在ISE上配置外部RADIUS伺服器

目錄

[簡介](#)

[必要條件](#)

- [需求](#)
- [採用元件](#)

[設定](#)

- [網路圖表](#)
- [配置ISE（前端伺服器）](#)
- [設定外部RADIUS伺服器](#)

[驗證](#)

[疑難排解](#)

- [案例 1.事件 — 5405 RADIUS要求已捨棄](#)
- [案例 2.事件 — 5400身份驗證失敗](#)

簡介

本檔案將說明ISE上的RADIUS伺服器設定為代理和授權伺服器。此處使用兩個ISE伺服器，其中一個用作外部伺服器。但是，可利用任何與RFC相容的RADIUS伺服器。

必要條件

需求

思科建議您瞭解以下主題：

- RADIUS通訊協定基礎知識
- 身份服務引擎(ISE)策略配置方面的專業知識

採用元件

本文檔中的資訊基於Cisco ISE版本2.2和2.4。

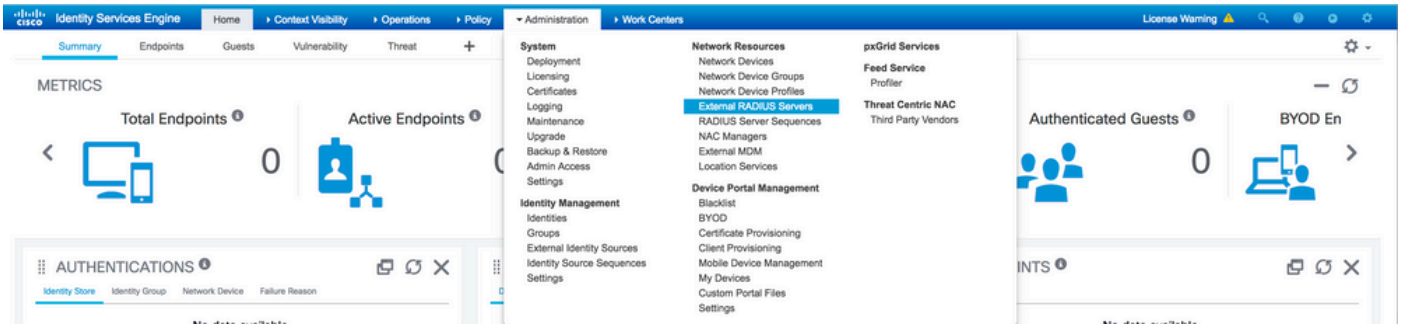
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

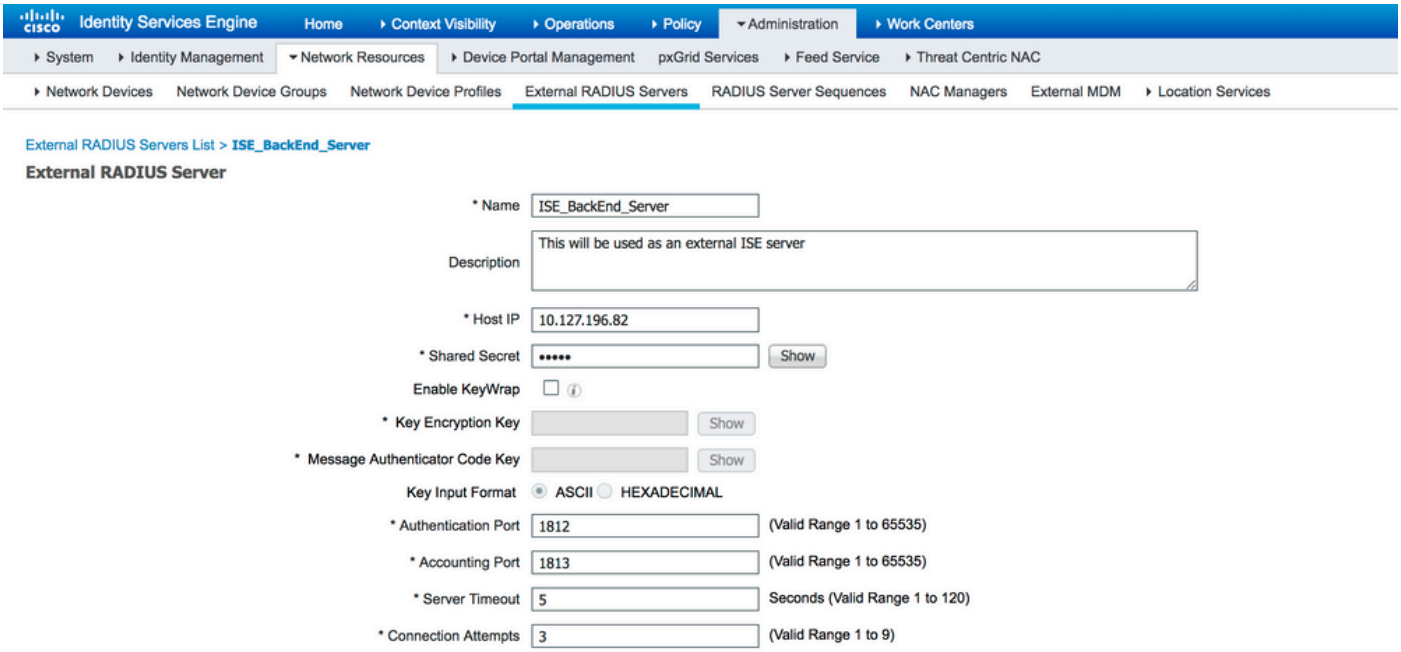
設定

網路圖表

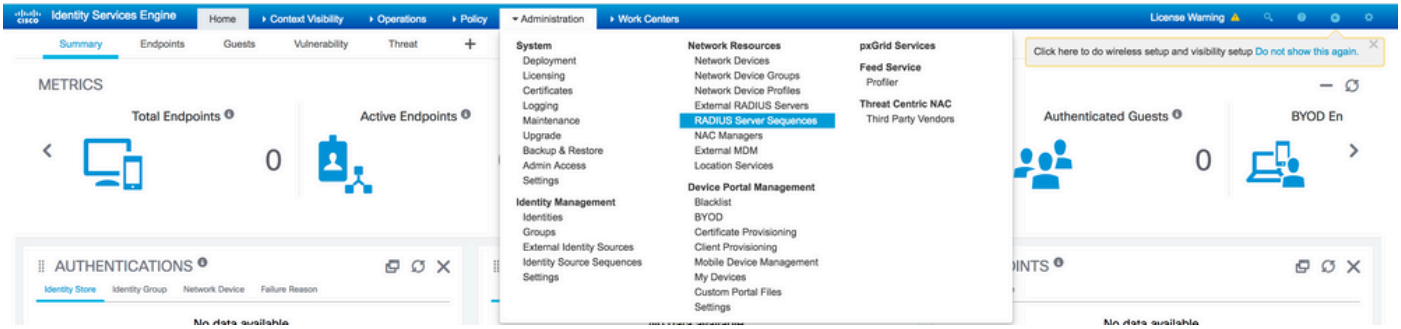
配置ISE（前端伺服器）

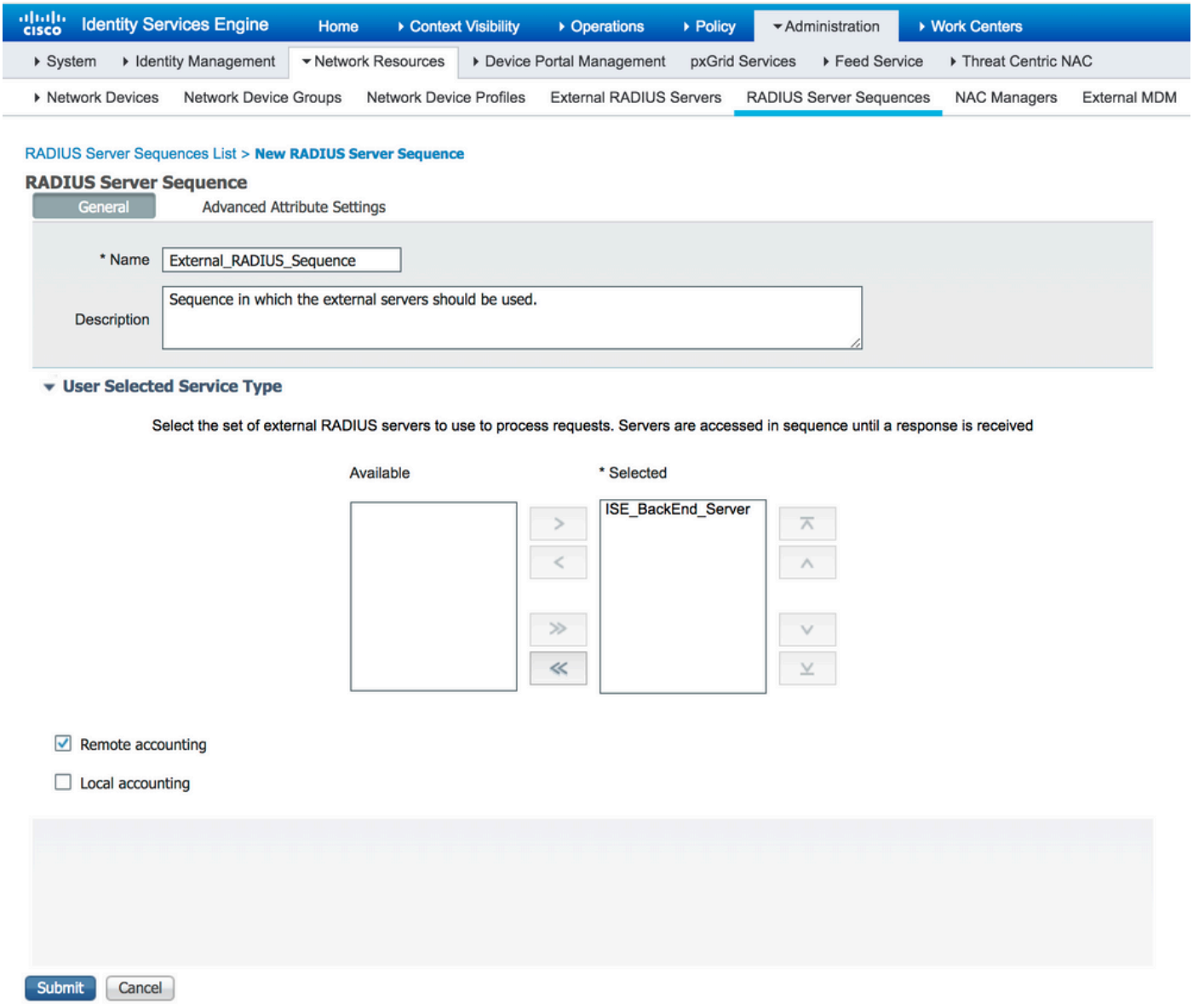
步驟 1.可以配置和使用多個外部RADIUS伺服器來驗證ISE上的使用者。若要設定外部RADIUS伺服器，請導覽至 Administration > Network Resources > External RADIUS Servers > Add中，如下圖所示：





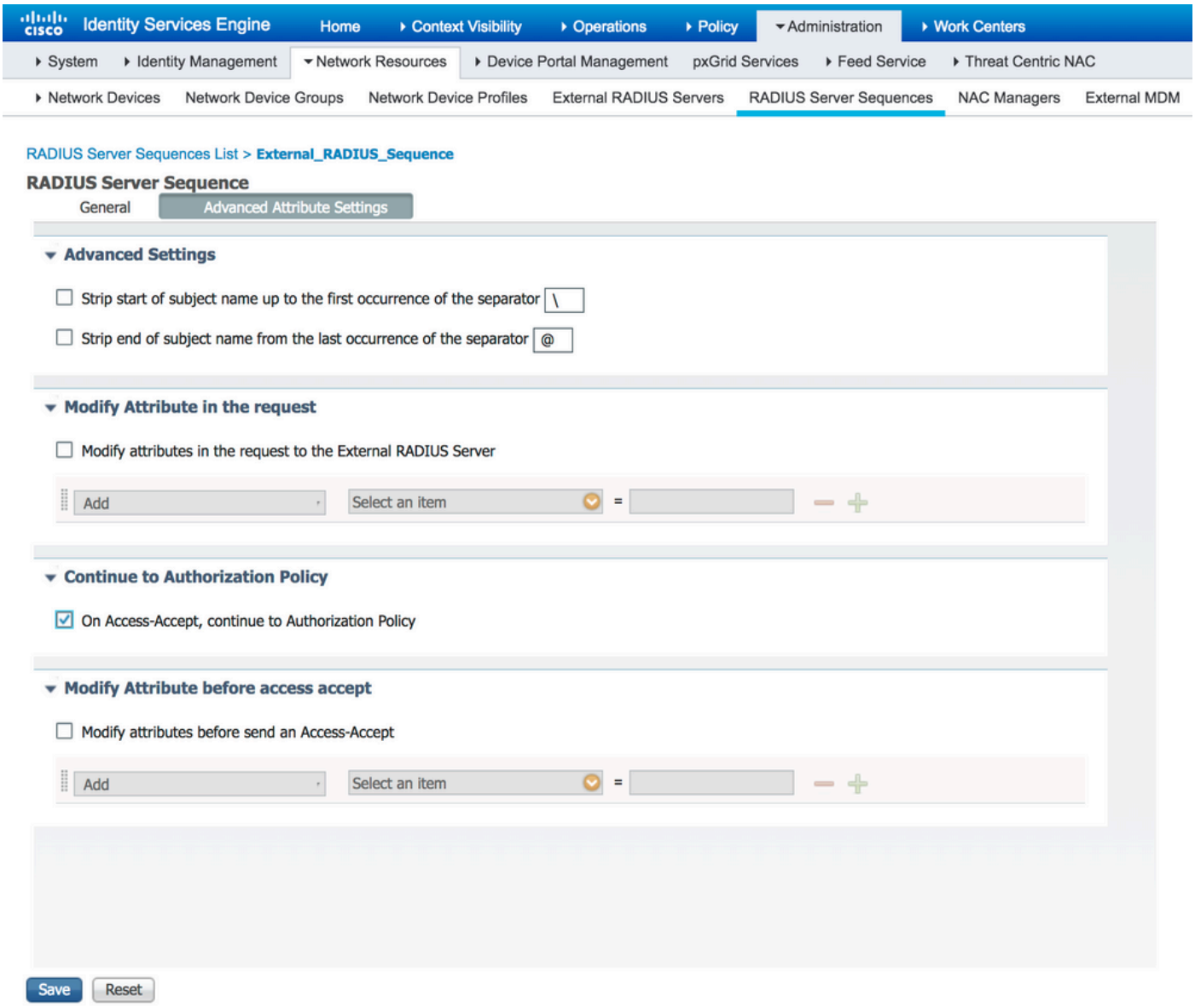
步驟 2.若要使用已配置的外部RADIUS伺服器，RADIUS伺服器序列必須配置為類似於身份源序列。要配置相同內容，請導航至 Administration > Network Resources > RADIUS Server Sequences > Add中，如圖所示。





注意：建立伺服器序列時可用的選項之一就是選擇是否必須在ISE本地或在外部RADIUS伺服器上進行記帳。根據此處選擇的選項，ISE決定代理記帳請求還是本地儲存這些日誌。

步驟 3.還有一個附加部分，為ISE代理外部RADIUS伺服器請求時必須如何行為提供了更大的靈活性。可在以下位置找到 Advance Attribute Settings中，如圖所示。



- 高級設定：提供用於刪除帶有分隔符的RADIUS請求中使用者名稱的開始或結束的選項。
- 修改請求中的屬性：提供用於修改RADIUS請求中的任何RADIUS屬性的選項。此處的清單顯示了可以新增/刪除/更新的屬性：

```
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]
```

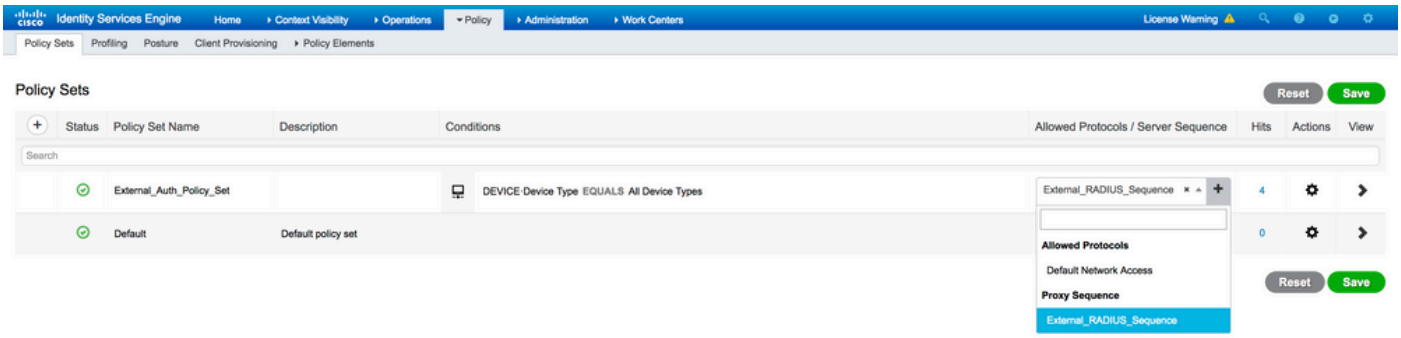
```
NAS-Identifier--[32]
Login-LAT-Service--[34]
Login-LAT-Node--[35]
Login-LAT-Group--[36]
Event-Timestamp--[55]
Egress-VLANID--[56]
Ingress-Filters--[57]
Egress-VLAN-Name--[58]
User-Priority-Table--[59]
NAS-Port-Type--[61]
Port-Limit--[62]
Login-LAT-Port--[63]
Password-Retry--[75]
Connect-Info--[77]
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]
```

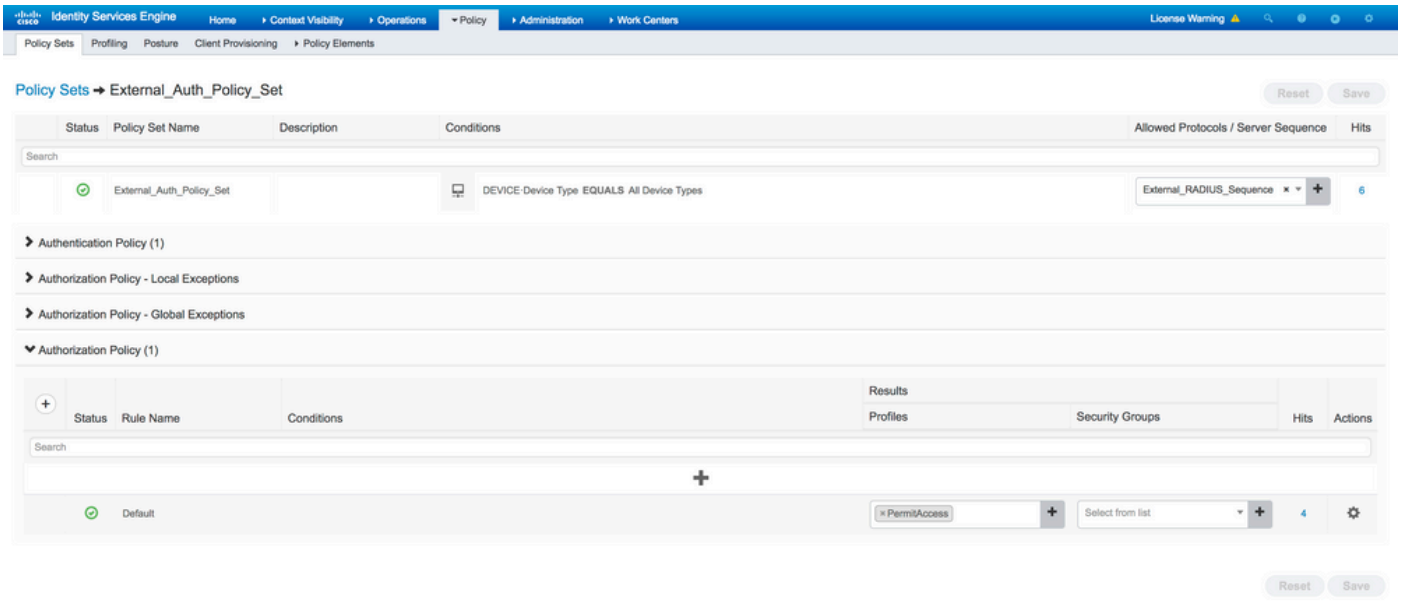
- Continue to Authorization Policy on Access-Accept：提供選項以選擇ISE是否必須按原樣傳送訪問接受，或根據ISE上配置的授權策略而不是外部RADIUS伺服器提供的授權繼續提供訪問。如果選擇此選項，外部RADIUS伺服器提供的授權將被ISE提供的授權覆蓋。

> 注意：此選項僅在外部RADIUS伺服器傳送一個 Access-Accept 響應代理的RADIUS訪問請求。

- Modify Attribute before Access-Accept：與 Modify Attribute in the request此外，前面提到的屬性可以在外部RADIUS伺服器傳送到網路裝置之前新增/刪除/更新外部RADIUS伺服器傳送的訪問接受內容。

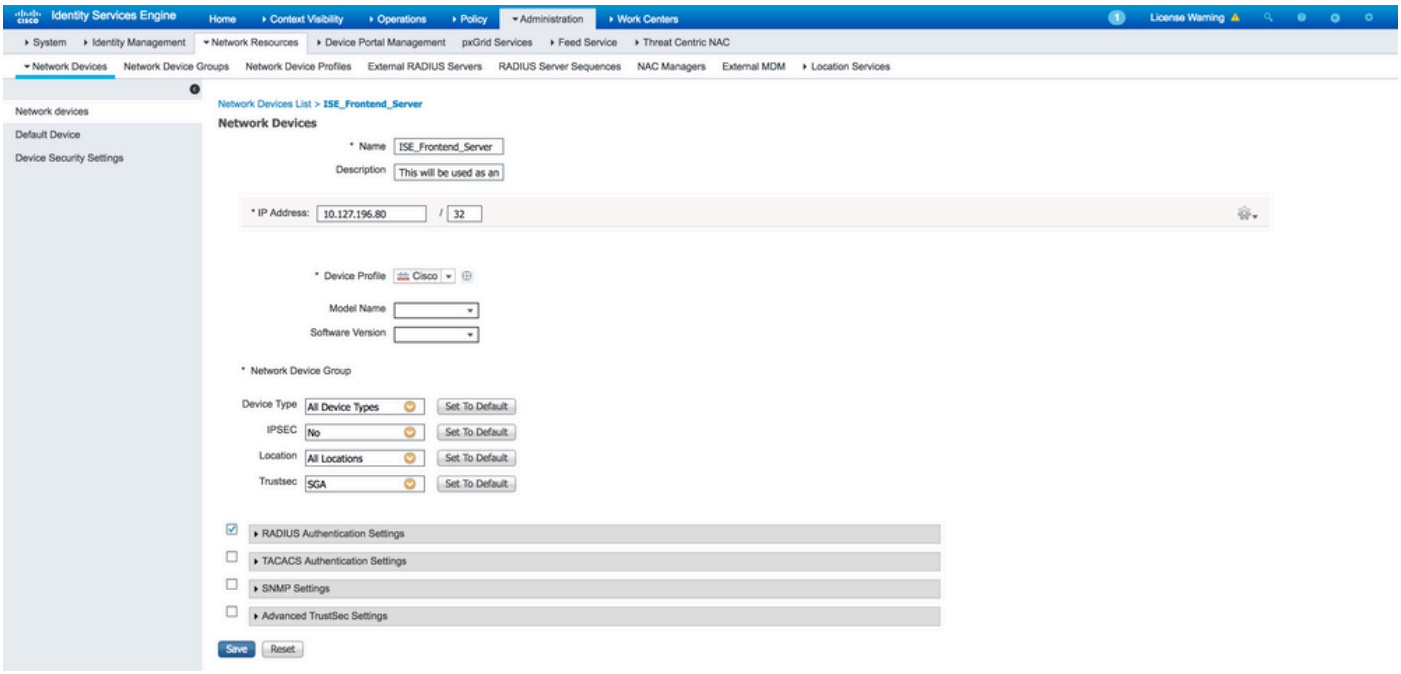
步驟 4.下一部分是配置策略集，以便使用RADIUS伺服器序列而不是允許的協定，以便將請求傳送到外部RADIUS伺服器。可在 Policy > Policy Sets.授權策略可在 Policy Set 但只有在以下情況下才會生效 Continue to Authorization Policy on Access-Accept 選項。否則，ISE僅充當RADIUS請求的代理，以便匹配為此策略集配置的條件。



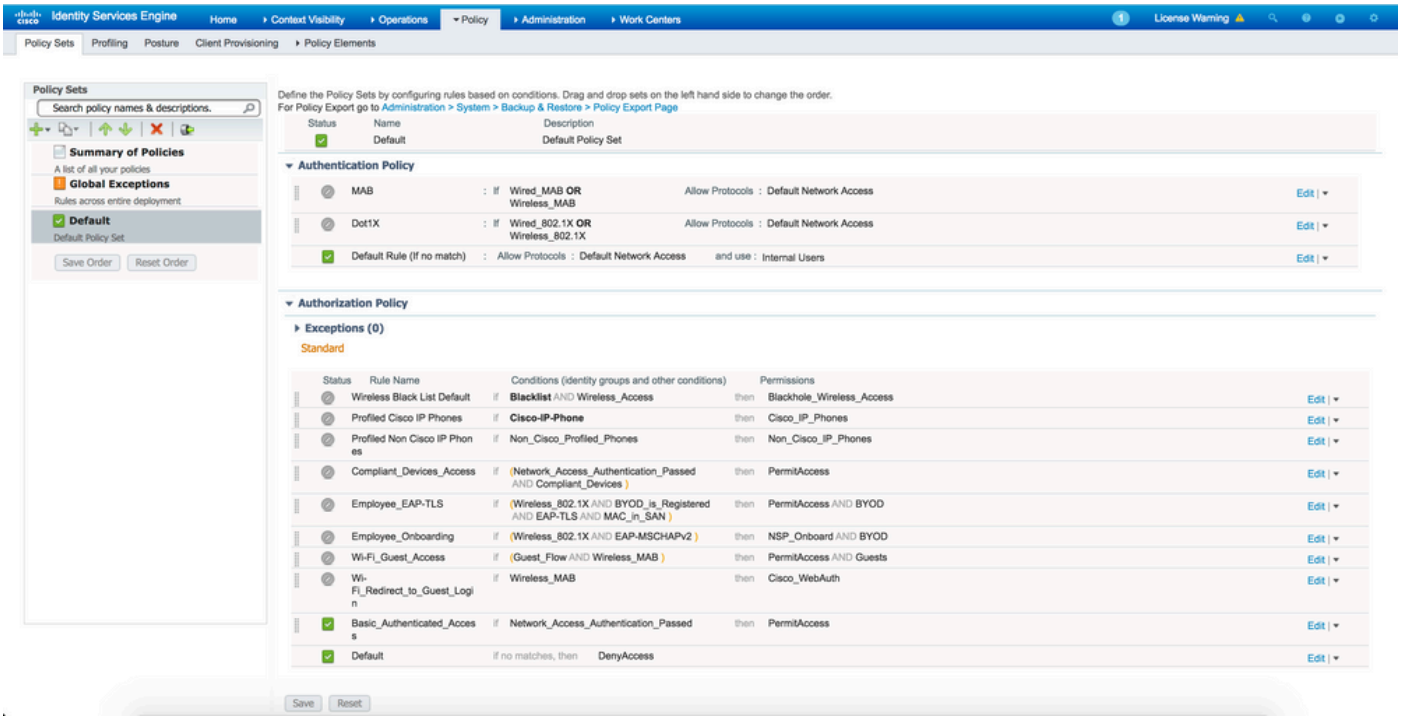


設定外部RADIUS伺服器

步驟 1.在本示例中，另一個ISE伺服器（版本2.2）用作名為的外部RADIUS伺服器ISE_Backend_Server.ISE(ISE_Frontend_Server)必須配置為網路裝置或外部RADIUS伺服器中傳統上稱為NAS(ISE_Backend_Server 在本例中)，因為 NAS-IP-Address 轉送到外部RADIUS伺服器的Access-Request中的屬性將替換為的IP位址ISE_Frontend_Server.要配置的共用金鑰與在上為外部RADIUS伺服器配置的共用金鑰相同 ISE_Frontend_Server.



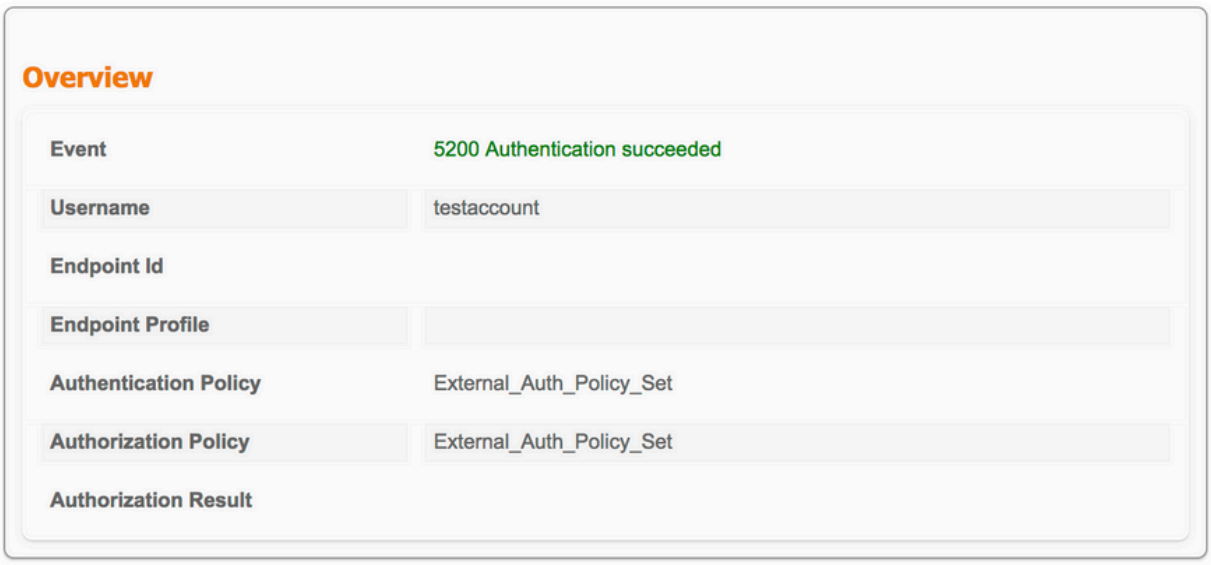
步驟 2.外部RADIUS伺服器可設定其自己的驗證和授權原則，以服務ISE代理的請求。在本示例中，配置了一個簡單策略，以便檢查內部使用者中的使用者，然後在通過驗證後允許訪問。



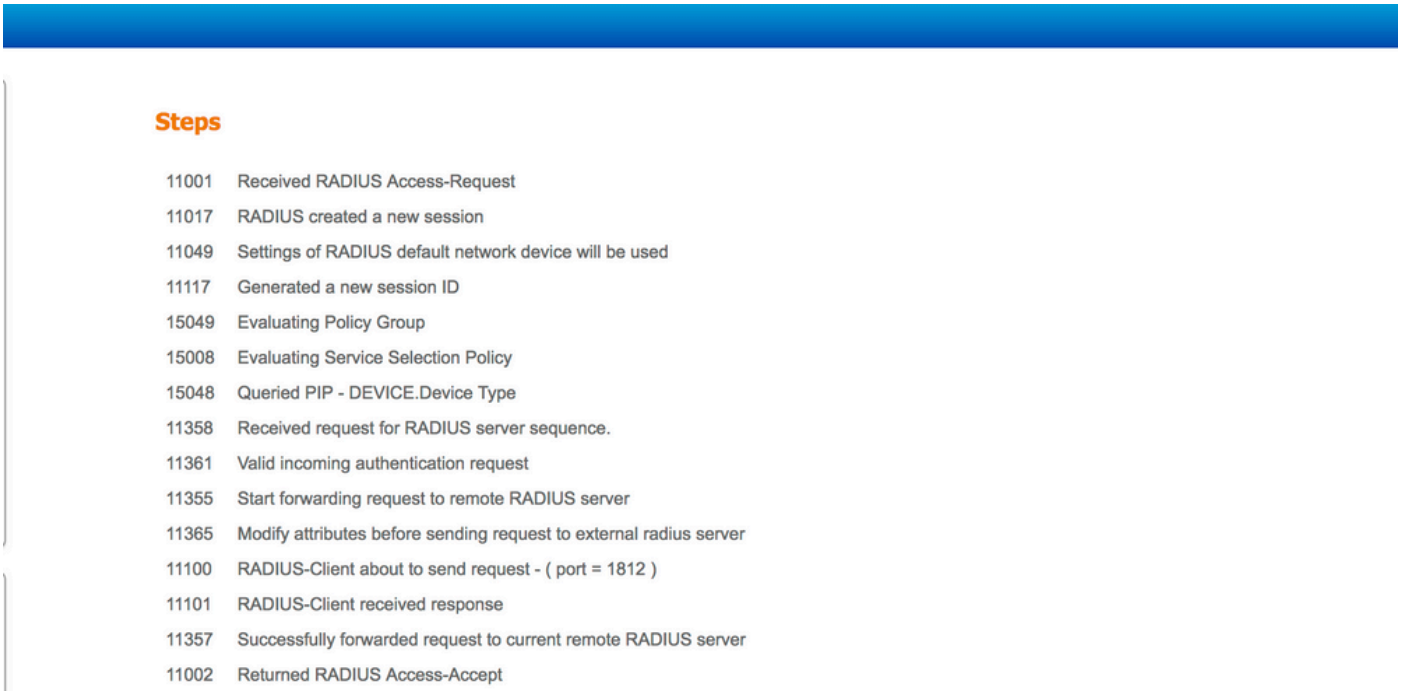
驗證

步驟 1.如果收到請求，請檢查ISE即時日誌，如圖所示。

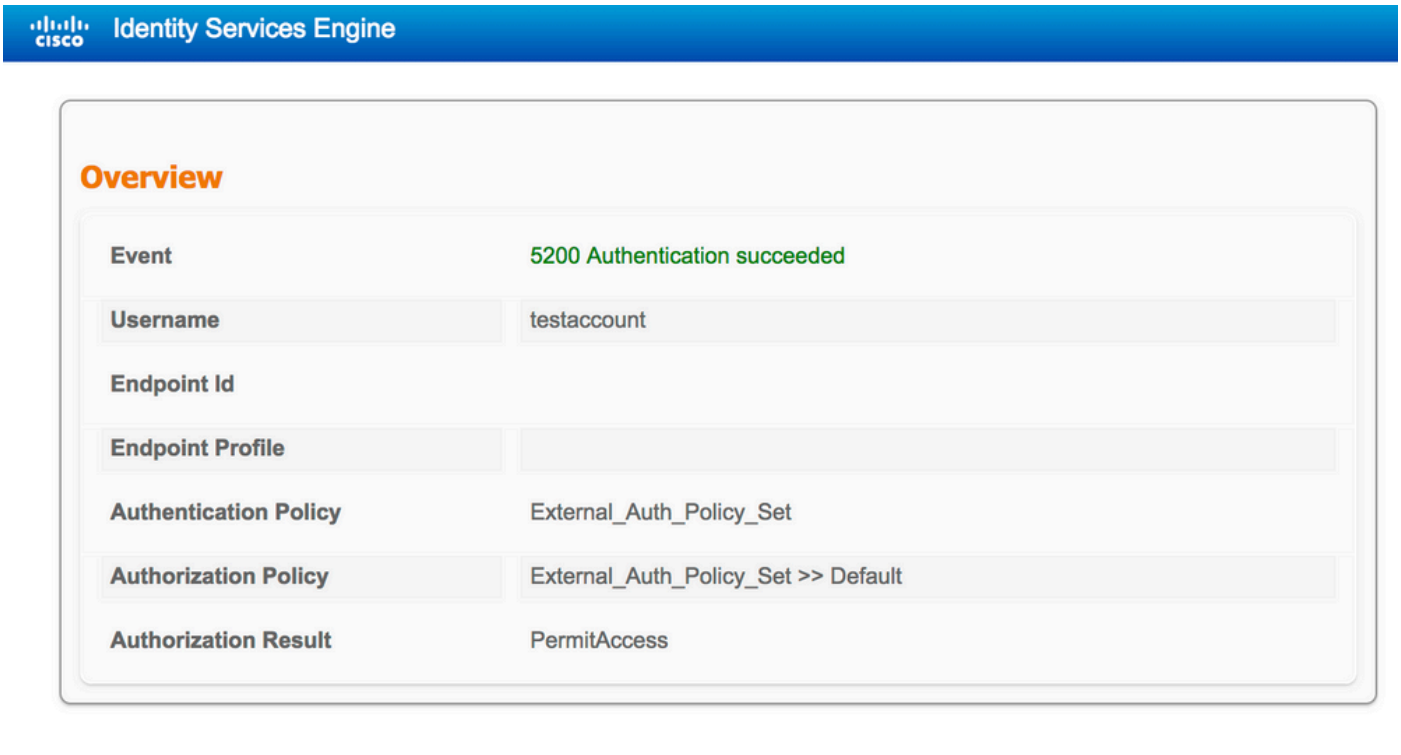
步驟 2.檢查是否選擇了正確的策略集，如下圖所示。

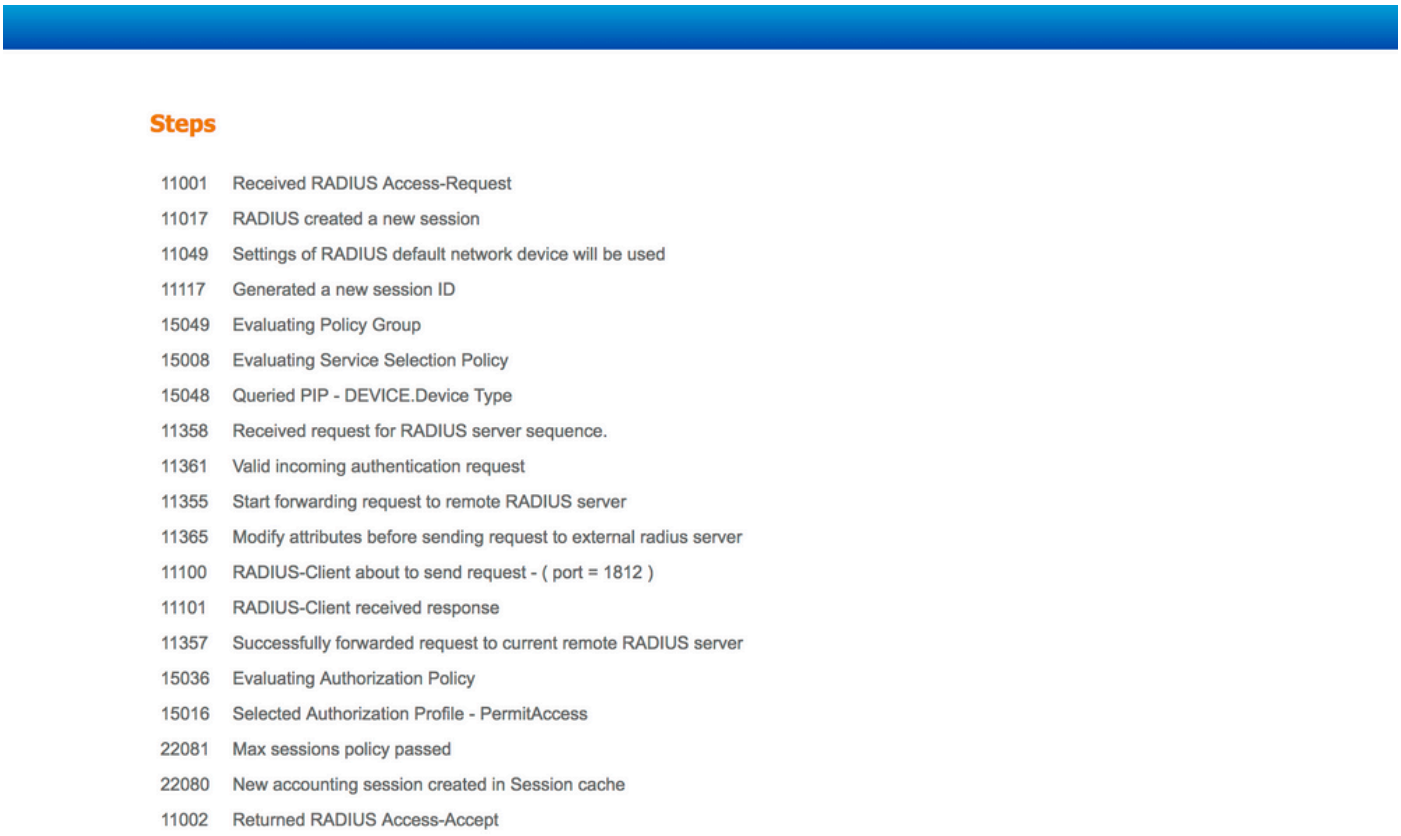


步驟 3.檢查是否將請求轉送到外部RADIUS伺服器。



4.如果 Continue to Authorization Policy on Access-Accept 選項，檢查是否評估授權策略。





疑難排解

案例 1.事件 — 5405 RADIUS要求已捨棄

- 必須驗證的最重要的事情是詳細身份驗證報告中的步驟。如果步驟顯示 RADIUS-Client request timeout expired則表示ISE未收到來自已配置外部RADIUS伺服器的任何響應。在以下情況下會發生這種情況：

1. 外部RADIUS伺服器存在連線問題。ISE無法到達為其配置的埠上的外部RADIUS伺服器。
2. ISE未配置為外部RADIUS伺服器上的網路裝置或NAS。
3. 外部RADIUS伺服器會因為組態或外部RADIUS伺服器上發生某些問題而捨棄封包。

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

檢查資料包捕獲，以檢視它是否不是錯誤消息，即ISE從伺服器接收資料包，但仍報告請求超時。

1041	6.537919	10.127.196.80	10.127.196.82	207	RADIUS	Access-Request(1) (id=10, l=165)
1718	11.542634	10.127.196.80	10.127.196.82	207	RADIUS	Access-Request(1) (id=10, l=165), Duplicate Request
2430	16.547029	10.127.196.80	10.127.196.82	207	RADIUS	Access-Request(1) (id=10, l=165), Duplicate Request

- 如果步驟顯示 Start forwarding request to remote RADIUS server 第一步就是 No more external RADIUS servers; can't perform failover中， 這表示所有已設定的外部RADIUS伺服器目前都標為dead，且要求僅在停用的計時器到期後才提供服務。

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

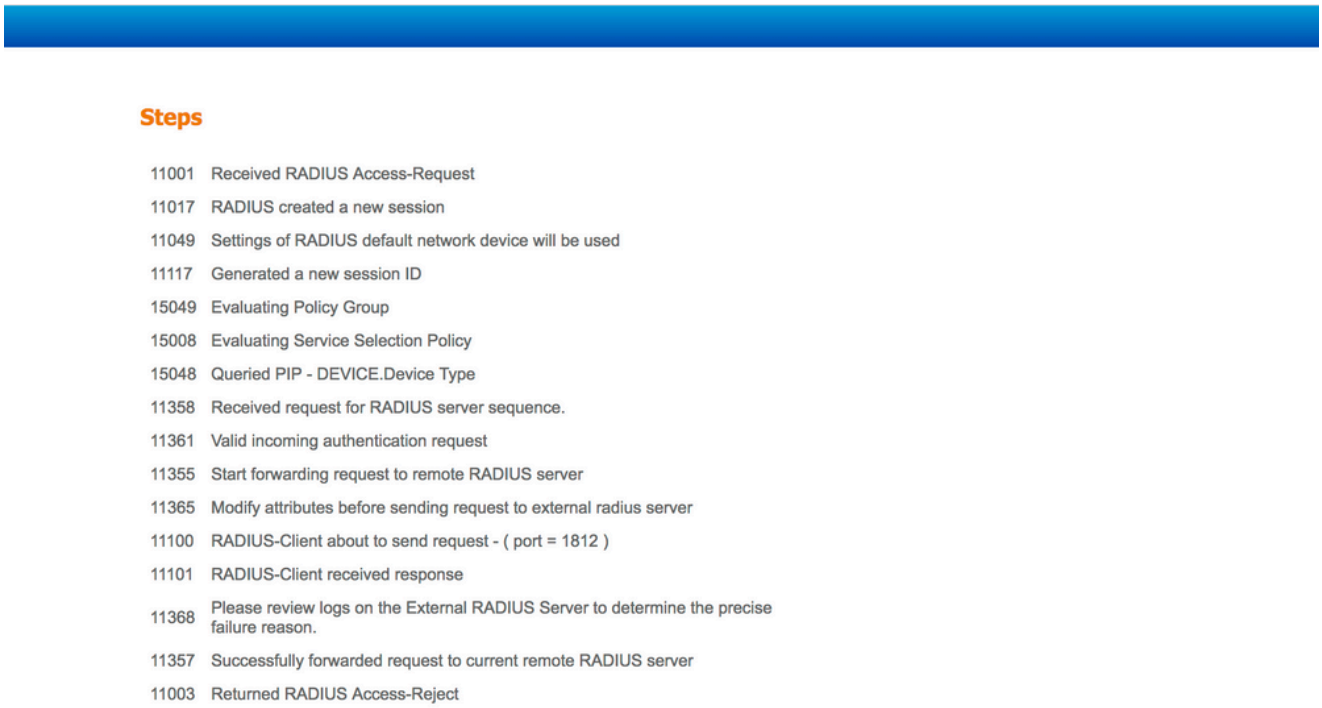
✎ 注意:ISE中外部RADIUS服務器的預設停機時間為5分鐘。此值是硬式編碼的，自此版本

起無法修改。

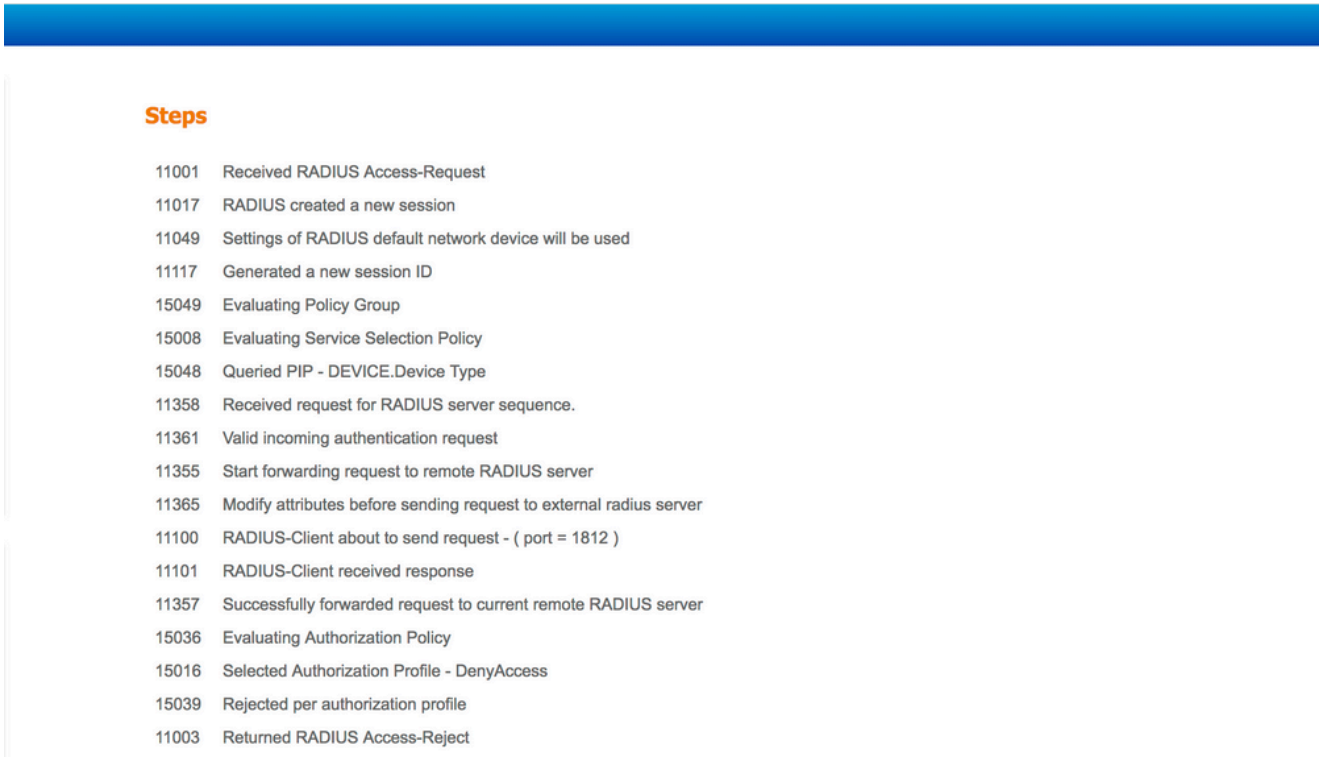
- 如果步驟顯示 RADIUS-Client encountered error during processing flow 然後是 Failed to forward request to current remote RADIUS server; an invalid response was received中，這表示ISE在向外部RADIUS伺服器轉發請求時遇到問題。當從網路裝置/NAS傳送到ISE的RADIUS請求沒有 NAS-IP-Address 作為屬性之一。如果沒有 NAS-IP-Address 屬性，如果外部RADIUS伺服器未使用，ISE會填充 NAS-IP-Address 欄位，其中包含資料包的源IP。但是，當使用外部RADIUS伺服器時，這不適用。

案例 2.事件 — 5400身份驗證失敗

- 在這種情況下，如果步驟顯示 11368 Please review logs on the External RADIUS Server to determine the precise failure reason，則表示驗證在外部RADIUS伺服器本身上已失敗，且已傳送Access-Reject。



- 如果步驟顯示 15039 Rejected per authorization profile，這意味著ISE從外部RADIUS伺服器收到訪問接受，但ISE根據配置的授權策略拒絕授權。



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 如果身份驗證失敗，則在ISE上除了此處提到的其他任何設定，那麼這可能意味著配置或ISE本身存在潛在問題。建議此時開啟TAC案例。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。