

# ISE での外部 Radius サーバの設定

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[ISE \(フロントエンドサーバ\) の設定](#)

[外部RADIUSサーバの設定](#)

[確認](#)

[トラブルシューティング](#)

[シナリオ 1. イベント - 5405 Radius 要求のドロップ](#)

[シナリオ 2. イベント - 5400 認証の失敗](#)

---

## はじめに

このドキュメントでは、プロキシおよび認可サーバとしてのISE上のRADIUSサーバの設定について説明します。ここでは、2台のISEサーバが使用され、1台は外部サーバとして機能します。ただし、任意のRFC準拠RADIUSサーバを使用できます。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- RADIUSプロトコルの基礎知識
- Identity Services Engine(ISE)ポリシー設定に関する専門知識

### 使用するコンポーネント

このドキュメントの情報は、Cisco ISEバージョン2.2および2.4に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

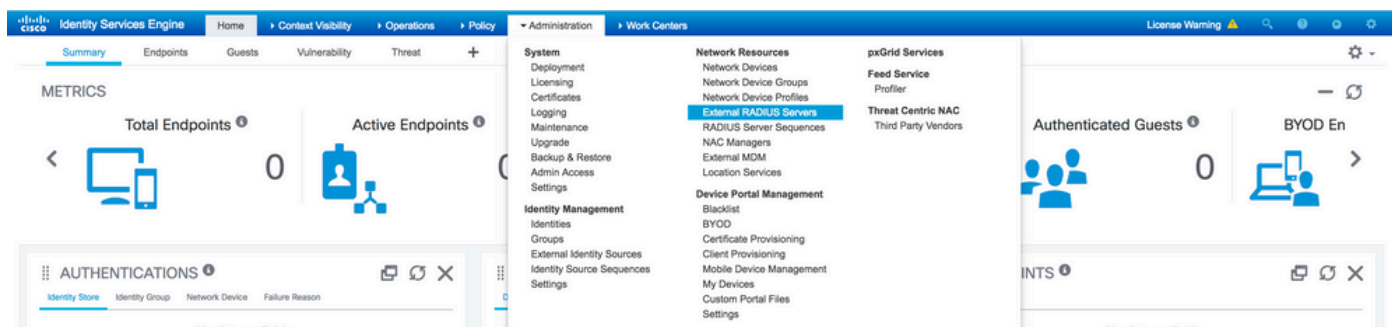
## 設定

## ネットワーク図



## ISE ( フロントエンドサーバ ) の設定

ステップ 1 : ISEでユーザを認証するために、複数の外部RADIUSサーバを設定して使用できます。外部RADIUSサーバを設定するには、Administration > Network Resources > External RADIUS Servers > Addを参照してください ( 図を参照 )。



The screenshot shows the 'External RADIUS Server' configuration form in the Cisco Identity Services Engine (ISE) Administration console. The form includes the following fields and values:

- Name: ISE\_BackEnd\_Server
- Description: This will be used as an external ISE server
- Host IP: 10.127.196.82
- Shared Secret: [Redacted]
- Enable KeyWrap: [Unchecked]
- Key Encryption Key: [Redacted]
- Message Authenticator Code Key: [Redacted]
- Key Input Format: ASCII (Selected)
- 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)

ステップ 2 : 設定済みの外部RADIUSサーバを使用するには、RADIUSサーバシーケンスをアイデンティティソースシーケンスと同様に設定する必要があります。同じものを設定するには、Administration > Network Resources > RADIUS Server Sequences > Addを参照してください。

[RADIUS Server Sequences List](#) > [New RADIUS Server Sequence](#)

### RADIUS Server Sequence

General      Advanced Attribute Settings

\* Name

Description

#### ▼ 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

Available		* Selected	
	>	ISE_BackEnd_Server	↑
	<		↓
	>>		⇩
	<<		⇧

- Remote accounting
- Local accounting

注：サーブシーケンスの作成時に使用できるオプションの1つは、アカウントリングをISEでローカルに実行するか、外部RADIUSサーバで実行するかを選択することです。ここで選択したオプションに基づいて、ISEはアカウントリング要求をプロキシするか、これらのログをローカルに保存するかを決定します。

ステップ 3：外部RADIUSサーバに要求をプロキシする際のISEの動作方法をより柔軟にする追加のセクションがあります。これは次の場所にあります。 [Advance Attribute Settings](#) を参照してください。

RADIUS Server Sequences List > External\_RADIUS\_Sequence

### RADIUS Server Sequence

General **Advanced Attribute Settings**

#### 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 =  - +

Save Reset

- 詳細設定：デリミタを使用してRADIUS要求のユーザ名の先頭または末尾を削除するオプションを提供します。
- Modify Attribute in the request:RADIUS要求のRADIUS属性を変更するオプションを提供します。次のリストに、追加、削除、または更新できる属性を示します。


```

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]

- Access-Acceptで認証ポリシーに進む：ISEがAccess-Acceptをそのまま送信するか、外部RADIUSサーバによって提供される認証ではなく、ISEで設定された認証ポリシーに基づいてアクセスを提供するために進むかを選択するオプションを提供します。このオプションを選択すると、外部RADIUSサーバによって提供された認可は、ISEによって提供された認可で上書きされます。

---

 注：このオプションは、外部RADIUSサーバが Access-Accept プロキシされる RADIUS Access-Requestに応答します。

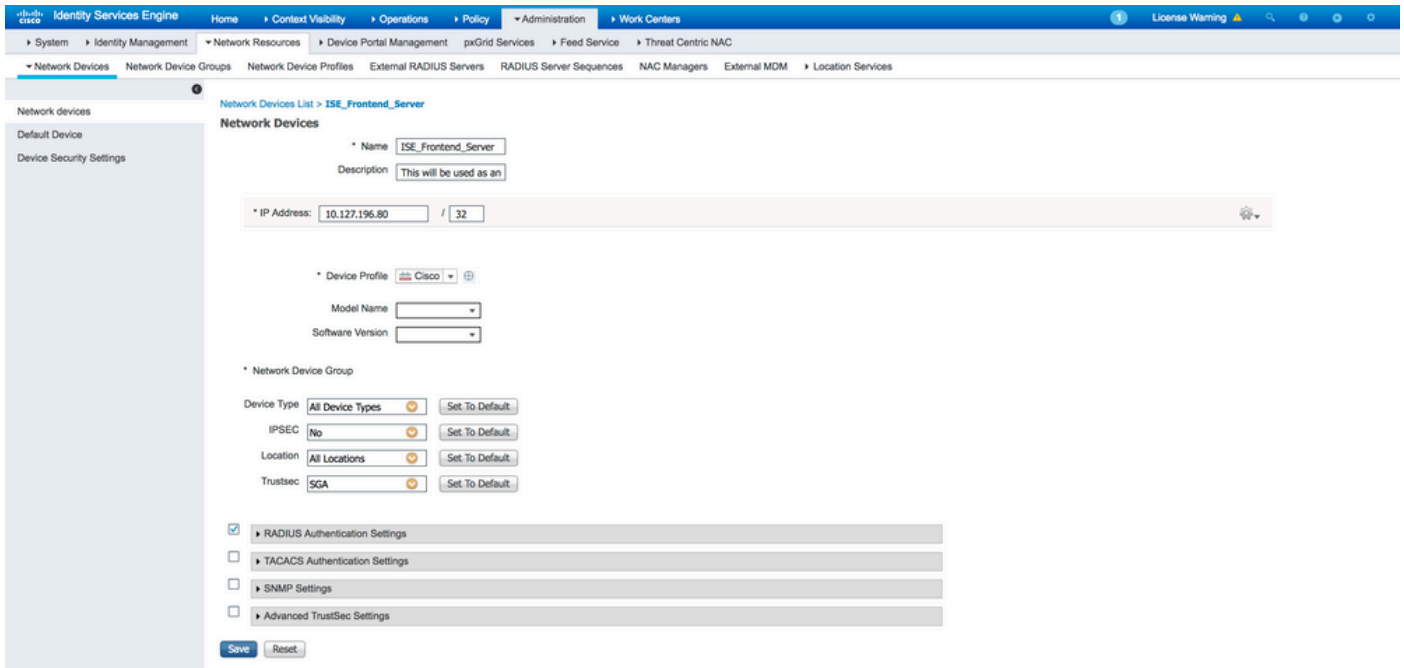
---

- Modify Attribute before Access-Accept：コマンドと同様に、Modify Attribute in the request外部RADIUSサーバからネットワークデバイスに送信される前に、外部RADIUSサーバから送信されるAccess-Acceptに含まれる前述の属性の追加、削除、更新を行うことができます。

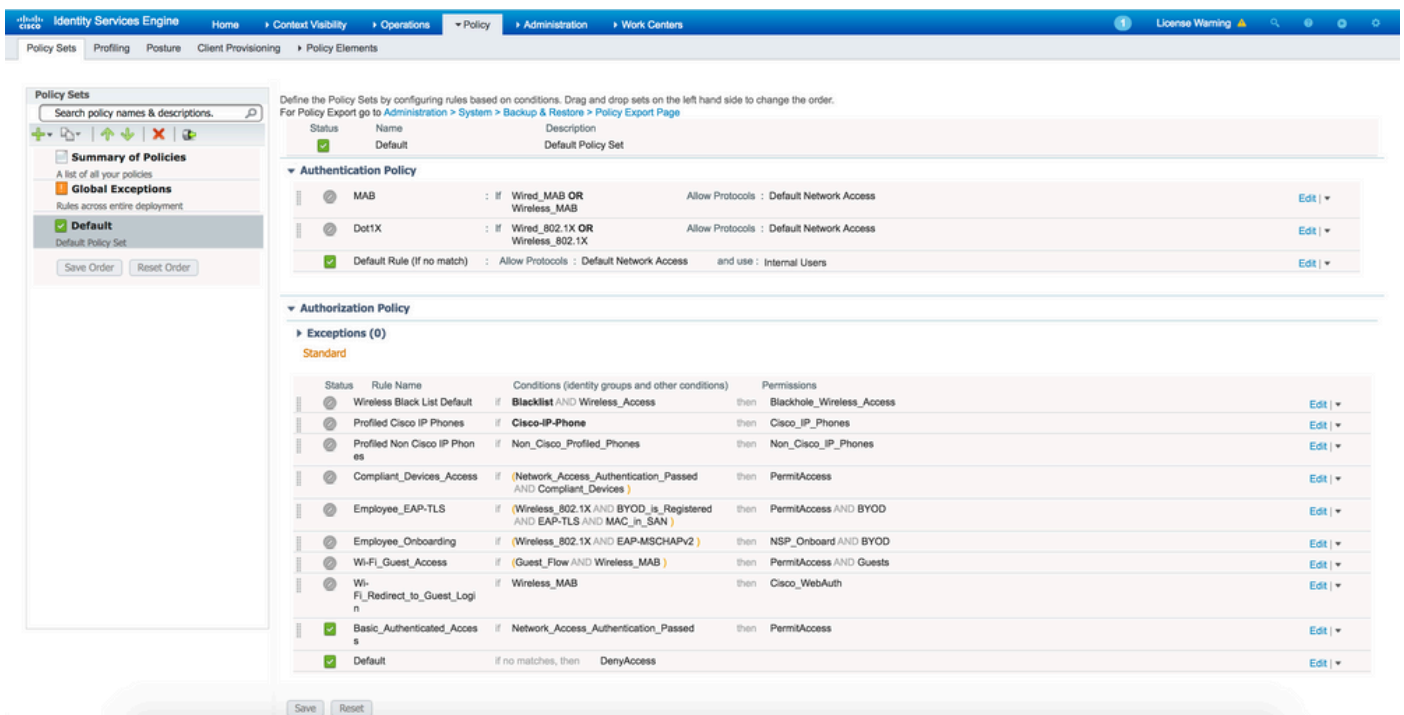
ステップ 4：次に、要求が外部RADIUSサーバに送信されるように、Allowed Protocolsの代わりにRADIUSサーバシーケンスを使用するようにポリシーセットを設定します。これは次の場所で設定できます。 Policy > Policy Setsを参照。許可ポリシーは、Policy Set ただし、この機能が有効になるのは、Continue to Authorization Policy on Access-Accept オプションが選択されます。そうでない場合、ISEは、このポリシーセットに設定された条件に一致するように、RADIUS要求のプロキシとして機能します。

## 外部RADIUSサーバの設定

ステップ 1: この例では、別のISEサーバ (バージョン2.2) が外部RADIUSサーバとして使用され、ISE\_Backend\_Serverを参照。ISE(ISE\_Frontend\_Server)をネットワークデバイスとして設定するか、従来は外部RADIUSサーバでNASと呼ばれていた(ISE\_Backend\_Server この例では)、NAS-IP-Address 外部RADIUSサーバに転送されるAccess-Request内の属性は、WLCのIPアドレスISE\_Frontend\_Serverを参照。設定する共有秘密は、WLCの外部RADIUSサーバに設定されているものと同じです。ISE\_Frontend\_Serverを参照。

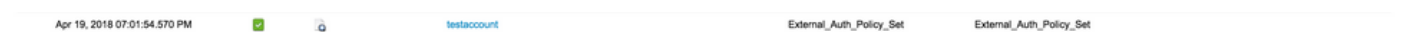


ステップ 2 : ISEによってプロキシされる要求を処理するために、外部RADIUSサーバに独自の認証および認可ポリシーを設定できます。この例では、内部ユーザのユーザを確認し、認証された場合はアクセスを許可する単純なポリシーが設定されています。



## 確認

ステップ 1 : 図に示すように、要求を受信した場合はISEライブログを確認します。



ステップ 2 : 図に示すように、正しいポリシーセットが選択されているかどうかを確認します。

## 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**

ステップ 3 : 要求が外部RADIUSサーバに転送されるかどうかを確認します。

## 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. Continue to Authorization Policy on Access-Accept オプションを選択し、認可ポリシーが評価されているかどうかを確認します。



## Overview

<b>Event</b>	5200 Authentication succeeded
<b>Username</b>	testaccount
<b>Endpoint Id</b>	
<b>Endpoint Profile</b>	
<b>Authentication Policy</b>	External_Auth_Policy_Set
<b>Authorization Policy</b>	External_Auth_Policy_Set >> Default
<b>Authorization Result</b>	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
  
```

## トラブルシューティング

### シナリオ 1. イベント - 5405 Radius 要求のドロップ

- 確認する必要がある最も重要なことは、詳細な認証レポートの手順です。この手順で RADIUS-Client request timeout expired と表示された場合、ISE は設定された外部 Radius サーバから応答を受信していません。これは次の場合に発生します。

1. 外部 Radius サーバとの接続に問題があります。設定されているポートで ISE が外部 Radius サーバに到達できません。
2. ISE が外部 Radius サーバのネットワークデバイスまたは NAS として設定されていません。
3. 設定または外部RADIUSサーバでの何らかの問題により、外部RADIUSサーバによってパケットが廃棄されます。

### 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

```

パケットキャプチャも確認して、これが偽のメッセージでないか、つまりISEがサーバからパケットを受信しているものの、要求がタイムアウトしたことを報告しているかを確認します。

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


- 手順に示されている場合 Start forwarding request to remote RADIUS server すぐに行うべきステップは – No more external RADIUS servers; can't perform failover、次に、設定されたすべての外部RADIUSサーバが現在deadとマークされ、deadタイマーが時間切れになった後にのみ要求が処理されることを意味します。

### 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:ISEの外部RADIUSサーバのデフォルトのデッドタイムは5分です。このバージョンでは、この値はハードコーディングされているため変更できません。

- 手順に示されている場合 RADIUS-Client encountered error during processing flow その後に Failed to forward request to current remote RADIUS server; an invalid response was received、これは、外部RADIUSサーバへの要求の転送中にISEで問題が発生したことを意味します。これは通常、ネットワークデバイス/NASからISEに送信されたRADIUS要求に NAS-IP-Address アトリビュートの1つとして使用します。存在しない場合 NAS-IP-Address 外部RADIUSサーバが使用されていない場合、ISEは NAS-IP-Address フィールドにパケットの送信元IPを入力します。ただし、これは外部 Radius サーバが使用中の場合は適用されません。

## シナリオ 2. イベント - 5400 認証の失敗

- この場合、次の手順を実行します 11368 Please review logs on the External RADIUS Server to determine the precise failure reasonこれは、外部RADIUSサーバ自体で認証が失敗し、Access-Rejectが送信されたことを意味します。

### 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
```

- 手順に示されている場合 15039 Rejected per authorization profileつまり、ISEは外部RADIUSサーバからAccess-Acceptを受信しましたが、ISEは設定された認可ポリシーに基づいて認可を拒否します。

## 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 iseでは、認証が失敗した場合に、ここで説明した以外の何らかの方法が使用されます。これは、設定またはISE自体の潜在的な問題を意味する場合があります。その場合は、この時点で TAC ケースを開くことをお勧めします。

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。