使用RADIUS进行设备管理，使用身份服务引擎

目录

简介

本文档介绍各种思科和非思科产品期望从AAA服务器（如Cisco ISE）接收的属性的集合。

背景信息

思科和非思科产品期望从身份验证、授权和记帐(AAA)服务器接收属性集合。在这种情况下，服务器是思科ISE，并且ISE会返回这些属性以及Access-Accept作为授权配置文件(RADIUS)的一部分。

本文档提供有关如何添加自定义属性授权配置文件的分步说明，还包含设备列表和设备期望从AAA服务器返回的RADIUS属性。所有主题都包含示例。

本文档中提供的属性列表既不详尽，也不具有权威性，可以随时更改，无需更新本文档。

网络设备的设备管理通常通过TACACS+协议实现，但如果网络设备不支持TACACS+或ISE没有设备管理许可证，也可以通过RADIUS以及网络设备支持RADIUS设备管理来实现。某些设备支持这两种协议，并且由用户决定使用哪种协议，但是TACACS+可能比较有利，因为它具有命令授权和命令记帐等功能。

先决条件

要求

思科建议您了解以下内容：

- 思科ISE作为所关注网络上的RADIUS服务器
- Radius协议的工作流程- RFC2865

使用的组件

本文档中的信息基于思科身份服务引擎(ISE) 3.x和ISE的更高版本。

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

步骤1:创建供应商特定属性(VSA)

可以为每个供应商创建各种词典，并且可以将属性添加到每个词典中。每个词典可以具有多个可在授权配置文件中使用的属性。通常，每个属性都定义用户登录网络设备时可以获得的设备管理不同角色。但是，该属性可用于在网络设备上执行不同操作或进行不同配置。

ISE附带为少数供应商预定义的属性。如果供应商未列出，可以将其添加为具有属性的词典。对于某些网络设备，属性是可配置的，并且可以针对各种访问类型进行更改，在这种情况下，必须使用网络设备期望的不同访问类型属性来配置ISE。

预期通过Radius Access-Accept发送的属性定义如下：

1. 导航到策略>Policy元素>词典>System > Radius > Radius供应商>Add。

2. 系统将输入并保存名称和供应商ID。

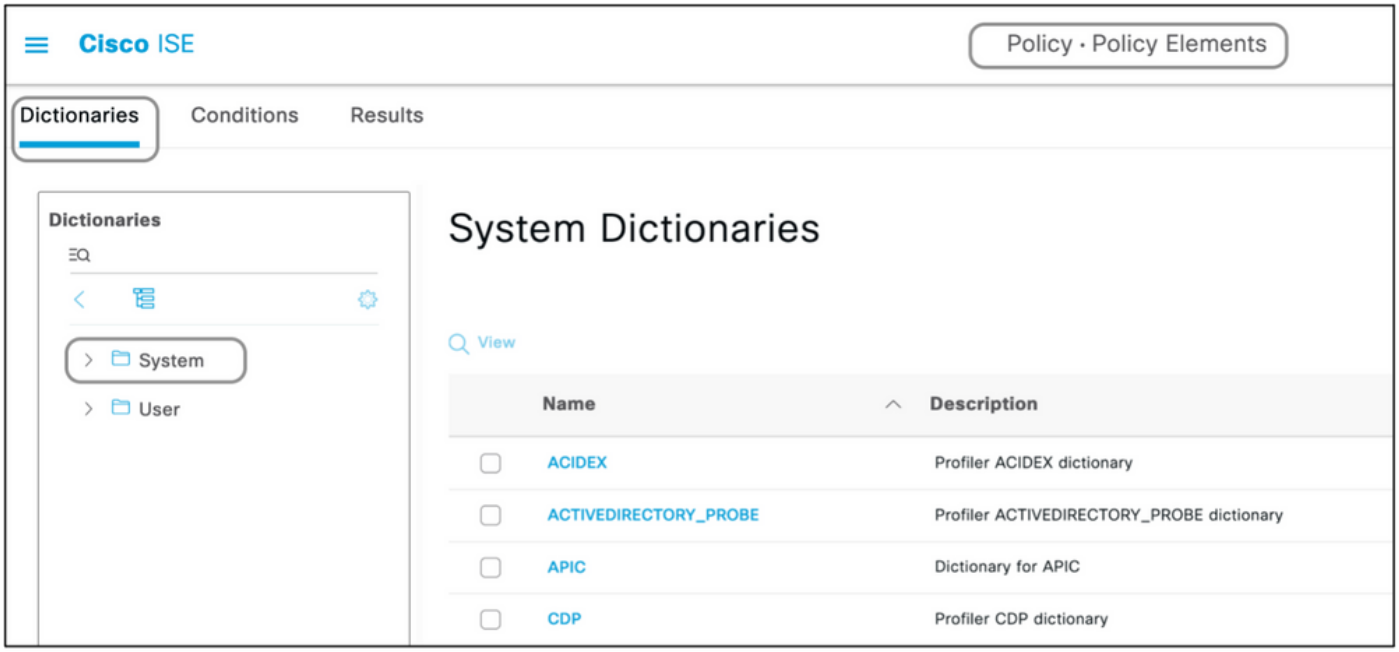
3. 单击保存的Radius供应商，然后导航到字典属性。

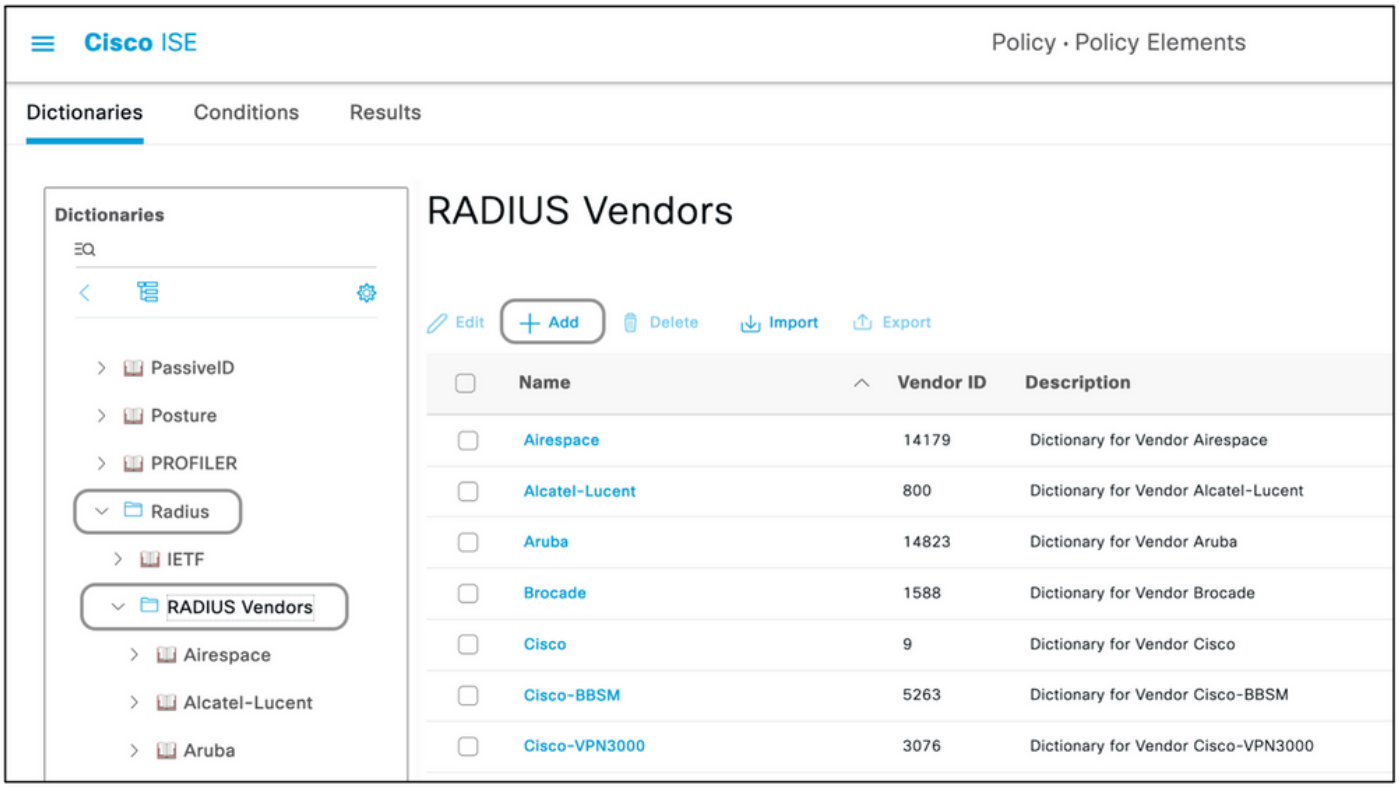
4. 单击Add并填写区分大小写的属性名称、数据类型、方向和ID。

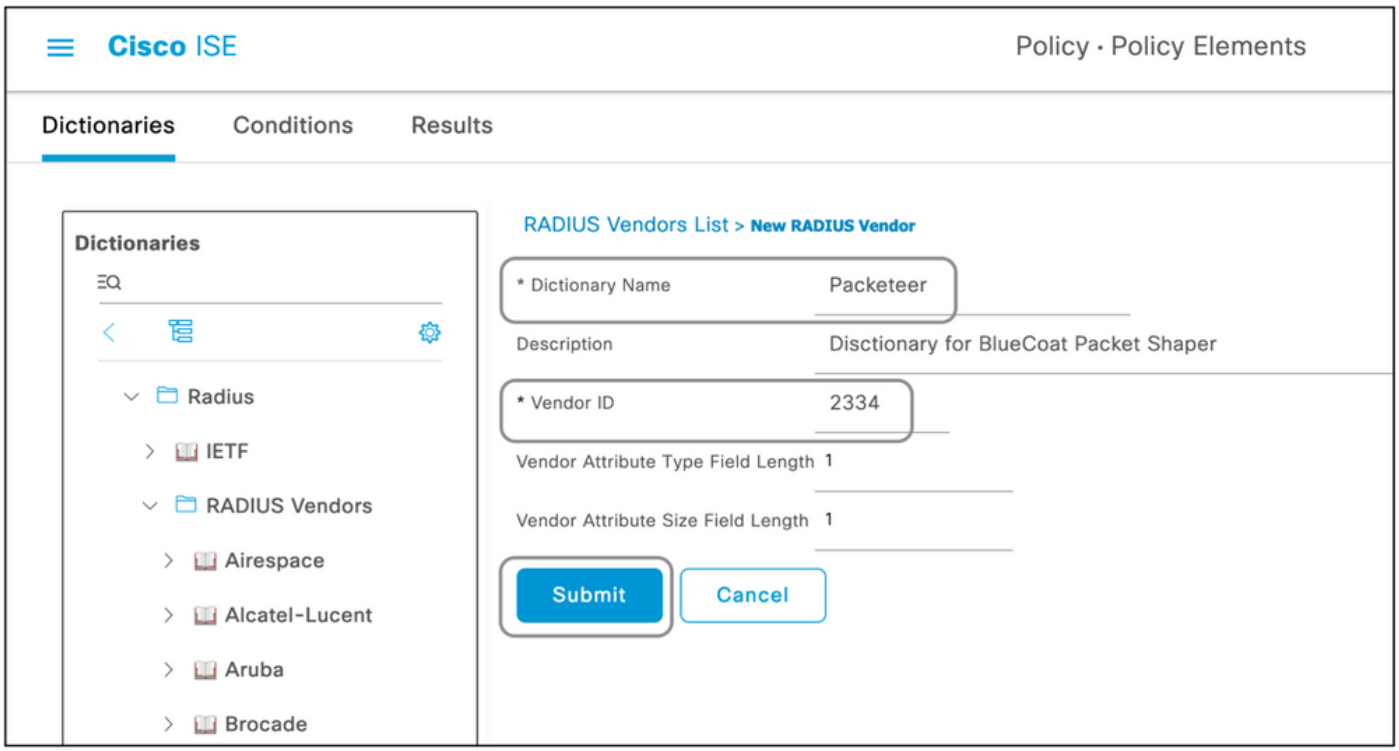
5. 保存属性。

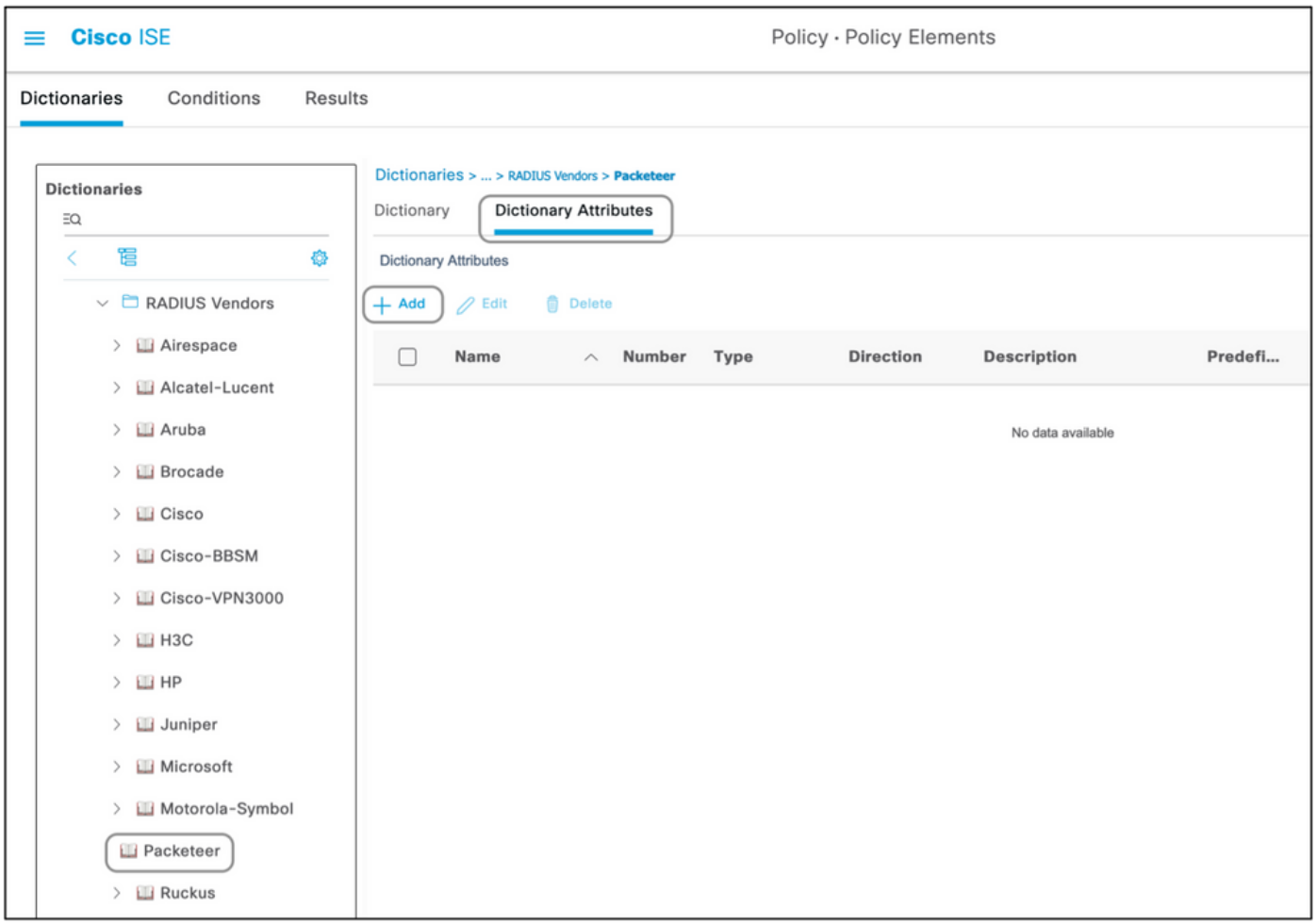
6. 如果要向同一词典添加多个属性，请在同一页面上添加其他属性。

注意：作为此部分中的值输入的每个字段将由供应商自己提供。如果不知道供应商网站，可以访问供应商网站或联系供应商支持。


Cisco ISE
Policy · Policy Elements
Dictionaries
Conditions
Results
Dictionaries
System
User
System Dictionaries
View
Name
Description
ACIDEX
Profiler ACIDEX dictionary
ACTIVEDIRECTORY_PROBE
Profiler ACTIVEDIRECTORY_PROBE dictionary
APIC
Dictionary for APIC
CDP
Profiler CDP dictionary


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


Cisco ISE
Policy · Policy Elements
Dictionaries
Conditions
Results
Dictionaries
RADIUS Vendors
Airespace
Alcatel-Lucent
Aruba
Brocade
Cisco
Cisco-BBSM
Cisco-VPN3000
H3C
HP
Juniper
Microsoft
Motorola-Symbol
Packeteer
Ruckus
Dictionaries > ... > RADIUS Vendors > Packeteer
Dictionary
Dictionary Attributes
Dictionary Attributes
Add
Edit
Delete
Name
Number
Type
Direction
Description
Predefi...
No data available

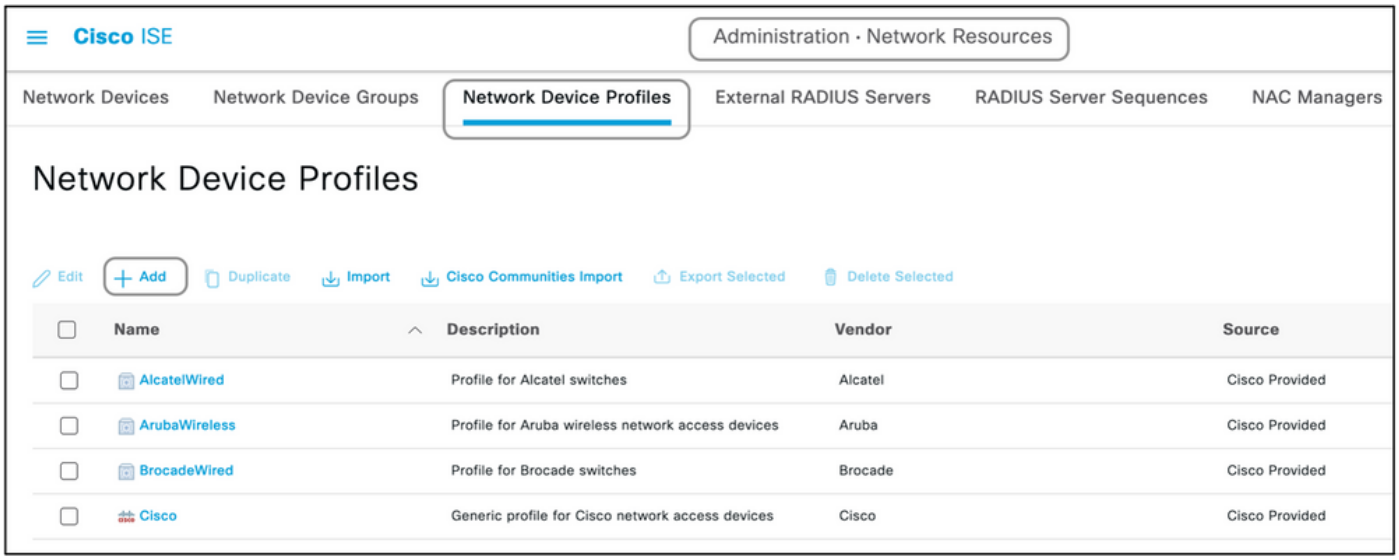
注意：并非所有供应商都要求添加特定词典。如果供应商可以使用IETF定义的RADIUS属性（已存在于ISE上），则可以跳过此步骤。

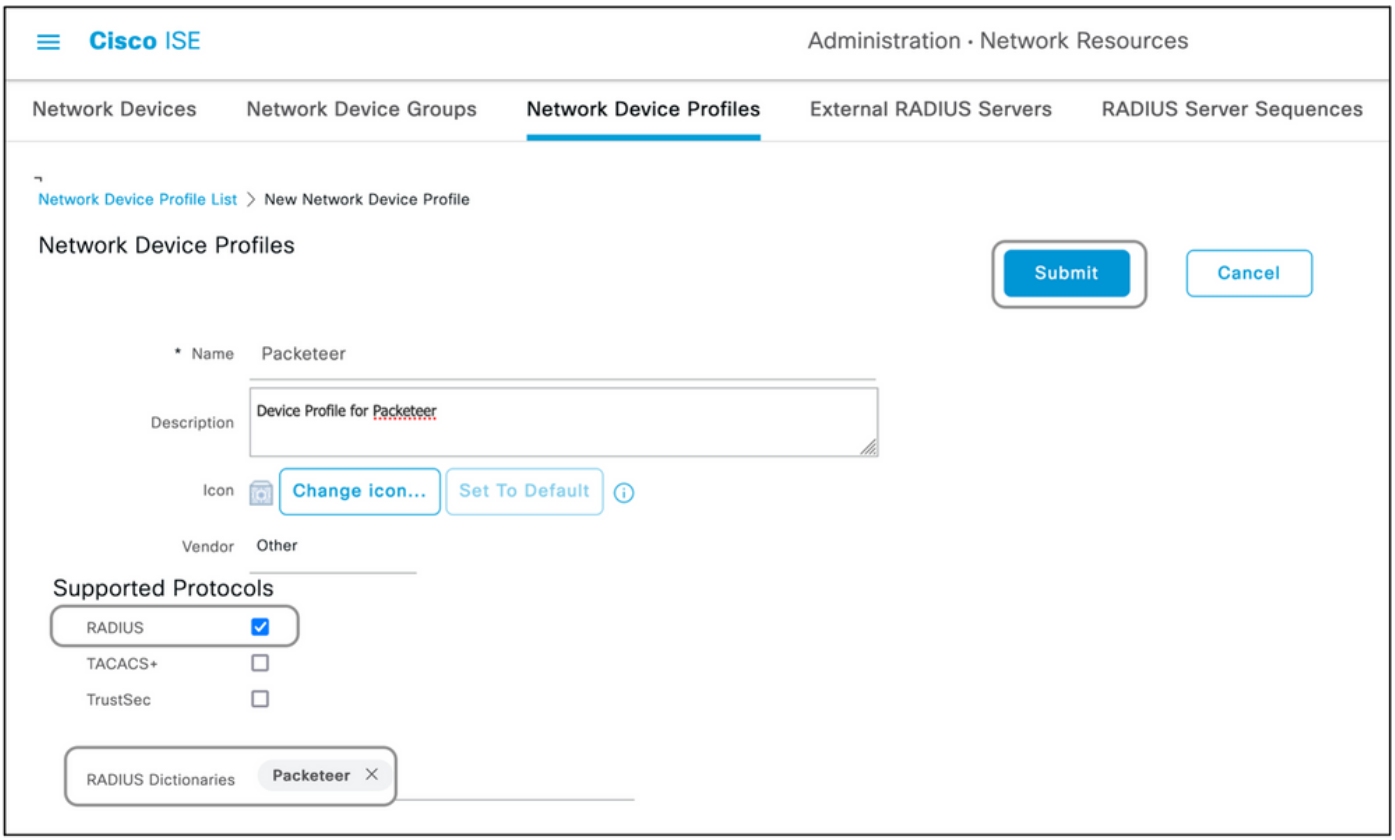
第二步：创建网络设备配置文件

此部分不是强制性的。网络设备配置文件有助于分离所添加的网络设备的类型，并为其创建适当的授权配置文件。与radius词典一样，ISE也有一些可以使用的预定义配置文件。如果不存在，则可以创建新的设备配置文件。

以下是添加网络配置文件的步骤：

1. 导航到管理>网络资源>网络设备配置文件>添加。
2. 指定名称并选中RADIUS所对应的框。
3. 在RADIUS Dictionaries下，选择上一部分中创建的词典。
4. 如果为相同类型的设备创建了多个词典，则可以在RADIUS词典下选择所有这些词典。
5. 保存配置文件。





第三步：在ISE上添加网络设备

设备管理所在的网络设备必须随在网络设备上定义的密钥一起添加到ISE中。在网络设备上，使用此密钥将ISE添加为RADIUS AAA服务器。

以下是在ISE上添加设备的步骤：

1. 导航到管理>网络资源>网络设备>添加。

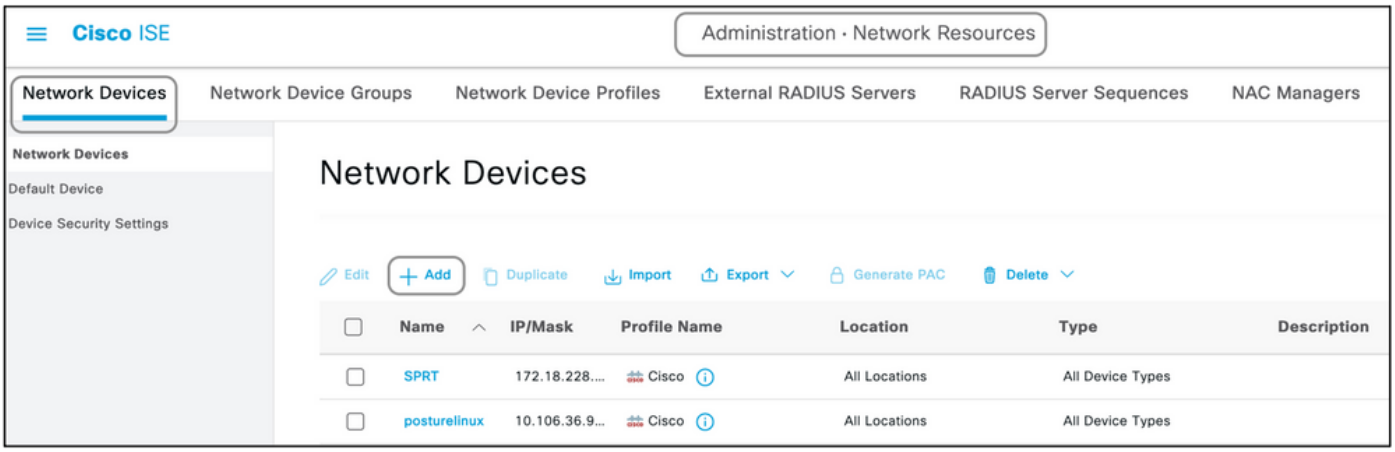
2. 提供名称和IP地址。

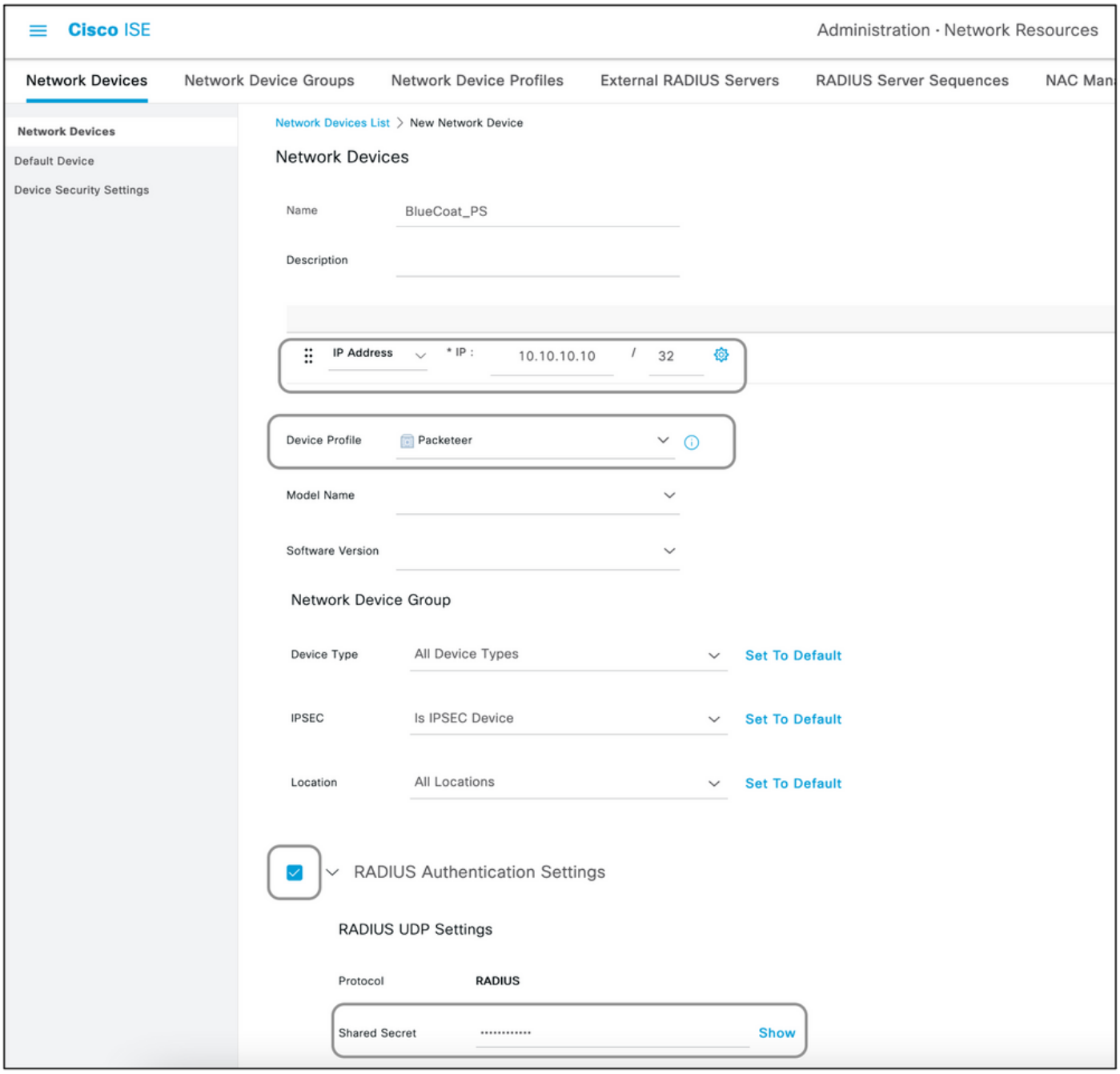
3. 可以从下拉列表中选择设备配置文件，使其成为上一节中定义的配置文件。如果未创建配置文

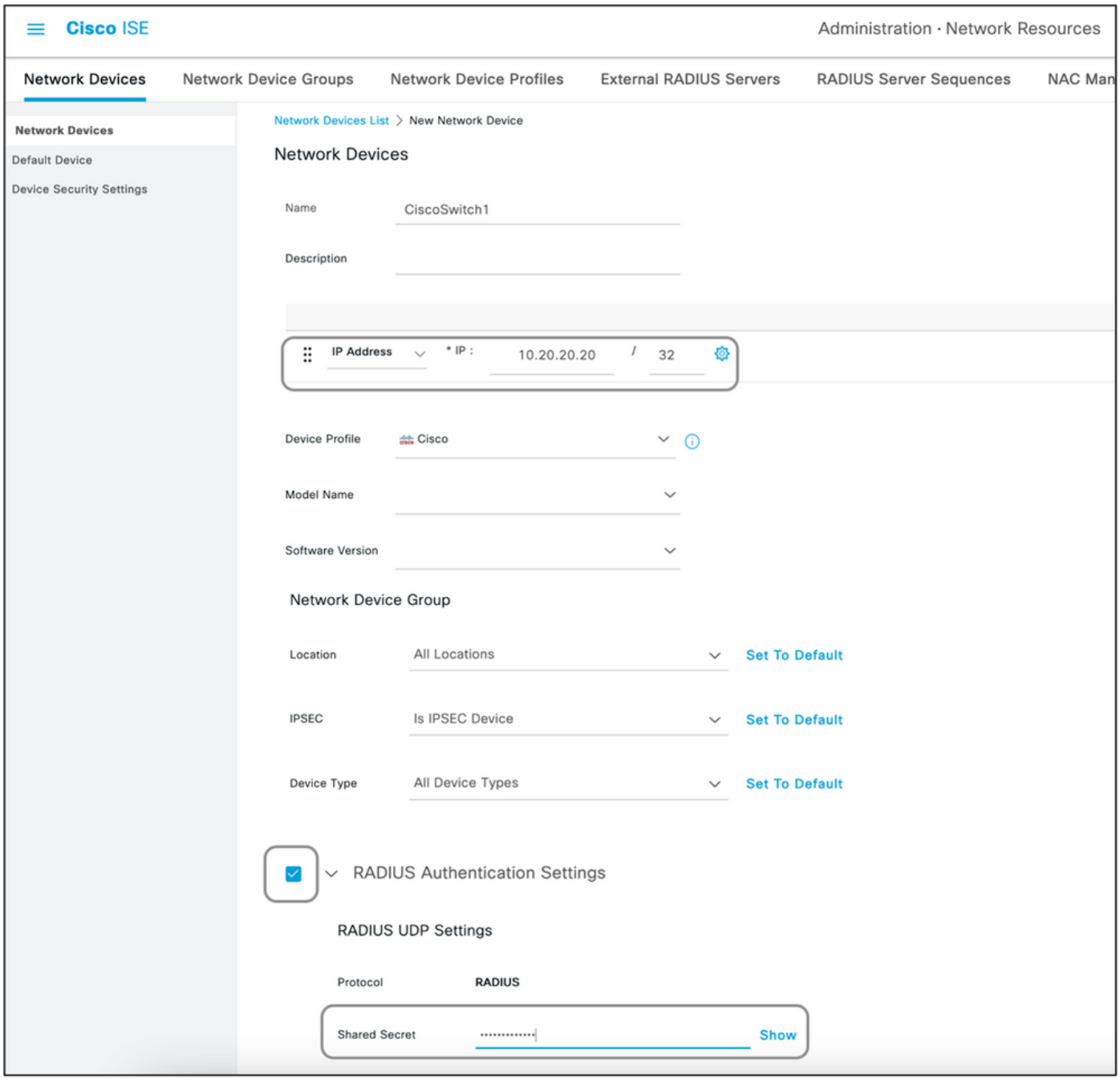
件，则可以使用默认思科。

4. 检查Radius身份验证设置。

5. 输入共享密钥并保存设备。




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



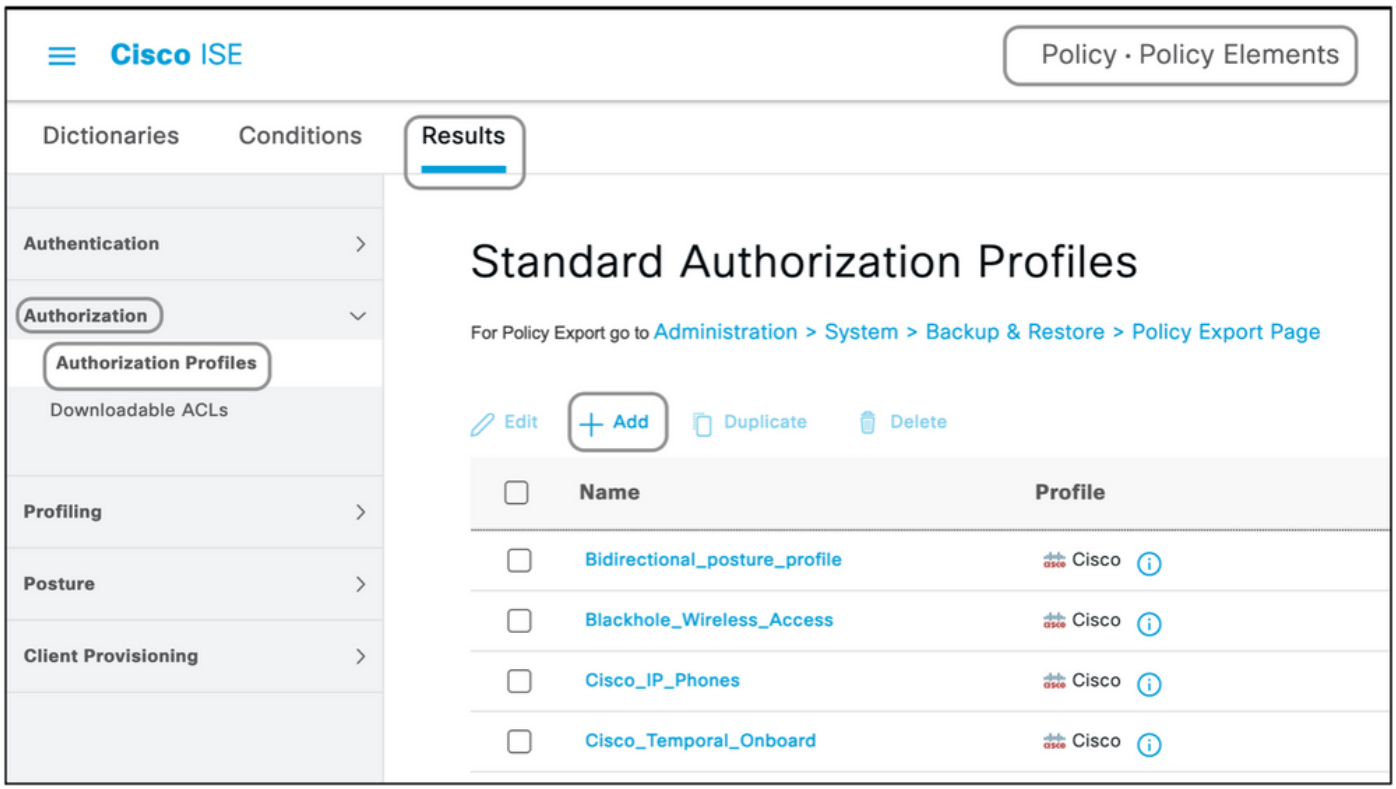
第四步：创建授权配置文件

从ISE推送的最终结果作为访问接受或访问拒绝在授权配置文件中定义。每个授权配置文件都可以推送网络设备期望的其他属性。

以下是创建授权配置文件的步骤：

1. 导航到策略>Policy元素>结果>授权>授权配置文件。

2. 在Standard Authorization Profiles下，单击Add。



可以添加的配置文件类型是Access-Accept和Access-Reject。

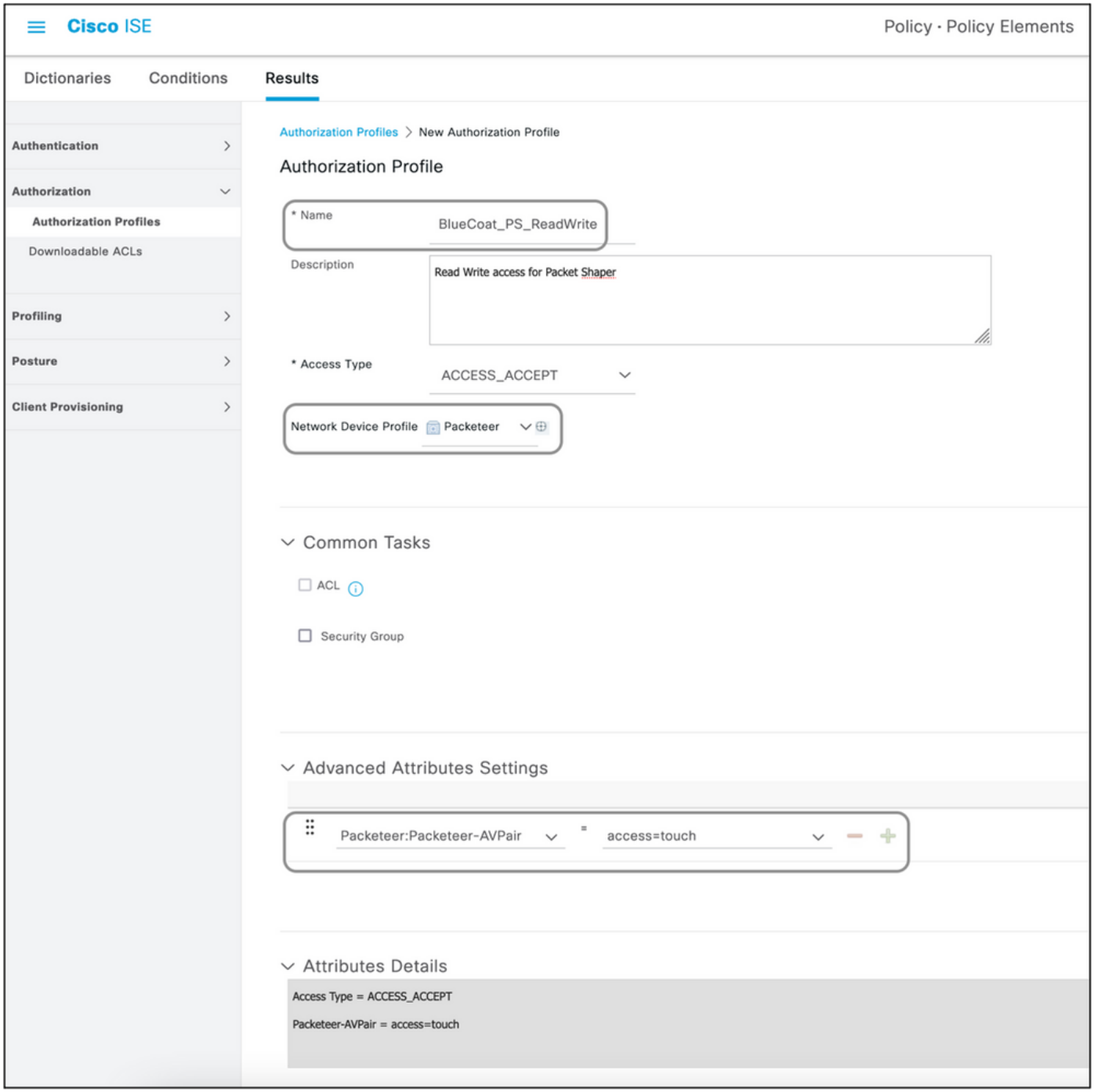
创建Access-Accept配置文件

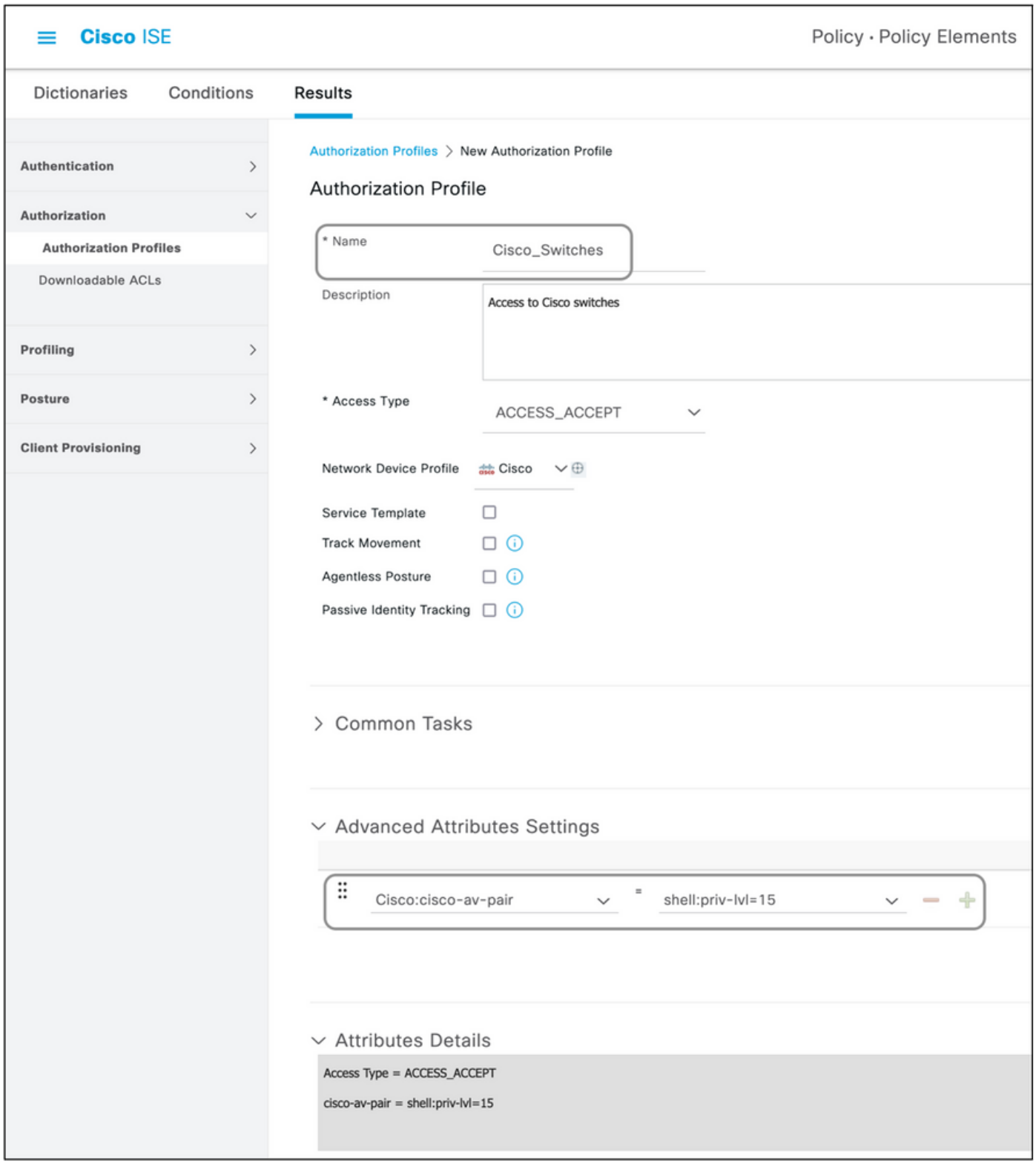
此配置文件用于以某种方式访问网络设备。此配置文件可同时传递多个属性。步骤如下：

1. 提供一个合理的名称，然后选择Access Type作为Access-Accept。
2. 选择在先前章节之一中创建的网络设备配置文件。如果未创建配置文件，则可以使用默认思科。
3. 选择不同类型的配置文件后，此处的页面会限制配置选项。
4. 在Advanced Attributes Settings下，选择词典和适用的属性(LHS)。
5. 从下拉列表中为属性分配值(RHS)（如果可用）或键入预期值。
6. 如果作为同一结果的一部分要发送多个属性，请点击+图标并重复步骤4和5。

为ISE预期发送的每个结果/角色/授权创建多个授权配置文件。

注：可以在“属性详细信息”字段下验证合并的属性。


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



创建Access-Reject配置文件

此配置文件用于发送拒绝设备管理的消息，但仍可用于同时发送属性。这用于发送Radius Access-Reject数据包。除必须选择Access-Reject而不是Access-Accept作为访问类型的步骤外，这些步骤保持不变。

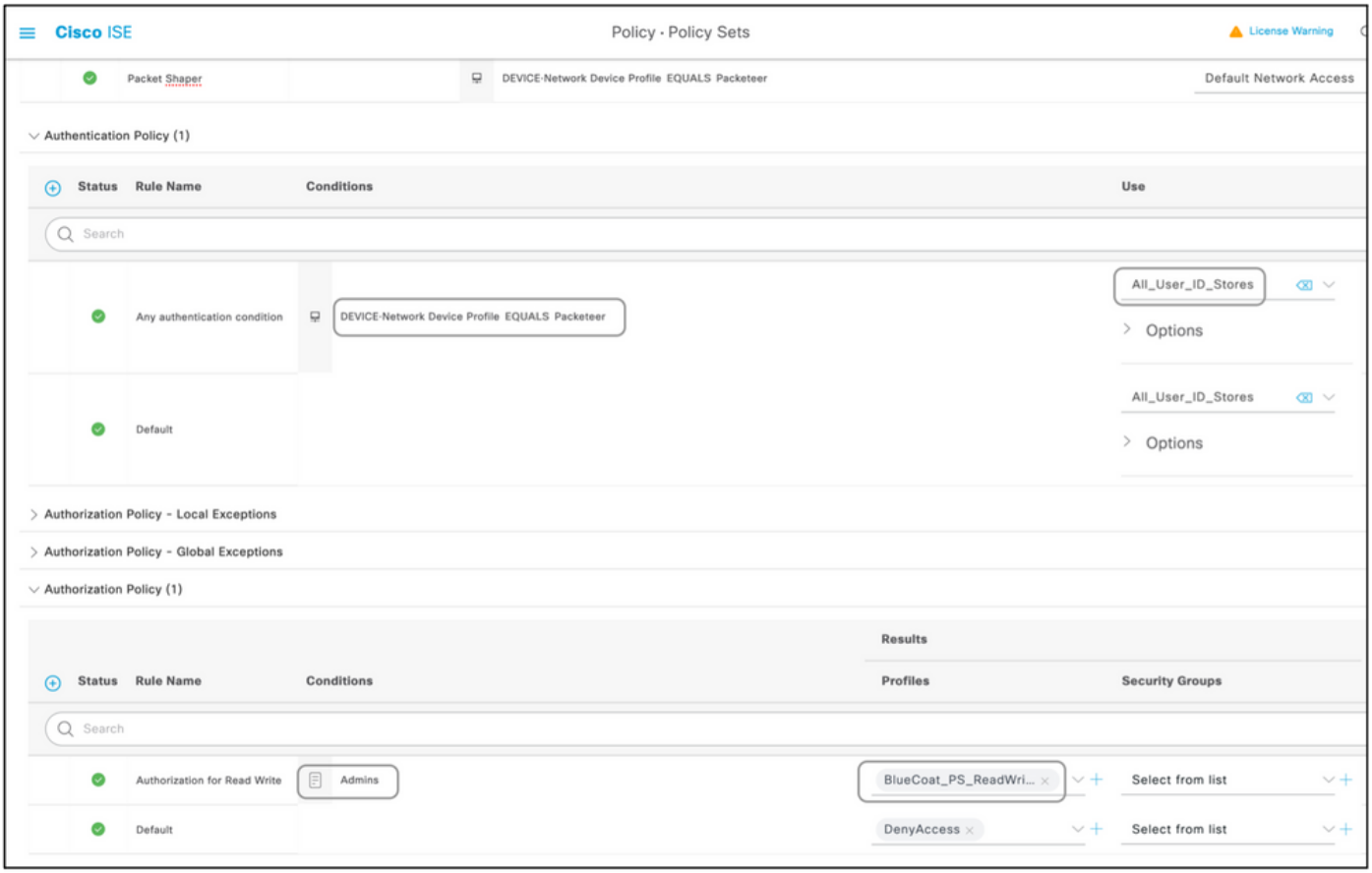
第五步：创建策略集

ISE上的策略集从上到下进行评估，第一个满足策略集中条件设置的策略集负责ISE对网络设备发送

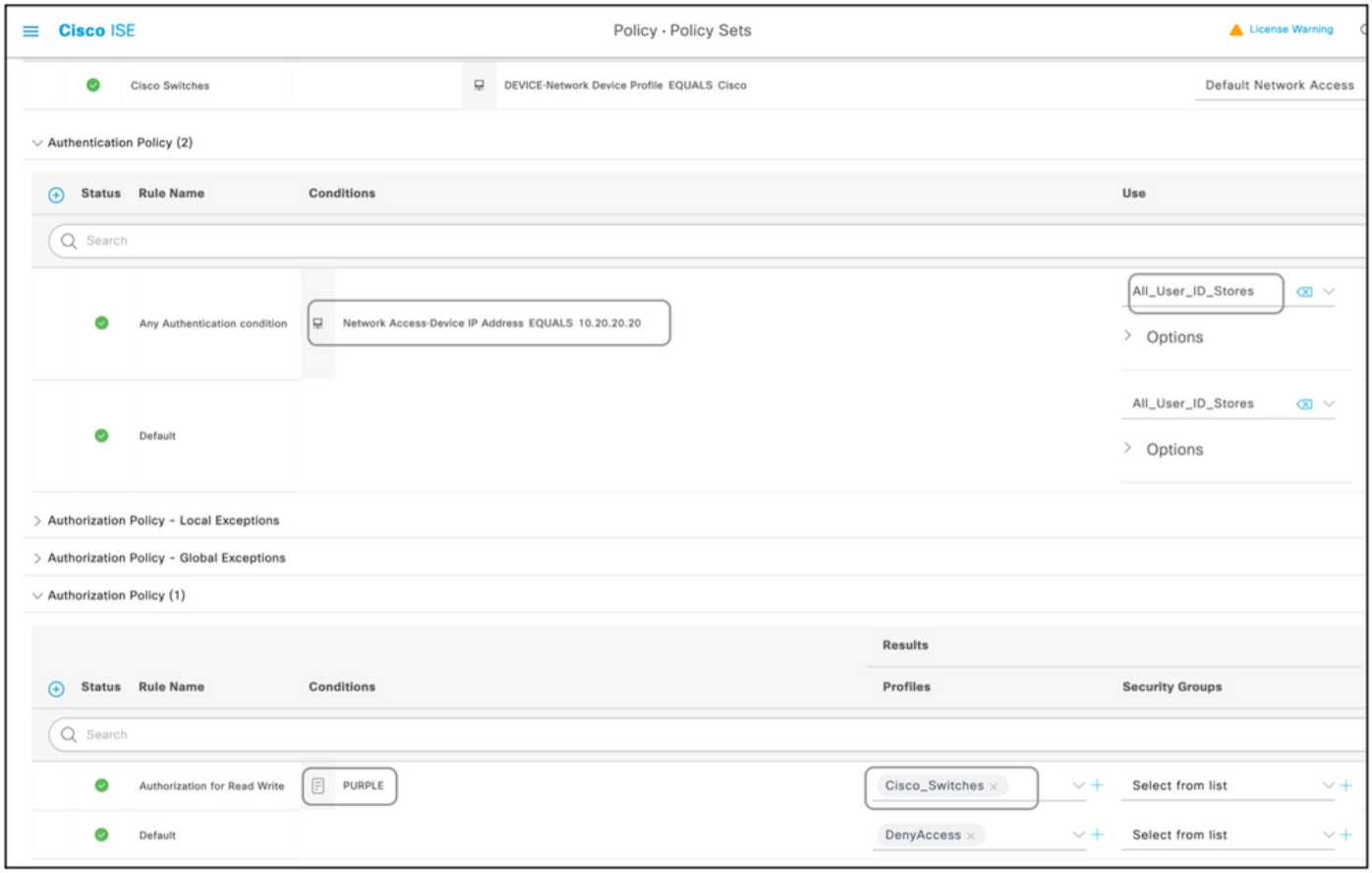
的RADIUS访问请求数据包的响应。思科建议为每种类型的设备设置一个唯一的策略。评估用户身份验证和授权的条件发生在评估时。如果ISE具有外部身份源，可用于授权类型。

典型的策略集创建方法如下：

1. 导航到策略>策略集> +。
2. 重命名New Policy Set 1。
3. 将条件设置为对于此设备唯一。
4. 展开Policy Set。
5. 展开Authentication Policy以设置身份验证规则。外部源或内部用户可用作身份源序列，ISE将根据这些序列检查用户。
6. 身份验证策略已全部设置。此时可以保存策略。
7. 展开Authorization Policy为用户添加授权条件。例如，检查特定AD组或ISE内部身份组。同样命名规则。
8. 可以从下拉列表中选择授权规则的结果。
9. 为供应商支持的不同类型的访问创建多个授权规则。


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



设备列表

通过Radius支持设备管理的任何设备都可以添加到ISE，只需对上一节中提到的所有步骤进行一些修改。因此，本文档列出了使用此部分提供的信息使用的设备。 本文档中提供的属性和值列表既不详尽，也不具有权威性，可以随时更改，无需更新本文档。请咨询供应商网站和供应商支持，以进行验证。

聚合服务路由器(ASR)

无需为此创建单独的字典和VSA，因为它使用ISE上已存在的思科AV对。

属性：cisco-av-pair

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

用法：将<role-name>的值设置为路由器上本地定义的角色的名称。角色层次结构可以用树来描述，其中role#rootis位于树顶部，role#leafer添加其他命令。如果为：shell：tasks="#root，#leaf"，这两个角色可以组合在一起并传回。

权限还可以按单个进程传回，以便授予用户对特定进程的读取、写入和执行权限。例如，要授予用户对BGP进程的读写权限，请将该值设置为：shell：tasks="#root，rw：bgp"。属性的顺序并不重要；不管值是设置为toshell：tasks="#root，rw：bgp"还是toshell：tasks="rw：bgp，#root"，结果都是相同的。

示例：将属性添加到授权配置文件。

词典类型	RADIUS属性	属性类型	属性值
RADIUS-Cisco	Cisco-AV-pair	字符串	shell：tasks="#root，#leaf，rwx：bgp，r：ospf"

Cisco交换机IOS®和Cisco IOS® XE

无需为此创建单独的字典和VSA，因为它使用ISE上已存在的RADIUS属性。

属性：cisco-av-pair

值：shell：priv-lvl=<level>

用法：将<level>的值设置为要发送的权限数。通常，如果发送15，则表示读写；如果发送7，则表示只读。

示例：将属性添加到授权配置文件。

词典类型	RADIUS属性	属性类型	属性值
RADIUS-Cisco	Cisco-AV-pair	字符串	shell：priv-lvl=15

BlueCoat数据包整形器

属性：Packeter-AVPair

值：access=<level>

Usage：<level>是授予的访问权限级别。Touch访问等效于读写，而look访问等效于只读。

使用下列值创建词典（如本文档所示）：

- 名称：Packeter
- 供应商ID：2334
- 供应商长度字段大小：1
- 供应商类型字段大小：1

输入属性的详细信息：

- 属性：Packeter-AVPair
- 说明：用于指定访问级别
- 供应商属性ID：1
- 方向：OUT
- 允许多个：False
- 允许标记：未选中
- 属性类型：字符串

示例：将属性添加到授权配置文件（用于只读访问）。

词典类型	RADIUS属性	属性类型	属性值

RADIUS打包程序	数据包AVPair	字符串	access=look

示例：将属性添加到授权配置文件（用于读写访问）。

词典类型	RADIUS属性	属性类型	属性值
RADIUS打包程序	数据包AVPair	字符串	access=touch

BlueCoat代理服务器(AV/SG)

属性：Blue-Coat-Authorization

值： <level>

Usage：<level>是授予的访问权限级别。0表示无访问，1表示只读访问，2表示读写访问。 Blue-Coat-Authorization属性是负责访问级别的属性。

使用下列值创建词典（如本文档所示）：

- 名称：BlueCoat
- 供应商ID：14501
- 供应商长度字段大小：1
- 供应商类型字段大小：1

输入属性的详细信息：

- 属性：Blue-Coat-Group
- 供应商属性ID：1
- 方向：两者
- 允许多个：False
- 允许标记：未选中
- 属性类型：无符号整数32 (UINT32)

输入第二个属性的详细信息：

- 属性：Blue-Coat-Authorization
- 说明：用于指定访问级别
- 供应商属性ID：2
- 方向：两者
- 允许多个：False
- 允许标记：未选中
- 属性类型：无符号整数32 (UINT32)

示例：将属性添加到授权配置文件（用于无访问权限）。

词典类型	RADIUS属性	属性类型	属性值
RADIUS-BlueCoat	Blue-Coat组	UINT32	0

示例：将属性添加到授权配置文件（用于只读访问）。

词典类型	RADIUS属性	属性类型	属性值
RADIUS-BlueCoat	Blue-Coat组	UINT32	1

示例：将属性添加到授权配置文件（用于读写访问）。

词典类型	RADIUS属性	属性类型	属性值
RADIUS-BlueCoat	Blue-Coat组	UINT32	2

Brocade交换机

无需为此创建单独的字典和VSA，因为它使用ISE上已存在的RADIUS属性。

属性：Tunnel-Private-Group-ID

值：U：<VLAN1>；T：<VLAN2>

用法：将<VLAN1>设置为数据VLAN的值。将<VLAN2>设置为语音VLAN的值。在本例中，数据VLAN是VLAN 10，语音VLAN是VLAN 21。

示例：将属性添加到授权配置文件。

词典类型	RADIUS属性	属性类型	属性值
RADIUS-IETF	Tunnel-Private-Group-ID	标记字符串	U：10；T：21

Infoblox

属性：Infoblox-Group-Info

值：<group-name>

Usage：<group-name>是具有授予用户的权限的组的名称。必须在Infoblox设备上配置此组。在此配置示例中，组名称为MyGroup。

使用下列值创建词典（如本文档所示）：

- 名称：Infoblox
- 供应商ID：7779
- 供应商长度字段大小：1
- 供应商类型字段大小：1

输入属性的详细信息：

- 属性：Infoblox-Group-Info
- 供应商属性ID：009
- 方向：OUT
- 允许多个：False
- 允许标记：未选中

- 属性类型：字符串

示例：将属性添加到授权配置文件。

词典类型	RADIUS属性	属性类型	属性值
RADIUS-Infoblox	Infoblox-Group-Info	字符串	我的组

思科Firepower管理中心

无需为此创建单独的字典和VSA，因为它使用ISE上已存在的RADIUS属性。

属性：cisco-av-pair

值：Class-[25]=<role>

用法：将<role>的值设置为FMC上本地定义的角色名称。在FMC上创建多个角色（例如管理员和只读用户），并将值分配给ISE上要由FMC接收的属性。

示例：将属性添加到授权配置文件。

词典类型	RADIUS属性	属性类型	属性值
RADIUS-Cisco	Cisco-AV-pair	字符串	Class-[25]=NetAdmins

Nexus交换机

无需为此创建单独的字典和VSA，因为它使用ISE上已存在的RADIUS属性。

属性：cisco-av-pair

值：shell：roles="<role1> <role2>"

用法：将<role1>和<role2>的值设置为交换机上本地定义的角色名称。创建多个角色时，请使用空格字符分隔这些角色。当多个角色从AAA服务器传回Nexus交换机时，结果是用户可以访问由所有三个角色联合定义的命令。

内置角色在配置用户帐户和RBAC中进行定义。

示例：将属性添加到授权配置文件。

词典类型	RADIUS属性	属性类型	属性值
RADIUS-Cisco	Cisco-AV-pair	字符串	shell：角色="network-admin vdc-admin vdc-operator"

无线局域网控制器(WLC)

无需为此创建单独的字典和VSA，因为它使用ISE上已存在的RADIUS属性。

属性：服务类型

值：管理(6) / NAS提示(7)

用法：要授予用户对无线局域网控制器(WLC)的读/写访问权限，值必须为Administrative；对于只读访问权限，值必须为NAS-Prompt。

有关详细信息，请参阅无线局域网控制器(WLC)上管理用户的RADIUS服务器身份验证配置示例

示例：将属性添加到授权配置文件（用于只读访问）。

词典类型	RADIUS属性	属性类型	属性值
RADIUS-IETF	服务类型	枚举	NAS提示符

示例：将属性添加到授权配置文件（用于读写访问）。

词典类型	RADIUS属性	属性类型	属性值
RADIUS-IETF	服务类型	枚举	管理

数据中心网络管理器(DCNM)

更改身份验证方法后，必须重新启动DCNM。否则，它可分配网络操作员权限而非网络管理员。

无需为此创建单独的字典和VSA，因为它使用ISE上已存在的RADIUS属性。

属性：cisco-av-pair

值：shell：roles=<role>

DCNM角色	RADIUS Cisco-AV-Pair
用户	shell：角色= "network-operator"
管理员	外壳：角色= "network-admin"

音频代码

属性：ACL身份验证级别

值：ACL-Auth-Level =“<integer>”

Usage：<integer>是要授予的访问权限级别。ACL-Auth-Level属性值（用户名为ACL-Auth-UserLevel）为50，ACL-Auth-Level属性值（管理员名为ACL-Auth-AdminLevel）为100，ACL-Auth-Level值（安全管理员名为ACL-Auth-SecurityAdminLevel）为200。可以跳过这些名称，属性值可直接作为授权配置文件高级AV对的值提供。

使用下列值创建词典（如本文档所示）：

- 名称：AudioCodes
- 供应商编号：5003

- 供应商长度字段大小：1
- 供应商类型字段大小：1

输入属性的详细信息：

- 属性：ACL-Auth-Level
- 说明：用于指定访问级别
- 供应商属性ID：35
- 方向：OUT
- 允许多个：False
- 允许标记：未选中
- 属性类型：整数

示例：将属性添加到授权配置文件（针对用户）。

词典类型	RADIUS属性	属性类型	属性值
RADIUS音频代码	ACL身份验证级别	整数	50

示例：将属性添加到授权配置文件（对于管理员）。

词典类型	RADIUS属性	属性类型	属性值
RADIUS音频代码	ACL身份验证级别	整数	100

示例：将属性添加到授权配置文件（适用于安全管理员）。

词典类型	RADIUS属性	属性类型	属性值
RADIUS音频代码	ACL身份验证级别	整数	200

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）。