在 ISE 上配置外部 RADIUS 服务器

目录

简介

本文档介绍在ISE上将RADIUS服务器配置为代理和授权服务器。此处使用两个ISE服务器，其中一个用作外部服务器。但是，可以使用任何符合RFC的RADIUS服务器。

先决条件

要求

Cisco 建议您了解以下主题：

- RADIUS协议的基本知识
- 身份服务引擎(ISE)策略配置方面的专业知识

使用的组件

本文档中的信息基于Cisco ISE版本2.2和2.4。

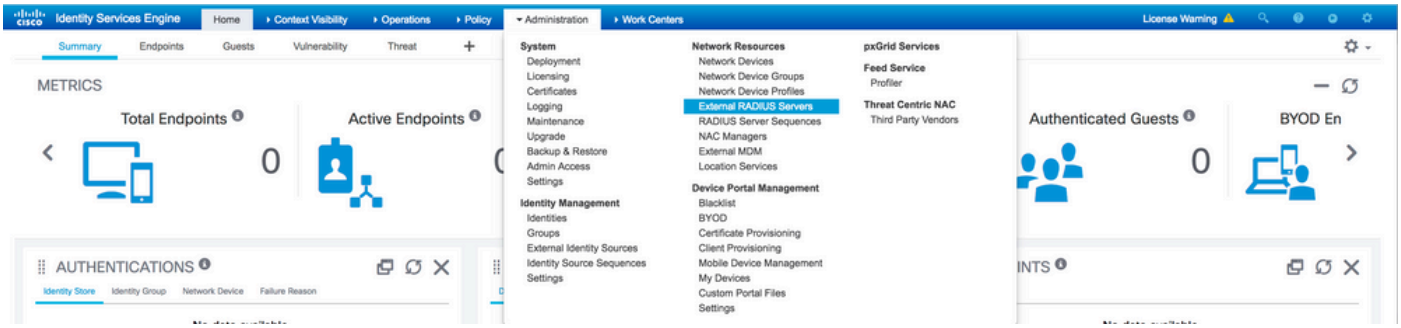
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

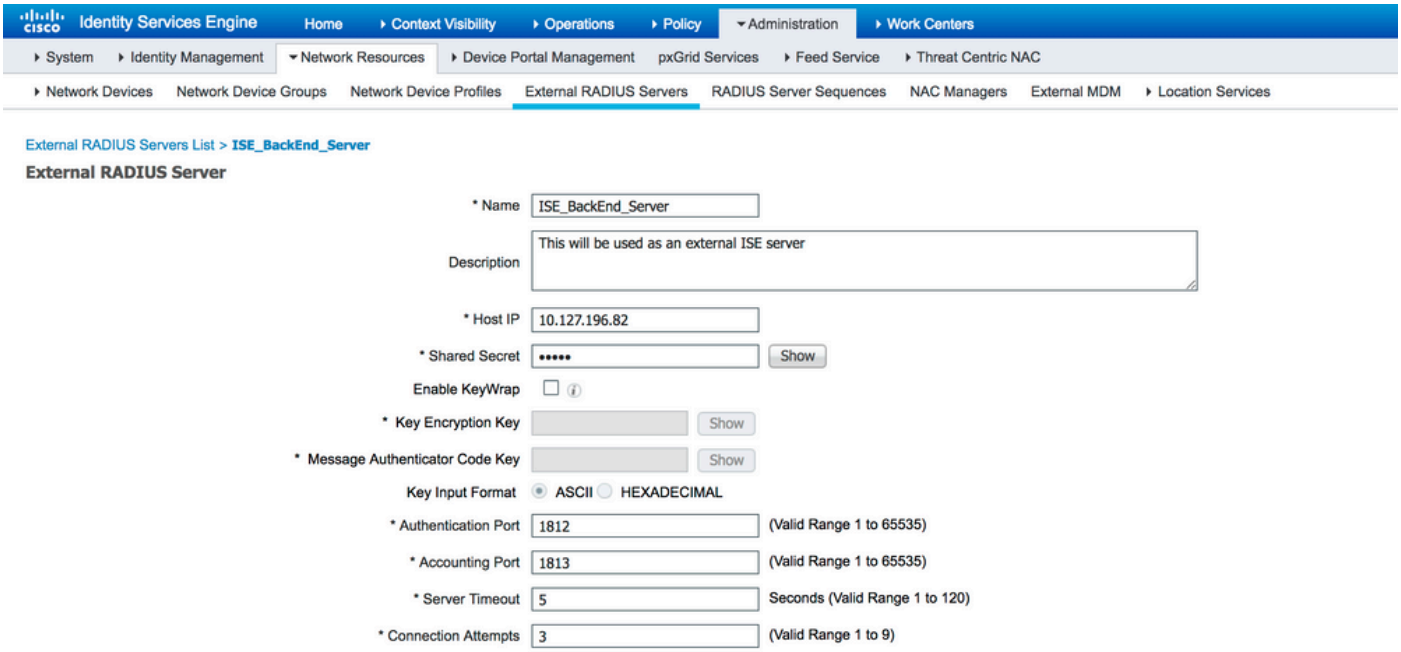
配置

网络图

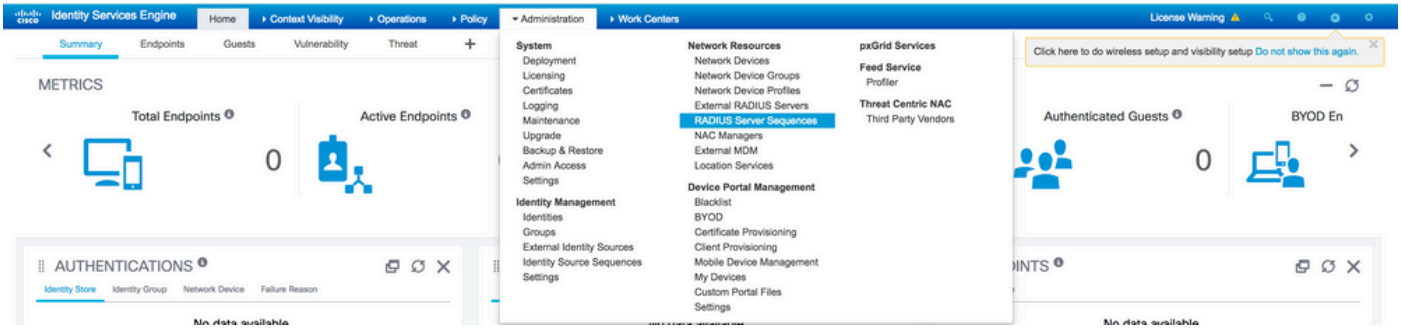
配置ISE（前端服务器）

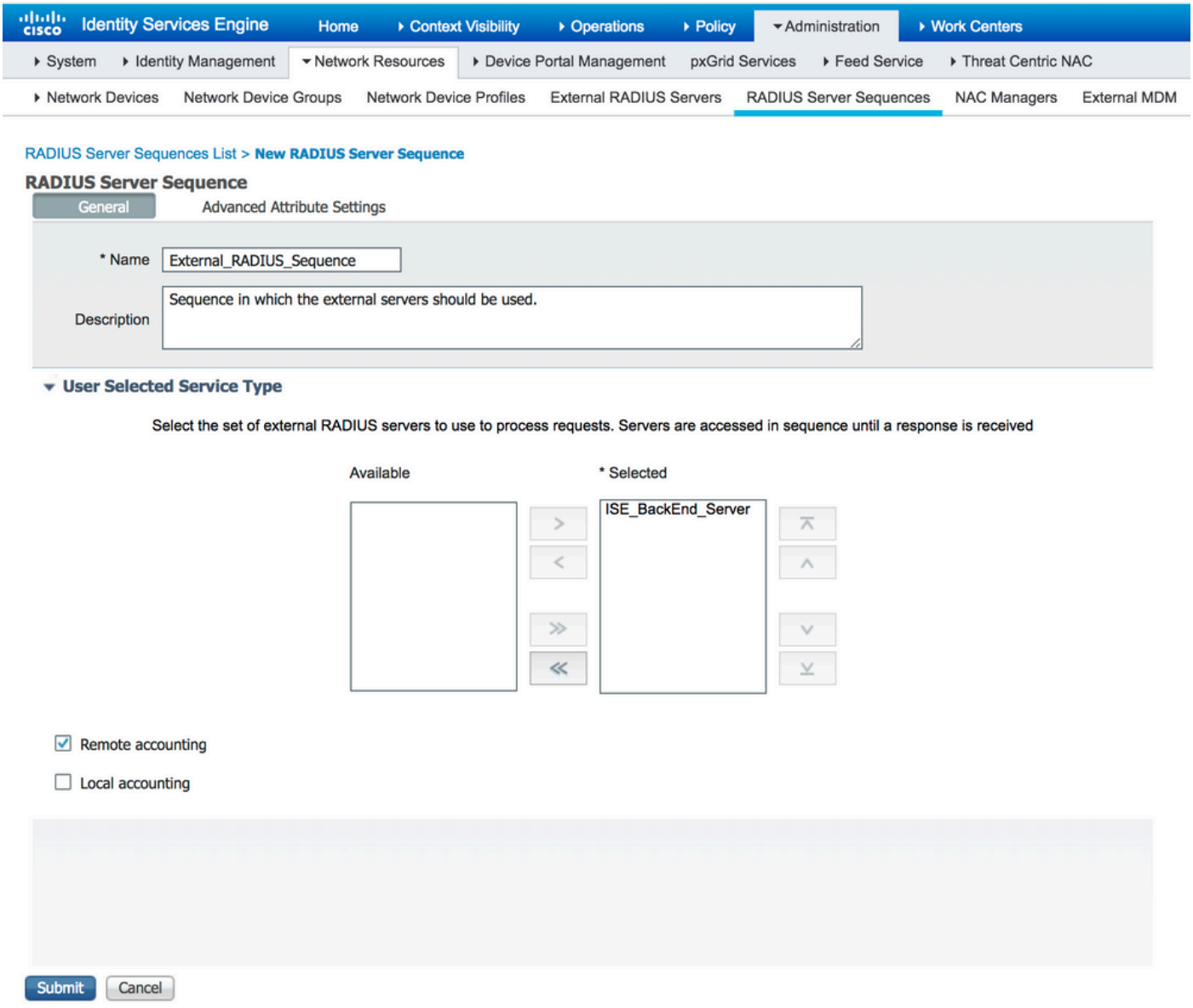
步骤1:可以配置和使用多个外部RADIUS服务器以对ISE上的用户进行身份验证。要配置外部RADIUS服务器，请导航至 Administration > Network Resources > External RADIUS Servers > Add,如图所示:





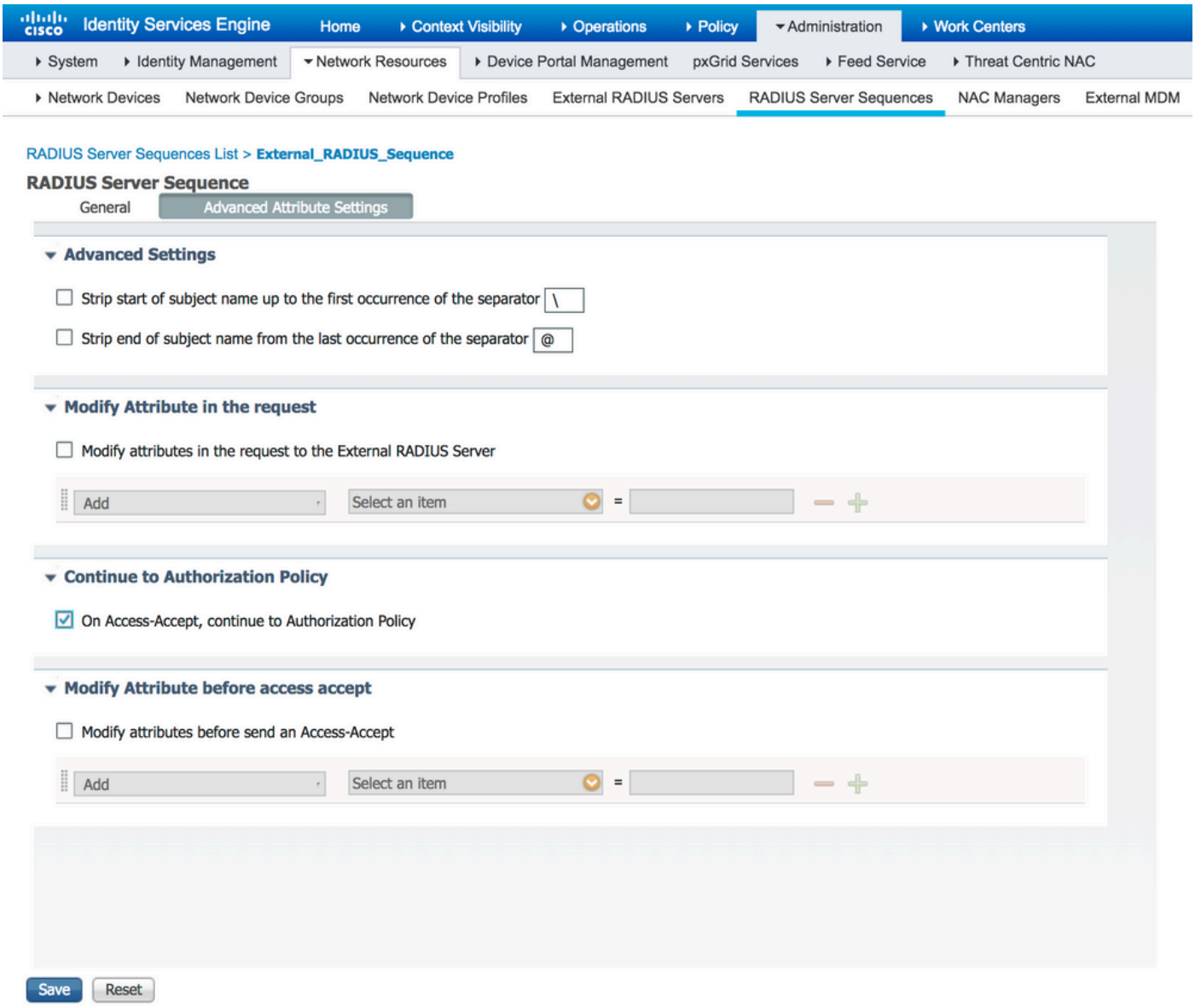
第二步：要使用已配置的外部RADIUS服务器，RADIUS服务器序列必须配置为类似于身份源序列。要配置相同内容，请导航至 Administration > Network Resources > RADIUS Server Sequences > Add,如图所示.





注：创建服务器序列时可用的其中一个选项是选择是否必须在ISE上本地或在外部RADIUS服务器上进行记帐。根据此处选择的选项，ISE决定是代理记帐请求还是将这些日志存储在本地。

第三步：还有一个章节为ISE代理外部RADIUS服务器请求时必须如何行为提供了更大的灵活性。可以在 Advance Attribute Settings,如图所示.



- Advanced Settings：提供使用分隔符删除RADIUS请求中用户名的开始或结尾的选项。
- 修改请求中的属性：提供用于修改RADIUS请求中的任何RADIUS属性的选项。此处的列表显示了可以添加/删除/更新的属性：

```
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]
```

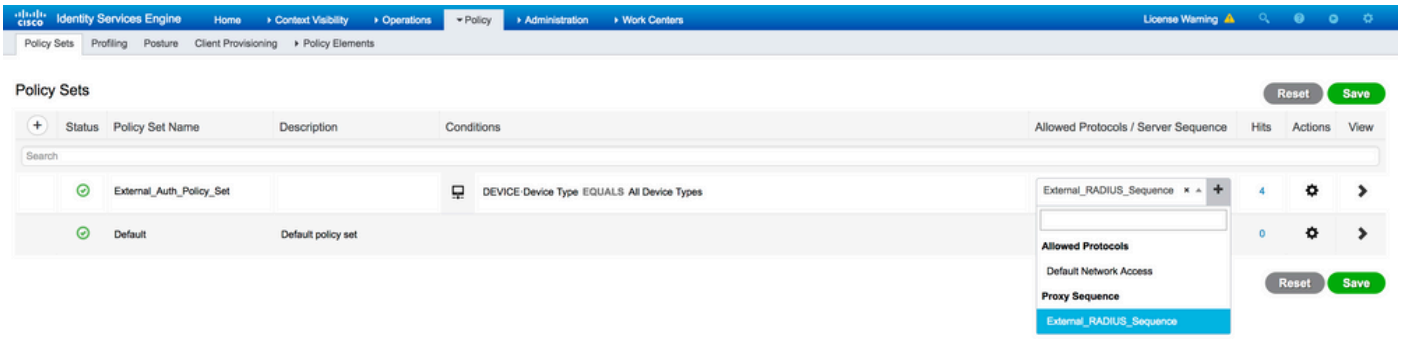
```
Login-LAT-Service--[34]
Login-LAT-Node--[35]
Login-LAT-Group--[36]
Event-Timestamp--[55]
Egress-VLANID--[56]
Ingress-Filters--[57]
Egress-VLAN-Name--[58]
User-Priority-Table--[59]
NAS-Port-Type--[61]
Port-Limit--[62]
Login-LAT-Port--[63]
Password-Retry--[75]
Connect-Info--[77]
NAS-Port-Id--[87]
Framed-Pool--[88]
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]
```

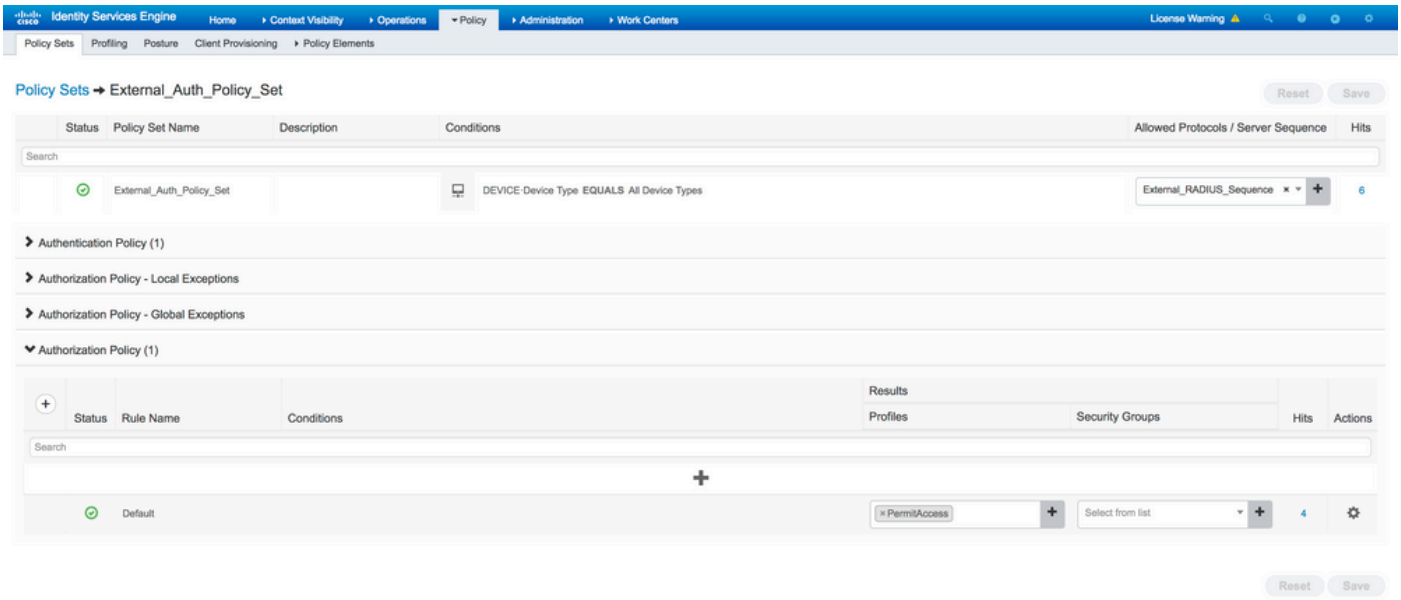
- Continue to Authorization Policy on Access-Accept：提供选项以选择ISE是否必须按原样发送访问接受，或继续根据ISE上配置的授权策略而不是外部RADIUS服务器提供的授权提供访问。如果选择此选项，外部RADIUS服务器提供的授权将被ISE提供的授权覆盖。

> 注意：仅当外部RADIUS服务器发送一个 Access-Accept 响应代理的RADIUS Access-Request。

- Modify Attribute before Access-Accept：与 Modify Attribute in the request，前面提到的属性可以在外部RADIUS服务器发送到网络设备之前添加/删除/更新Access-Accept中的存在。

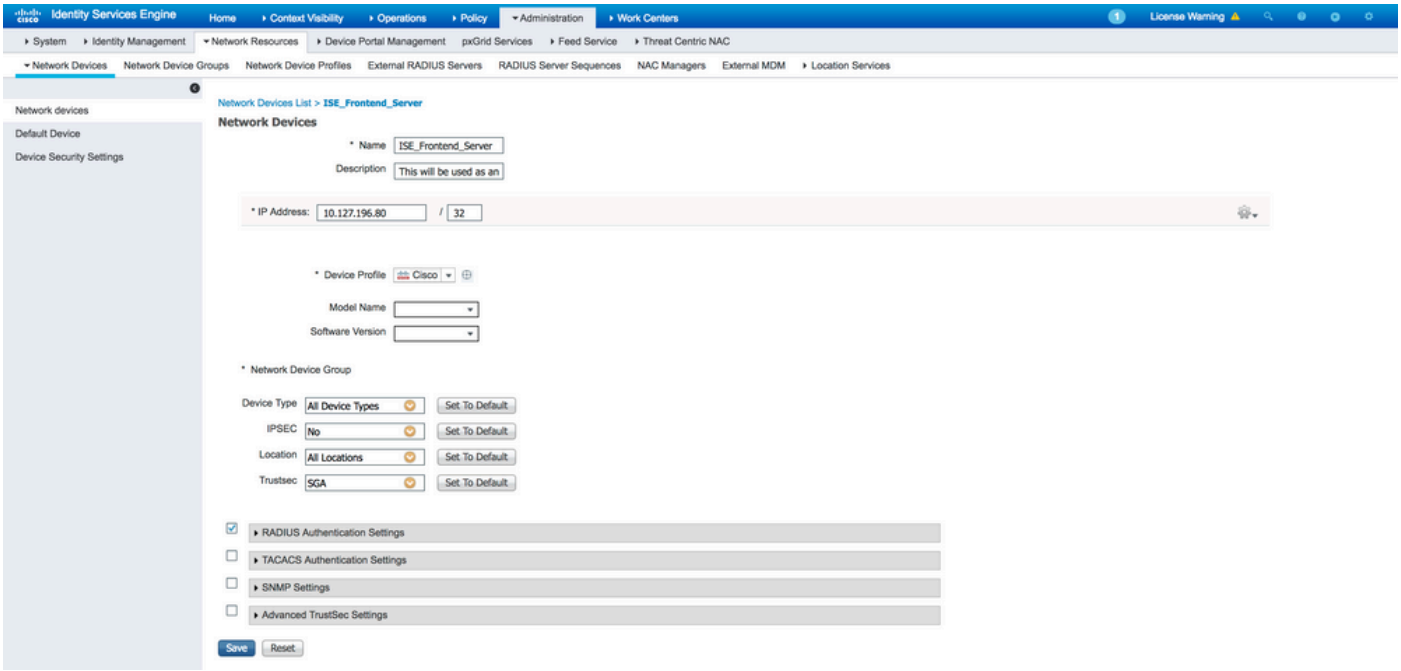
第四步：下一部分是配置策略集，以便使用RADIUS服务器序列而不是允许的协议，以便将请求发送到外部RADIUS服务器。可以在 Policy > Policy Sets.授权策略可在 Policy Set 但只有在以下情况下，Continue to Authorization Policy on Access-Accept 选项。否则，ISE仅充当RADIUS请求的代理，以便匹配为此策略集配置的条件。



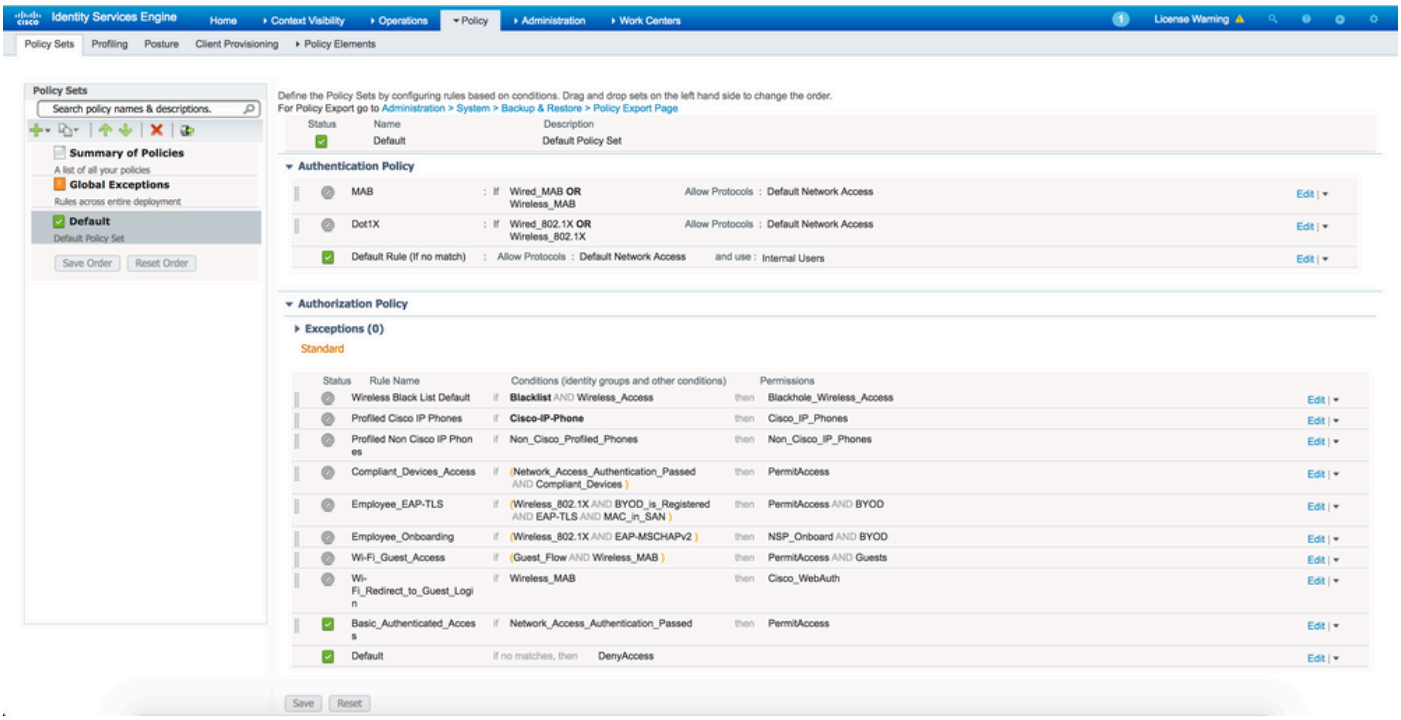


配置外部RADIUS服务器

步骤1:在本示例中，另一个ISE服务器（版本2.2）用作名为 ISE_Backend_Server.ISE(ISE_Frontend_Server)必须配置为网络设备或通常在外部RADIUS服务器中称为NAS(ISE_Backend_Server 在本例中)，因为 NAS-IP-Address 转发到外部RADIUS服务器的Access-Request中的属性将替换为的IP地址ISE_Frontend_Server.要配置的共享密钥与在上为外部RADIUS服务器配置的共享密钥相同 ISE_Frontend_Server.



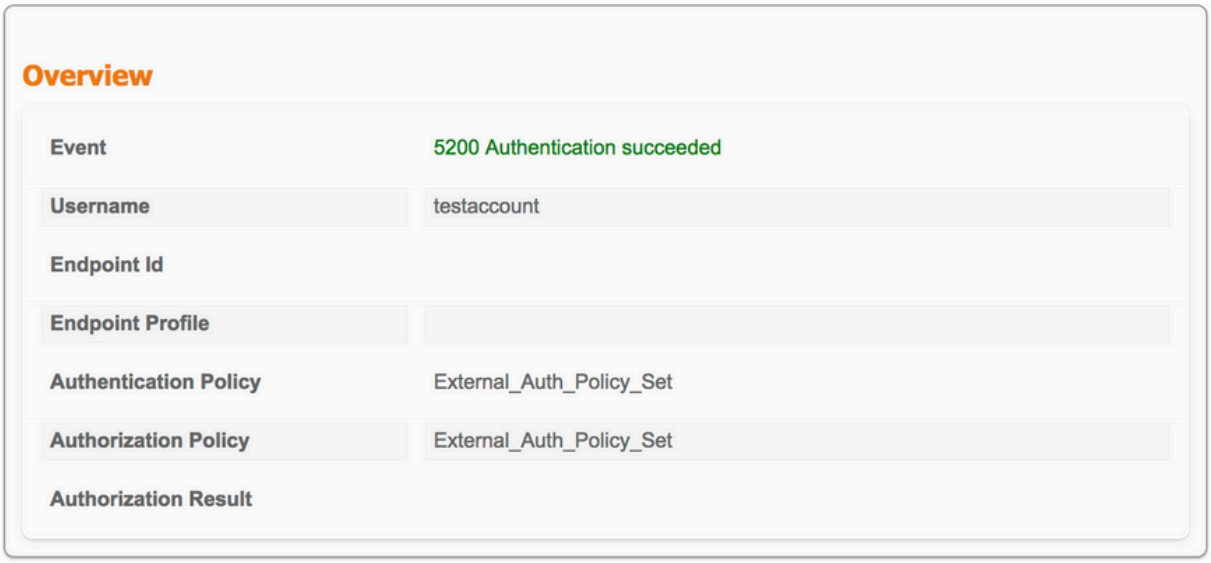
第二步：外部RADIUS服务器可以配置其自己的身份验证和授权策略，以便为ISE代理的请求提供服务。在本示例中，配置简单策略以检查内部用户中的用户，然后在经过身份验证后允许访问。



验证

步骤1:如果收到请求，请检查ISE实时日志，如图所示。

第二步：检查是否选择了正确的策略集，如图所示。



第三步：检查请求是否转发到外部RADIUS服务器。

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.如果 Continue to Authorization Policy on Access-Accept 选项，检查是否评估授权策略。

Identity Services Engine

Overview

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

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

故障排除

场景 1.事件 — 5405 RADIUS请求已丢弃

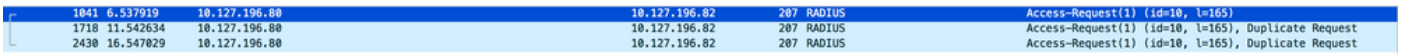
- 必须验证的最重要的事情是详细身份验证报告中的步骤。如果步骤显示 RADIUS-Client request timeout expired，则表示ISE未收到来自已配置的外部RADIUS服务器的任何响应。在下列情况下，可能会发生这种情况：

1. 外部RADIUS服务器存在连接问题。ISE无法到达为其配置的端口上的外部RADIUS服务器。
2. ISE未配置为外部RADIUS服务器上的网络设备或NAS。
3. 外部RADIUS服务器通过配置或由于外部RADIUS服务器上的某些问题丢弃数据包。

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

检查数据包捕获，以查看它是否不是错误消息，即ISE从服务器接收数据包，但仍报告请求超时。



- 如果步骤显示 Start forwarding request to remote RADIUS server 第一步是 No more external RADIUS servers; can't perform failover, 然后，这意味着所有已配置的外部RADIUS服务器当前都标记为dead，并且请求仅在dead计时器过期后才会得到处理。

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
11353	No more external RADIUS servers; can't perform failover

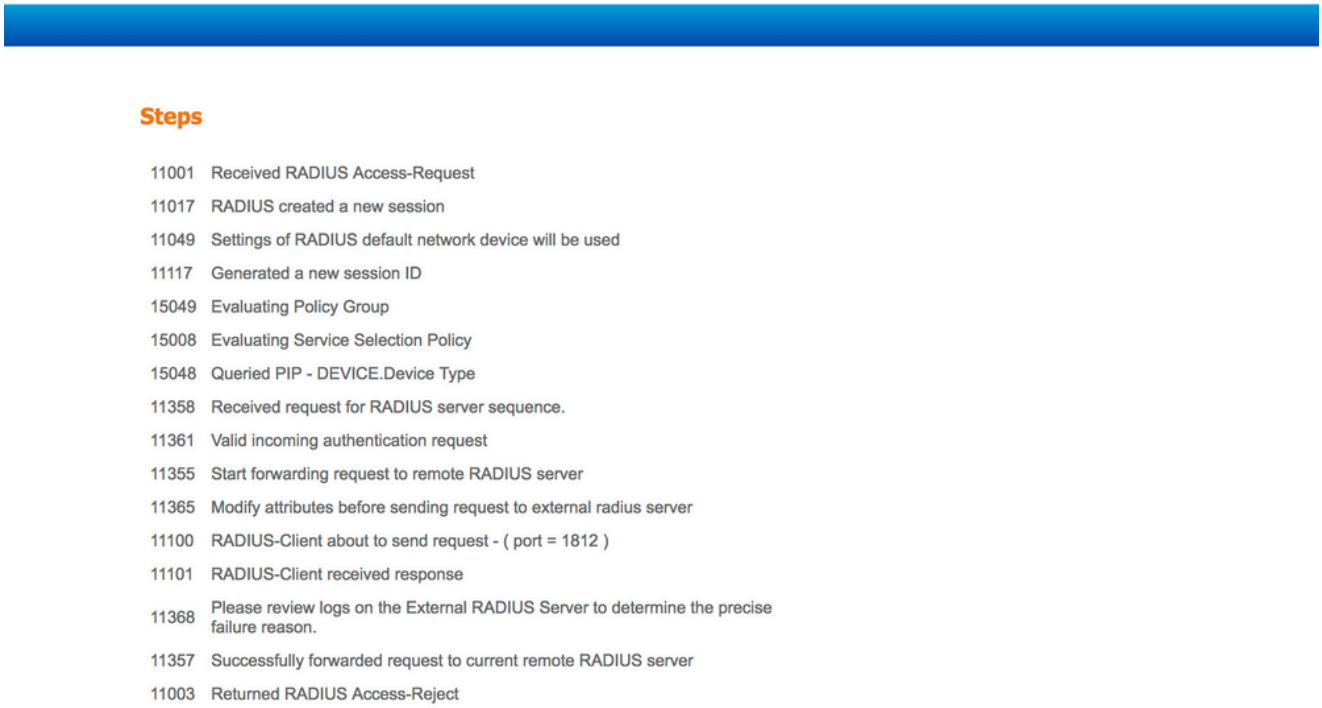
注意:ISE中外部RADIUS服务器的默认停顿时间为5分钟。此值是硬编码的，自此版本起无法修改。

- 如果步骤显示 RADIUS-Client encountered error during processing flow 然后是 Failed to forward request to current remote RADIUS server; an invalid response was received,这表示ISE在转发到外部RADIUS服务器的请求时遇到问题

。当从网络设备/NAS发送到ISE的RADIUS请求没有 NAS-IP-Address 作为属性之一。如果没有 NAS-IP-Address 属性，如果外部RADIUS服务器未使用，ISE会填充 NAS-IP-Address 字段的源IP地址。但是，当使用外部RADIUS服务器时，该选项不适用。

场景 2：事件 — 5400身份验证失败

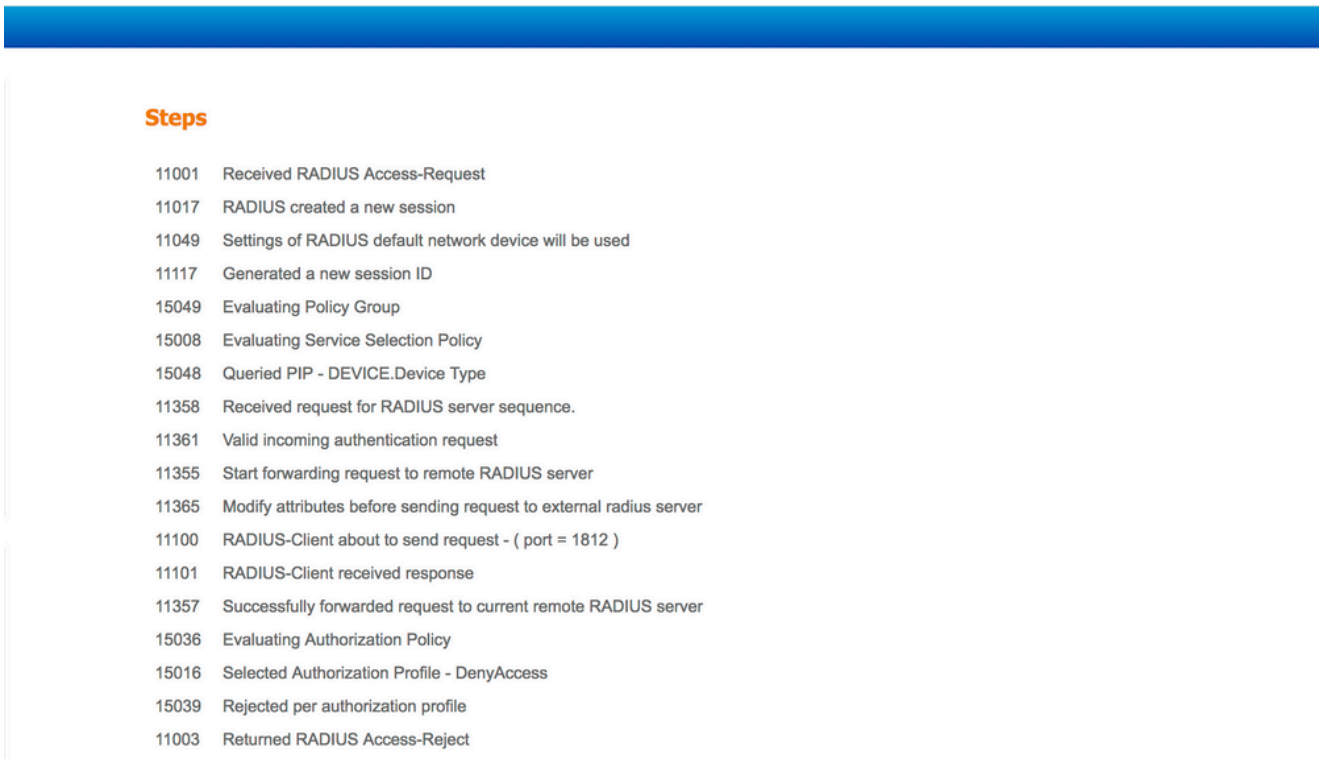
- 在这种情况下，如果步骤显示 11368 Please review logs on the External RADIUS Server to determine the precise failure reason，则表示身份验证在外部RADIUS服务器本身上失败，并且已发送Access-Reject。



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

- 如果步骤显示 15039 Rejected per authorization profile，这意味着ISE从外部RADIUS服务器收到访问接受，但ISE根据配置的授权策略拒绝授权。



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

- 如果 Failure Reason 在ISE上，除了此处提到的身份验证故障之外，还有任何其他情况，那么这可能意味着配置或ISE本身存在潜在问题。建议此时打开TAC案例。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。