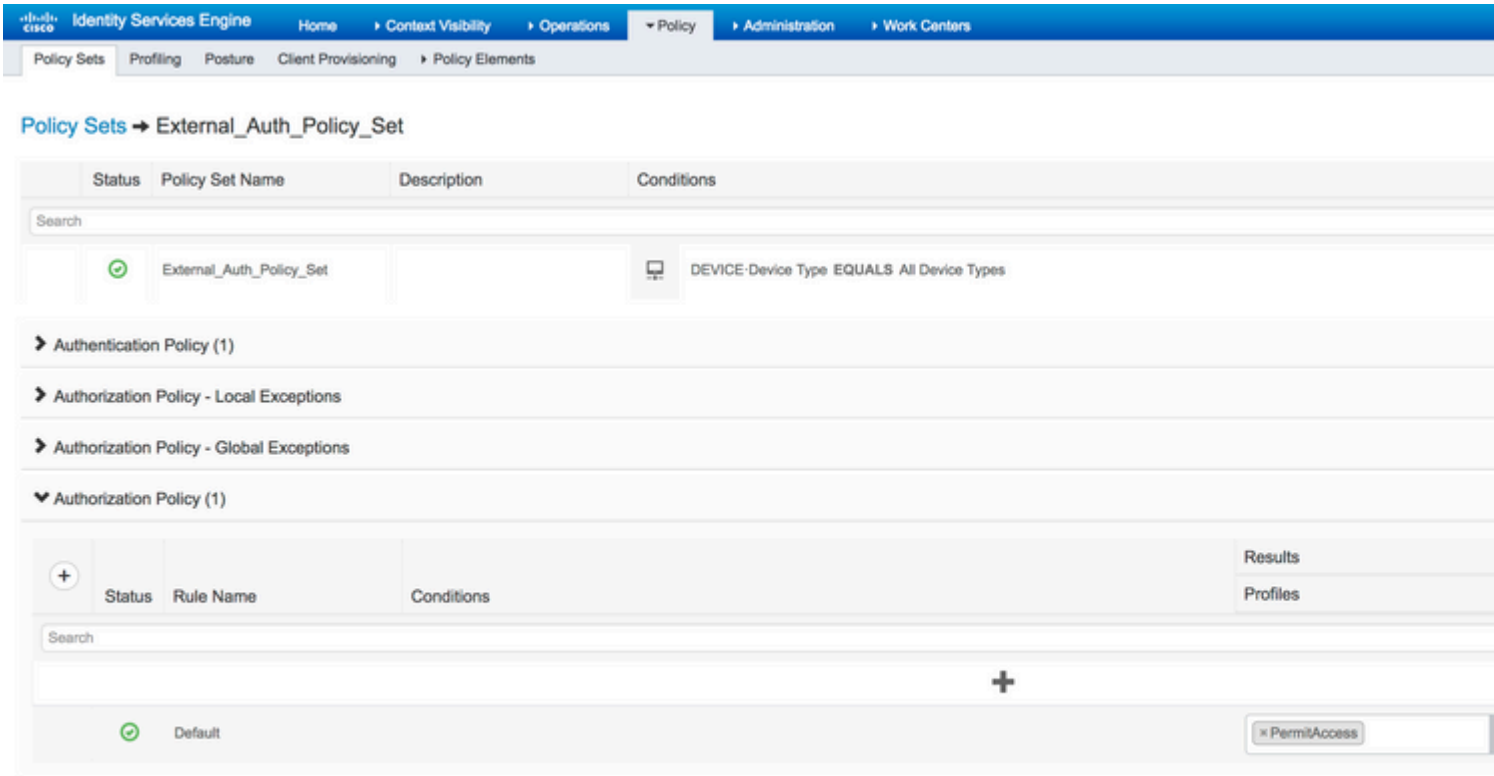
- Continue to Authorization Policy on Access-Accept (Weiter zur Autorisierungsrichtlinie bei Access-Accept): Stellt eine Option bereit, mit der festgelegt werden kann, ob die ISE den Access-Accept so senden muss, wie er ist, oder ob sie den Zugriff basierend auf den auf der ISE konfigurierten Autorisierungsrichtlinien und nicht auf der vom externen RADIUS-Server bereitgestellten Autorisierung bereitstellen muss. Wenn diese Option aktiviert ist, wird die vom externen RADIUS-Server bereitgestellte Autorisierung mit der von der ISE bereitgestellten Autorisierung überschrieben.

> **Hinweis**: Diese Option funktioniert nur, wenn der externe RADIUS-Server eine Access-Accept als Antwort auf die RADIUS-Proxyzugriffsanforderung.

- Attribut vor Access-Accept ändern: Ähnlich wie bei Modify Attribute in the requestkönnen die zuvor genannten Attribute hinzugefügt, entfernt oder aktualisiert werden, die im Access-Accept enthalten sind, das vom externen RADIUS-Server gesendet wird, bevor es an das Netzwerkgerät gesendet wird.

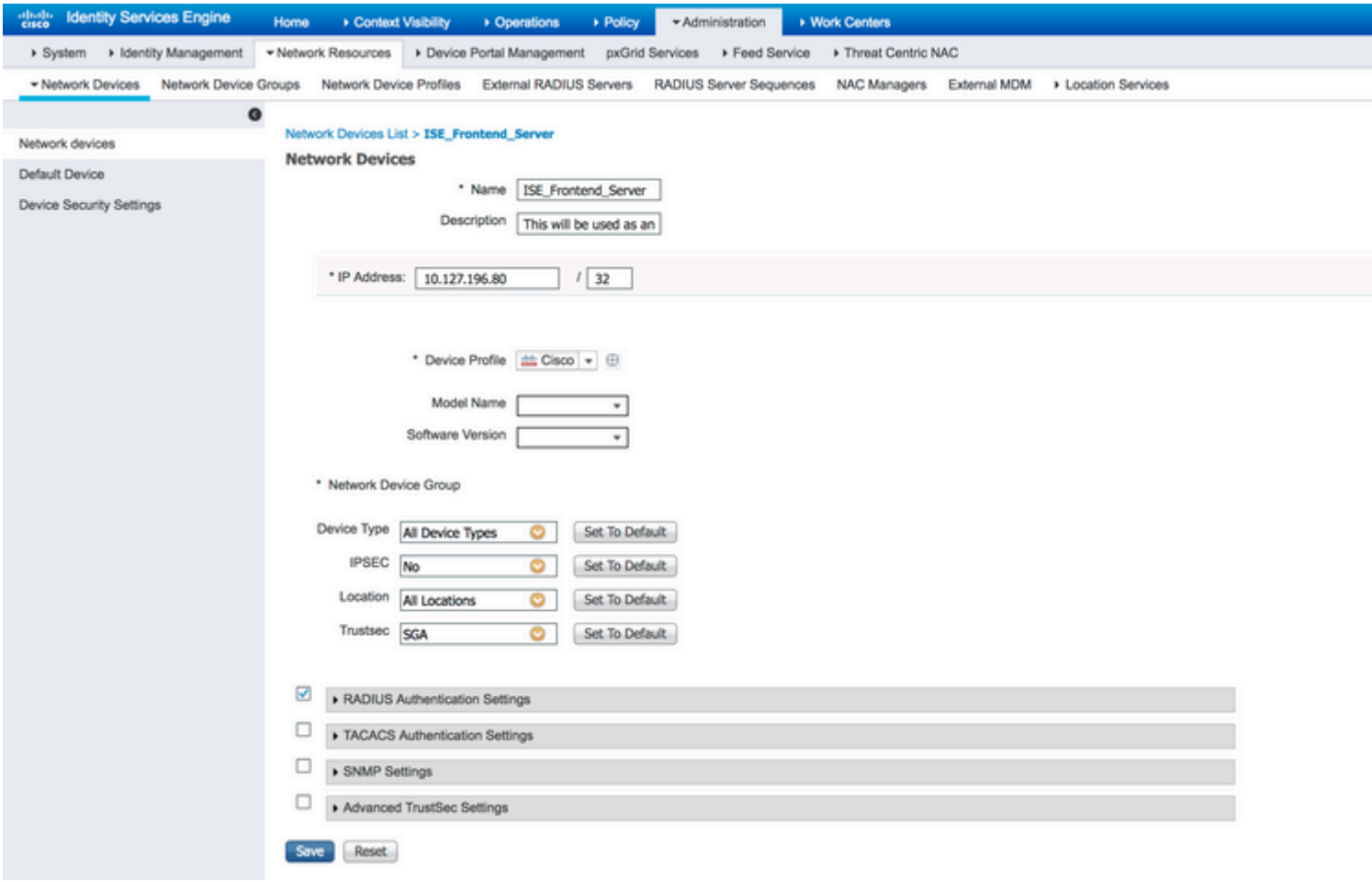
Schritt 4: Im nächsten Schritt werden die Richtliniensätze so konfiguriert, dass die RADIUS-Serversequenz anstelle der zulässigen Protokolle verwendet wird, sodass die Anforderungen an den externen RADIUS-Server gesendet werden. Sie kann konfiguriert werden unter Policy > Policy Sets. Autorisierungsrichtlinien können konfiguriert werden unter Policy Set aber nur dann in Kraft treten, wenn Continue to Authorization Policy on Access-Accept ausgewählt. Wenn nicht, fungiert die ISE lediglich als Proxy für die RADIUS-Anfragen, um die für diesen Richtliniensatz konfigurierten Bedingungen zu erfüllen.



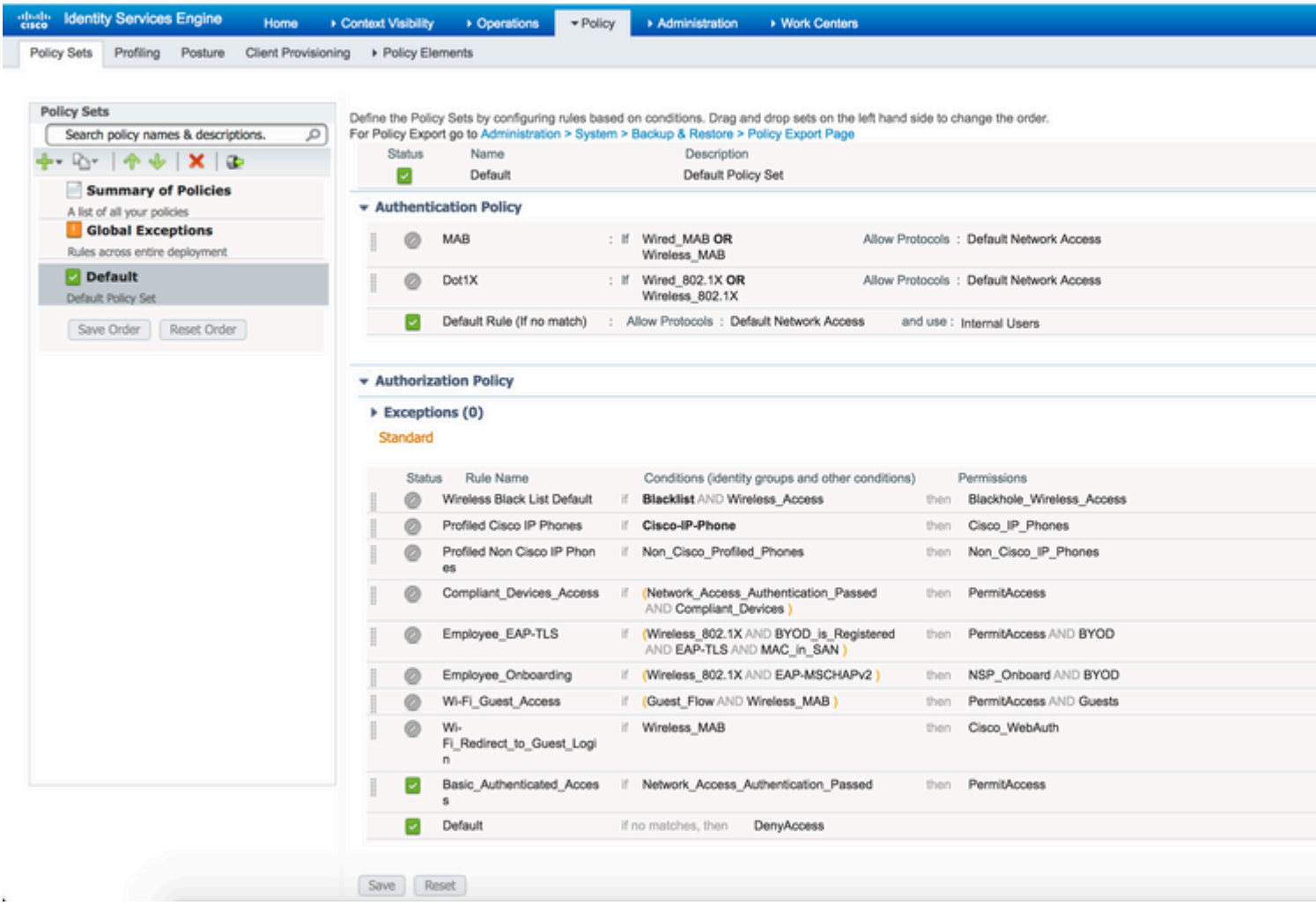


Konfigurieren des externen RADIUS-Servers

Schritt 1: In diesem Beispiel wird ein anderer ISE-Server (Version 2.2) als externer RADIUS-Server mit dem Namen ISE_Backend_Server. Die ISE (ISE_Frontend_Server) muss als Netzwerkgerät konfiguriert sein oder im externen RADIUS-Server üblicherweise als NAS bezeichnet werden (ISE_Backend_Server in diesem Beispiel), da die NAS-IP-Address -Attribut in der an den externen RADIUS-Server weitergeleiteten Access-Request wird durch die IP-Adresse desISE_Frontend_Server. Der zu konfigurierende gemeinsame geheime Schlüssel ist derselbe wie der, der für den externen RADIUS-Server auf dem ISE_Frontend_Server.



Schritt 2: Der externe RADIUS-Server kann mit eigenen Authentifizierungs- und Autorisierungsrichtlinien konfiguriert werden, um die von der ISE übermittelten Anfragen zu bedienen. In diesem Beispiel wird eine einfache Richtlinie konfiguriert, um den Benutzer in den internen Benutzern zu überprüfen und dann den Zugriff zuzulassen, wenn er authentifiziert ist.



Überprüfung

Schritt 1: Überprüfen Sie die ISE-Live-Protokolle, wenn die Anforderung empfangen wird, wie im Image gezeigt.

Schritt 2: Überprüfen Sie, ob der richtige Richtliniensatz ausgewählt ist, wie im Bild gezeigt.

Overview

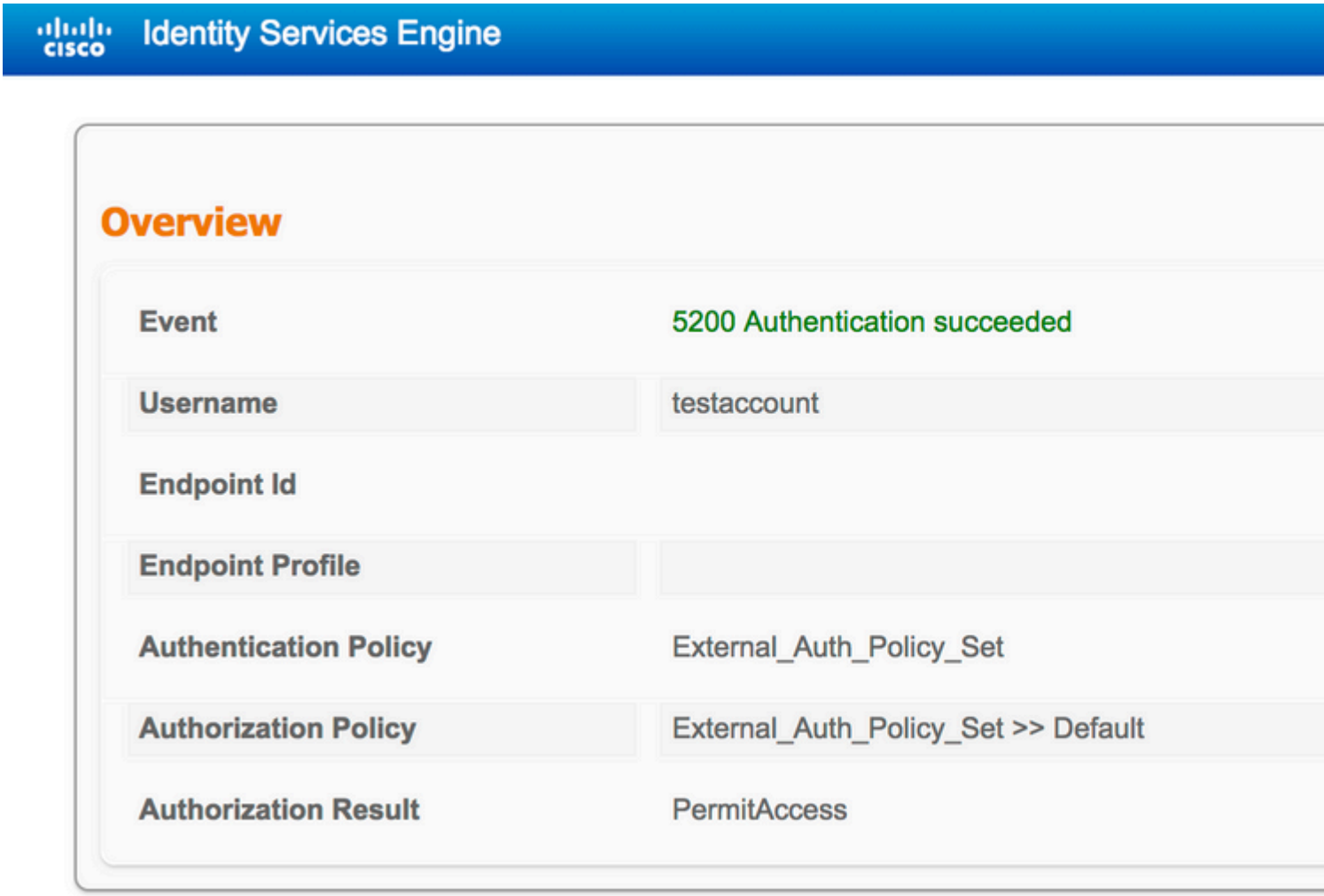
Event	5200 Authentication succeeded
Username	testaccount
Endpoint Id	
Endpoint Profile	
Authentication Policy	External_Auth_Policy_Set
Authorization Policy	External_Auth_Policy_Set
Authorization Result	

Schritt 3: Überprüfen Sie, ob die Anforderung an den externen RADIUS-Server weitergeleitet wird.

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. Wenn der Continue to Authorization Policy on Access-Accept aktiviert ist, überprüfen Sie, ob die Autorisierungsrichtlinie ausgewertet wird.



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

Fehlerbehebung

Szenario 1. Ereignis - 5405 RADIUS-Anfrage abgebrochen

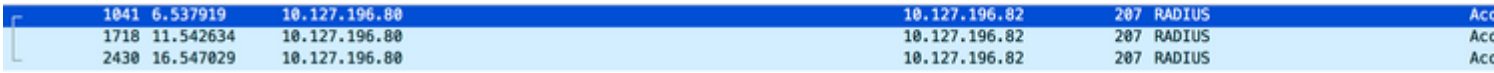
- Das Wichtigste, was überprüft werden muss, sind die Schritte im detaillierten Authentifizierungsbericht. Wenn auf den Stufen die RADIUS-Client request timeout expiredbedeutet dies, dass die ISE keine Antwort vom konfigurierten externen RADIUS-Server erhalten hat. Dies kann in folgenden Fällen geschehen:

1. Es liegt ein Verbindungsproblem mit dem externen RADIUS-Server vor. Die ISE kann den externen RADIUS-Server an den dafür konfigurierten Ports nicht erreichen.
2. Die ISE ist auf dem externen RADIUS-Server nicht als Netzwerkgerät oder NAS konfiguriert.
3. Pakete werden vom externen RADIUS-Server entweder aufgrund einer Konfiguration oder aufgrund eines Problems auf dem externen RADIUS-Server verworfen.

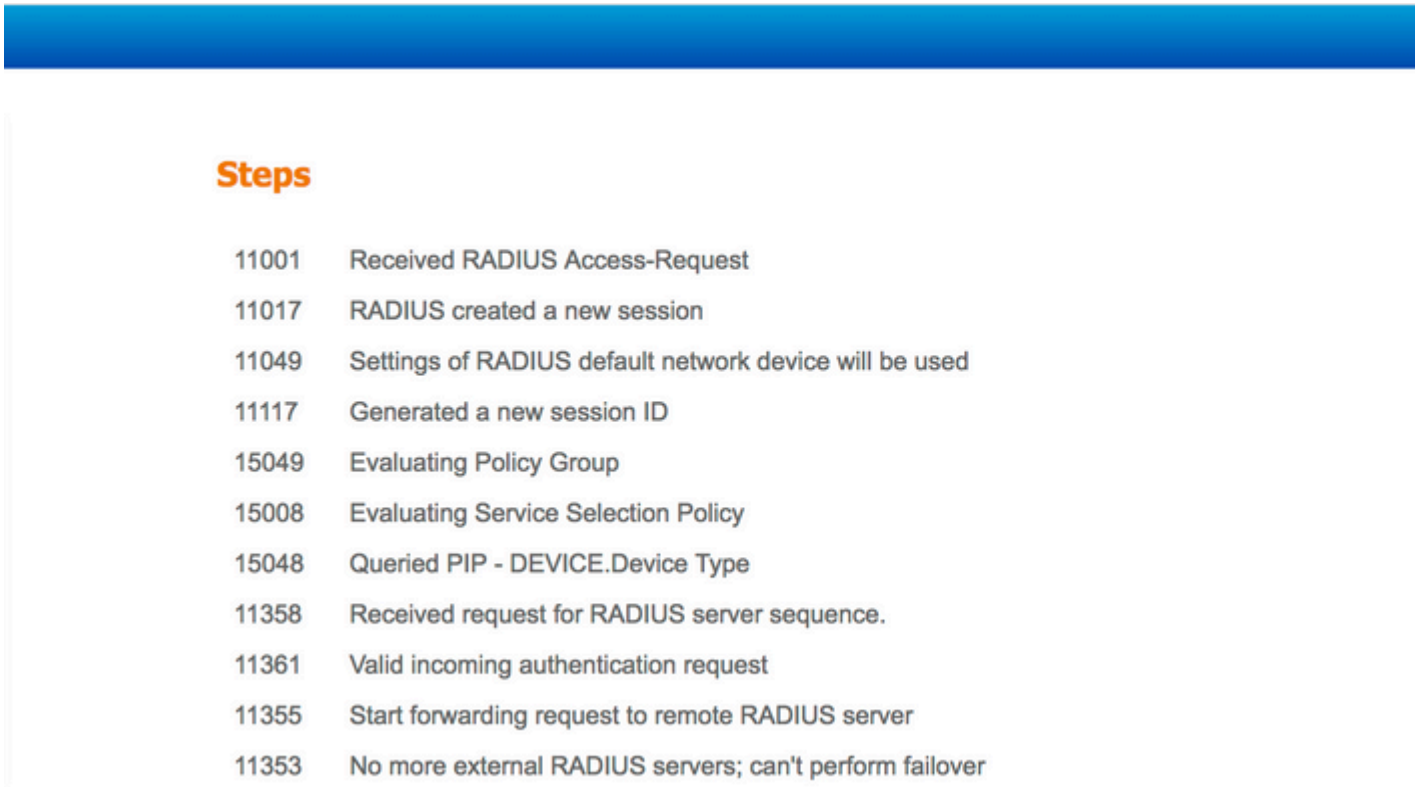
Steps

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

Überprüfen Sie auch die Paketerfassung, um festzustellen, ob es sich nicht um eine falsche Nachricht handelt, d. h., die ISE empfängt das Paket vom Server zurück, meldet jedoch, dass die Anforderung abgelaufen ist.



- Wenn die Schritte Start forwarding request to remote RADIUS server und sofort beginnt die No more external RADIUS servers; can't perform failover, bedeutet dies, dass alle konfigurierten externen RADIUS-Server derzeit als **ausgefallen** markiert sind und die Anfragen erst nach Ablauf des Zeitgebers bearbeitet werden.



Hinweis: Die standardmäßige **Ausfallzeit** für externe RADIUS-Server in der ISE beträgt **5 Minuten**. Dieser Wert ist fest codiert und kann ab dieser Version nicht mehr geändert werden.

- Wenn die Schritte RADIUS-Client encountered error during processing flow gefolgt von Failed to forward request to current remote RADIUS server; an invalid response was received,bedeutet dies, dass bei der Weiterleitung der Anforderung an den externen RADIUS-Server ein Problem mit der ISE aufgetreten ist. Dies tritt in der Regel dann auf, wenn die vom Netzwerkgerät/NAS an die ISE gesendete RADIUS-Anforderung nicht über die NAS-IP-Address als eines der Attribute. Wenn es keine NAS-IP-Address -Attribut hinzu, und wenn keine externen RADIUS-Server verwendet werden, füllt die ISE die NAS-IP-Address mit der Quell-IP-Adresse des Pakets. Dies gilt jedoch nicht, wenn ein externer RADIUS-Server verwendet wird.

Szenario 2. Ereignis - 5400 Authentifizierung fehlgeschlagen

- Wenn in diesem Fall die Schritte 11368 Please review logs on the External RADIUS Server to determine the precise failure reasonist, bedeutet dies, dass die Authentifizierung auf dem externen RADIUS-Server selbst fehlgeschlagen ist und eine Access-Reject-Nachricht gesendet wurde.

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

- Wenn die Schritte 15039 Rejected per authorization profilebedeutet dies, dass die ISE vom externen RADIUS-Server eine Access-Accept-Nachricht erhalten hat, die ISE die Autorisierung jedoch auf Grundlage der konfigurierten Autorisierungsrichtlinien ablehnt.

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

- Wenn die Failure Reason auf der ISE alle anderen als die hier genannten Fälle bei einem Authentifizierungsfehler auftreten, kann dies ein potenzielles Problem mit der Konfiguration oder mit der ISE selbst bedeuten. Es wird empfohlen, an dieser Stelle ein TAC-Ticket zu öffnen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.