Identity Services Engineでのデバイス管理にRADIUSを使用する

内容

はじめに

このドキュメントでは、さまざまなシスコ製品およびシスコ以外の製品がCisco ISEなどのAAAサーバから受信する属性のコンパイルについて説明します。

背景説明

シスコ製品およびシスコ以外の製品では、認証、許可、およびアカウンティング(AAA)サーバから属性のコンパイルを受け取ることを想定しています。この場合、サーバはCisco ISEであり、ISEは認可プロファイル(RADIUS)の一部としてアクセス承認とともにこれらの属性を返します。

このドキュメントでは、カスタム属性認可プロファイルを追加する方法の手順を説明し、デバイスのリストと、デバイスがAAAサーバから返されることを期待するRADIUS属性を示します。これらにはすべて例が示されます。

このドキュメントに記載されている属性のリストは、完全なものでも正式なものでもありません

。また、このドキュメントを更新しなくても、いつでも変更できます。

ネットワークデバイスのデバイス管理は、通常はTACACS+プロトコルを使用して行われますが、ネットワークデバイスがTACACS+をサポートしていない場合、またはISEにデバイス管理ライセンスがない場合は、ネットワークデバイスがRADIUSデバイス管理をサポートしていればRADIUSでも行うことができます。一部のデバイスは両方のプロトコルをサポートしており、使用するプロトコルはユーザが決定しますが、TACACS+にはコマンド許可やコマンドアカウンティングなどの機能があるため、好ましい結果が得られます。

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。

- 対象ネットワーク上のRADIUSサーバとしてのCisco ISE
- RADIUSプロトコルのワークフロー：RFC2865

使用するコンポーネント

このドキュメントの情報は、Cisco Identity Services Engine(ISE)3.x以降のバージョンのISE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

ステップ 1：ベンダー固有属性(VSA)の作成

ベンダーごとに作成された各種の辞書があり、これらの辞書に属性を追加できます。各辞書には、認可プロファイルで使用できる複数の属性を設定できます。各属性は、一般に、ユーザがネットワークデバイスにログインするときに取得できるデバイス管理のさまざまな役割を定義します。ただし、ネットワークデバイス上での動作や設定の目的に応じて、アトリビュートを使用することもできます。

ISEには、一部のベンダー向けに事前定義された属性が用意されています。ベンダーがリストされていない場合は、属性を持つディクショナリとして追加できます。一部のネットワークデバイスでは、属性は設定可能であり、さまざまなタイプのアクセスに対して変更できます。その場合、ISEは、ネットワークデバイスが異なるタイプのアクセスに対して期待する属性で設定する必要があります。

Radius Access-Acceptで送信されることが想定される属性は、次のように定義されます。

1. Policy > Policy Elements > Dictionaries > System > Radius > Radius Vendors > Addの順に移動します。

2. 名前とベンダーIDを入力して保存します。

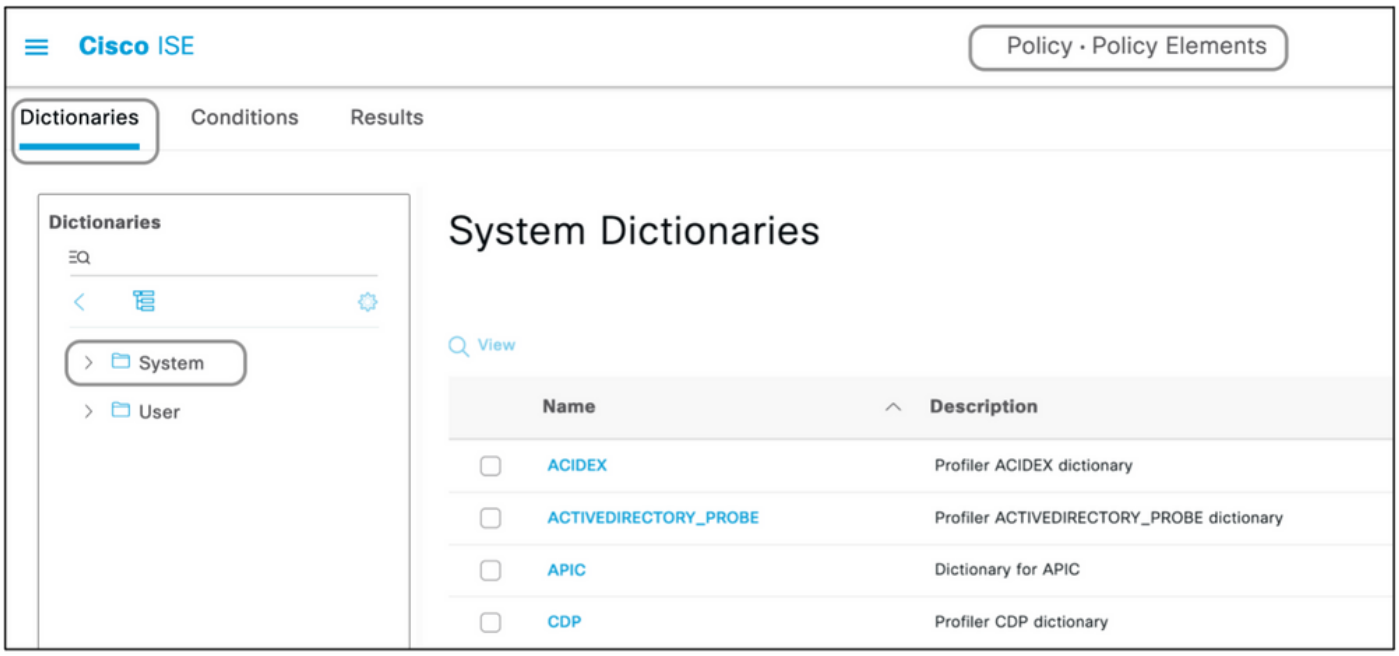
3. 保存したRadius Vendorをクリックし、Dictionary Attributesに移動します。

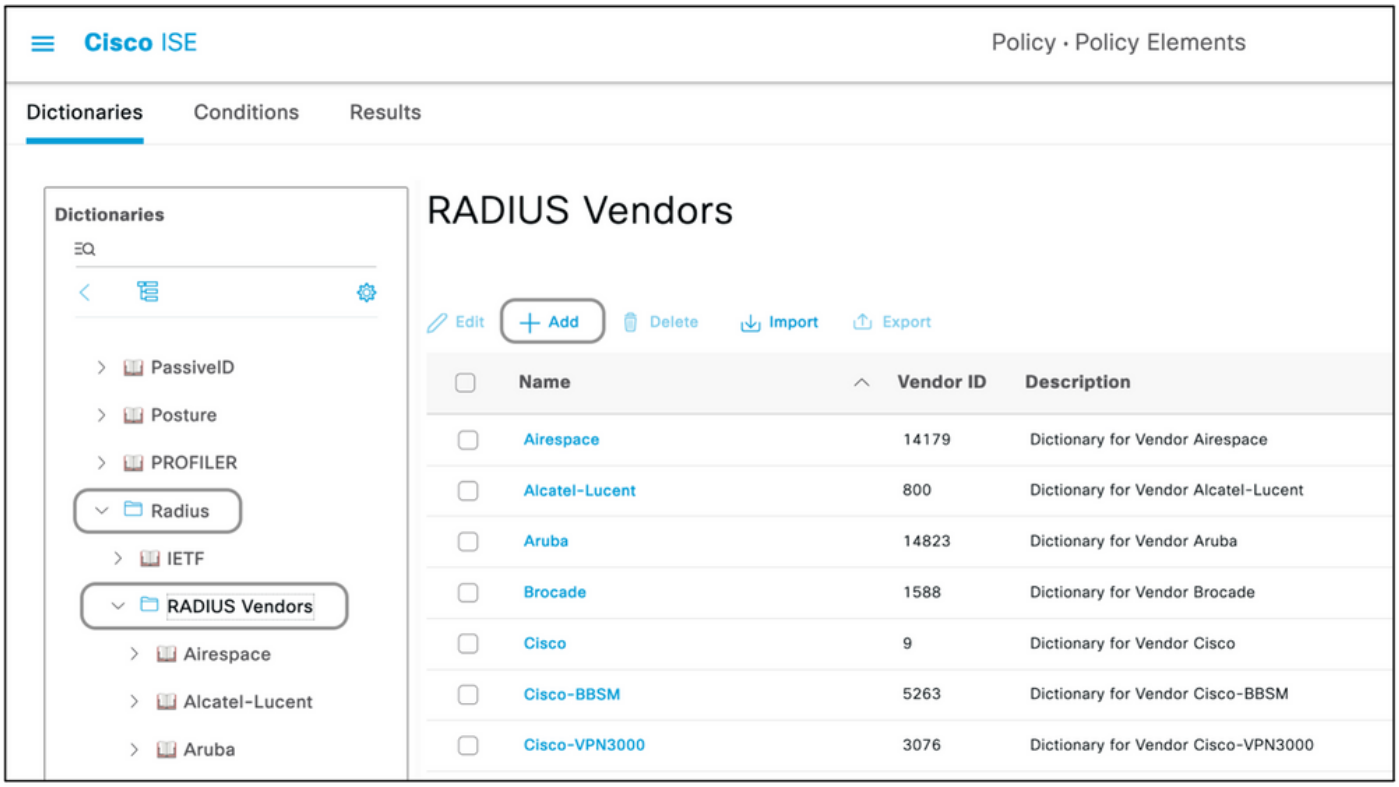
4. Addをクリックし、属性名、データタイプ、方向、およびIDに大文字と小文字を区別して入力します。

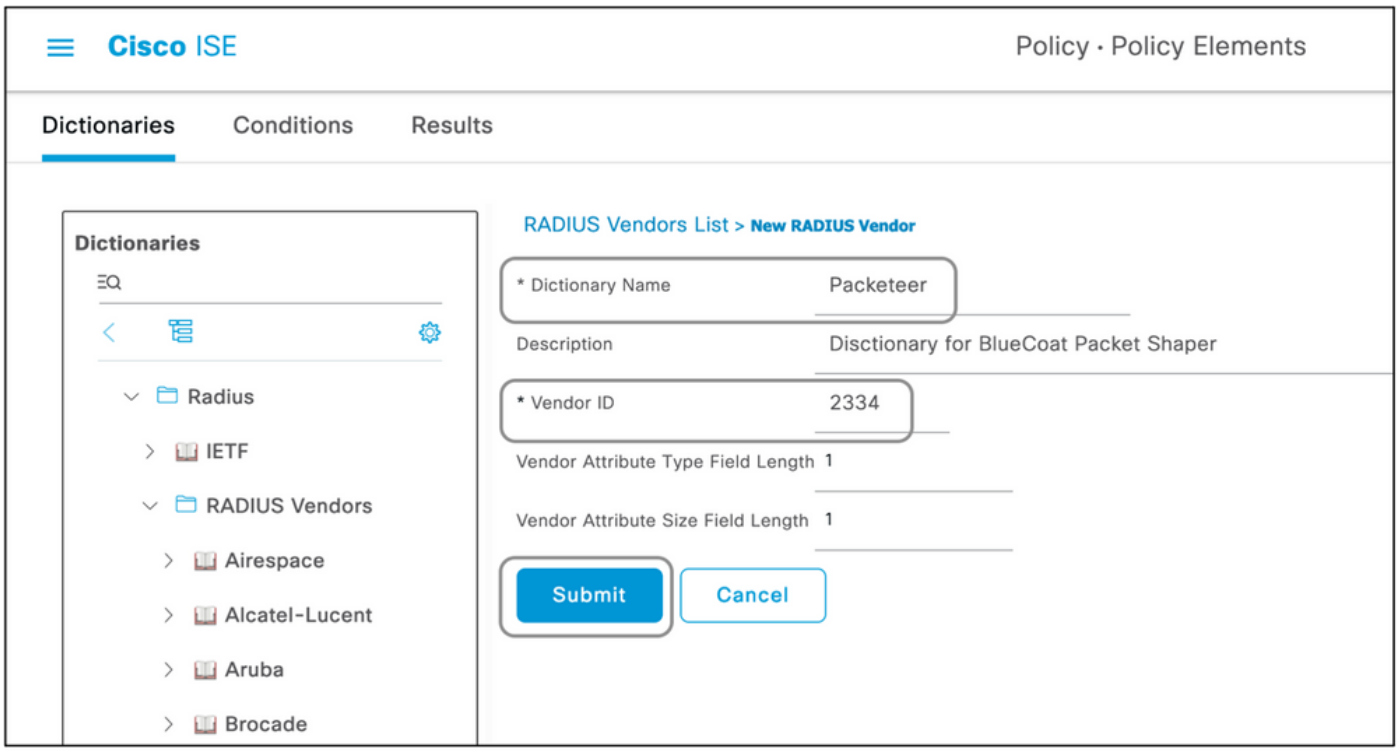
5. 属性を保存します。

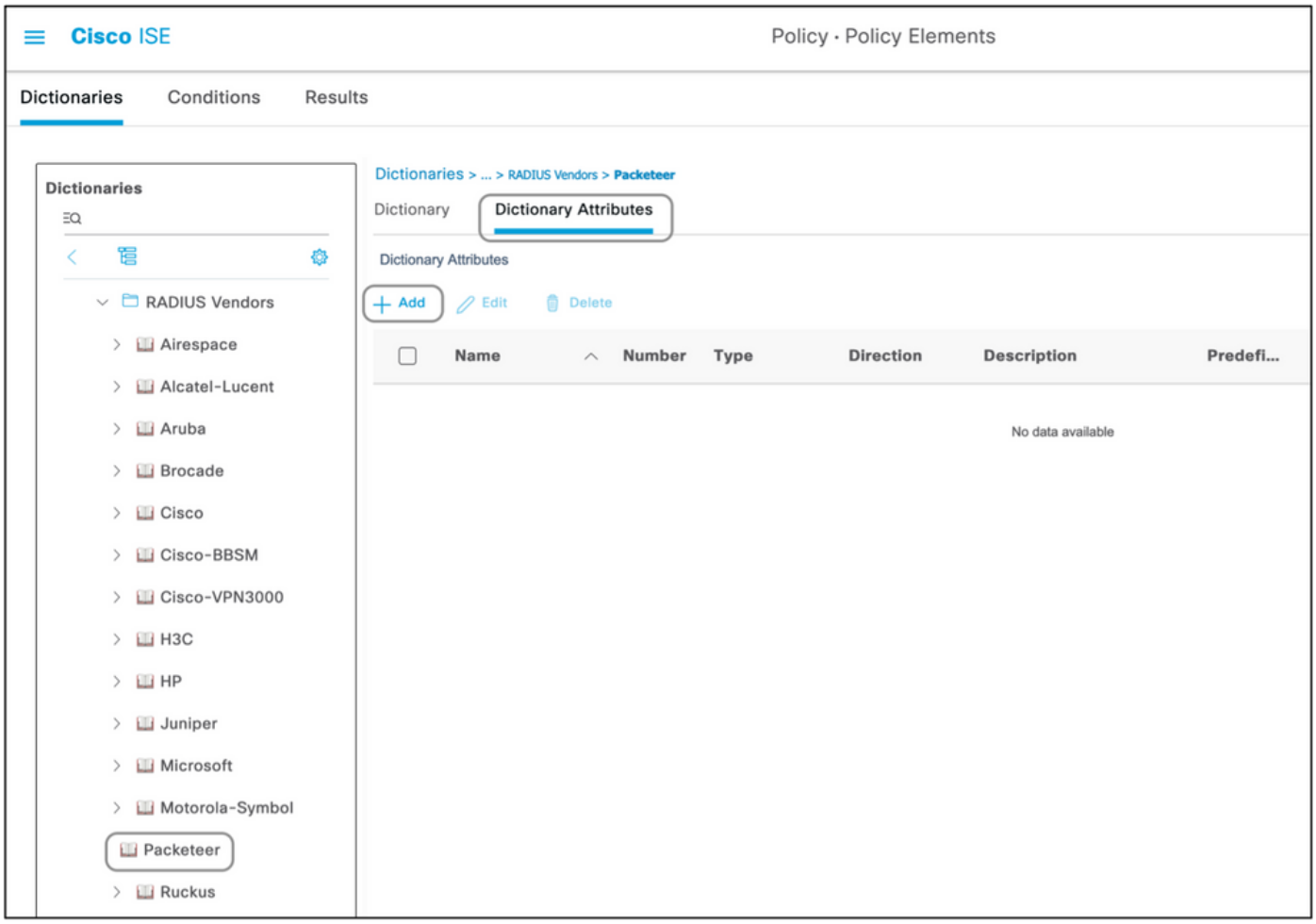
6. 同じディクショナリに複数の属性を追加する場合は、同じページに他の属性を追加します。

注：このセクションの値として入力される各フィールドは、ベンダー自身によって提供されます。ベンダーのWebサイトにアクセスしたり、ベンダーのサポートに問い合わせたりできます。




Cisco ISE
Policy · Policy Elements
Dictionaries
Conditions
Results
Dictionaries
PassiveID
Posture
PROFILER
Radius
IETF
RADIUS Vendors
Airespace
Alcatel-Lucent
Aruba
RADIUS Vendors
Edit
Add
Delete
Import
Export
Name
Vendor ID
Description
Airespace 14179 Dictionary for Vendor Airespace
Alcatel-Lucent 800 Dictionary for Vendor Alcatel-Lucent
Aruba 14823 Dictionary for Vendor Aruba
Brocade 1588 Dictionary for Vendor Brocade
Cisco 9 Dictionary for Vendor Cisco
Cisco-BBSM 5263 Dictionary for Vendor Cisco-BBSM
Cisco-VPN3000 3076 Dictionary for Vendor Cisco-VPN3000


Cisco ISE
Policy · Policy Elements
Dictionaries
Conditions
Results
Dictionaries
Radius
IETF
RADIUS Vendors
Airespace
Alcatel-Lucent
Aruba
Brocade
RADIUS Vendors List > New RADIUS Vendor
* Dictionary Name Packeteer
Description Disctionary for BlueCoat Packet Shaper
* Vendor ID 2334
Vendor Attribute Type Field Length 1
Vendor Attribute Size Field Length 1
Submit
Cancel



注：一部のベンダーでは、特定の辞書を追加する必要はありません。ベンダーがIETFによって定義されたRADIUS属性を使用できる場合（すでにISEに存在します）、この手順はスキップできます。

ステップ 2：ネットワークデバイスプロファイルの作成

このセクションは必須ではありません。ネットワークデバイスプロファイルは、追加されるネットワークデバイスのタイプを分離し、それぞれに適した認可プロファイルを作成するのに役立ちます。RADIUSディクショナリと同様に、ISEには使用可能な事前定義されたプロファイルがいくつかあります。まだ存在していない場合は、新しいデバイスプロファイルを作成できます。

ネットワークプロファイルを追加する手順を次に示します。

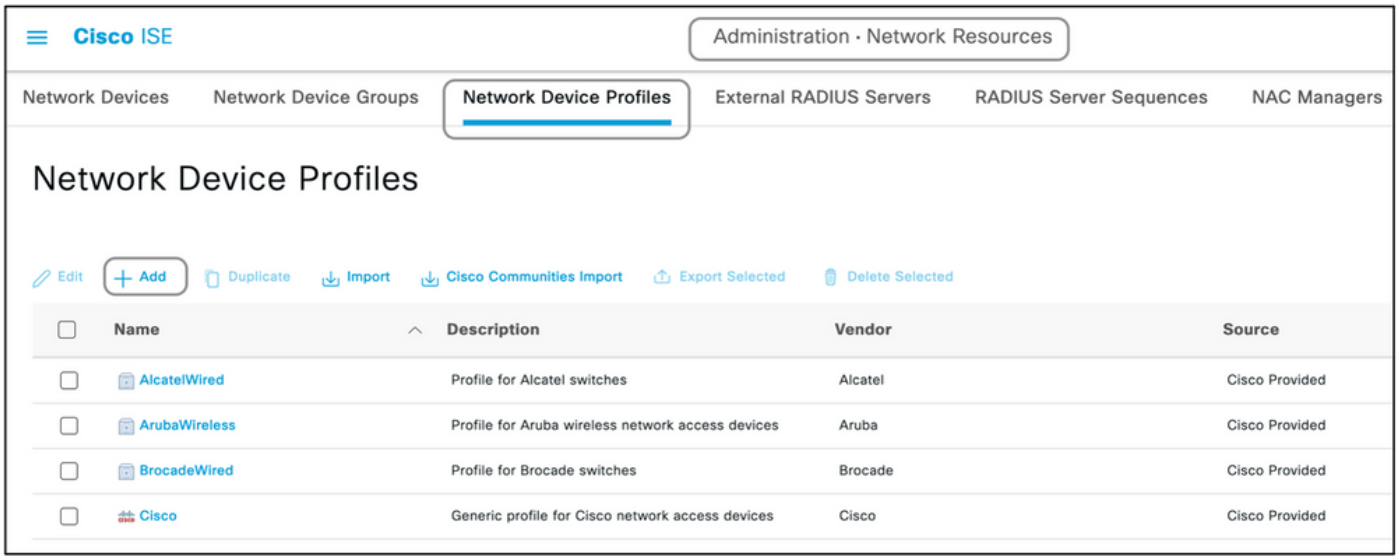
1. Administration > Network Resources > Network Device Profiles > Addの順に移動します。

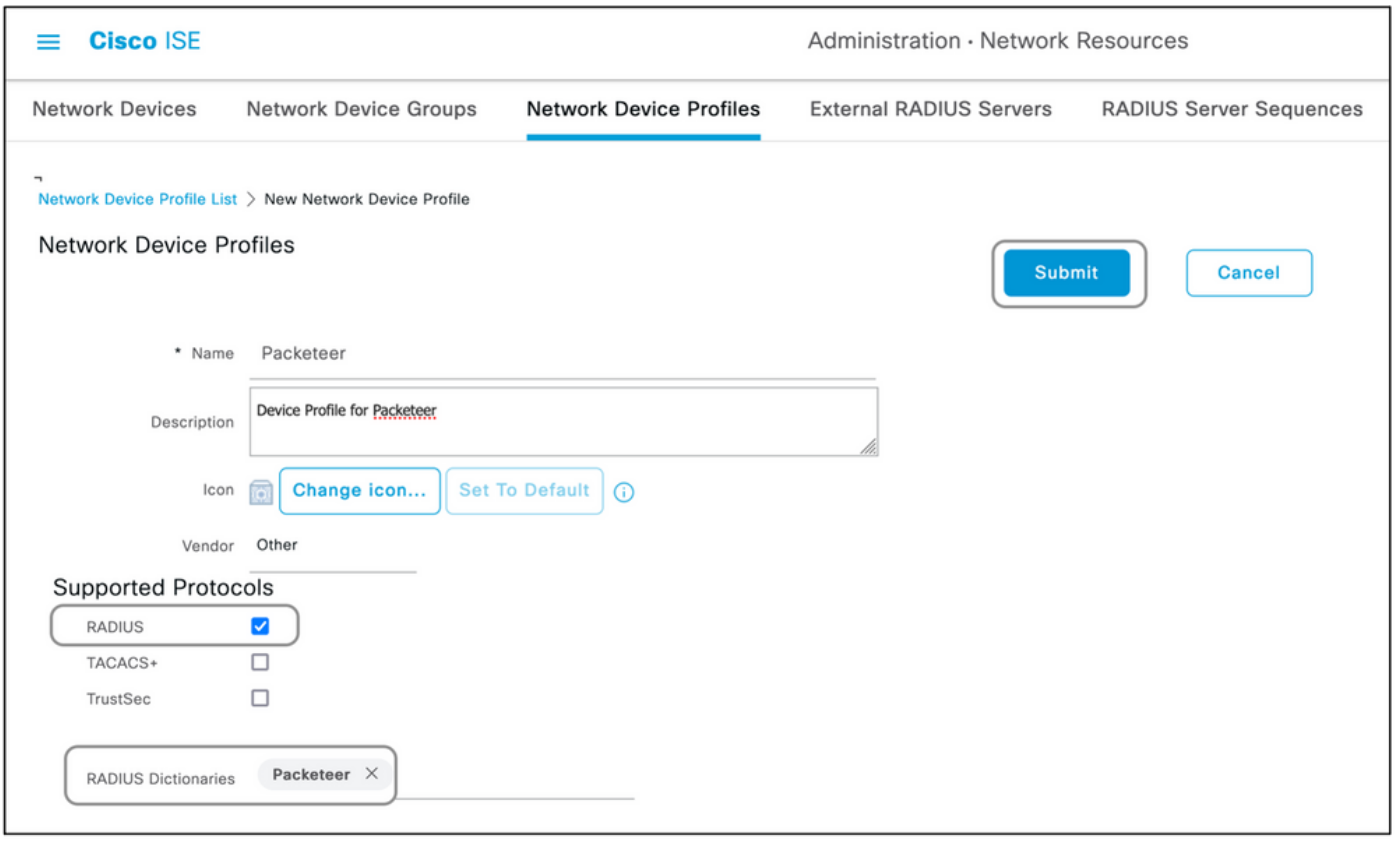
2. 名前を入力し、RADIUSのチェックボックスをオンにします。

3. RADIUS Dictionariesの下で、前のセクションで作成したディクショナリを選択します。

4. 同じタイプのデバイスに対して複数のディクショナリが作成されている場合は、それらすべてをRADIUSディクショナリの下で選択できます。

5. プロファイルを保存します。





ステップ 3：ISEでのネットワークデバイスの追加

デバイス管理を行うネットワークデバイスは、ネットワークデバイスで定義されたキーとともにISEに追加する必要があります。ネットワークデバイスで、ISEはこのキーを持つRADIUS AAAサーバとして追加されます。

ISEにデバイスを追加する手順を次に示します。

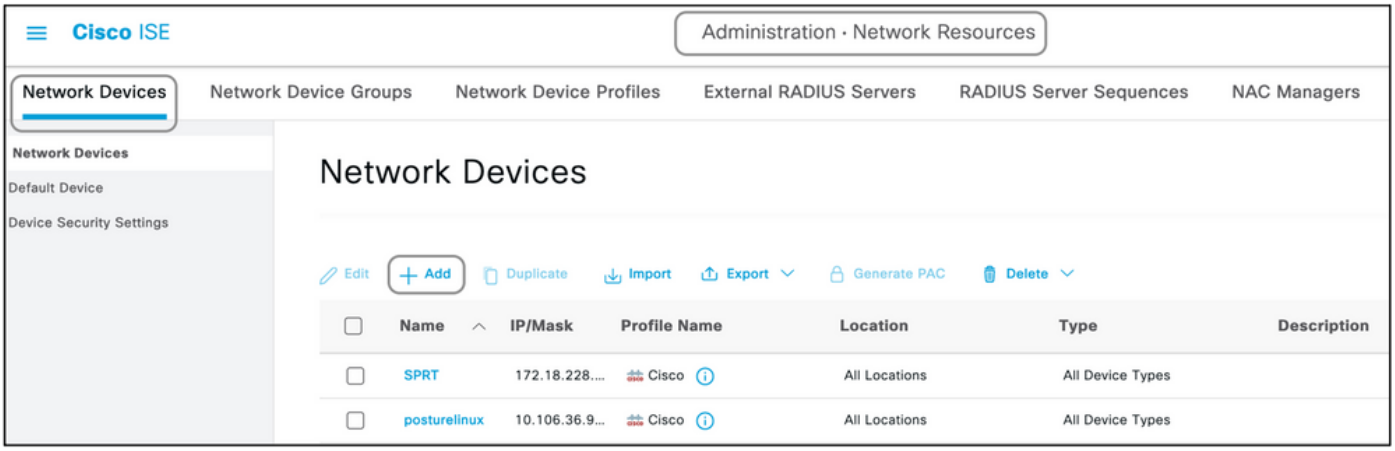
1. Administration > Network Resources > Network Devices > Addの順に移動します。

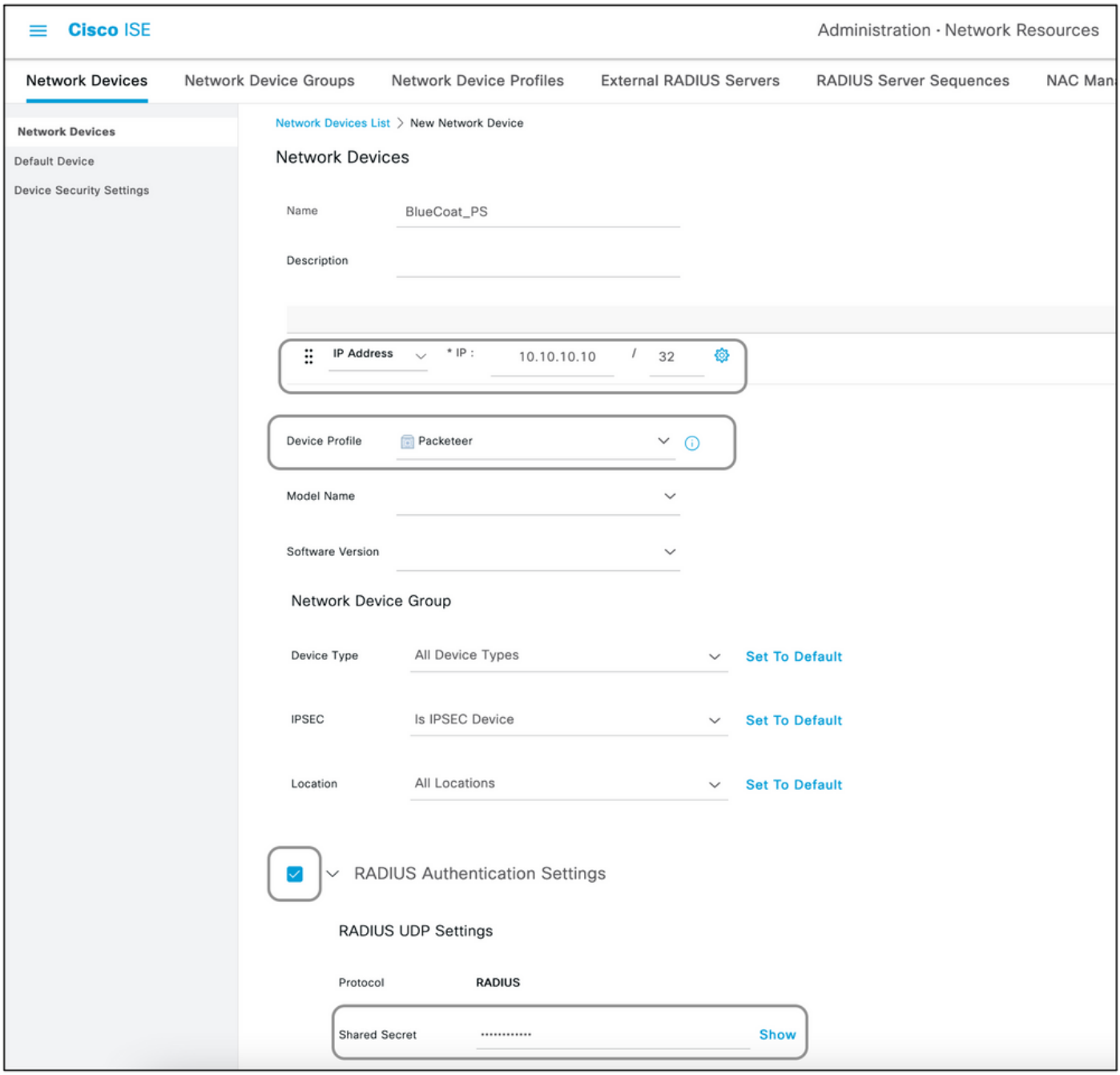
2. 名前とIPアドレスを指定します。

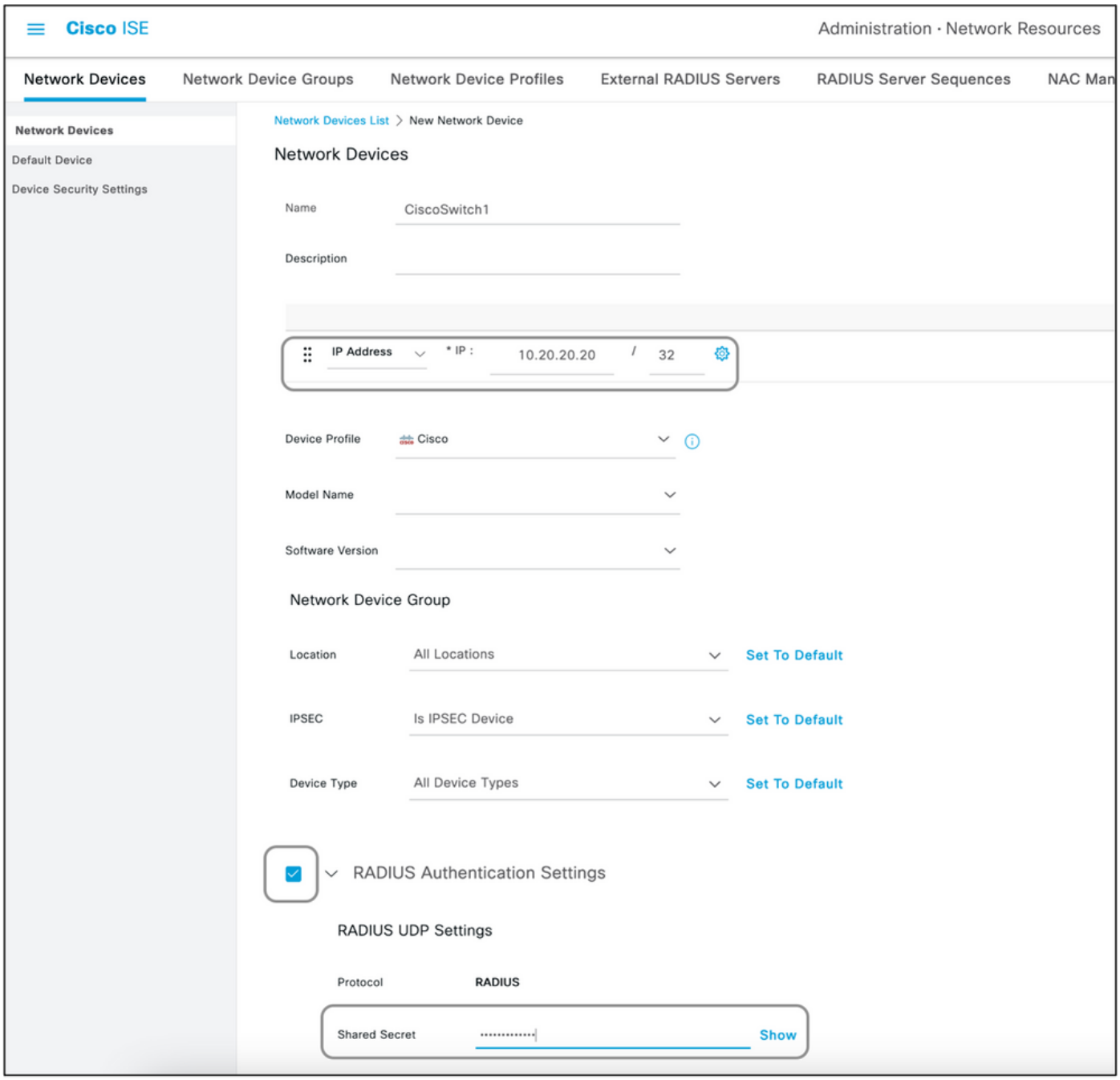
3. デバイスプロファイルは、前のセクションで定義したプロファイルになるようにドロップダウンリストから選択できます。プロファイルが作成されていない場合は、デフォルトのCiscoをそのまま使用できます。

4. Radius認証設定を確認します。

5. 共有秘密キーを入力し、デバイスを保存します。


Cisco ISE
Administration · Network Resources
Network Devices
Network Device Groups
Network Device Profiles
External RADIUS Servers
RADIUS Server Sequences
NAC Managers
Network Devices
Default Device
Device Security Settings
Network Devices
Edit
Add
Duplicate
Import
Export
Generate PAC
Delete
Name
IP/Mask
Profile Name
Location
Type
Description
SPRT
172.18.228....
Cisco
All Locations
All Device Types
posturelinux
10.106.36.9...
Cisco
All Locations
All Device Types


Cisco ISE
Administration · Network Resources
Network Devices
Network Device Groups
Network Device Profiles
External RADIUS Servers
RADIUS Server Sequences
NAC Man
Network Devices
Default Device
Device Security Settings
Network Devices List > New Network Device
Network Devices
Name
BlueCoat_PS
Description
IP Address
* IP :
10.10.10.10
/
32
Device Profile
Packeteer
Model Name
Software Version
Network Device Group
Device Type
All Device Types
Set To Default
IPSEC
Is IPSEC Device
Set To Default
Location
All Locations
Set To Default
RADIUS Authentication Settings
RADIUS UDP Settings
Protocol
RADIUS
Shared Secret
Show



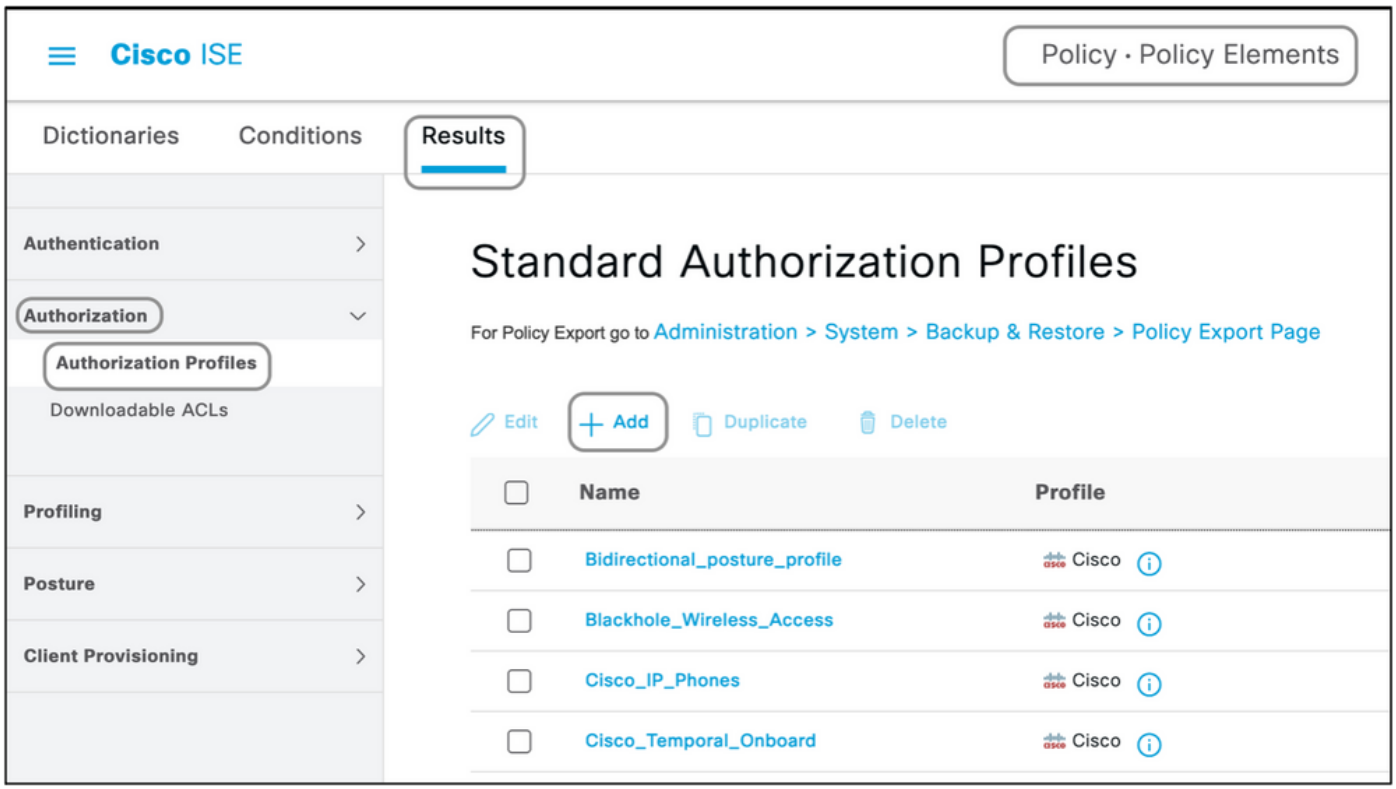
ステップ 4：認可プロファイルの作成

Access-AcceptまたはAccess-RejectとしてISEからプッシュされる最終結果は、認可プロファイルで定義されます。各認可プロファイルは、ネットワークデバイスが期待する追加の属性をプッシュできます。

次に、認可プロファイルを作成する手順を示します。

1. [Policy] > [Policy Elements] > [Results] > [Authorization] > [Authorization Profiles] の順に選択します。

2. Standard Authorization Profilesの下で、Addをクリックします。



追加できるプロファイルのタイプは、Access-AcceptとAccess-Rejectです。

Access-Acceptプロファイルの作成

このプロファイルは、ネットワークデバイスへの何らかのアクセスに使用されます。このプロファイルには、複数の属性を渡すことができます。内容は次のとおりです。

1. わかりやすい名前を付け、アクセスタイプとしてAccess-Acceptを選択します。

2. 前のいずれかのセクションで作成したネットワークデバイスプロファイルを選択します。プロファイルが作成されていない場合は、デフォルトのCiscoを使用できます。

3. 異なるタイプのプロファイルが選択されている場合は、このページで設定のオプションを制限します。

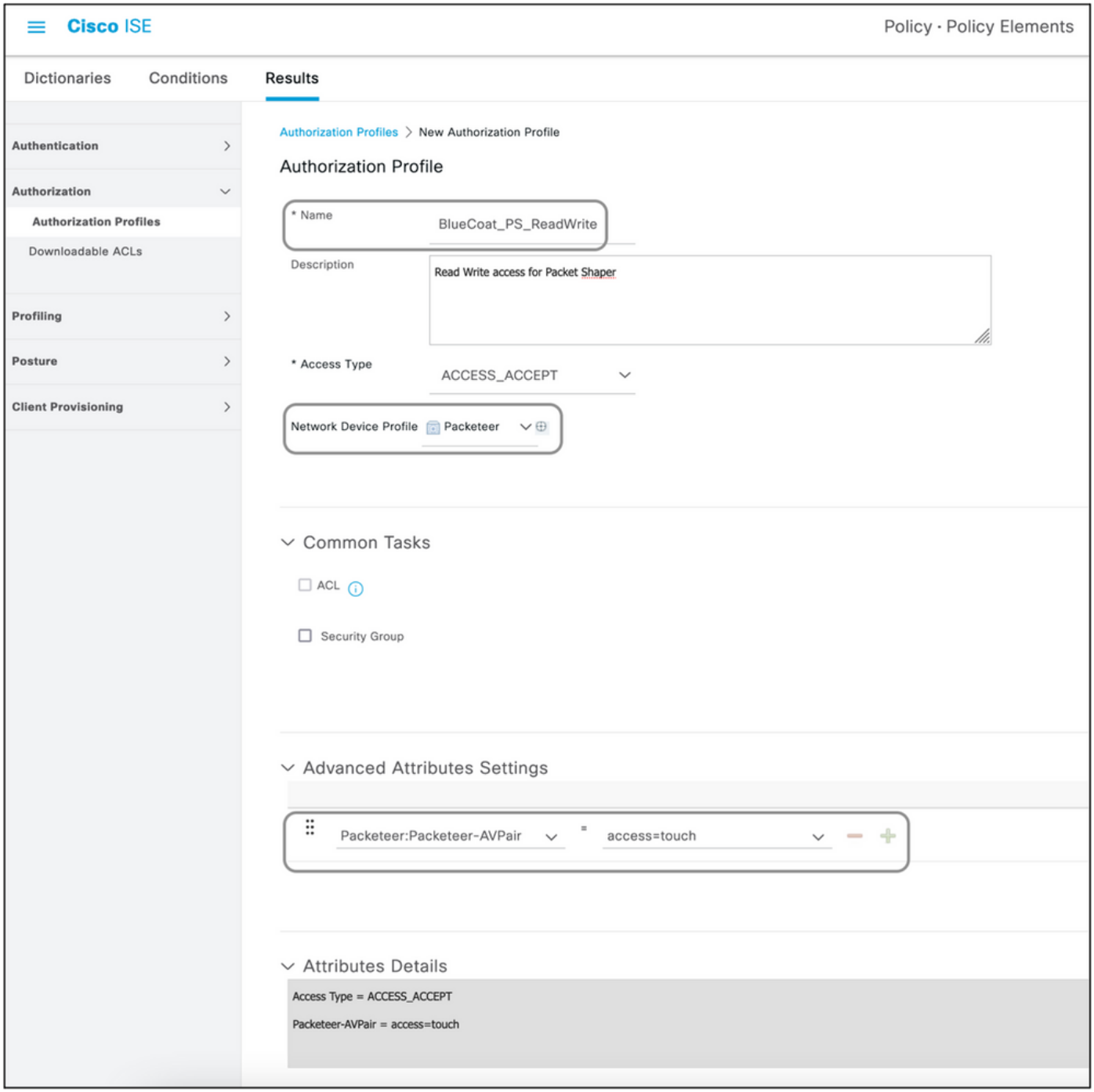
4. Advanced Attributes Settingsで、ディクショナリと適用可能な属性(LHS)を選択します。

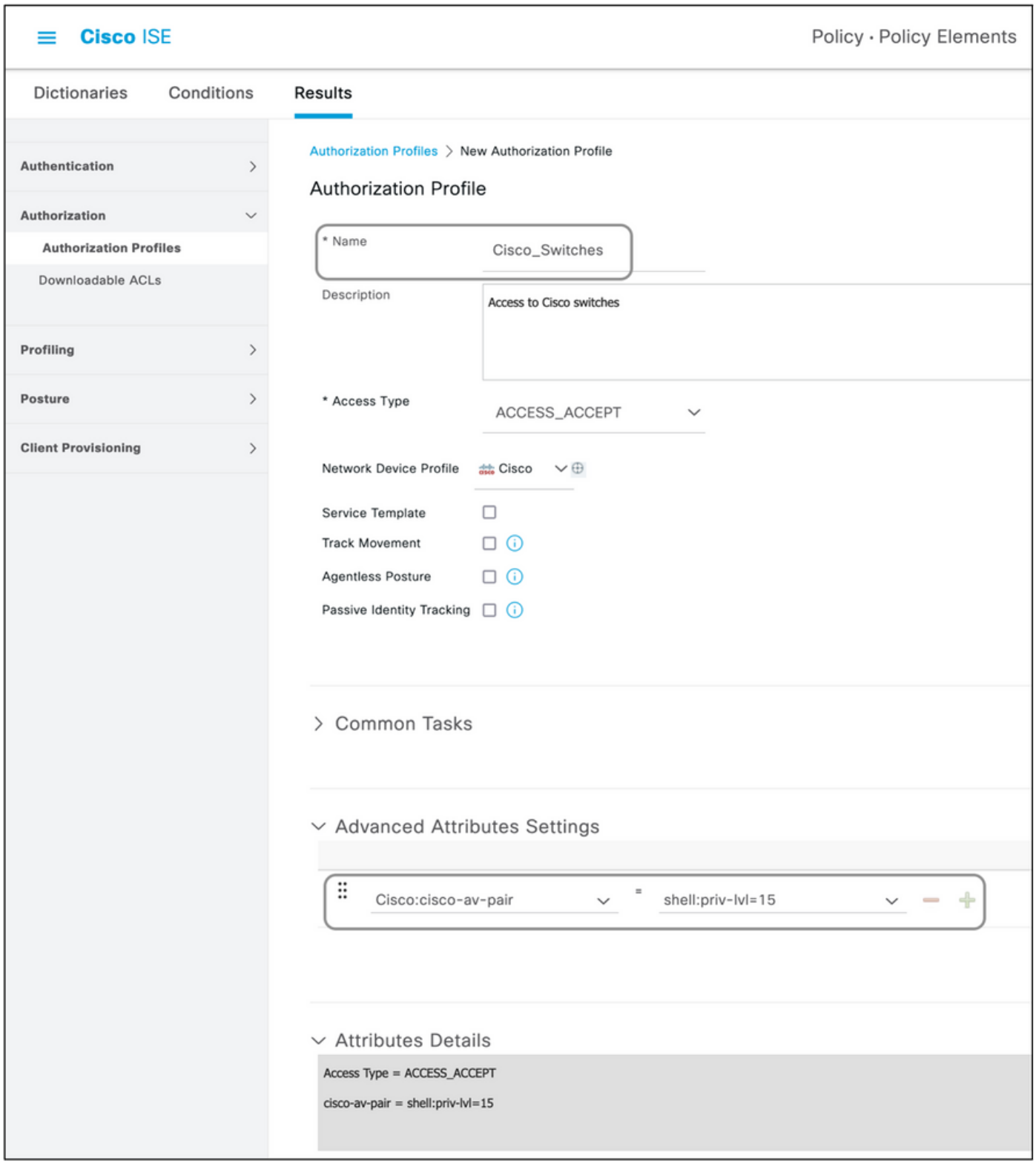
5. 該当する場合は、ドロップダウンから属性に値(RHS)を割り当てるか、必要な値を入力します。

6. 同じ結果の一部として送信される属性がさらに存在する場合は、+アイコンをクリックして、ステップ4と5を繰り返します。

ISEが送信する予定の結果、ロール、認可のそれぞれに対して複数の認可プロファイルを作成します。

注：統合された属性は、「属性の詳細」フィールドで確認できます。


Cisco ISE
Policy · Policy Elements
Dictionaries
Conditions
Results
Authentication
Authorization
Authorization Profiles
Downloadable ACLs
Profiling
Posture
Client Provisioning
Authorization Profiles > New Authorization Profile
Authorization Profile
* Name
BlueCoat_PS_ReadWrite
Description
Read Write access for Packet Shaper
* Access Type
ACCESS_ACCEPT
Network Device Profile
Packeteer
Common Tasks
ACL
Security Group
Advanced Attributes Settings
Packeteer:Packeteer-AVPair
=
access=touch
Attributes Details
Access Type = ACCESS_ACCEPT
Packeteer-AVPair = access=touch



アクセス拒否プロファイルの作成

このプロファイルは、デバイス管理の拒否を送信するために使用されますが、属性を一緒に送信するために引き続き使用できます。これは、Radius Access-Rejectパケットを送信するために使用されます。ステップ1では、アクセスタイプとしてAccess-Acceptではなく Access-Rejectを選択する必要がありますが、それ以外は同じです。

ステップ 5：ポリシーセットの作成

ISE上のポリシーセットは上から下へと評価され、ポリシーセット内の条件セットを満たす最初のポリシーセットが、ネットワークデバイスから送信されるRadius Access-Requestパケットに対するISEの応答を受け持ちます。デバイスのタイプごとに一意のポリシーセットを使用することをお勧めします。ユーザの認証と許可を評価する条件は、評価時に発生します。ISEに外部アイデンティティソースがある場合は、認証のタイプに使用できます。

一般的なポリシーセットは次のように作成されます。

1. Policy > Policy Sets > +の順に移動します。

2. New Policy Set 1の名前を変更します。

3. このデバイスに固有の条件を設定します。

4. Policy Setを展開します。

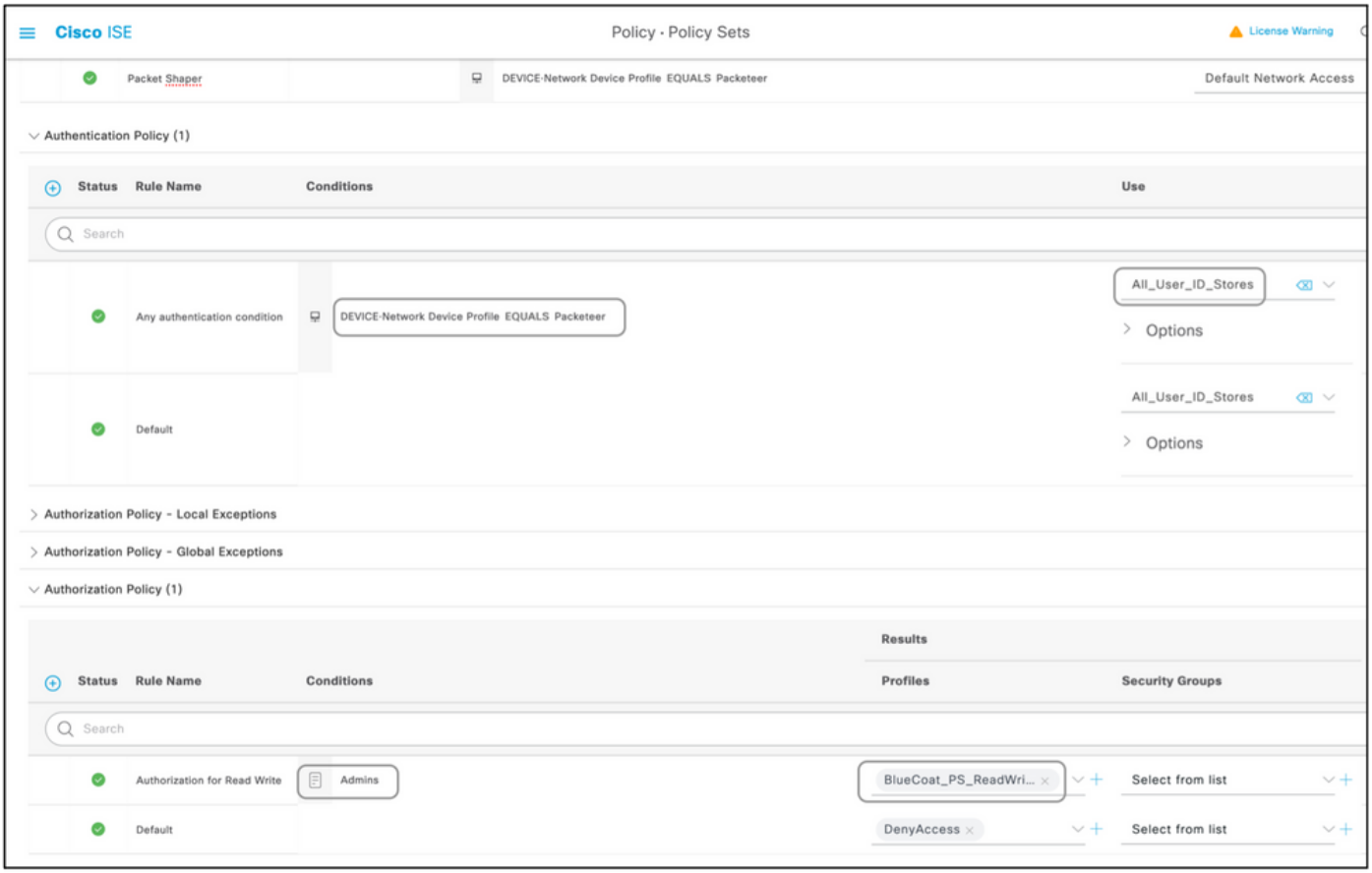
5. Authentication Policyを展開して、認証ルールを設定します。外部ソースまたは内部ユーザは、ISEがユーザを確認する対象となるアイデンティティソースシーケンスとして使用できる例です。

6. 認証ポリシーがすべて設定されています。この時点でポリシーを保存できます。

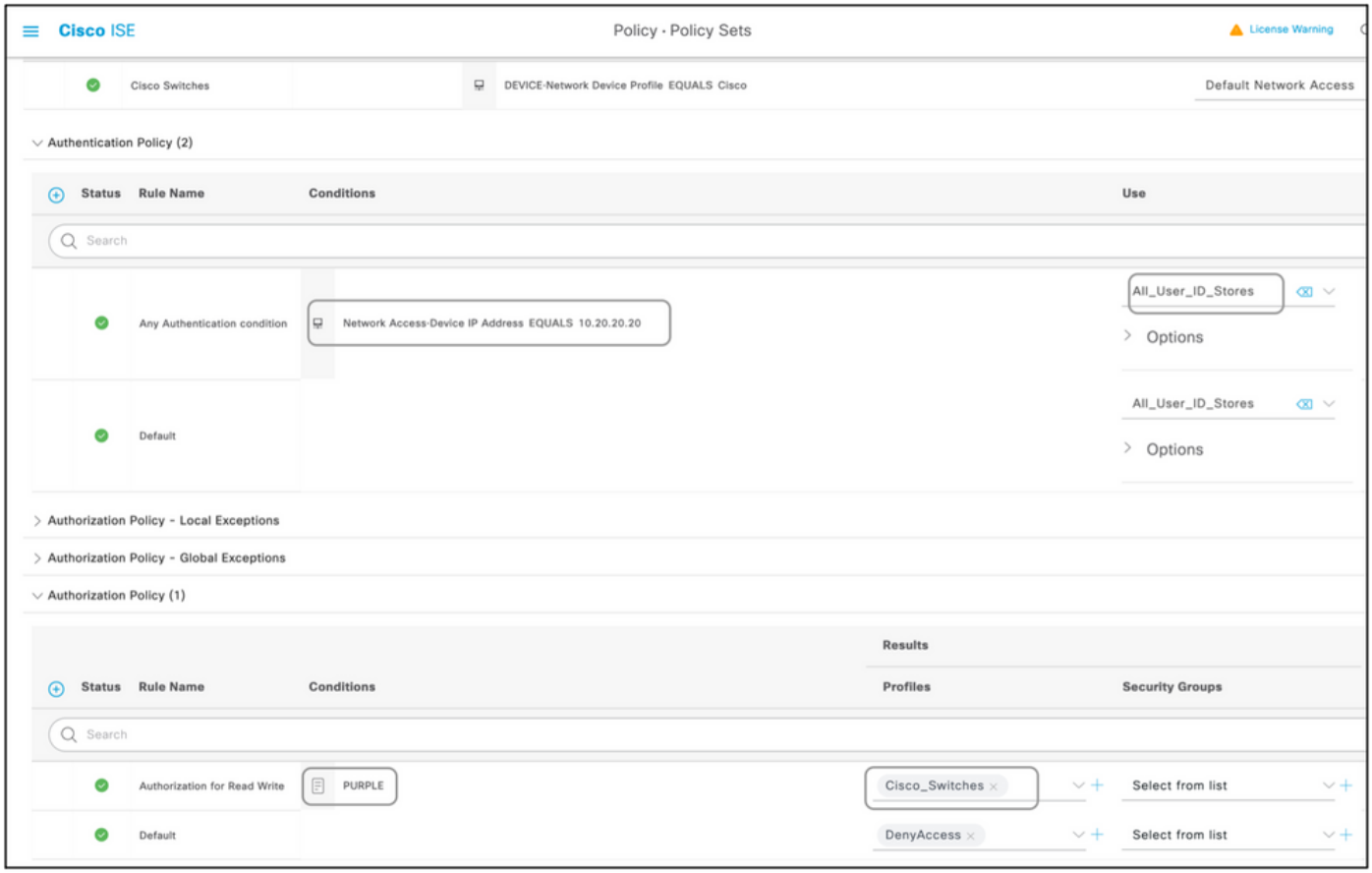
7. Authorization Policyを展開して、ユーザの認可条件を追加します。たとえば、特定のADグループまたはISE内部IDグループを確認します。ルールに同じ名前を付けます。

8. 許可ルールの結果は、ドロップダウンから選択できます。

9. ベンダーがサポートするアクセスのタイプごとに複数の認可ルールを作成します。


Cisco ISE
Policy - Policy Sets
License Warning
Packet Shaper
DEVICE-Network Device Profile EQUALS Packeteer
Default Network Access
Authentication Policy (1)
Status
Rule Name
Conditions
Use
Search
Any authentication condition
DEVICE-Network Device Profile EQUALS Packeteer
All_User_ID_Stores
Options
Default
All_User_ID_Stores
Options
Authorization Policy - Local Exceptions
Authorization Policy - Global Exceptions
Authorization Policy (1)
Results
Status
Rule Name
Conditions
Profiles
Security Groups
Search
Authorization for Read Write
Admins
BlueCoat_PS_ReadWri...
Select from list
Default
DenyAccess
Select from list


Cisco ISE
Policy - Policy Sets
License Warning
Policy Sets
Reset
Reset Policyset Hitcounts
Save
Status
Policy Set Name
Description
Conditions
Allowed Protocols / Server Sequence
Hits
Actions
View
Search
Cisco Switches
DEVICE-Network Device Profile EQUALS Cisco
Default Network Access
0



デバイス リスト

Radiusによるデバイス管理をサポートするデバイスは、前のセクションで説明したすべての手順を少し変更するだけでISEに追加できます。したがって、このドキュメントでは、このセクションで提供される情報を使用するデバイスのリストを示します。 このドキュメントに記載されている属性および値のリストは、完全なものでも信頼できるものでもありません。また、このドキュメントを更新しなくても、いつでも変更できます。検証については、ベンダーのWebサイトとベンダーサポートを参照してください。

アグリゲーション サービス ルータ（ASR）

ISEにすでに存在するCisco AVペアを使用するため、このために個別のディクショナリとVSAを作成する必要はありません。

属性：cisco-av-pair

値： shell:tasks="#<role-name>,<permission>:<process>"

使用法：<role-name>の値を、ルータでローカルに定義されているロールの名前に設定します。ロール階層はツリー形式で記述できます。ツリーの最上部にrole#rootisがあり、role#leafdsが追加コマンドを追加します。これら2つのロールは、shell:tasks="#root,#leaf"の場合に結合して返すことができます。

個々のプロセスに基づいて許可を返すことができるので、特定のプロセスの読み取り、書き込み、実行権限をユーザに付与できます。たとえば、ユーザにBGPプロセスの読み取りおよび書き込

み権限を付与するには、値をshell:tasks="#root,rw:bgp"に設定します。属性の順序は重要ではありません。結果は、値がtoshell:tasks="#root,rw:bgp"またはtoshell:tasks="rw:bgp,#root"のどちらに設定されていても同じです。

例：許可プロファイルへの属性の追加

Dictionary Type	RADIUS Attribute	Attribute Type	Attribute Value
RADIUS-Cisco	cisco-av-pair	String	shell:tasks="#root,#leaf,rwx:bgp,r:ospf"

CiscoスイッチIOS®およびCisco IOS® XE

ISEにすでに存在するRADIUS属性が使用されるため、この目的のために個別のディクショナリとVSAを作成する必要はありません。

属性：cisco-av-pair

値：shell:priv-lvl=<レベル>

使用法：<level>の値を、基本的に送信される特権の数である数値に設定します。通常、15が送信される場合は読み取り/書き込みを意味し、7が送信される場合は読み取り専用を意味します。

例：許可プロファイルへの属性の追加

Dictionary Type	RADIUS Attribute	Attribute Type	Attribute Value
RADIUS-Cisco	cisco-av-pair	String	シェル：priv-lvl=15

BlueCoat パケット シェーパ

属性：Packeter-AVPair

値：access=<level>

使用法：<level>は付与するアクセスのレベルです。touch アクセスは読み取りおよび書き込みと同じで、look アクセスは読み取り専用と同じです。

次の値を使用して、このドキュメントに示すようにディクショナリを作成します。

- Name（名前）:Packeter
- ベンダー ID：2334
- ベンダー長フィールドサイズ：1
- 仕入先タイプフィールドサイズ： 1

属性の詳細を入力します。

- 属性：Packeter-AVPair（パケット受信者 – AVPair）

- 説明：アクセスレベルを指定するために使用します。
- ベンダー属性ID: 1
- 方向：アウト
- 複数を許可： False
- タグ付けを許可：オフ
- 属性の種類：文字列

例：許可プロファイルへの属性の追加（読み取り専用アクセス用）

Dictionary Type	RADIUS Attribute	Attribute Type	Attribute Value
RADIUSパケット送信者	Packeteer-AVPair	String	アクセス=ルック

例：許可プロファイルへの属性の追加（読み取り/書き込みアクセス用）

Dictionary Type	RADIUS Attribute	Attribute Type	Attribute Value
RADIUSパケット送信者	Packeteer-AVPair	String	アクセス=タッチ

BlueCoatプロキシサーバ(AV/SG)

属性：Blue-Coat-Authorization

値： <level>

使用法：<level>は付与するアクセスのレベルです。0はアクセス権がないことを意味し、1は読み取り専用アクセスを意味し、2は読み取り/書き込みアクセスを意味します。 Blue-Coat-Authorization属性は、アクセスレベルを制御する属性です。

次の値を使用して、このドキュメントに示すようにディクショナリを作成します。

- 名前：BlueCoat
- ベンダー ID：14501
- ベンダー長フィールドサイズ：1
- 仕入先タイプフィールドサイズ： 1

属性の詳細を入力します。

- 属性：Blue-Coat-Group
- ベンダー属性ID: 1
- 方向：両方
- 複数を許可： False
- タグ付けを許可：オフ
- 属性の種類：符号なし整数32 (UINT32)

2番目の属性の詳細を入力します。

- 属性：Blue-Coat-Authorization
- 説明：アクセスレベルを指定するために使用します。

- ベンダー属性ID: 2
- 方向：両方
- 複数を許可： False
- タグ付けを許可：オフ
- 属性の種類：符号なし整数32 (UINT32)

例：許可プロファイルに属性を追加する（アクセスなし）。

Dictionary Type	RADIUS Attribute	Attribute Type	Attribute Value
RADIUS-BlueCoat	ブルー・コート・グループ	UINT32	0

例：許可プロファイルへの属性の追加（読み取り専用アクセス用）

Dictionary Type	RADIUS Attribute	Attribute Type	Attribute Value
RADIUS-BlueCoat	ブルー・コート・グループ	UINT32	1

例：許可プロファイルへの属性の追加（読み取り/書き込みアクセス用）

Dictionary Type	RADIUS Attribute	Attribute Type	Attribute Value
RADIUS-BlueCoat	ブルー・コート・グループ	UINT32	2

Brocade スイッチ

ISEにすでに存在するRADIUS属性が使用されるため、この目的のために個別のディクショナリとVSAを作成する必要はありません。

属性：Tunnel-Private-Group-ID

値：U:<VLAN1>; T:<VLAN2>

使用法：<VLAN1>をデータVLANの値に設定します。<VLAN2>を音声VLANの値に設定します。この例では、データ VLAN は VLAN 10 で、音声 VLAN は VLAN 21 です。

例：許可プロファイルへの属性の追加

Dictionary Type	RADIUS Attribute	Attribute Type	Attribute Value
RADIUS-IETF	Tunnel-Private-Group-ID	Tagged String	U:10;T:21

Infoblox

属性：Infoblox-Group-Info

値：<グループ名>

Usage:<group-name>は、ユーザに付与される権限を持つグループの名前です。このグループは、Infoblox デバイスで設定する必要があります。この設定例では、グループ名は MyGroup です。

次の値を使用して、このドキュメントに示すようにディクショナリを作成します。

- 名前： Infoblox
- ベンダー ID：7779
- ベンダー長フィールドサイズ：1
- 仕入先タイプフィールドサイズ： 1

属性の詳細を入力します。

- 属性：Infoblox-Group-Info
- ベンダー属性ID: 009
- 方向：アウト
- 複数を許可： False
- タグ付けを許可：オフ
- 属性の種類：文字列

例：許可プロファイルへの属性の追加

Dictionary Type	RADIUS Attribute	Attribute Type	Attribute Value
RADIUS-Infoblox	Infoblox-Group-Info	String	マイグループ

Cisco Firepower Management Center

ISEにすでに存在するRADIUS属性が使用されるため、この目的のために個別のディクショナリとVSAを作成する必要はありません。

属性：cisco-av-pair

値：Class-[25]=<role>

使用法：<role>の値をFMCでローカルに定義されているロールの名前に設定します。FMCでadminやread-onlyユーザなどの複数のロールを作成し、ISEの属性に値を割り当てて、FMCが受信できるようにします。

例：許可プロファイルへの属性の追加

Dictionary Type	RADIUS Attribute	Attribute Type	Attribute Value
RADIUS-Cisco	cisco-av-pair	String	Class-[25]=NetAdmins

Nexus スイッチ

ISEにすでに存在するRADIUS属性が使用されるため、この目的のために個別のディクショナリとVSAを作成する必要はありません。

属性：cisco-av-pair

値：shell:roles="<role1> <role2>"

使用法：<role1>と<role2>の値を、スイッチでローカルに定義されているロールの名前に設定します。複数のロールを作成する場合は、それらを空白文字で区切ります。複数のロールが AAA サーバから Nexus スイッチに返されると、ユーザは、3 つのロールすべてで定義されるコマンドにアクセスできます。

組み込みロールは、ユーザアカウントとRBACの設定で定義されます。

例：許可プロファイルへの属性の追加

Dictionary Type	RADIUS Attribute	Attribute Type	Attribute Value
RADIUS-Cisco	cisco-av-pair	String	shell:roles="network-admin vdc-admin vdc-operator"

ワイヤレス LAN コントローラ（WLC）

ISEにすでに存在するRADIUS属性が使用されるため、この目的のために個別のディクショナリとVSAを作成する必要はありません。

属性：Service-Type（サービスタイプ）

値：Administrative (6) / NAS-Prompt (7)

使用法：ワイヤレスLANコントローラ(WLC)への読み取り/書き込みアクセスをユーザに許可するには、値がAdministrativeである必要があります。読み取り専用アクセスの場合、値はNAS-Promptである必要があります。

詳細については、「ワイヤレスLANコントローラ(WLC)での管理ユーザのRADIUSサーバ認証の設定例」を参照してください。

例：許可プロファイルへの属性の追加（読み取り専用アクセス用）

Dictionary Type	RADIUS Attribute	Attribute Type	Attribute Value
RADIUS-IETF	Service-Type	Enumeration	NASプロンプト

例：許可プロファイルへの属性の追加（読み取り/書き込みアクセス用）

Dictionary Type	RADIUS Attribute	Attribute Type	Attribute Value
RADIUS-IETF	Service-Type	Enumeration	管理

Data Center Network Manager（DCNM）

認証方式を変更した場合、DCNM を再起動する必要があります。それ以外の場合は、network-admin権限ではなくnetwork-operator権限を割り当てることができます。

ISEにすでに存在するRADIUS属性が使用されるため、この目的のために個別のディクショナリとVSAを作成する必要はありません。

属性：cisco-av-pair

値：shell:roles=<role>

DCNM Role	RADIUS Cisco-AV-Pair
User	シェル：ロール= "network-operator"
Administrator	シェル：ロール= "network-admin"

音声コード

属性：ACL-Auth-Level

値：ACL-Auth-Level = "<integer>"

使用法：<integer>は付与するアクセスレベルです。ユーザのACL-Auth-UserLevelという名前のACL-Auth-Level属性の値50、adminのACL-Auth-AdminLevelという名前のACL-Auth-Level属性の値100、security adminのACL-Auth-SecurityAdminLevelという名前のACL-Auth-Levelの値200。名前はスキップでき、属性の値は許可プロファイルの高度なAVペアの値として直接指定できます。

次の値を使用して、このドキュメントに示すようにディクショナリを作成します。

- 名前：AudioCodes
- ベンダー ID：5003
- ベンダー長フィールドサイズ：1
- 仕入先タイプフィールドサイズ： 1

属性の詳細を入力します。

- 属性：ACL-Auth-Level
- 説明：アクセスレベルを指定するために使用します。
- ベンダー属性ID: 35
- 方向：アウト
- 複数を許可： False
- タグ付けを許可：オフ
- 属性の種類：整数

例：許可プロファイル（ユーザ用）への属性の追加。

Dictionary Type	RADIUS Attribute	Attribute Type	Attribute Value
RADIUSオーディオコード	ACL認証レベル	整数	50

例：許可プロファイルへの属性の追加（admin用）

Dictionary Type	RADIUS Attribute	Attribute Type	Attribute Value
RADIUSオーディオコード	ACL認証レベル	整数	100

例：許可プロファイルへの属性の追加（セキュリティ管理者用）。

Dictionary Type	RADIUS Attribute	Attribute Type	Attribute Value
RADIUSオーディオコード	ACL認証レベル	整数	200

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。