Configure External RADIUS Servers on ISE

Contents

Introduction

This document describes how to configure two RFC-compliant RADIUS servers on ISE as proxy and authorization, respectively.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of RADIUS protocol
- Expertise in Identity Services Engine (ISE) policy configuration

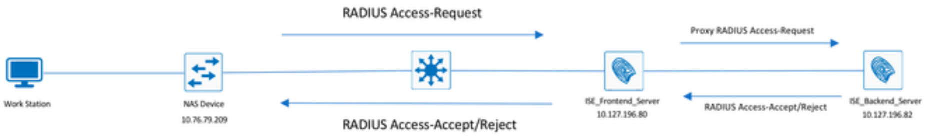
Components Used

The information in this document is based on Cisco ISE versions 2.2 and 2.4.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

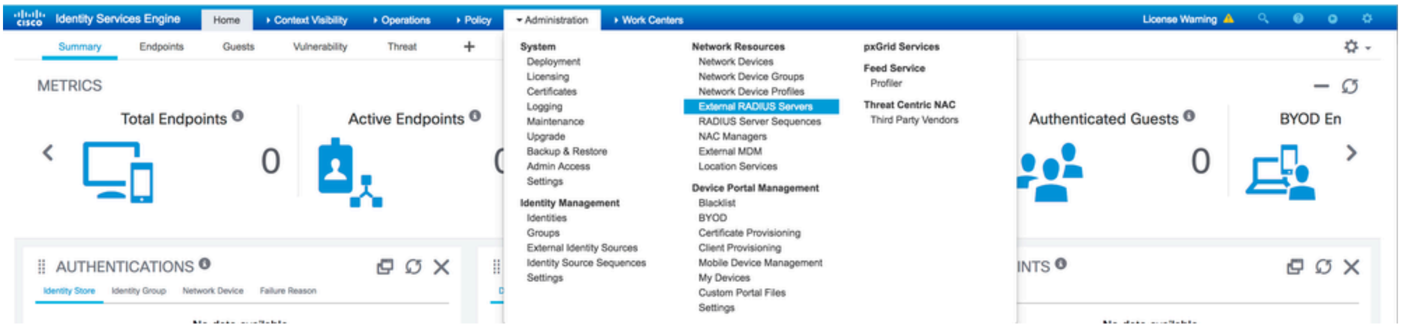
Configure

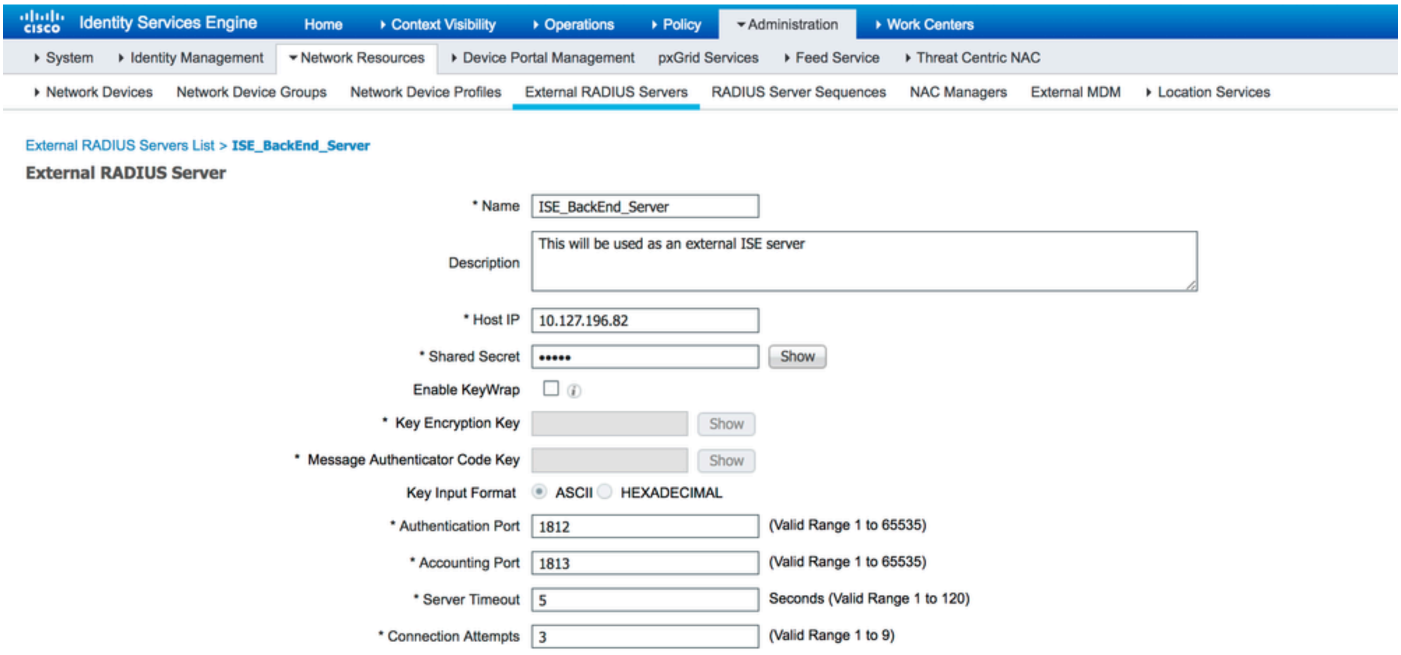
Network Diagram



Configure ISE (Frontend Server)

Step 1. Multiple external RADIUS servers can be configured and used in order to authenticate users on the ISE. In order to configure external RADIUS servers, navigate to Administration > Network Resources > External RADIUS Servers > Add, as shown in the image:



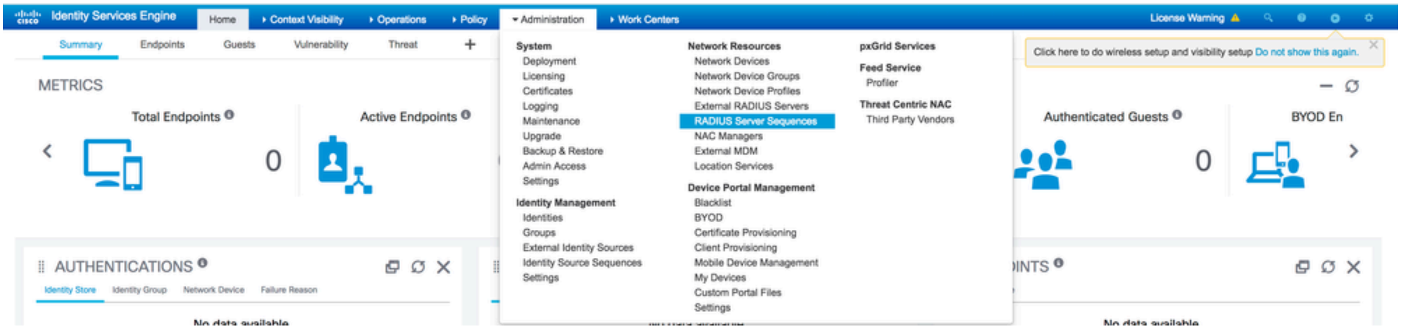


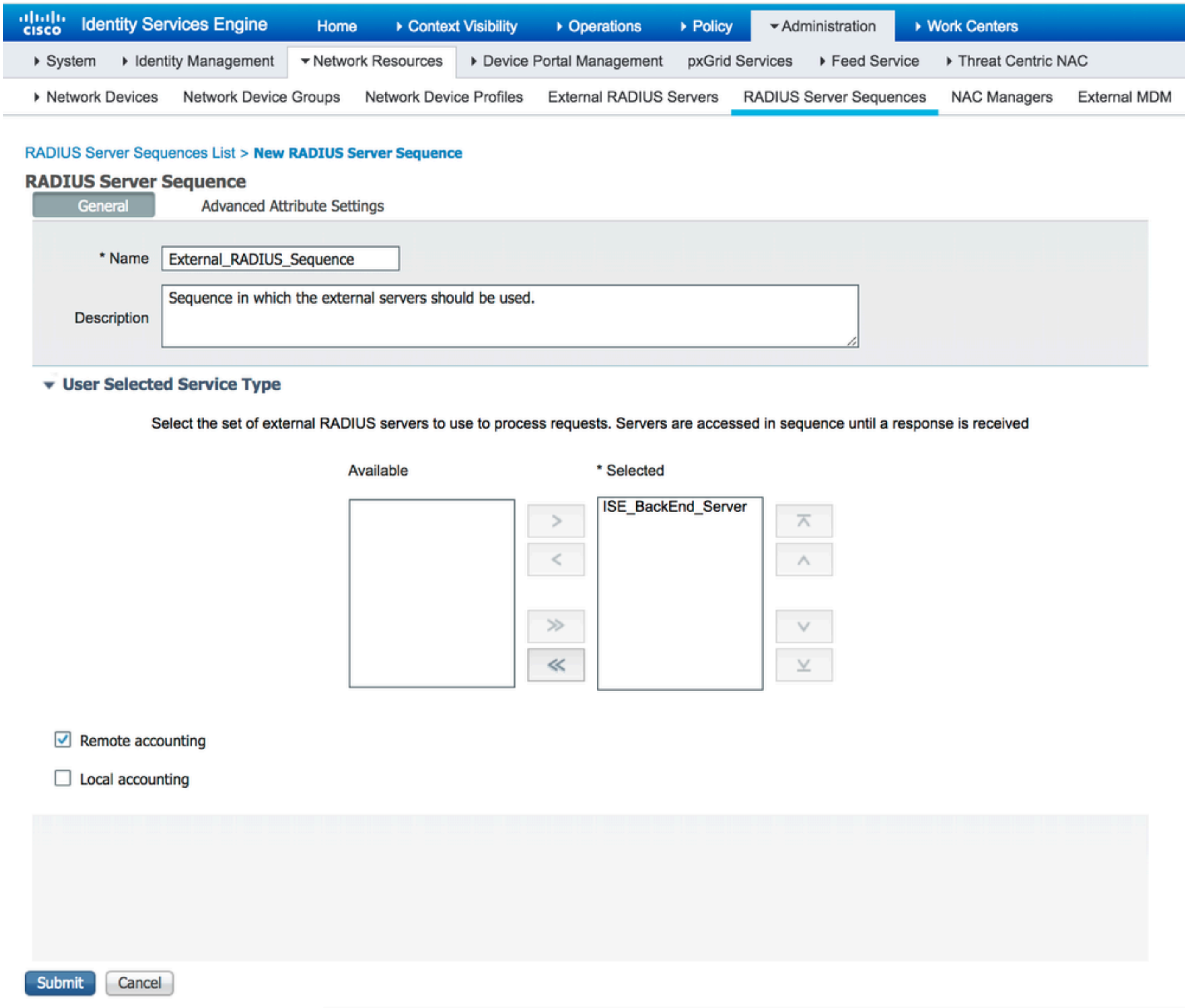
External RADIUS Servers List > ISE_BackEnd_Server

External RADIUS Server

* Name	ISE_BackEnd_Server
Description	This will be used as an external ISE server
* Host IP	10.127.196.82
* Shared Secret	•••••
Enable KeyWrap	□
* Key Encryption Key	
* Message Authenticator Code Key	
Key Input Format	● ASCII ○ HEXADECIMAL
* Authentication Port	1812 (Valid Range 1 to 65535)
* Accounting Port	1813 (Valid Range 1 to 65535)
* Server Timeout	5 Seconds (Valid Range 1 to 120)
* Connection Attempts	3 (Valid Range 1 to 9)

Step 2. In order to use the configured external RADIUS server, a RADIUS server sequence must be configured similar to the Identity source sequence. In order to configure the same, navigate to Administration > Network Resources > RADIUS Server Sequences > Add, as shown in the image:





RADIUS Server Sequence

* Name: External_RADIUS_Sequence

Description: Sequence in which the external servers should be used.

User Selected Service Type

Select the set of external RADIUS servers to use to process requests. Servers are accessed in sequence until a response is received

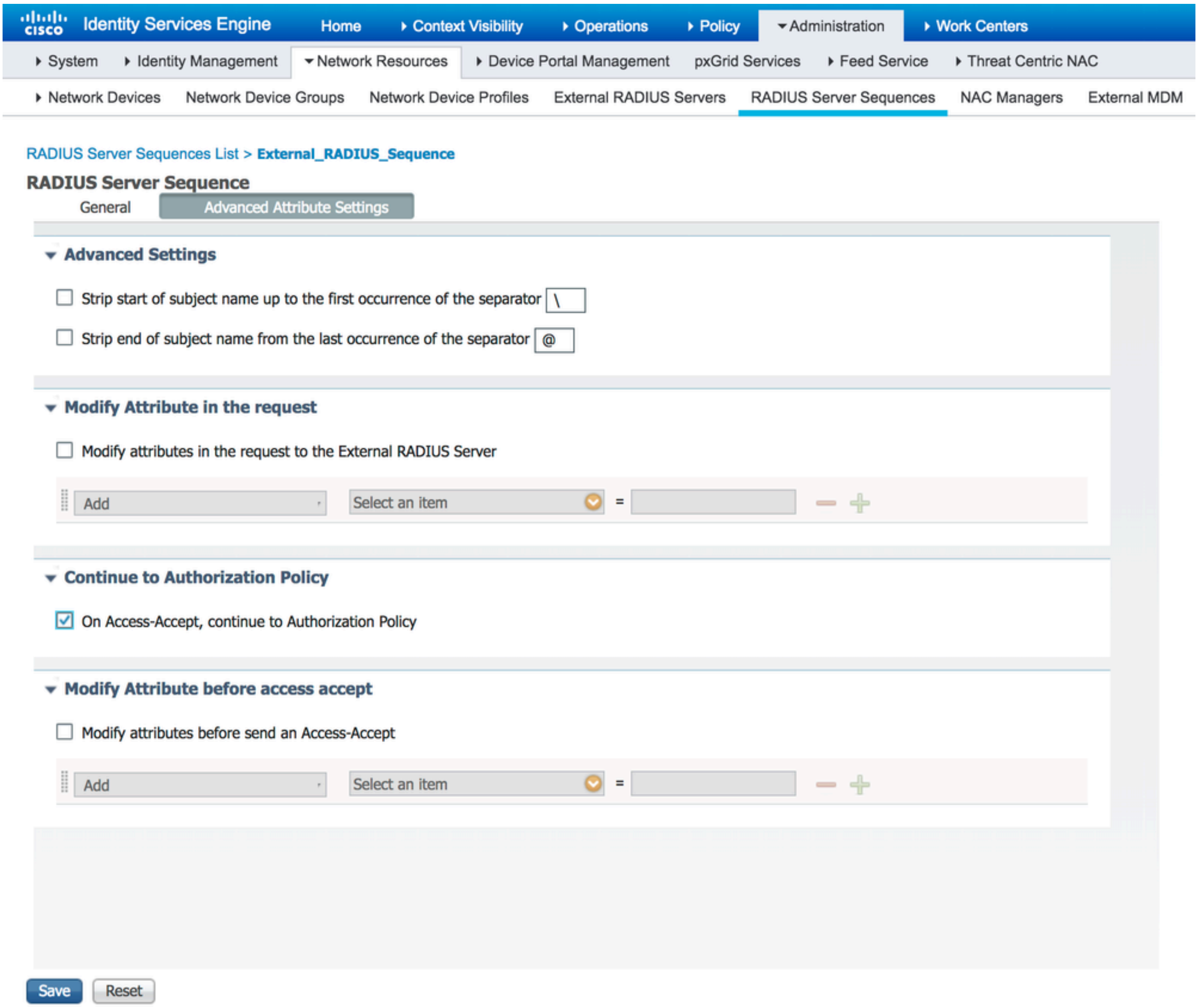
* Selected: ISE_BackEnd_Server

☑ Remote accounting

□ Local accounting

Note: One of the options available while the server sequence is created is to choose whether accounting must be done locally on the ISE or on the external RADIUS server. Based on the option chosen here, ISE decides on whether to proxy the accounting requests or store those logs locally.

Step 3. There is an additional section that gives more flexibility on how ISE must behave when it proxies requests to external RADIUS servers. It can be found under Advance Attribute Settings, as shown in the image:



RADIUS Server Sequences List > **External_RADIUS_Sequence**

RADIUS Server Sequence

Advanced Settings

□ Strip start of subject name up to the first occurrence of the separator \

□ Strip end of subject name from the last occurrence of the separator @

Modify Attribute in the request

□ Modify attributes in the request to the External RADIUS Server

Add | Select an item | =

Continue to Authorization Policy

☑ On Access-Accept, continue to Authorization Policy

Modify Attribute before access accept

□ Modify attributes before send an Access-Accept

Add | Select an item | =

- Advanced Settings: Provides options to strip the start or the end of the username in RADIUS requests with a delimiter.
- Modify Attribute in the request: Provides the option to modify any RADIUS attribute in the RADIUS requests. The list here shows the attributes that can be added/removed/updated:

```
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]
```

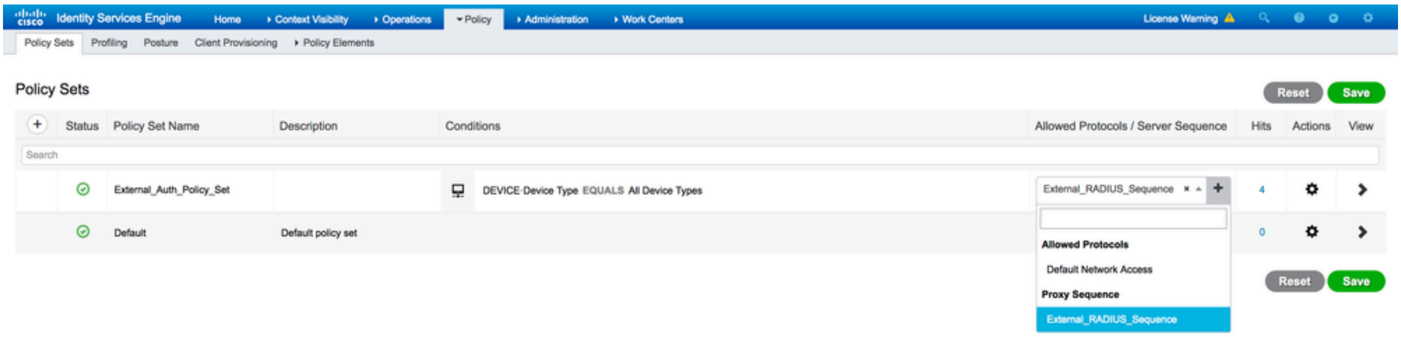
```
Login-LAT-Service--[34]
Login-LAT-Node--[35]
Login-LAT-Group--[36]
Event-Timestamp--[55]
Egress-VLANID--[56]
Ingress-Filters--[57]
Egress-VLAN-Name--[58]
User-Priority-Table--[59]
NAS-Port-Type--[61]
Port-Limit--[62]
Login-LAT-Port--[63]
Password-Retry--[75]
Connect-Info--[77]
NAS-Port-Id--[87]
Framed-Pool--[88]
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: Provides an option to choose if ISE must just send the Access-Accept as it is or proceed to provide access based on the Authorization Policies configured on the ISE rather than the authorization provided by the external RADIUS server. If this option is selected, the authorization provided by the external RADIUS server is overwritten with the authorization provided by ISE.

  Note: This option works only if the external RADIUS server sends an Access-Accept in response to the proxied RADIUS Access-Request.

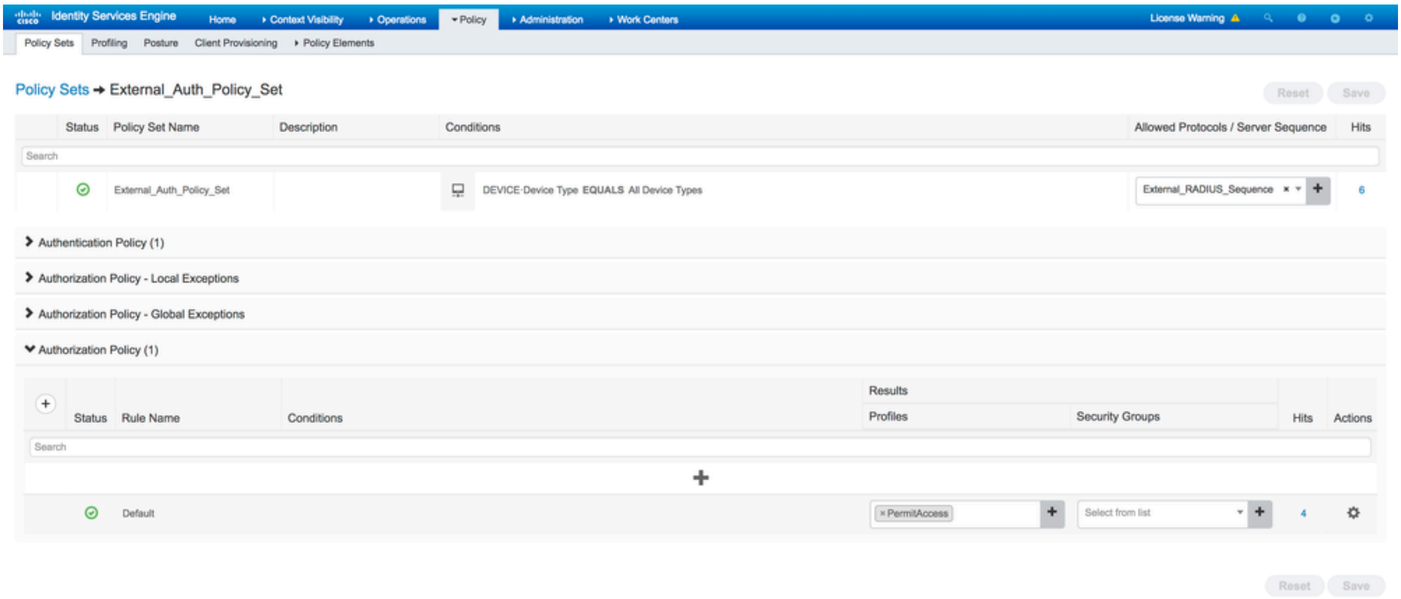
- Modify Attribute before Access-Accept: Similar to the Modify Attribute in the request, the attributes mentioned earlier can be added/removed/updated present in the Access-Accept sent by the external RADIUS server before it is sent to the network device.

Step 4. The next part is to configure the Policy Sets in order to use the RADIUS Server Sequence instead of Allowed Protocols so that the requests are sent to the external RADIUS server. It can be configured under Policy > Policy Sets. Authorization policies can be configured under the Policy Set but only come into effect if the Continue to Authorization Policy on Access-Accept option is chosen. If not, ISE simply acts as a proxy for the RADIUS requests in order to match the conditions configured for this Policy Set.



Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	External_Auth_Policy_Set		DEVICE·Device Type EQUALS All Device Types	External_RADIUS_Sequence	4	⚙	>
✓	Default	Default policy set			0	⚙	>



Policy Sets → External_Auth_Policy_Set

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	External_Auth_Policy_Set		DEVICE·Device Type EQUALS All Device Types	External_RADIUS_Sequence	6

> Authentication Policy (1)

> Authorization Policy - Local Exceptions

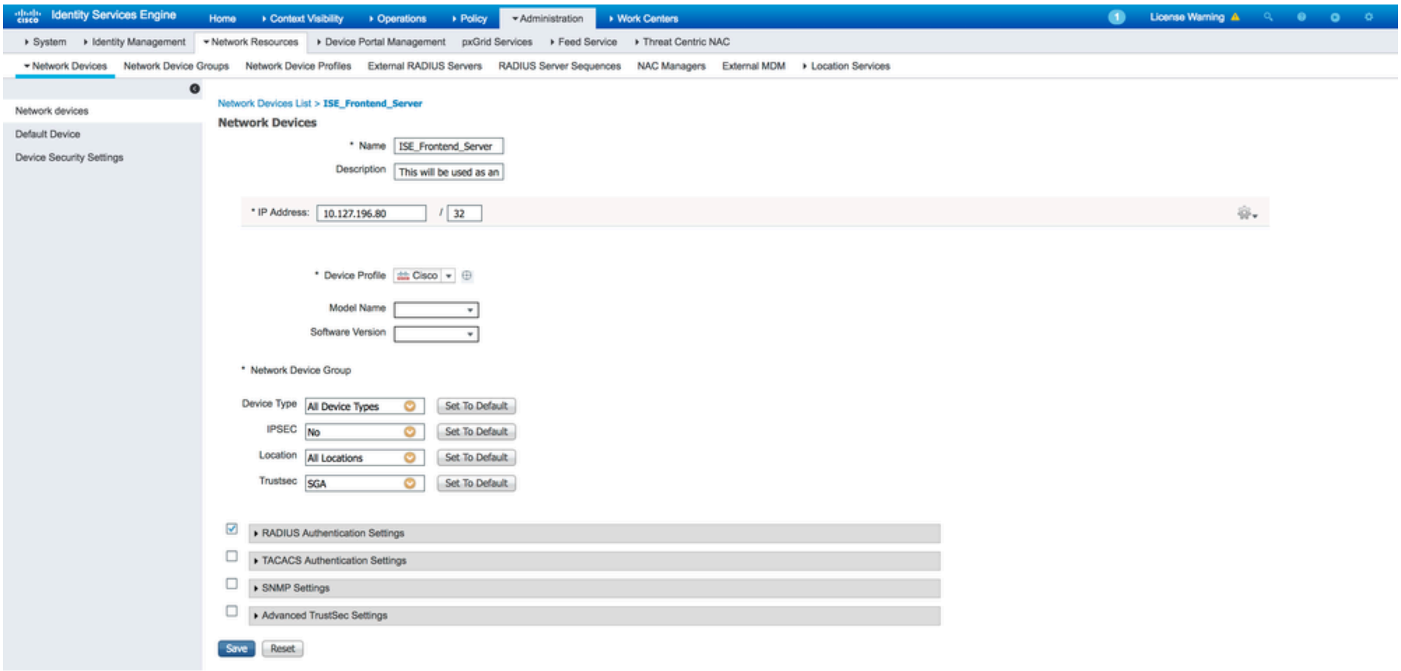
> Authorization Policy - Global Exceptions

Authorization Policy (1)

Status	Rule Name	Conditions	Results Profiles	Security Groups	Hits	Actions
✓	Default		×PermitAccess	Select from list	4	⚙

Configure the External RADIUS Server

Step 1. In this example, another ISE server (version 2.2) is used as an external RADIUS server named ISE_Backend_Server. The ISE (ISE_Frontend_Server) must be configured as a network device or traditionally called NAS in the external RADIUS server (ISE_Backend_Server in this example), since the NAS-IP-Address attribute in the Access-Request that is forwarded to the external RADIUS server is replaced with the IP address of theISE_Frontend_Server. The shared secret to be configured is the same as the one configured for the external RADIUS server on the ISE_Frontend_Server.



Network Devices List > ISE_Frontend_Server

Network Devices

* Name: ISE_Frontend_Server

Description: This will be used as an

* IP Address: 10.127.196.80 / 32

* Device Profile: Cisco

Model Name:

Software Version:

* Network Device Group

Device Type	All Device Types	Set To Default
IPSEC	No	Set To Default
Location	All Locations	Set To Default
Trustsec	SGA	Set To Default

☑ RADIUS Authentication Settings

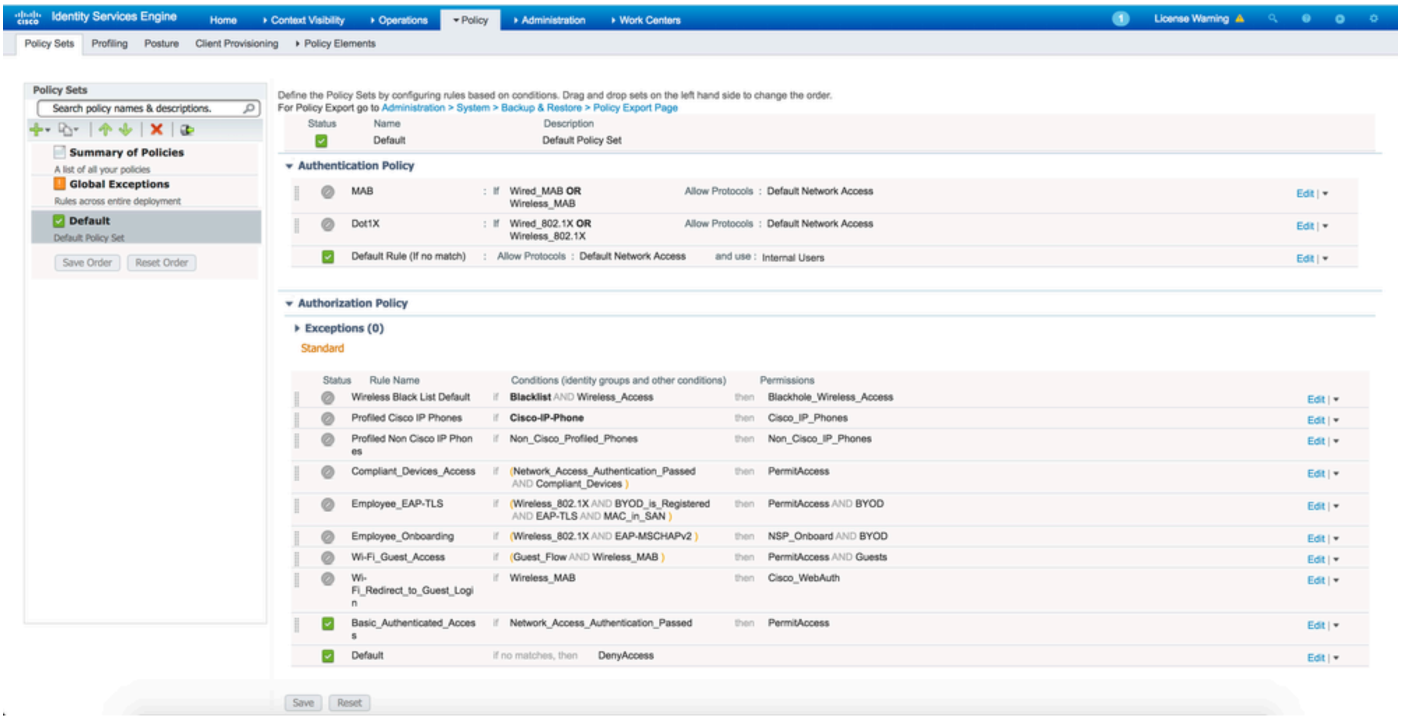
□ TACACS Authentication Settings

□ SNMP Settings

□ Advanced TrustSec Settings

Save Reset

Step 2. The external RADIUS server can be configured with its own authentication and authorization policies in order to serve the requests proxied by the ISE. In this example, a simple policy is configured in order to check the user in the internal users and then permit access if authenticated.



Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Status	Name	Description
✓	Default	Default Policy Set

Authentication Policy

MAB	If	Wired_MAB OR Wireless_MAB	Allow Protocols : Default Network Access	Edit
Dot1X	If	Wired_802.1X OR Wireless_802.1X	Allow Protocols : Default Network Access	Edit
Default Rule (If no match)		Allow Protocols : Default Network Access	and use : Internal Users	Edit

Authorization Policy

Exceptions (0)

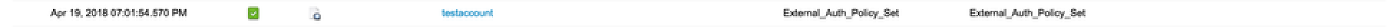
Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
⊘	Wireless Black List Default	if	Blacklist AND Wireless_Access	then	Blackhole_Wireless_Access	Edit
⊘	Profiled Cisco IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phones	Edit
⊘	Profiled Non Cisco IP Phones	if	Non_Cisco_Profiled_Phones	then	Non_Cisco_IP_Phones	Edit
⊘	Compliant_Devices_Access	if	(Network_Access_Authentication_Passed AND Compliant_Devices)	then	PermitAccess	Edit
⊘	Employee_EAP-TLS	if	(Wireless_802.1X AND BYOD_is_Registered AND EAP-TLS AND MAC_in_SAN)	then	PermitAccess AND BYOD	Edit
⊘	Employee_Onboarding	if	(Wireless_802.1X AND EAP-MSCHAPv2)	then	NSP_Onboard AND BYOD	Edit
⊘	Wi-Fi_Guest_Access	if	(Guest_Flow AND Wireless_MAB)	then	PermitAccess AND Guests	Edit
⊘	Wi-Fi_Redirect_to_Guest_Login	if	Wireless_MAB	then	Cisco_WebAuth	Edit
✓	Basic_Authenticated_Access	if	Network_Access_Authentication_Passed	then	PermitAccess	Edit
✓	Default	if no matches, then	DenyAccess			Edit

Save Reset

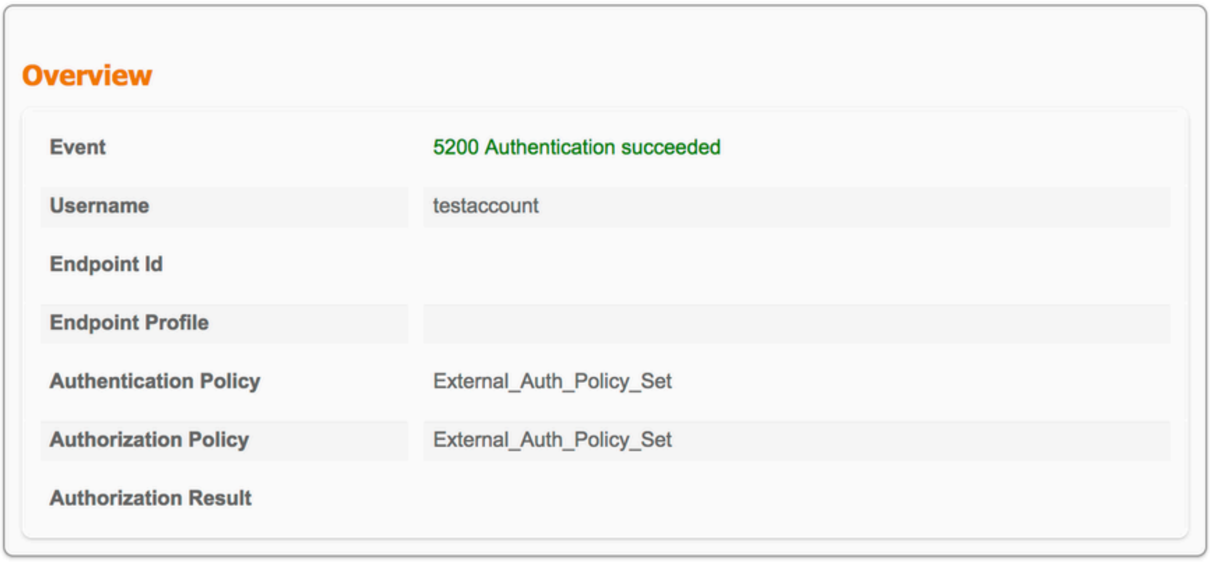
Verify

Step 1. Check ISE live logs if the request is received, as shown in the image.



```
Apr 19, 2018 07:01:54.570 PM    ✓    testaccount    External_Auth_Policy_Set    External_Auth_Policy_Set
```

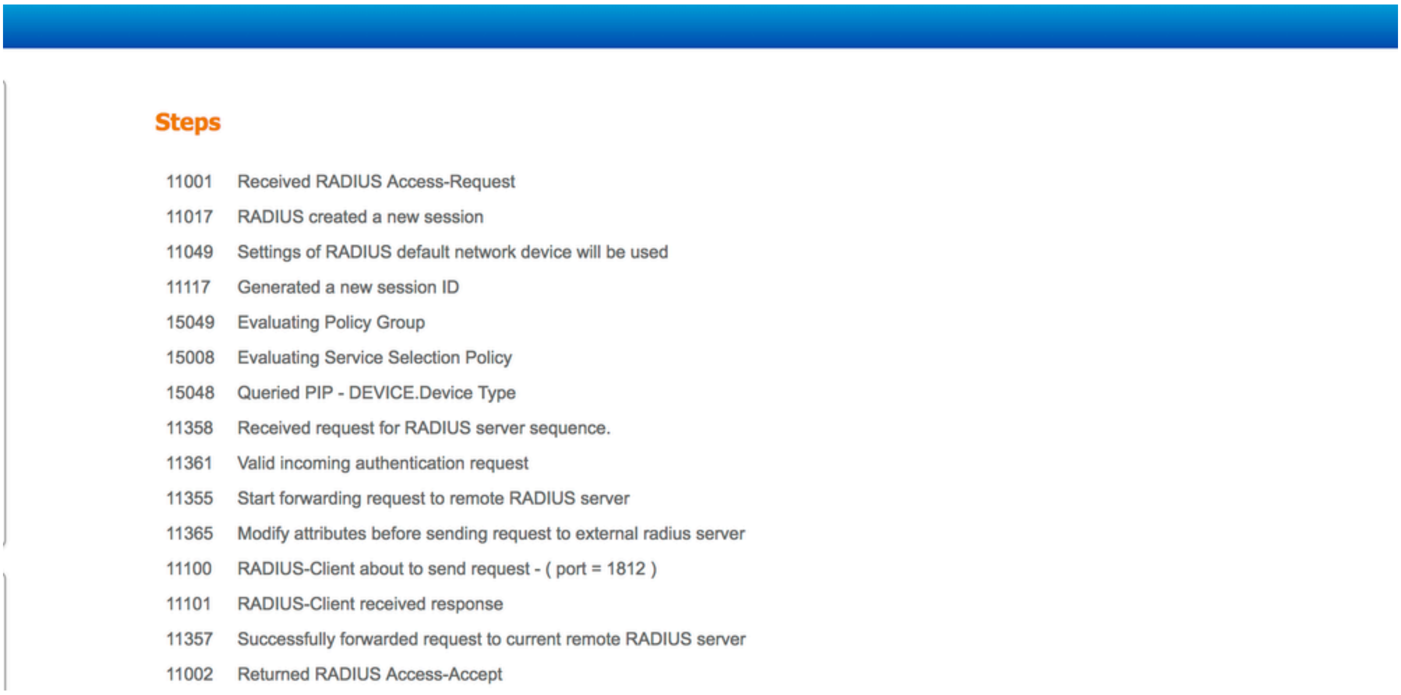
Step 2. Check if the correct policy set is selected, as shown in the image.



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	

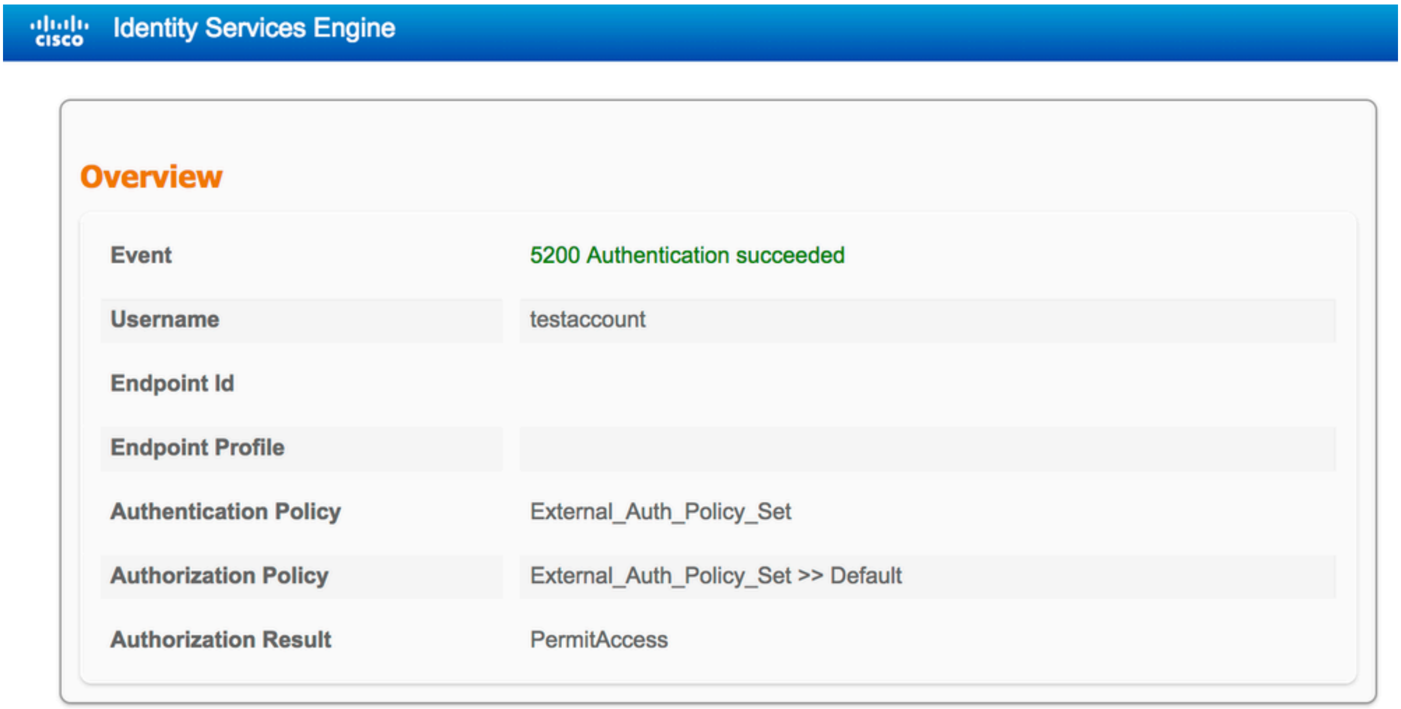
Step 3. Check if the request is forwarded to the external RADIUS server.



Steps

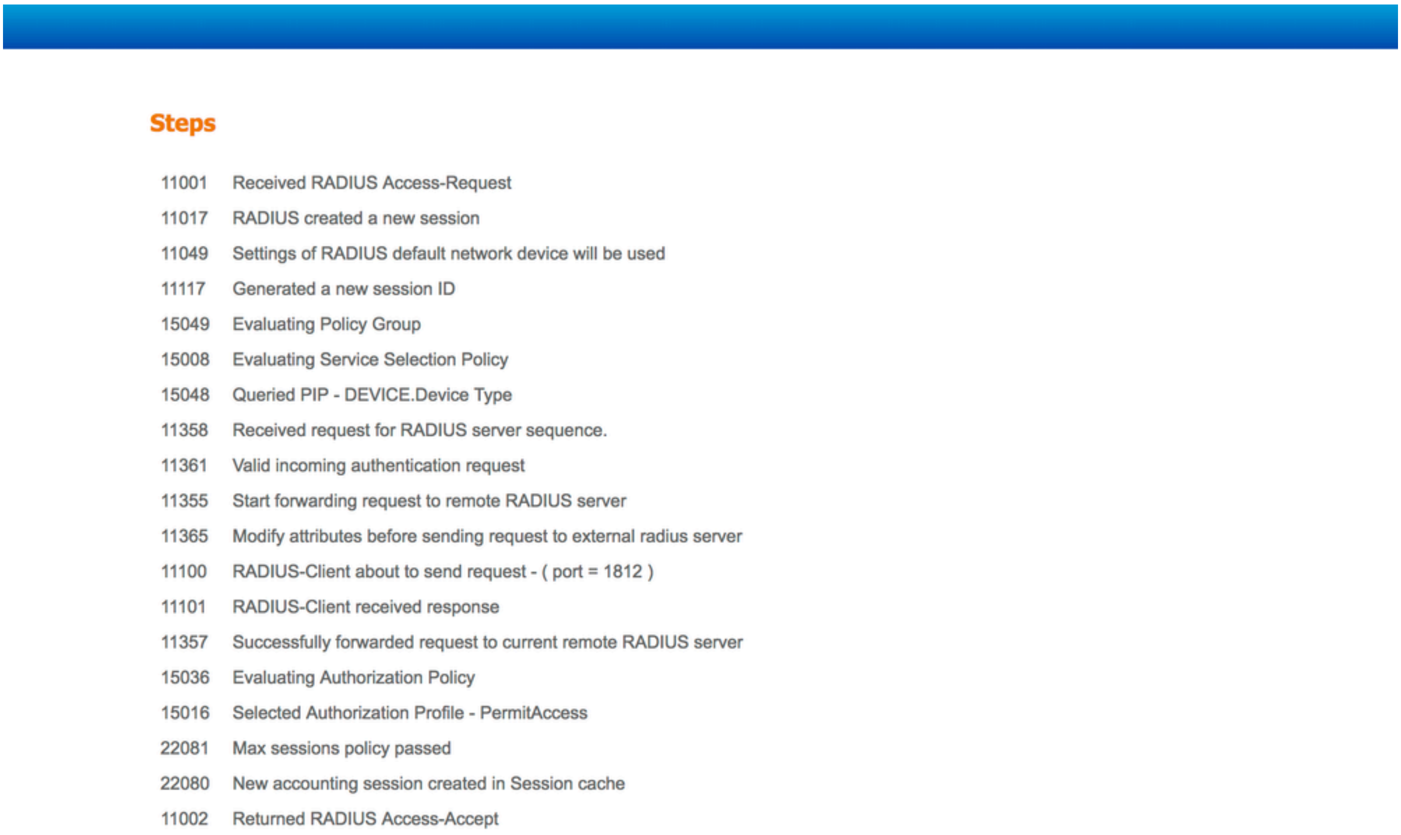
11001	Received RADIUS Access-Request
11017	RADIUS created a new session
11049	Settings of RADIUS default network device will be used
11117	Generated a new session ID
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15048	Queried PIP - DEVICE.Device Type
11358	Received request for 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)
11101	RADIUS-Client received response
11357	Successfully forwarded request to current remote RADIUS server
11002	Returned RADIUS Access-Accept

4. If the Continue to Authorization Policy on Access-Accept option is chosen, check if the authorization policy is evaluated.



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

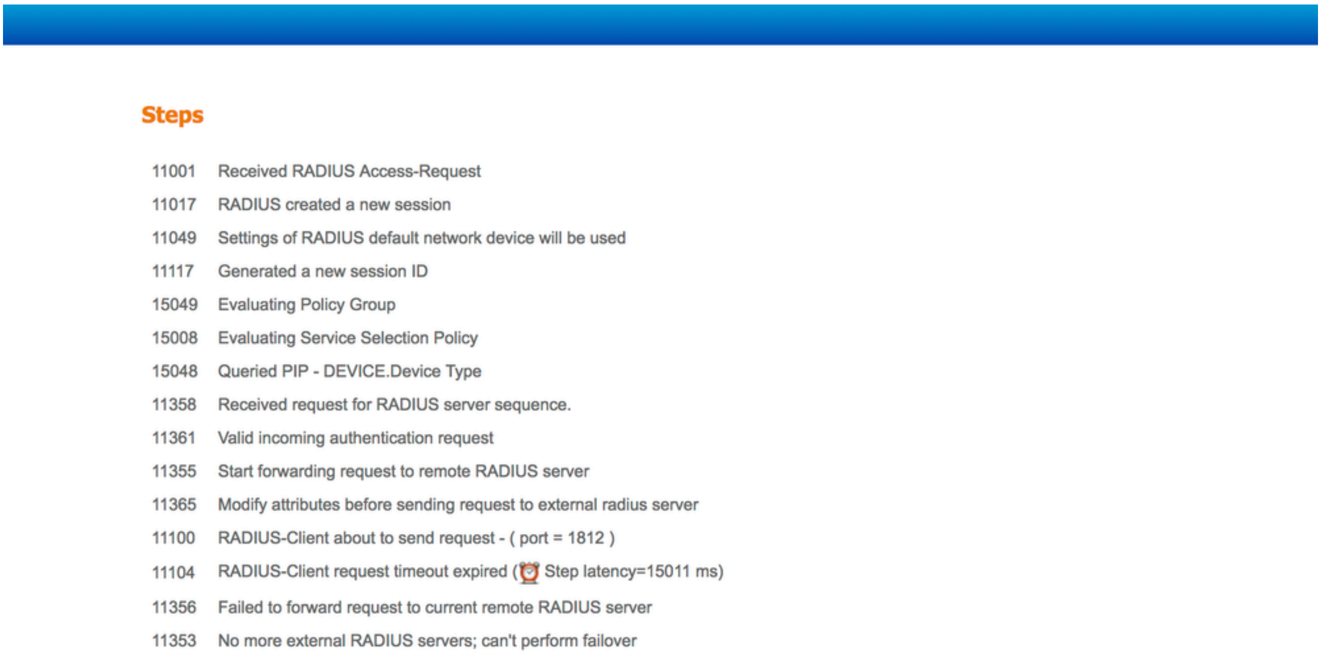
11001	Received RADIUS Access-Request
11017	RADIUS created a new session
11049	Settings of RADIUS default network device will be used
11117	Generated a new session ID
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15048	Queried PIP - DEVICE.Device Type
11358	Received request for 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

Troubleshoot

Scenario 1. Event - 5405 RADIUS Request Dropped

- The most important thing that must be verified is the steps in the detailed authentication report. If the steps say the "**RADIUS-Client request timeout expired**", it means that the ISE did not receive any response from the configured external RADIUS server. This can happen when:

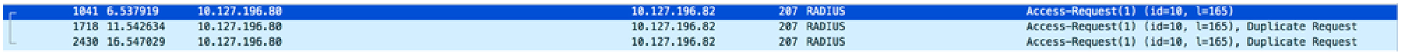
1. There is a connectivity issue with the external RADIUS server. ISE is unable to reach the external RADIUS server on the ports configured for it.
2. ISE is not configured as a Network Device or NAS on the external RADIUS Server.
3. Packets are dropped by the external RADIUS Server either by configuration or because of some problem on the external RADIUS server.



Steps

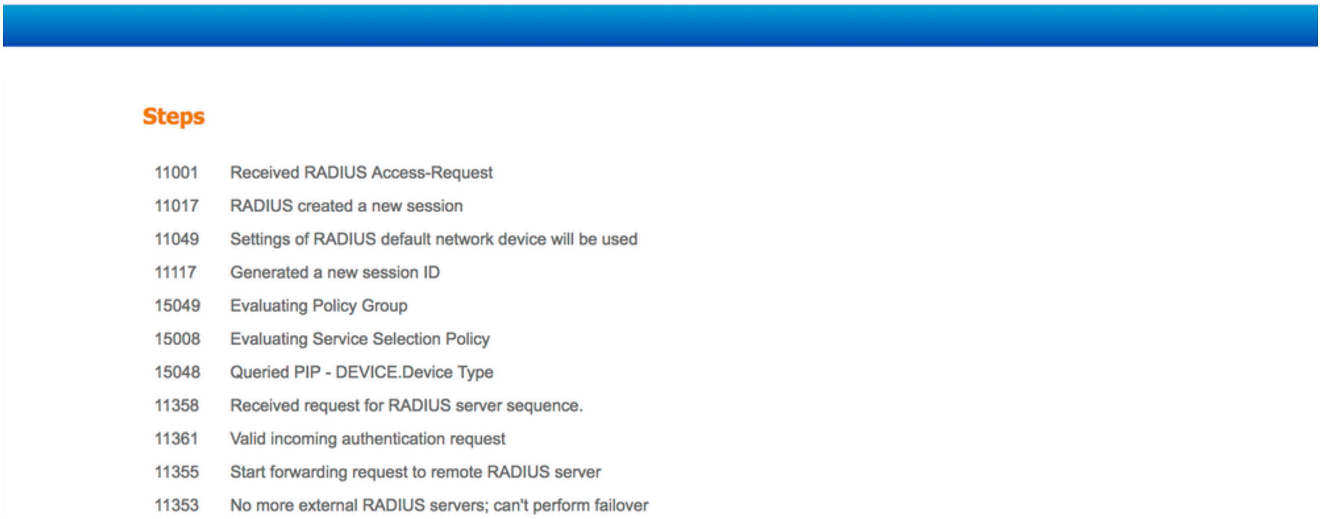
```
11001   Received RADIUS Access-Request
11017   RADIUS created a new session
11049   Settings of RADIUS default network device will be used
11117   Generated a new session ID
15049   Evaluating Policy Group
15008   Evaluating Service Selection Policy
15048   Queried PIP - DEVICE.Device Type
11358   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
```

Check packet captures as well in order to see if it is not a false message; that is, ISE receives the packet back from the server but still reports that the request timed out.



```
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
```

- If the steps say "**Start forwarding request to remote RADIUS server"** and the immediate step is "**No more external RADIUS servers; cannot perform failover"**, it means that all the configured external RADIUS servers are currently marked **dead** and the requests are only served after the dead timer expires.



Steps

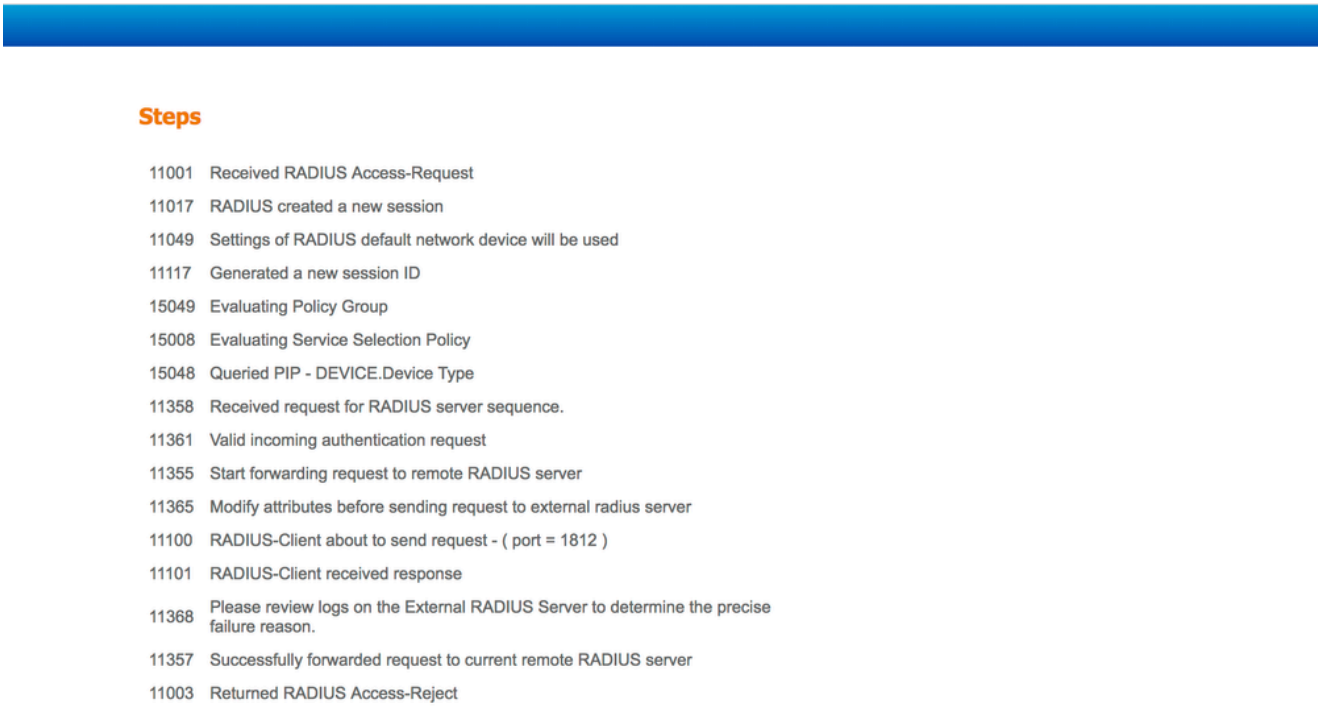
```
11001   Received RADIUS Access-Request
11017   RADIUS created a new session
11049   Settings of RADIUS default network device will be used
11117   Generated a new session ID
15049   Evaluating Policy Group
15008   Evaluating Service Selection Policy
15048   Queried PIP - DEVICE.Device Type
11358   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
```

Note: The default **dead time** for external RADIUS Servers in ISE is **5 minutes**. This value is hardcoded and cannot be modified as of this version.

- If the steps say "**RADIUS-Client encountered error during processing flow"** and are followed by **"Failed to forward request to current remote RADIUS server; an invalid response was received"**, it means that ISE has encountered a problem while the request to the external RADIUS server was forwarded. This is usually seen when the RADIUS request sent from the Network Device/NAS to the ISE does not have the **NAS-IP-Address** as one of the attributes. If there is no **NAS-IP-Address** attribute and if external RADIUS servers are not in use, ISE populates the **NAS-IP-Address** field with the source IP of the packet. However, this does not apply when an external RADIUS server is in use.

Scenario 2. Event - 5400 Authentication Failed

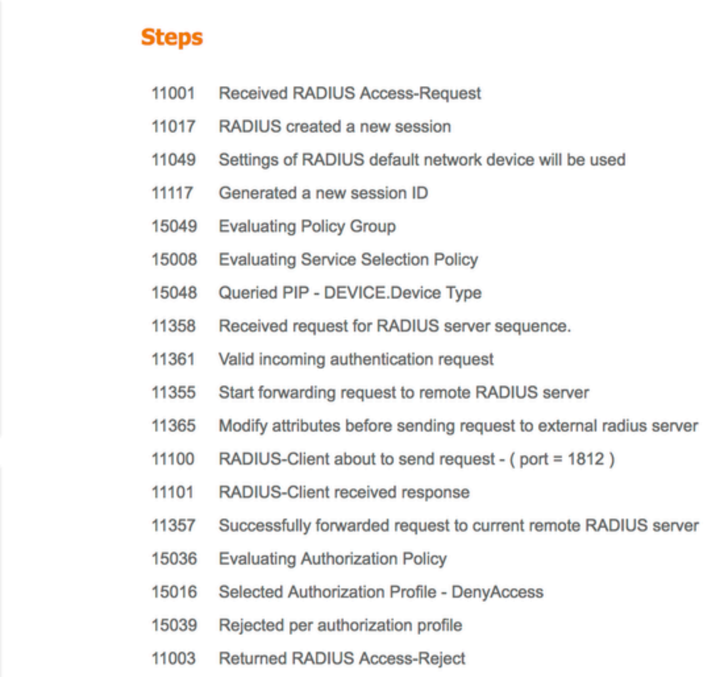
- In this event, if the steps say **"11368 Please review logs on the External RADIUS Server to determine the precise failure reason"**, it means that the authentication has failed on the external RADIUS server itself and it has sent an Access-Reject.



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
```

- If the steps say "**15039 Rejected per authorization profile"**, it means that ISE received an Access-Accept from the external RADIUS server but ISE rejects the authorization based on the authorization policies configured.



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

- If the **Failure Reason** on the ISE is anything else apart from the ones mentioned here in case of an authentication failure, then it can mean a potential issue with the configuration or with the ISE itself. A TAC case is recommended to be opened at this point.