Configure servidores RADIUS externos en ISE

Contenido

Introducción

Este documento describe la configuración de un servidor RADIUS en ISE como proxy y servidor de autorización. Aquí se utilizan dos servidores ISE y uno actúa como servidor externo. Sin embargo, se puede utilizar cualquier servidor RADIUS compatible con RFC.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico del protocolo RADIUS
- Experiencia en la configuración de políticas de Identity Services Engine (ISE)

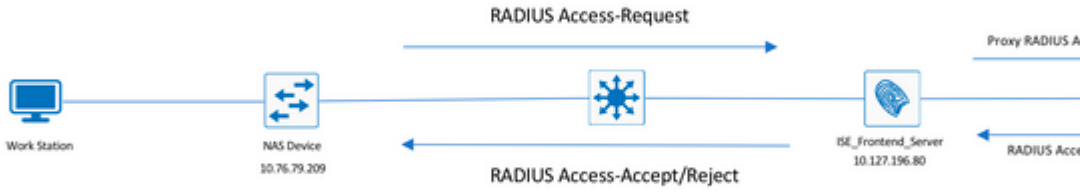
Componentes Utilizados

La información de este documento se basa en las versiones 2.2 y 2.4 de Cisco ISE.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

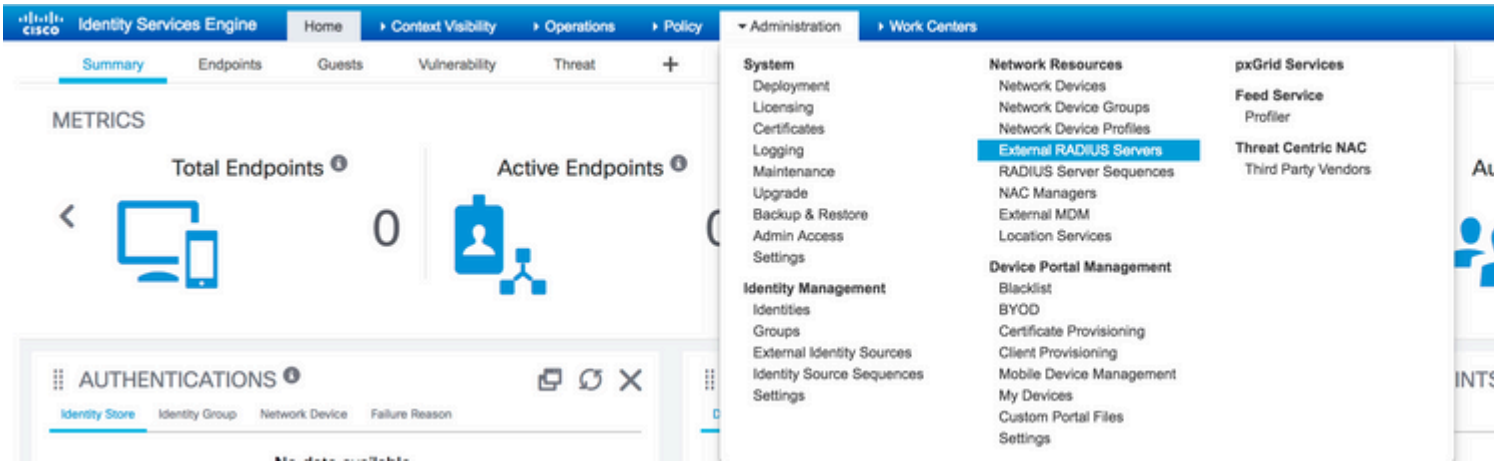
Configurar

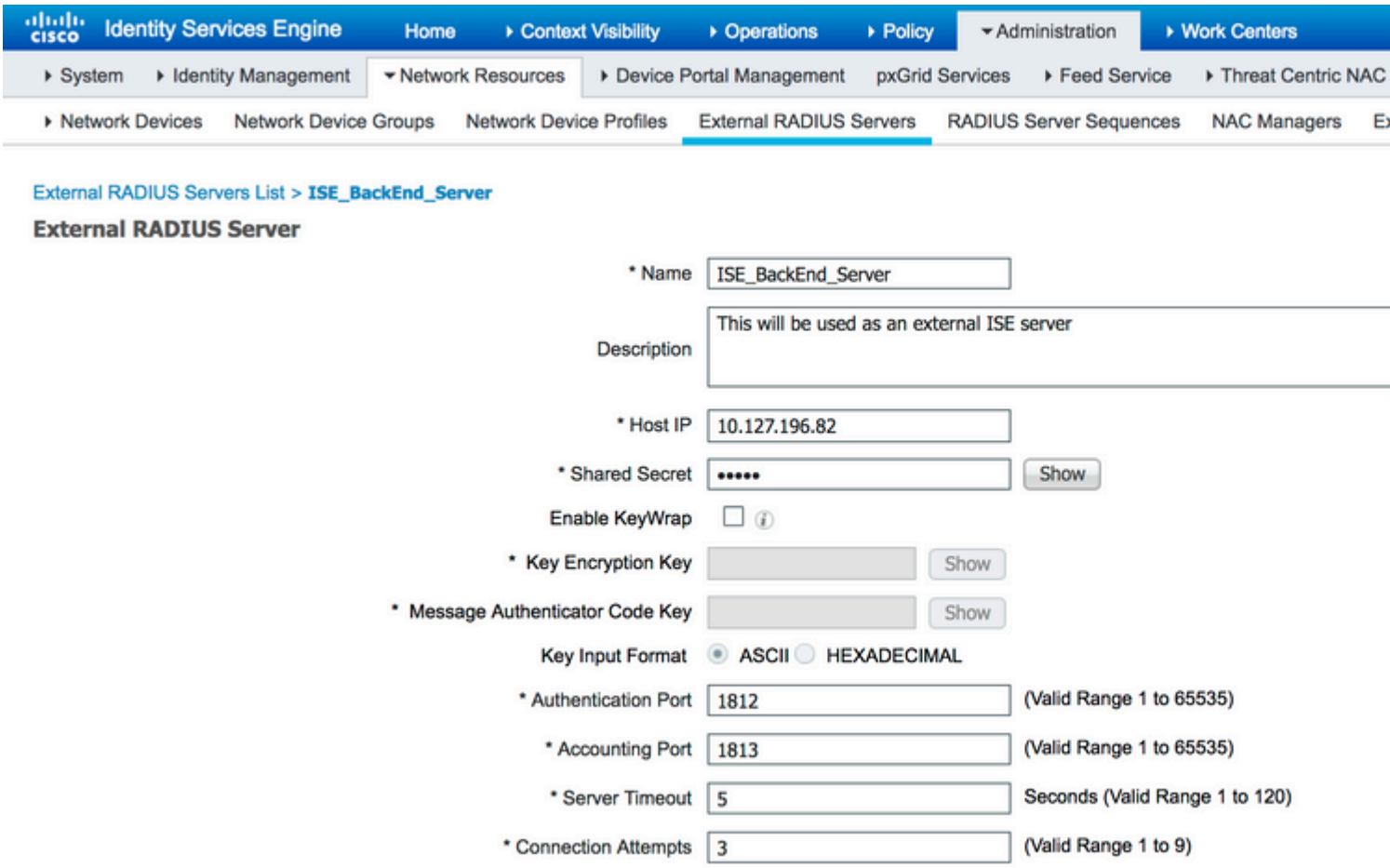
Diagrama de la red



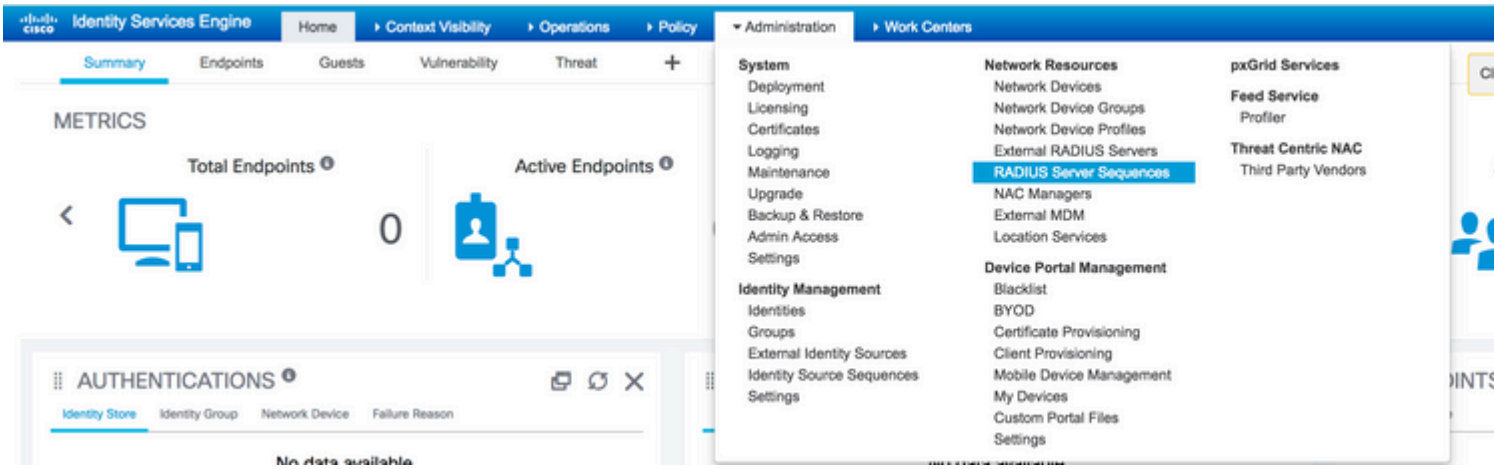
Configuración de ISE (Frontend Server)

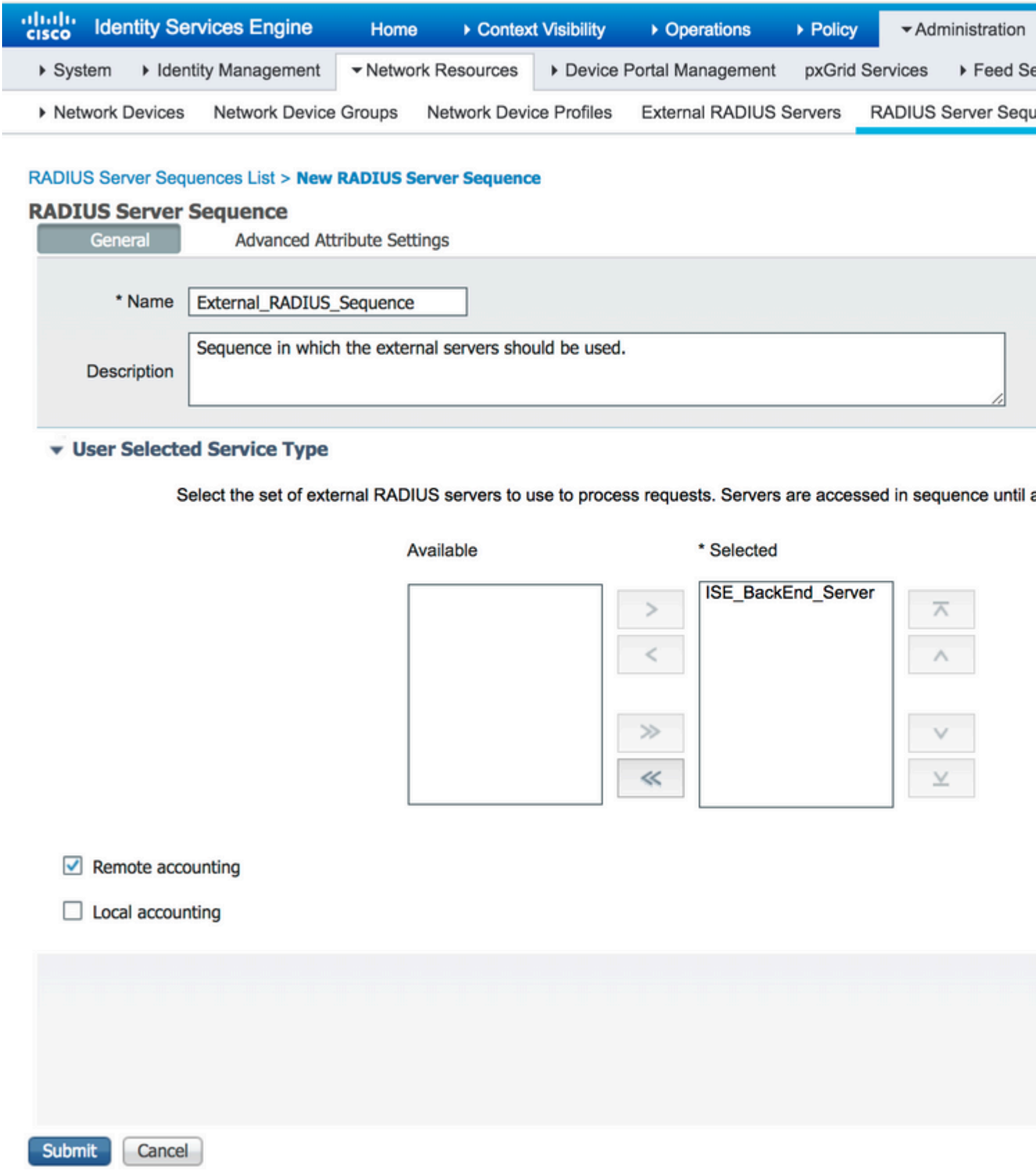
Paso 1. Se pueden configurar y utilizar varios servidores RADIUS externos para autenticar a los usuarios en ISE. Para configurar servidores RADIUS externos, navegue hasta Administration > Network Resources > External RADIUS Servers > Add, como se muestra en la imagen:





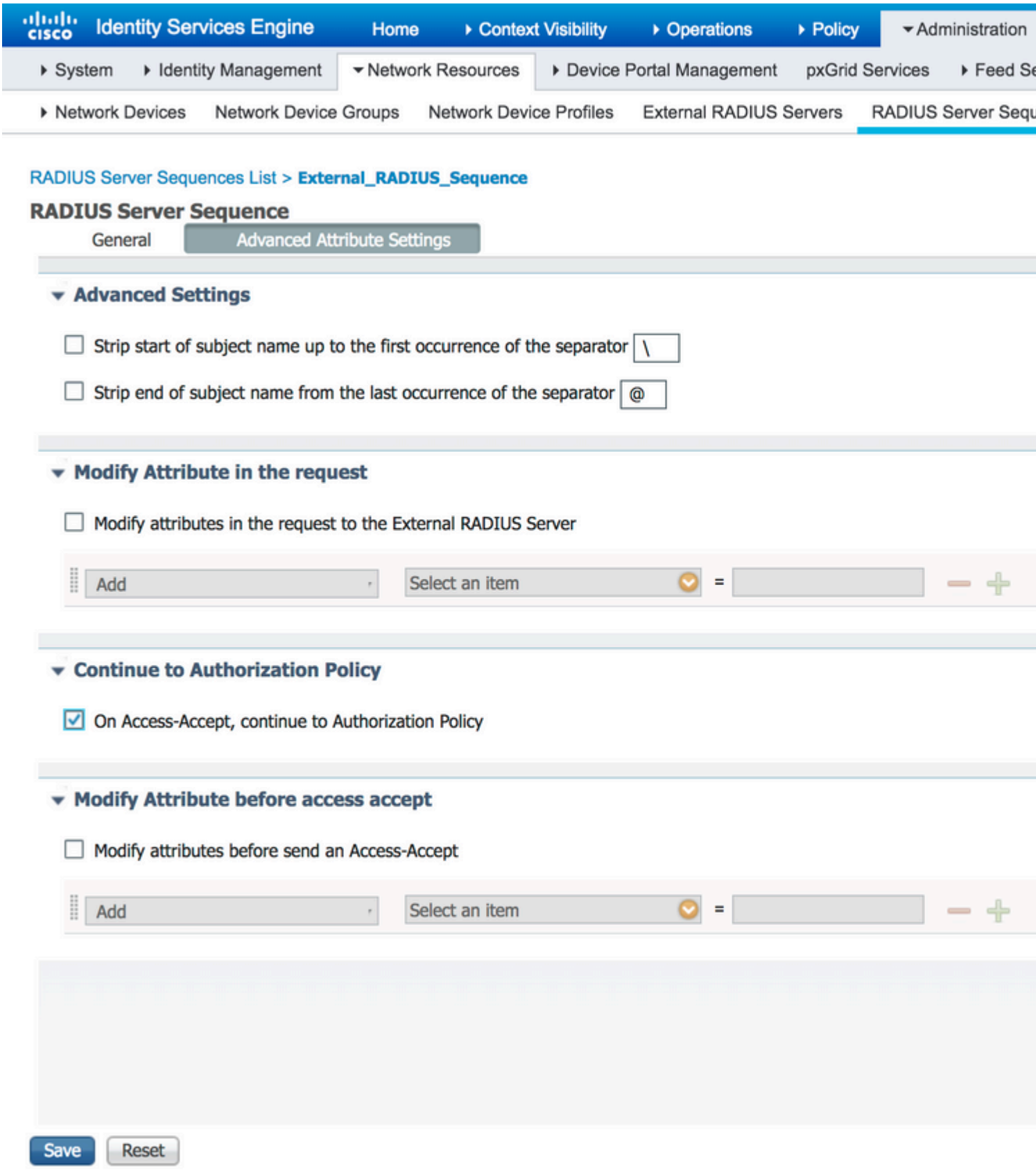
Paso 2. Para utilizar el servidor RADIUS externo configurado, se debe configurar una secuencia de servidor RADIUS similar a la secuencia de origen de identidad. Para configurar el mismo, navegue hasta Administration > Network Resources > RADIUS Server Sequences > Add, como se muestra en la imagen.





Nota: una de las opciones disponibles mientras se crea la secuencia de servidor es elegir si la contabilización debe realizarse localmente en ISE o en el servidor RADIUS externo. En función de la opción elegida aquí, ISE decide si realiza proxy de las solicitudes de contabilidad o si almacena esos registros localmente.

Paso 3. Hay una sección adicional que ofrece más flexibilidad sobre cómo debe comportarse ISE cuando hace proxy de las solicitudes a servidores RADIUS externos. Se puede encontrar en Advance Attribute Settings, como se muestra en la imagen.



- Configuración avanzada: proporciona opciones para eliminar el inicio o el final del nombre de usuario en solicitudes RADIUS con un delimitador.

- Modificar atributo en la solicitud: proporciona la opción de modificar cualquier atributo RADIUS en las solicitudes RADIUS. La lista muestra los atributos que se pueden agregar/eliminar/actualizar:

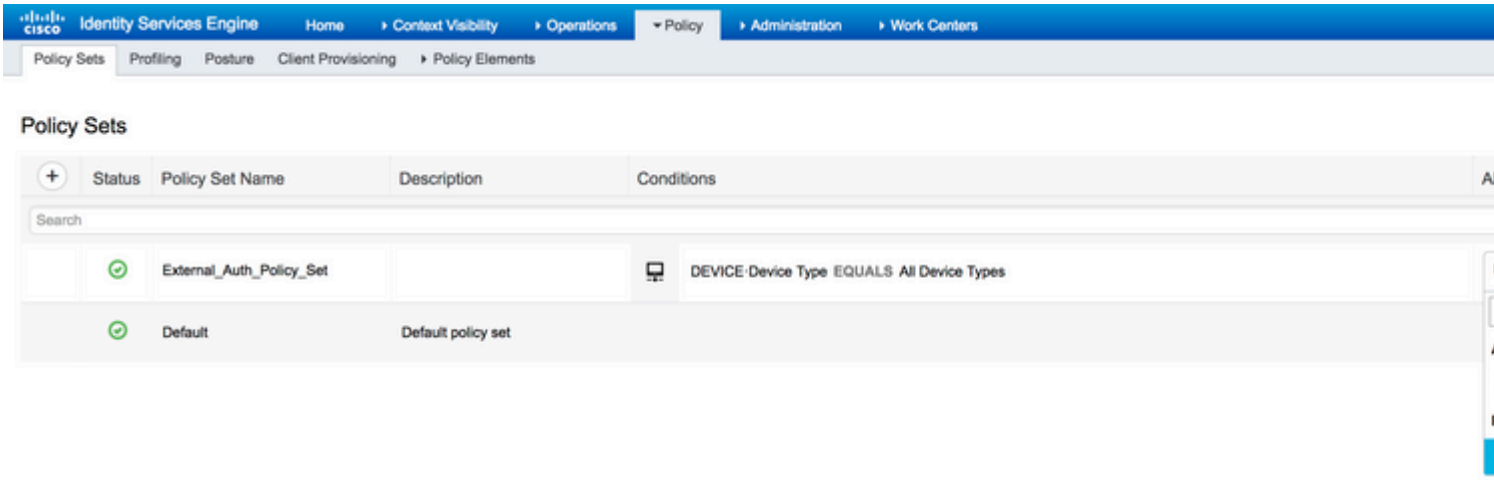
```
User-Name--[1]
NAS-IP-Address--[4]
NAS-Port--[5]
Service-Type--[6]
Framed-Protocol--[7]
Framed-IP-Address--[8]
Framed-IP-Netmask--[9]
Filter-ID--[11]
Framed-Compression--[13]
Login-IP-Host--[14]
Callback-Number--[19]
State--[24]
VendorSpecific--[26]
Called-Station-ID--[30]
Calling-Station-ID--[31]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

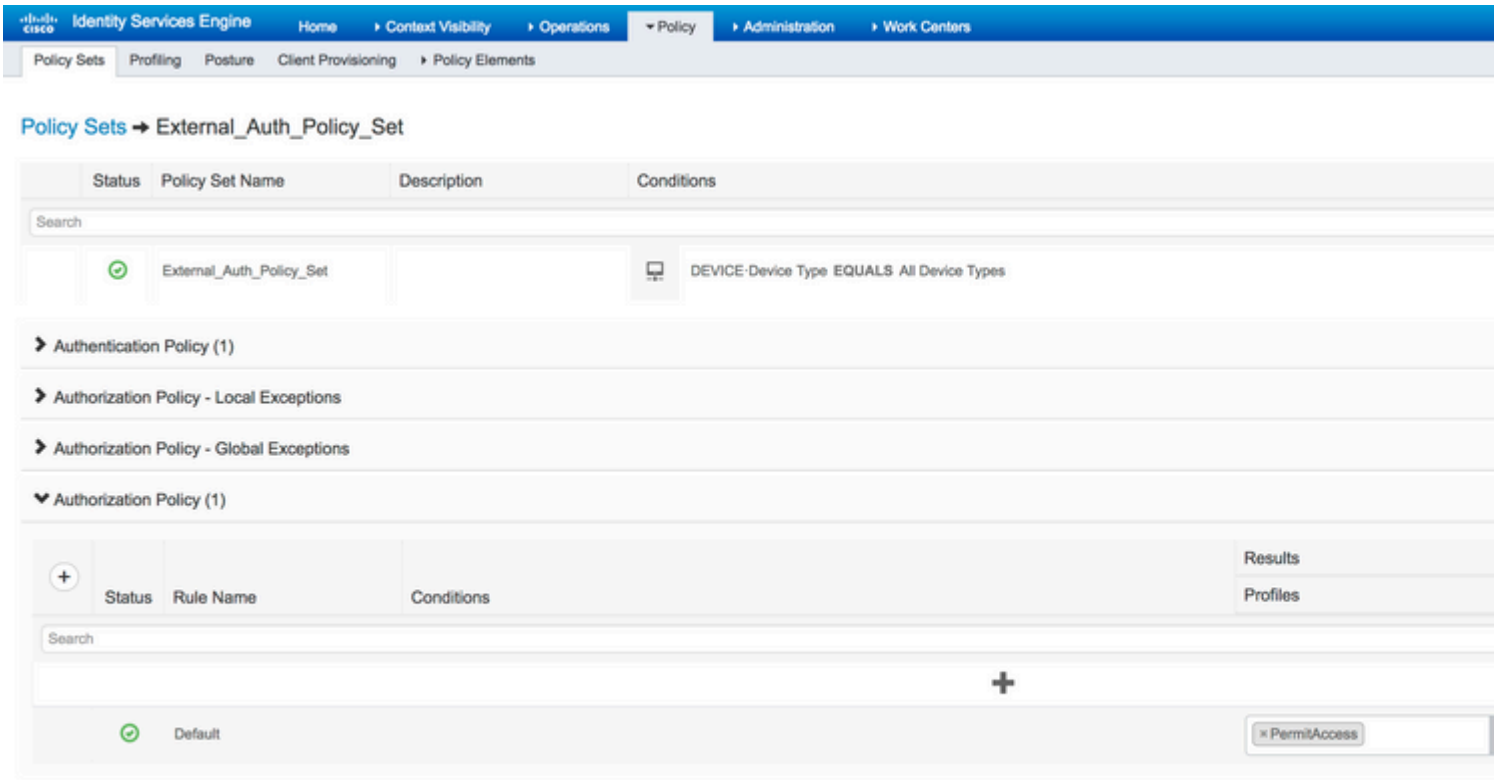
- Continuar con la política de autorización en la aceptación de acceso: proporciona una opción para elegir si ISE debe enviar la aceptación de acceso tal como está o continuar proporcionando acceso basándose en las políticas de autorización configuradas en ISE en lugar de la autorización proporcionada por el servidor RADIUS externo. Si se selecciona esta opción, la autorización proporcionada por el servidor RADIUS externo se sobrescribe con la autorización proporcionada por ISE.

> **Nota**: Esta opción sólo funciona si el servidor RADIUS externo envía un Access-Accept en respuesta a la solicitud de acceso RADIUS con proxy.

- Modificar atributo antes de aceptar acceso: similar a la Modify Attribute in the request, los atributos mencionados anteriormente se pueden agregar/eliminar/actualizar presentes en la aceptación de acceso enviada por el servidor RADIUS externo antes de que se envíe al dispositivo de red.

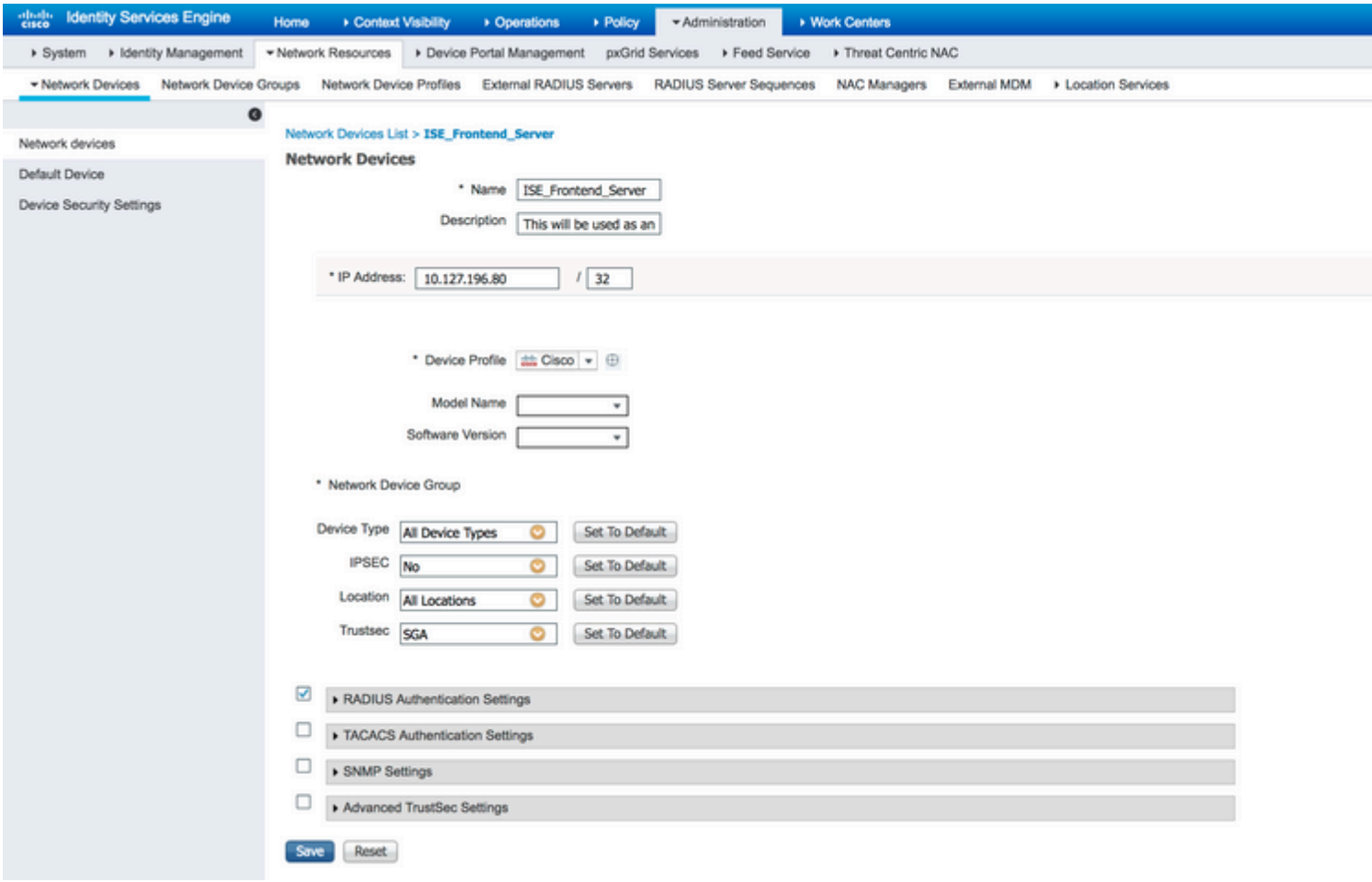
Paso 4. La siguiente parte es configurar los conjuntos de directivas para utilizar la secuencia del servidor RADIUS en lugar de los protocolos permitidos para que las solicitudes se envíen al servidor RADIUS externo. Se puede configurar en Policy > Policy Sets. Las directivas de autorización se pueden configurar en el Policy Set pero solo entran en vigor si la Continue to Authorization Policy on Access-Accept opción seleccionada. Si no es así, ISE simplemente actúa como proxy para las solicitudes RADIUS con el fin de cumplir las condiciones configuradas para este conjunto de políticas.



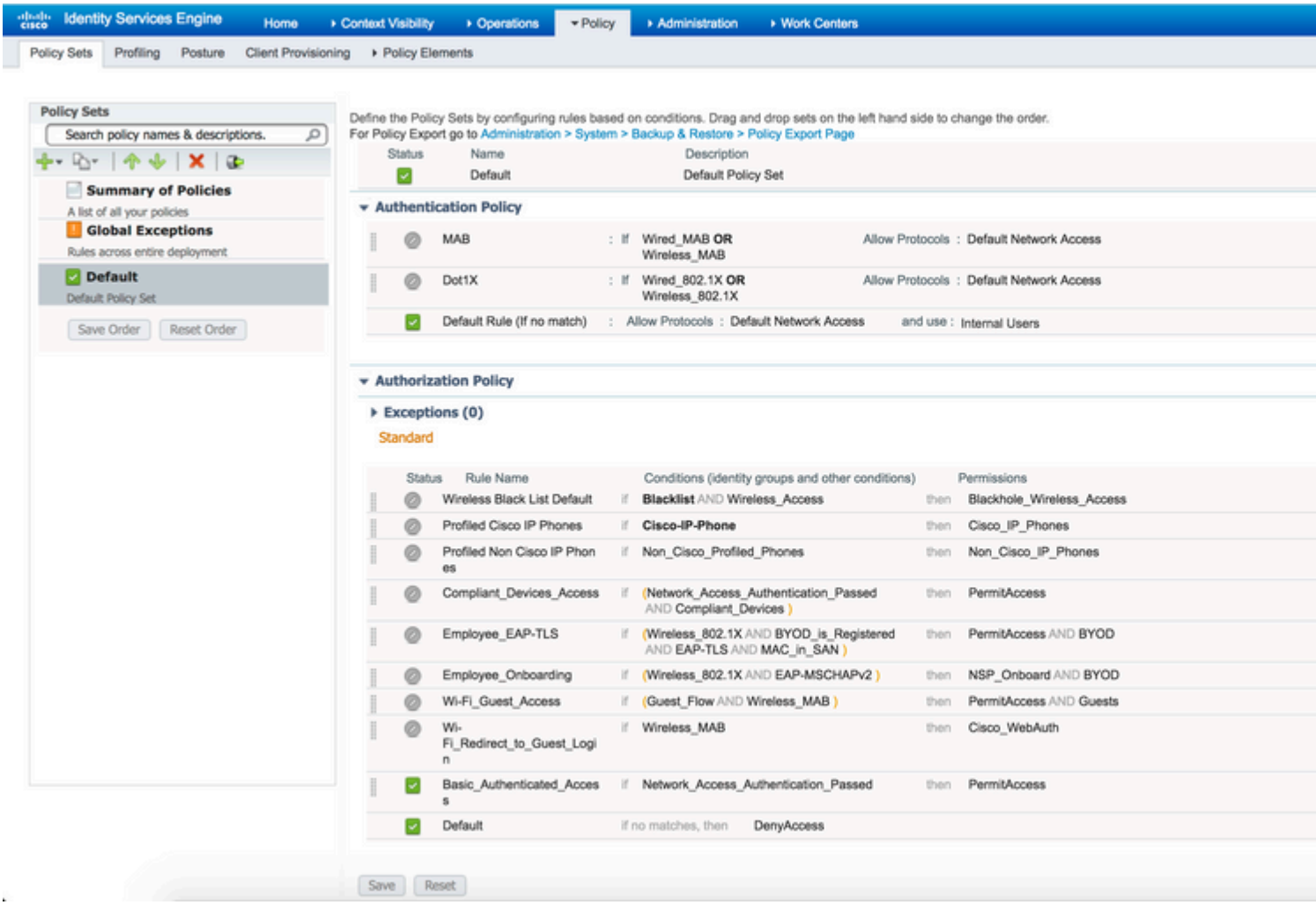


Configuración del servidor RADIUS externo

Paso 1. En este ejemplo, se utiliza otro servidor ISE (versión 2.2) como servidor RADIUS externo denominado ISE_Backend_Server. El ISE (ISE_Frontend_Server) debe configurarse como un dispositivo de red o llamado tradicionalmente NAS en el servidor RADIUS externo (ISE_Backend_Server en este ejemplo), ya que el NAS-IP-Address en Access-Request que se reenvía al servidor RADIUS externo se reemplaza con la dirección IP delISE_Frontend_Server. El secreto compartido que se va a configurar es el mismo que el configurado para el servidor RADIUS externo en el ISE_Frontend_Server.



Paso 2. El servidor RADIUS externo se puede configurar con sus propias políticas de autenticación y autorización para atender las solicitudes procesadas como proxy por ISE. En este ejemplo, se configura una política simple para verificar el usuario en los usuarios internos y luego permitir el acceso si se autentica.



Verificación

Paso 1. Compruebe los registros en directo de ISE si se recibe la solicitud, como se muestra en la imagen.

Paso 2. Compruebe si está seleccionado el conjunto de directivas correcto, como se muestra en la imagen.

Overview

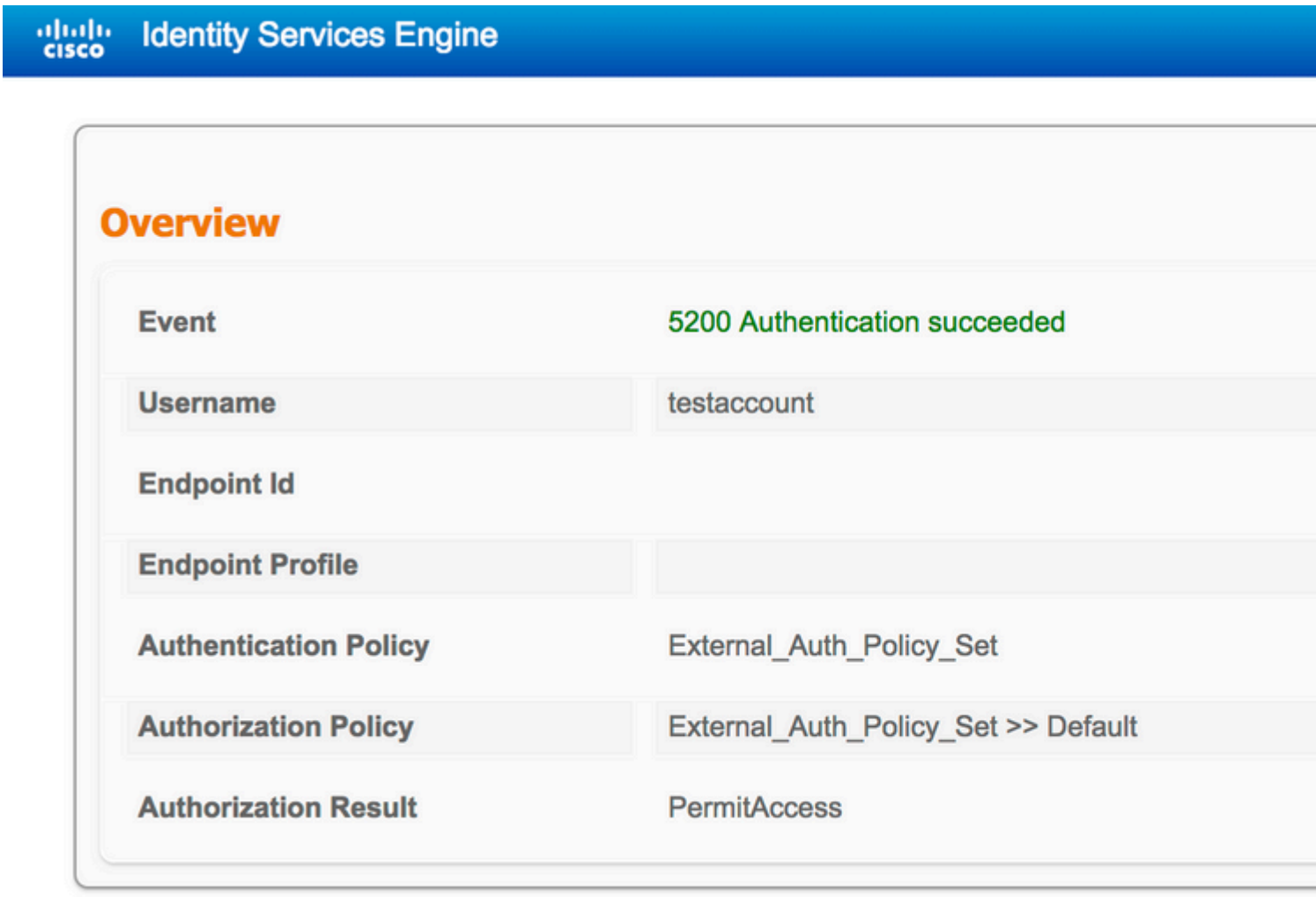
Event	5200 Authentication succeeded
Username	testaccount
Endpoint Id	
Endpoint Profile	
Authentication Policy	External_Auth_Policy_Set
Authorization Policy	External_Auth_Policy_Set
Authorization Result	

Paso 3. Compruebe si la solicitud se reenvía al servidor RADIUS externo.

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. Si el Continue to Authorization Policy on Access-Accept , compruebe si se ha evaluado la directiva de autorización.



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

Troubleshoot

Escenario 1. Evento - Solicitud 5405 RADIUS rechazada

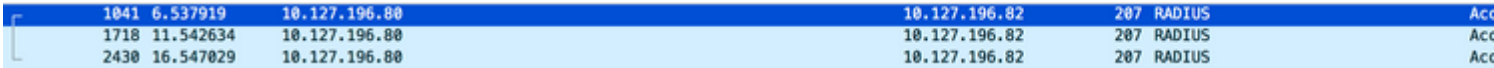
- Lo más importante que debe verificarse son los pasos del informe de autenticación detallado. Si los pasos indican RADIUS-Client request timeout expired, significa que ISE no recibió ninguna respuesta del servidor RADIUS externo configurado. Esto puede suceder cuando:

1. Hay un problema de conectividad con el servidor RADIUS externo. ISE no puede alcanzar el servidor RADIUS externo en los puertos configurados para él.
2. ISE no está configurado como dispositivo de red o NAS en el servidor RADIUS externo.
3. El servidor RADIUS externo descarta los paquetes bien por la configuración o debido a algún problema en el servidor RADIUS externo.

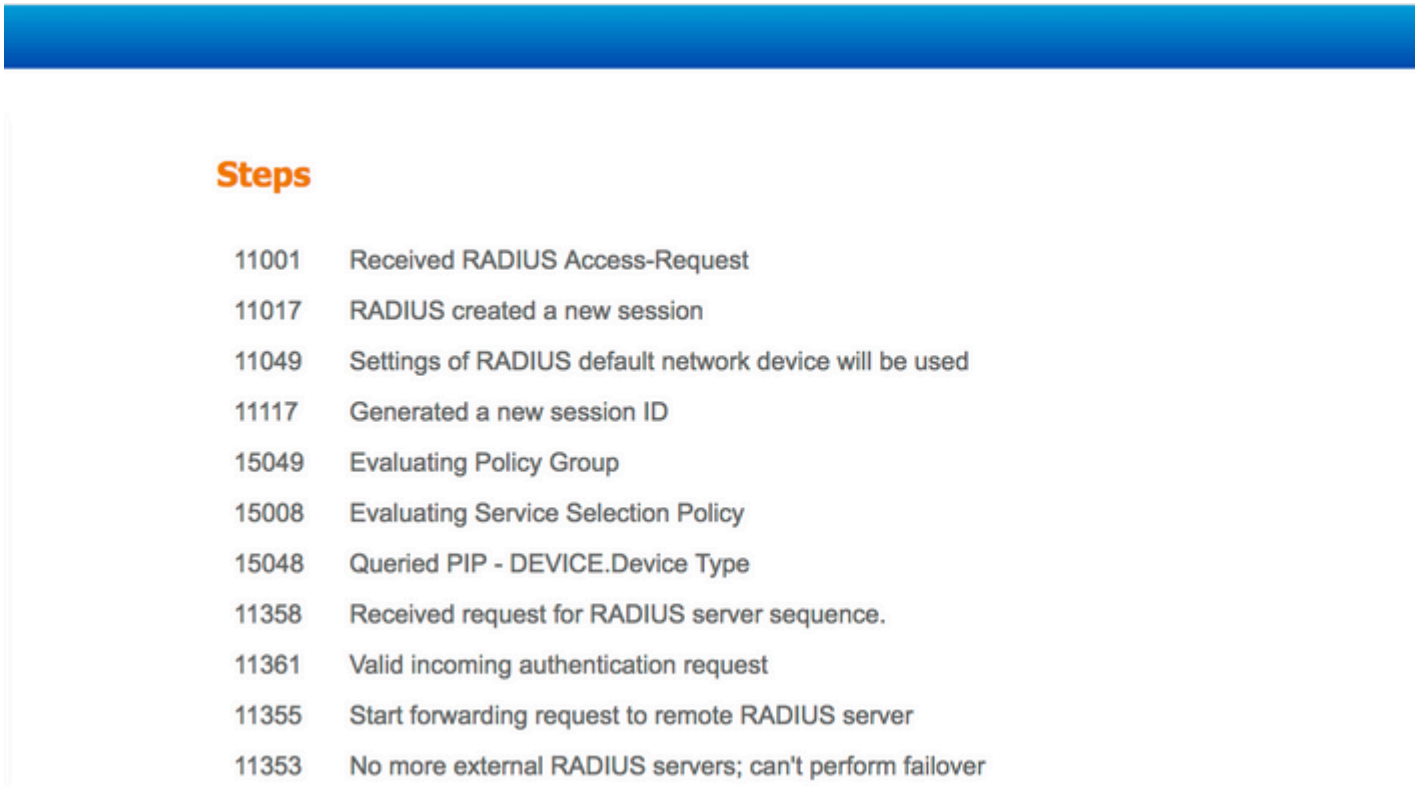
Steps

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

Verifique también las capturas de paquetes para ver si no se trata de un mensaje falso, es decir, ISE recibe el paquete de vuelta del servidor pero aún informa que la solicitud ha agotado el tiempo de espera.



- Si los pasos indican Start forwarding request to remote RADIUS server y el paso inmediato es No more external RADIUS servers; can't perform failover, entonces significa que todos los servidores RADIUS externos configurados están marcados actualmente como **dead** y que las solicitudes se atienden solamente después de que caduque el temporizador de inactividad.



Nota: el **tiempo muerto** predeterminado para los servidores RADIUS externos en ISE es de **5 minutos**. Este valor está codificado y no se puede modificar en esta versión.

- Si los pasos indican RADIUS-Client encountered error during processing flow y van seguidas de Failed to forward request to current remote RADIUS server; an invalid response was received,esto significa que ISE ha encontrado un problema mientras se reenviaba la solicitud al servidor RADIUS externo. Esto suele ocurrir cuando la solicitud RADIUS enviada desde el dispositivo de red/NAS al ISE no tiene el NAS-IP-Address como uno de los atributos. Si no hay NAS-IP-Address y, si los servidores RADIUS externos no están en uso, ISE rellena el NAS-IP-Address con la IP de origen del paquete. Sin embargo, esto no se aplica cuando un servidor RADIUS externo está en uso.

Situación hipotética 2. Evento - Error de autenticación 5400

- En este caso, si los pasos indican 11368 Please review logs on the External RADIUS Server to determine the precise failure reason, significa que la autenticación ha fallado en el servidor RADIUS externo y ha enviado un Access-Reject.

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

- Si los pasos indican 15039 Rejected per authorization profile, significa que ISE recibió una aceptación de acceso del servidor RADIUS externo, pero ISE rechaza la autorización en función de las políticas de autorización configuradas.

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

- Si Failure Reason en el ISE es cualquier otra cosa aparte de las mencionadas aquí en caso de una falla de autenticación, entonces puede significar un problema potencial con la configuración o con el ISE en sí. Se recomienda abrir un caso TAC en este momento.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).