Uso de RADIUS para la administración de dispositivos con Identity Services Engine

Contenido

Introducción

Este documento describe la compilación de atributos que varios productos de Cisco y de otros fabricantes esperan recibir de un servidor AAA como Cisco ISE.

Antecedentes

Los productos de Cisco y de terceros esperan recibir una compilación de atributos de un servidor de autenticación, autorización y contabilidad (AAA). En este caso, el servidor es un Cisco ISE e ISE devolvería estos atributos junto con una aceptación de acceso como parte de un perfil de autorización (RADIUS).

Este documento proporciona instrucciones paso a paso sobre cómo agregar perfiles de autorización de atributos personalizados y también contiene una lista de dispositivos y los atributos RADIUS que los dispositivos esperan ver devueltos por el servidor AAA. Todos los temas incluyen ejemplos.

La lista de atributos proporcionada en este documento no es exhaustiva ni autorizada y puede cambiar en cualquier momento sin una actualización de este documento.

La administración de dispositivos de un dispositivo de red se consigue generalmente con el protocolo TACACS+, pero si el dispositivo de red no es compatible con TACACS+ o si ISE no tiene una licencia de administración de dispositivos, también se puede conseguir con RADIUS si el dispositivo de red admite la administración de dispositivos RADIUS. Algunos dispositivos soportan ambos protocolos y depende de los usuarios decidir qué protocolo usar, pero TACACS+ puede ser favorable ya que tiene funciones como autorización de comandos y contabilidad de comandos.

Prerequisites

Requirements

Cisco recomienda que tenga el conocimiento de lo siguiente:

- Cisco ISE como servidor Radius en la red de interés
- El flujo de trabajo del protocolo Radius: RFC2865

Componentes Utilizados

La información de este documento se basa en Cisco Identity Services Engine (ISE) 3.x y versiones posteriores de ISE.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Paso 1. Crear los atributos específicos del proveedor (VSA)

Puede haber varios diccionarios creados para cada uno de los proveedores, y se pueden agregar atributos a cada uno de estos diccionarios. Cada diccionario puede tener varios atributos que se pueden utilizar en los perfiles de autorización. Cada atributo, en general, define la función diferente de administración de dispositivos que un usuario podría obtener cuando inicia sesión en el dispositivo de red. Sin embargo, el atributo puede estar pensado para diferentes propósitos de operación o configuración en el dispositivo de red.

ISE incluye atributos predefinidos para unos pocos proveedores. Si el proveedor no aparece en la lista, se puede agregar como un diccionario con atributos. En el caso de algunos dispositivos de red, los atributos se pueden configurar y modificar para distintos tipos de acceso. En tal caso, ISE debe configurarse con los atributos que el dispositivo de red espera para los distintos tipos de acceso.

Los atributos que se espera que se envíen con una aceptación de acceso de RADIUS se definen como se muestra a continuación:

1. Navegue hasta Política > Elementos de Política > Diccionarios > Sistema > Radius > Proveedores Radius > Agregar.

2. El nombre y los ID de proveedor deben introducirse y guardarse.

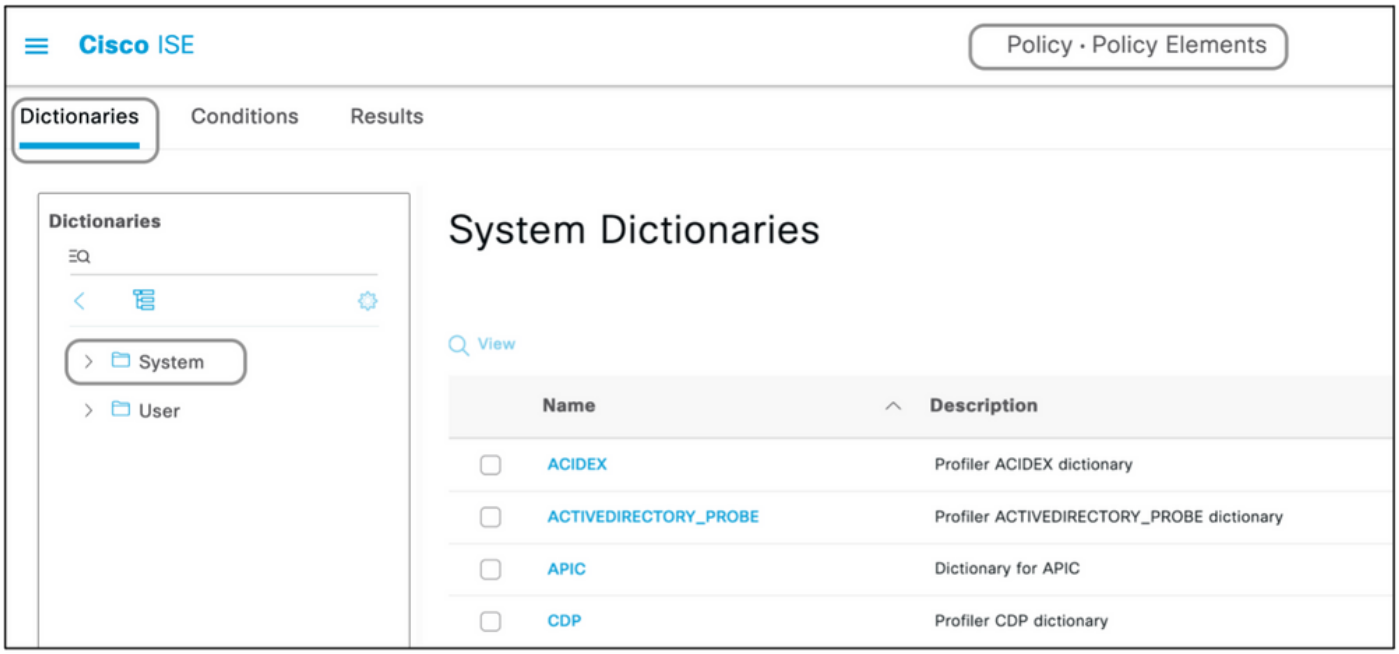
3. Haga clic en el proveedor Radius guardado y navegue hasta Atributos de diccionario.

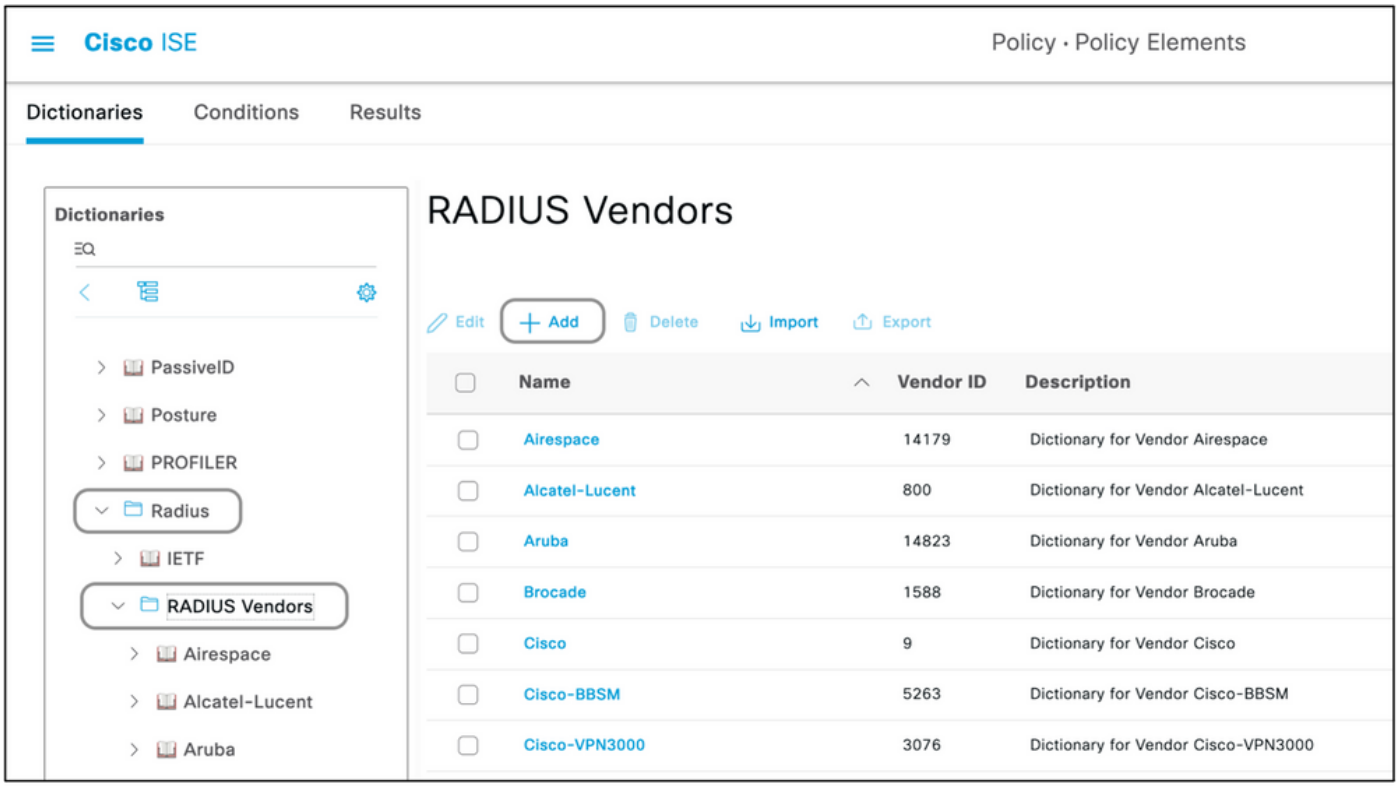
4. Haga clic en Agregar y rellene los campos Nombre de atributo, Tipo de datos, Dirección e ID, que distinguen entre mayúsculas y minúsculas.

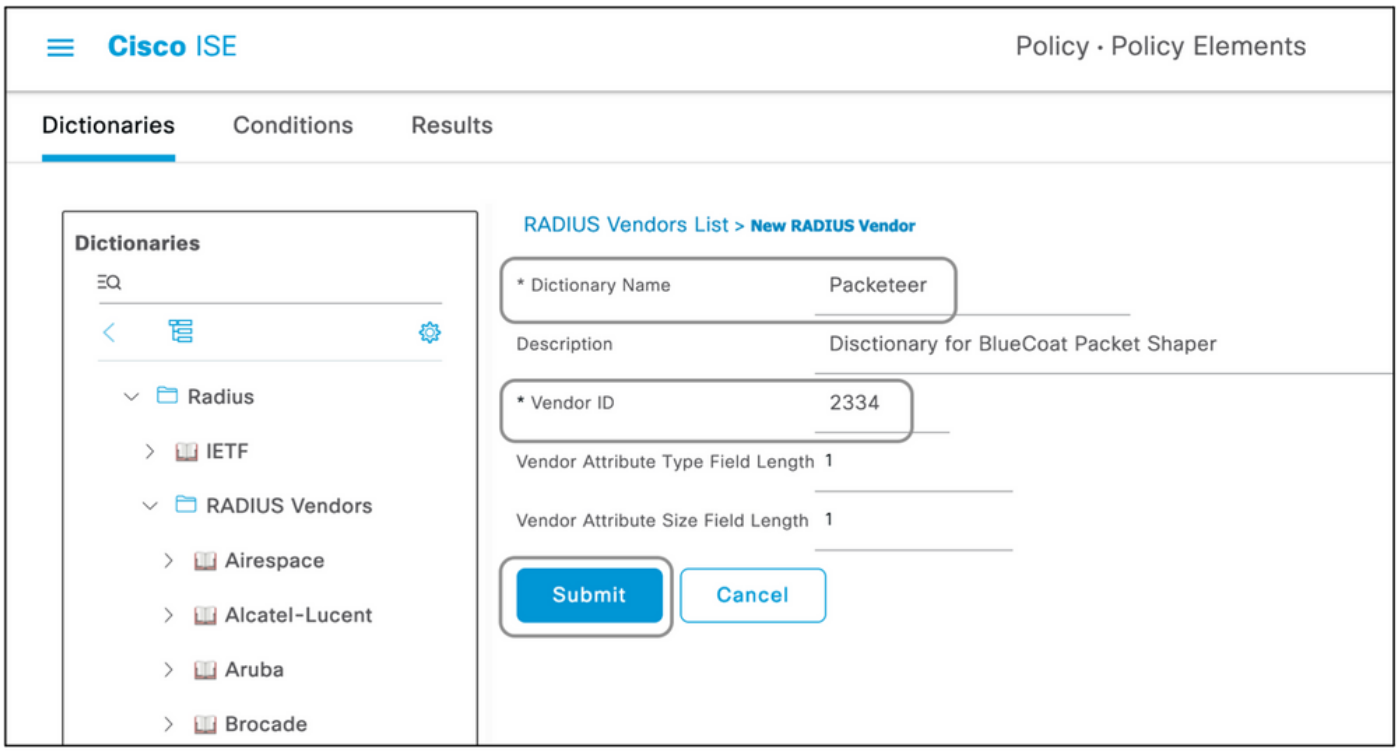
5. Guarde el atributo.

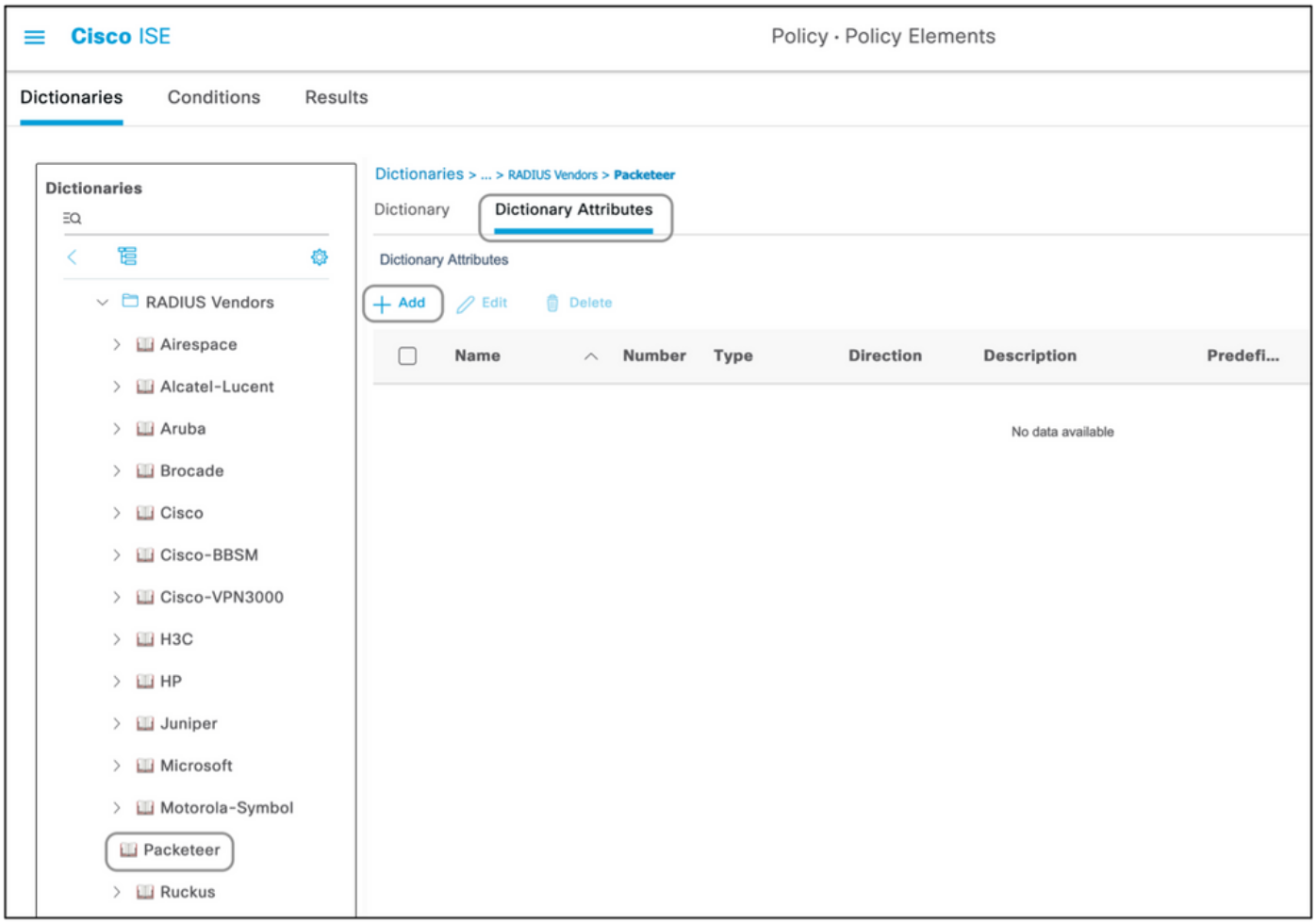
6. Agregue otros atributos en la misma página si hay varios atributos que agregar al mismo diccionario.

Nota: Cada uno de los campos introducidos como valores en esta sección debe proporcionarlo el propio proveedor. Es posible visitar los sitios web de los proveedores o ponerse en contacto con el servicio de asistencia para proveedores en caso de que no se conozcan.




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



Nota: no todos los proveedores necesitan que se agregue un diccionario específico. Si el proveedor puede utilizar los atributos radius definidos por IETF, que ya existen en ISE, se puede omitir este paso.

Paso 2. Crear un perfil de dispositivo de red

Esta sección no es obligatoria. Un perfil de dispositivo de red ayuda a separar el tipo de dispositivo de red que se agrega y a crear perfiles de autorización adecuados para ellos. Al igual que los diccionarios RADIUS, ISE tiene algunos perfiles predefinidos que se pueden utilizar. Si aún no está presente, se puede crear un nuevo perfil de dispositivo.

Este es el procedimiento para agregar un perfil de red :

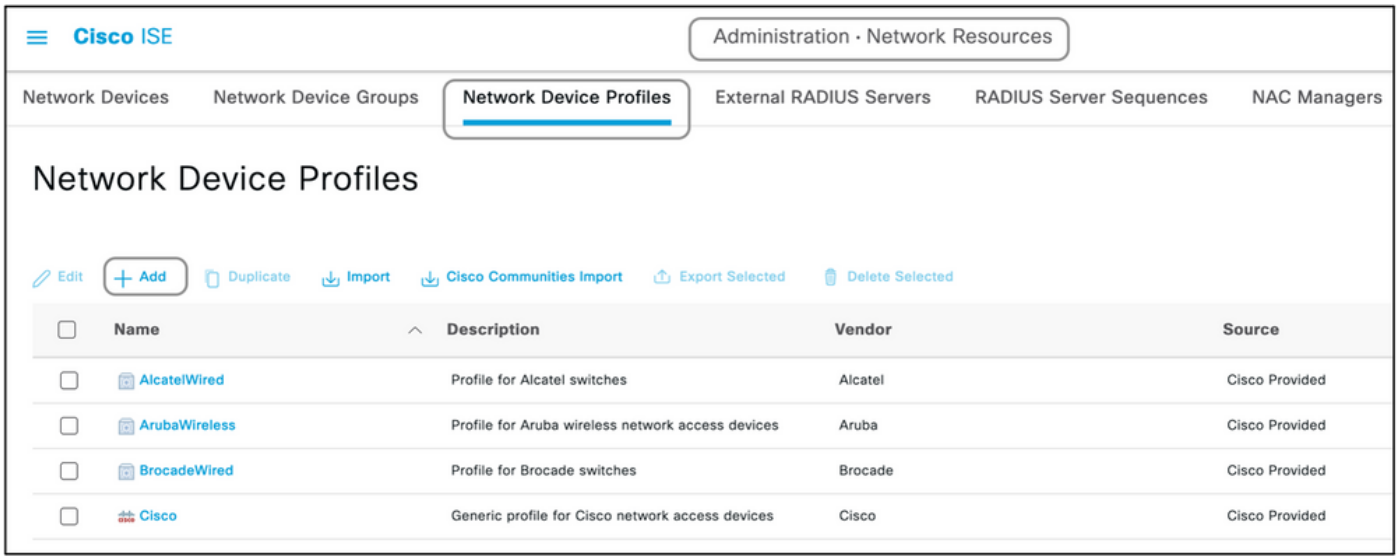
1. Vaya a Administration > Network Resources > Network Device Profiles > Add.

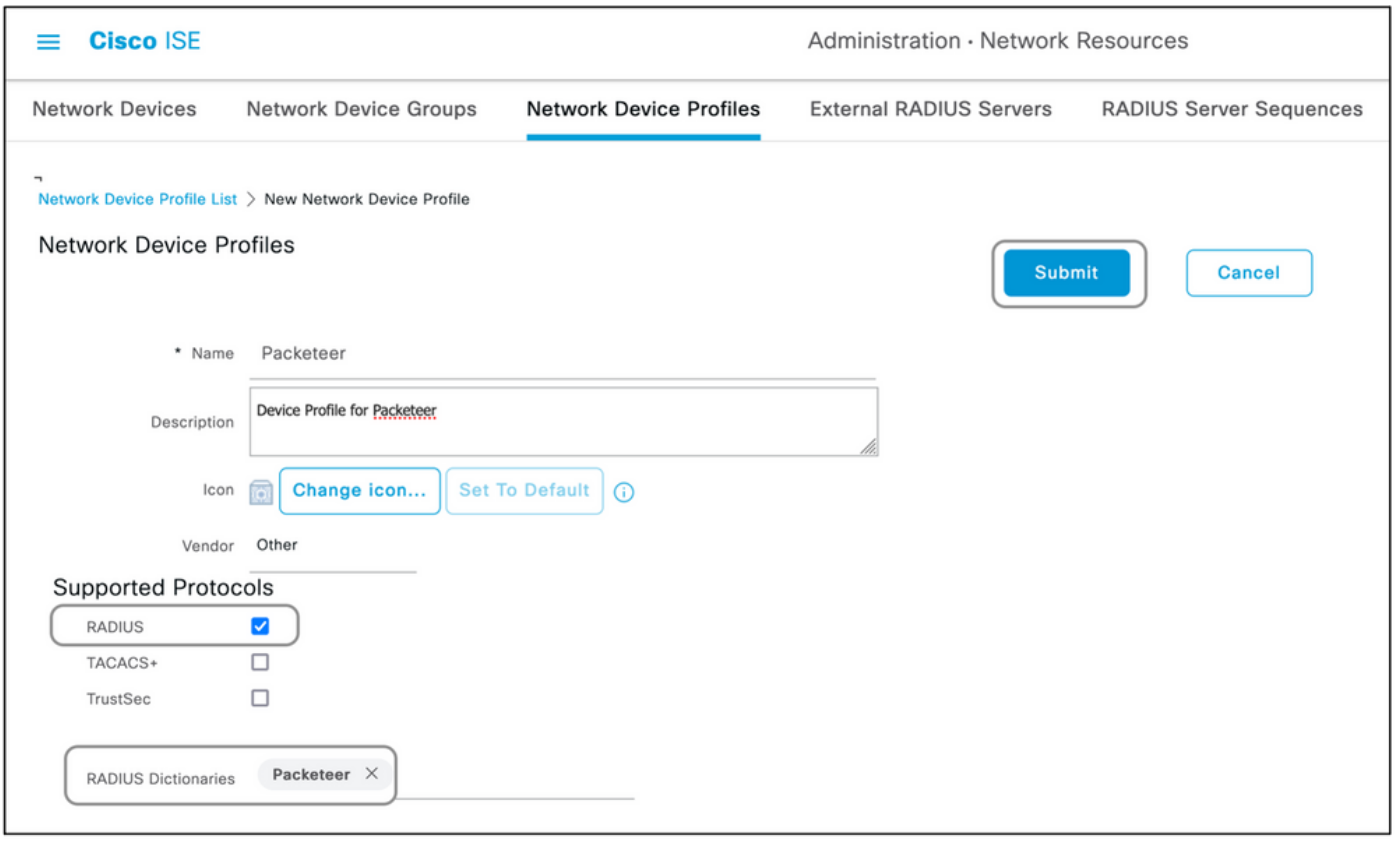
2. Dé un nombre y marque la casilla para RADIUS.

3. Bajo los Diccionarios RADIUS, seleccione el diccionario creado en la sección anterior.

4. Si se crearon varios diccionarios para el mismo tipo de dispositivo, se pueden seleccionar todos en Diccionarios RADIUS.

5. Guarde el perfil.





Paso 3. Agregar el dispositivo de red en ISE

El dispositivo de red en el que se logra la administración de dispositivos debe agregarse en ISE junto con una clave definida en el dispositivo de red. En el dispositivo de red, ISE se agrega como servidor AAA de radio con esta clave.

Este es el procedimiento para agregar un dispositivo en ISE:

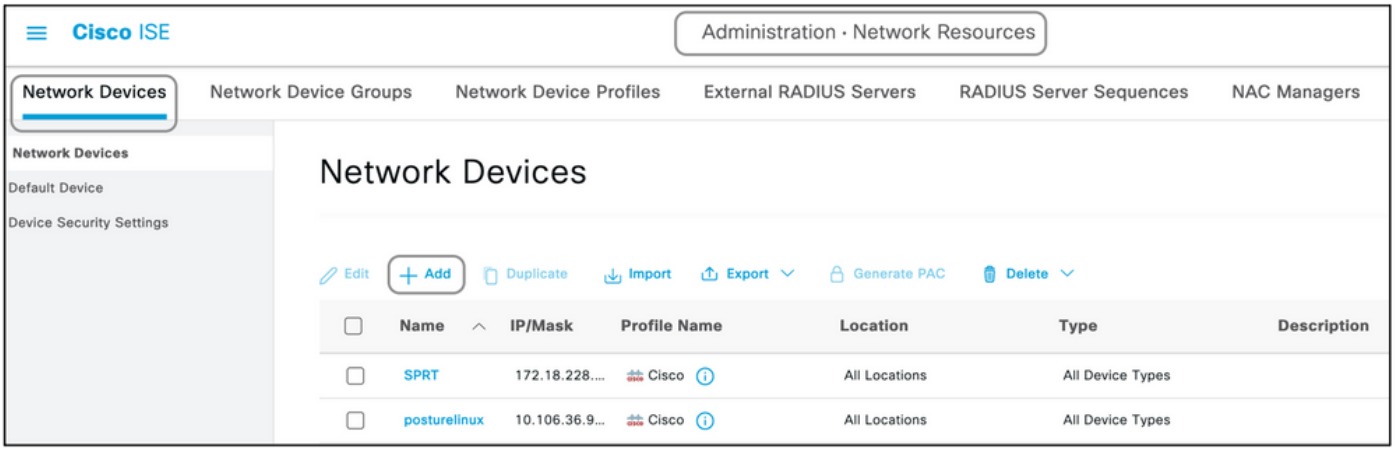
1. Vaya a Administration > Network Resources > Network Devices > Add.

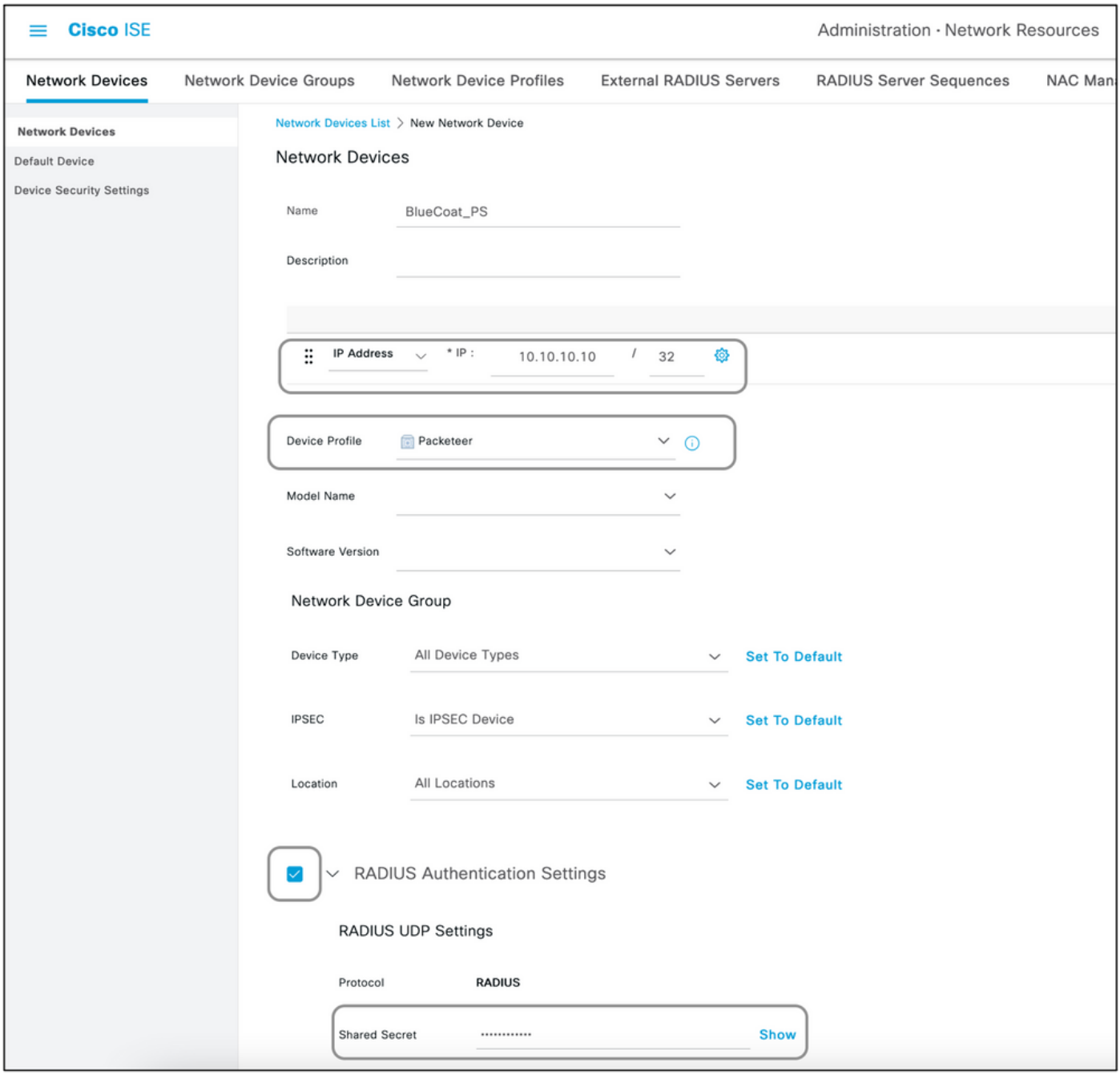
2. Especifique un nombre y la dirección IP.

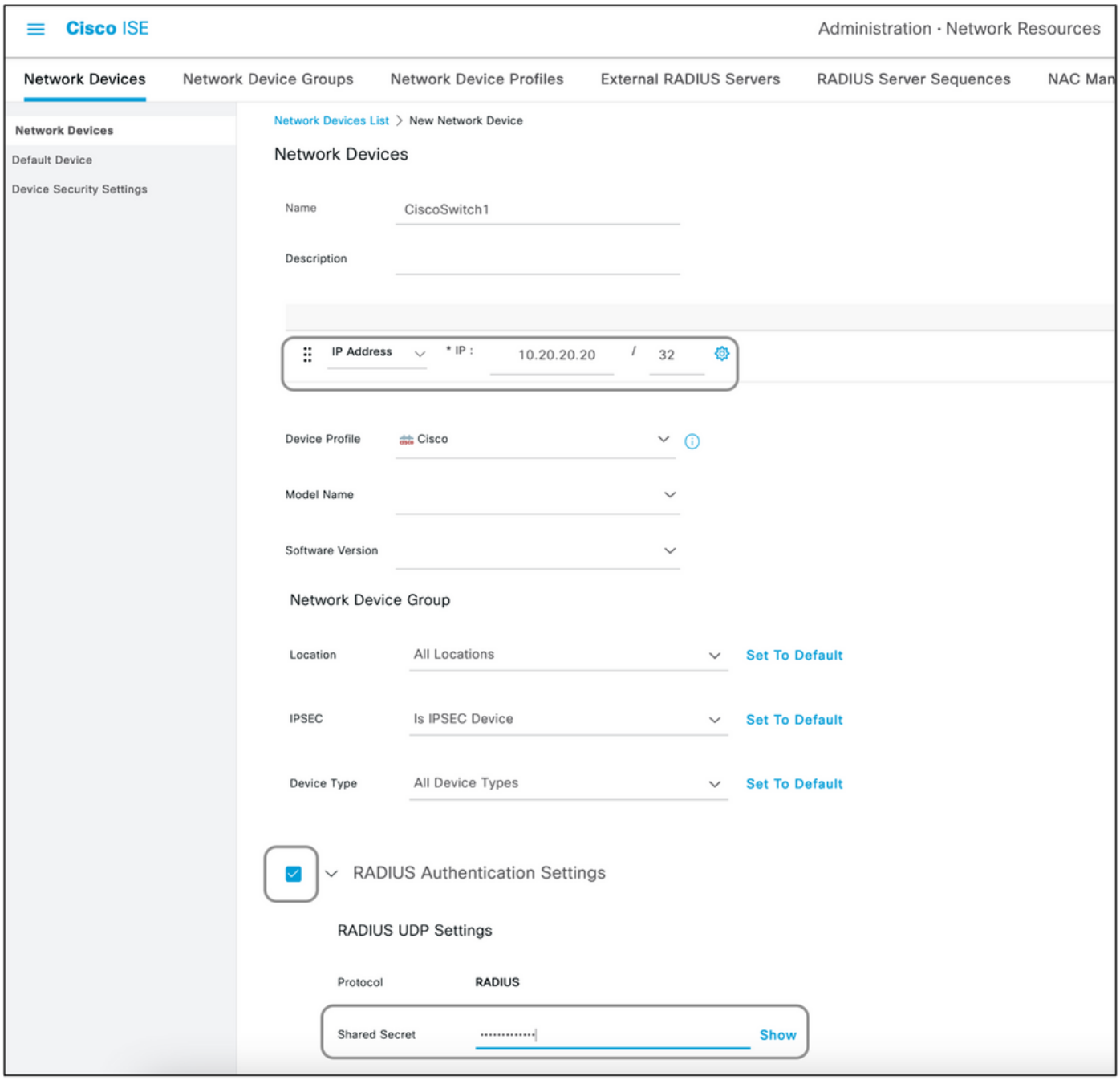
3. El perfil de dispositivo se puede seleccionar de la lista desplegable para que sea el definido en la sección anterior. Si no se ha creado un perfil, se puede utilizar el Cisco predeterminado tal cual.

4. Compruebe La Configuración De Autenticación Radius.

5. Introduzca la clave secreta compartida y guarde el dispositivo.


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



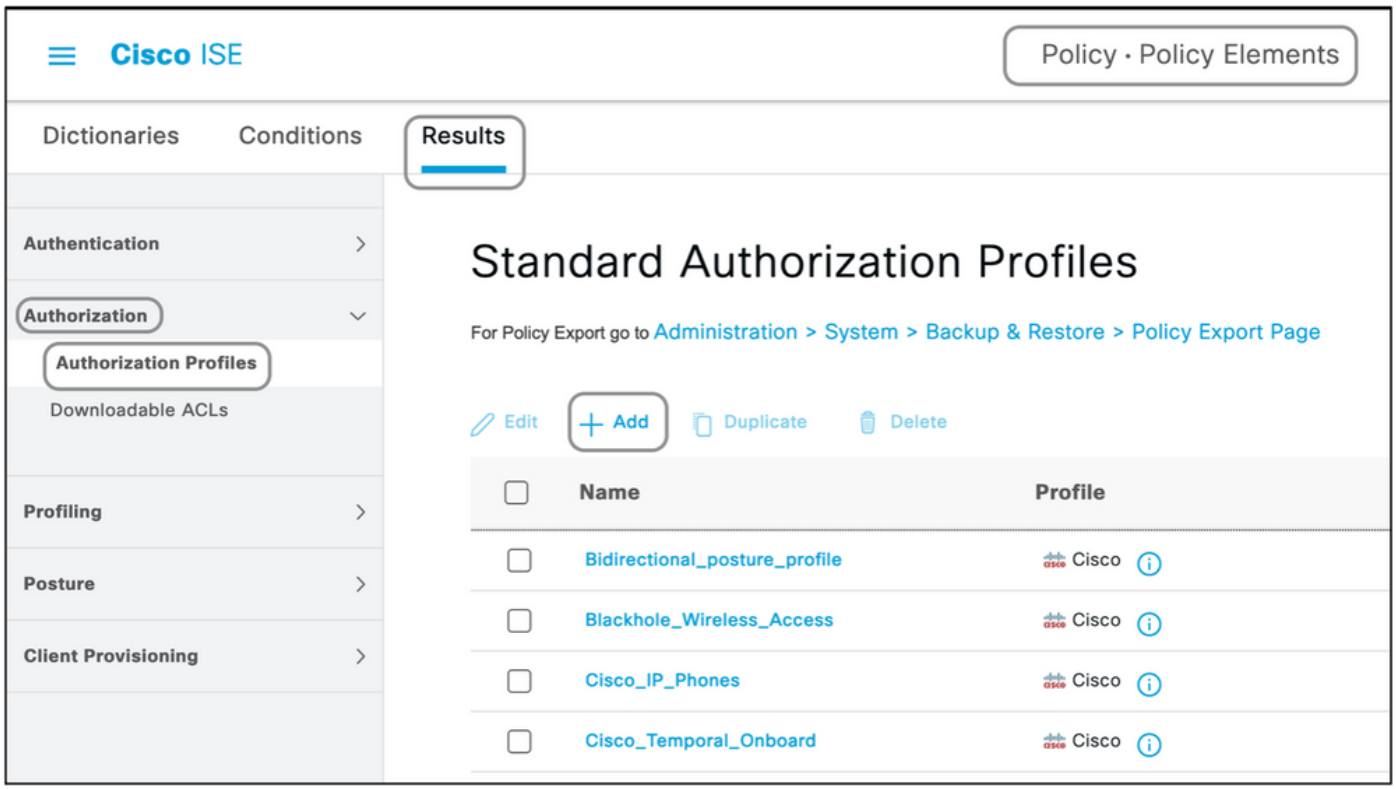
Paso 4. Crear perfiles de autorización

El resultado final que se obtiene de ISE como aceptación o rechazo de acceso se define en un perfil de autorización. Cada perfil de autorización puede insertar atributos adicionales que el dispositivo de red espera.

Este es el procedimiento para crear un perfil de autorización:

1. Vaya a Política > Elementos de política > Resultados > Autorización > Perfiles de autorización.

2. En Perfiles de autorización estándar, haga clic en Agregar.



Los tipos de perfiles que se pueden agregar son Access-Accept y Access-Reject.

Crear un perfil de aceptación de acceso

Este perfil se utiliza para algún tipo de acceso al dispositivo de red. Este perfil puede tener varios atributos transferidos junto con él. Éstos son los pasos:

1. Dé un nombre razonable y elija Access Type (Tipo de acceso) como Access-Accept (Aceptar acceso).

2. Elija el perfil de dispositivo de red que se creó en una de las secciones anteriores. Si no se ha creado ningún perfil, se puede utilizar el predeterminado de Cisco.

3. Con los diferentes tipos de perfiles elegidos, la página aquí limita las opciones de configuración.

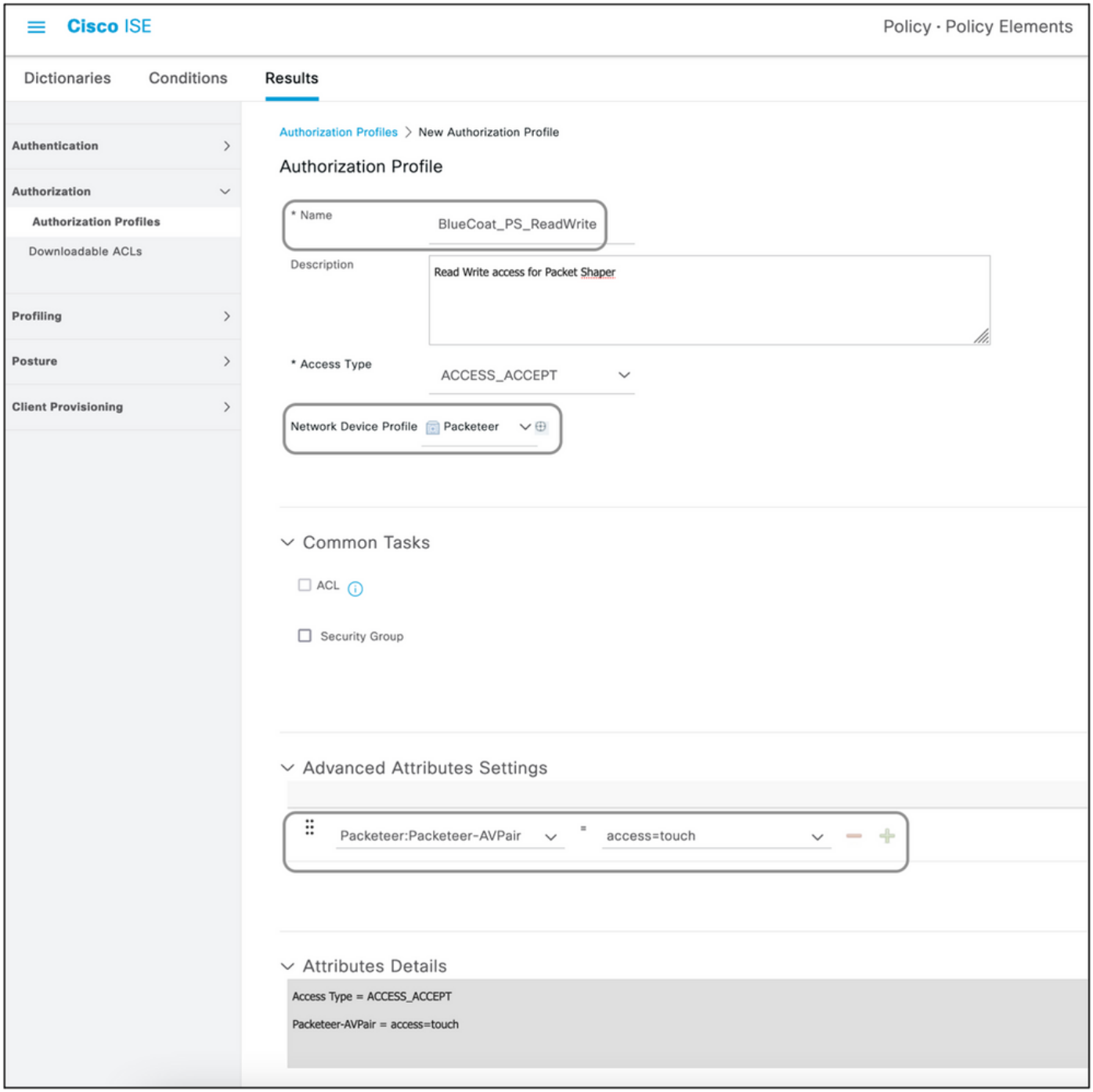
4. En Configuración de atributos avanzados, elija el diccionario y el atributo aplicable (LHS).

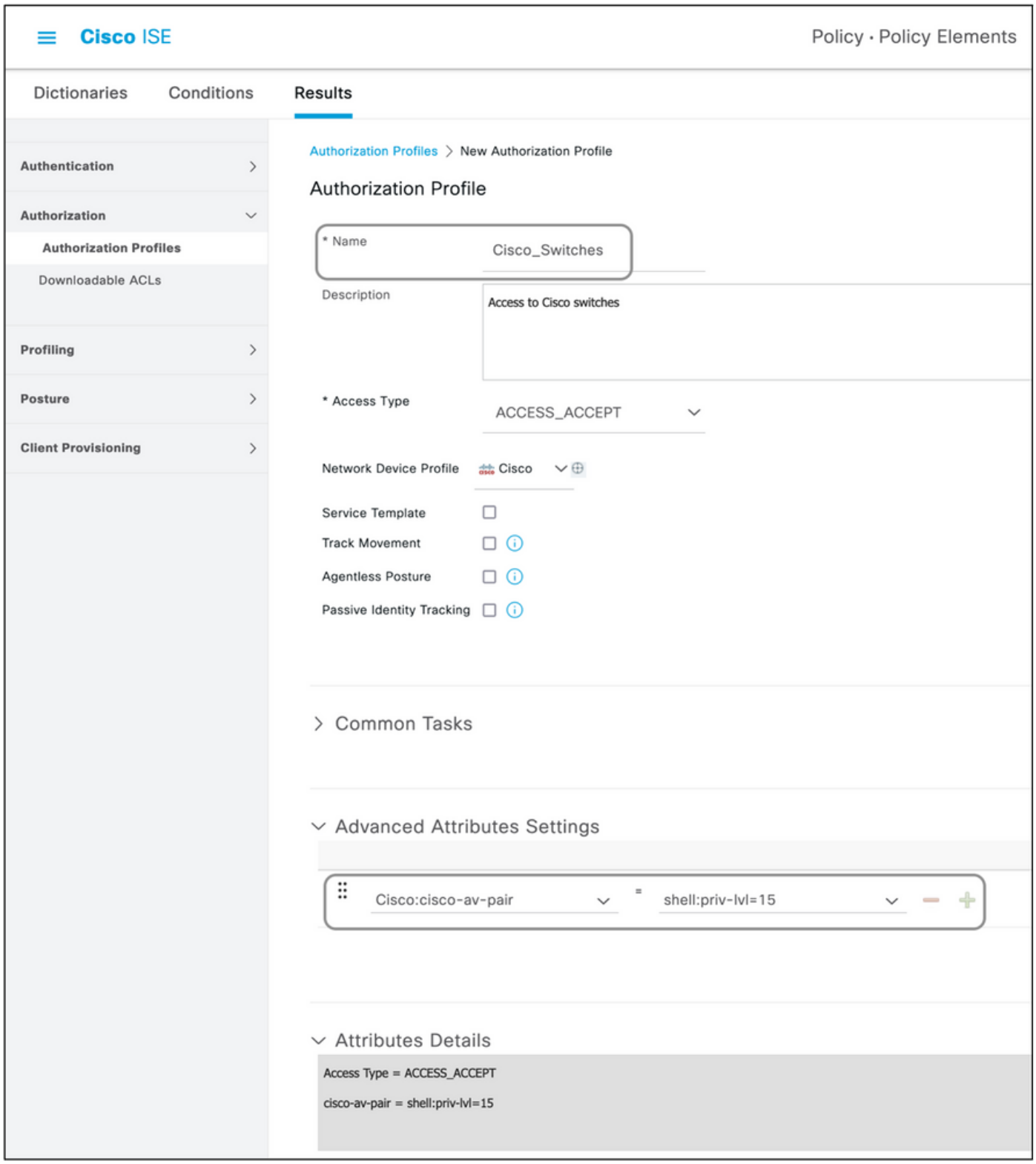
5. Asigne un valor (RHS) al atributo en el menú desplegable, si está disponible, o escriba el valor esperado.

6. Si hay más atributos para enviar como parte del mismo resultado, haga clic en el icono + y repita los pasos 4 y 5.

Cree varios perfiles de autorización para cada uno de los resultados, roles o autorizaciones que ISE debe enviar.

Nota: Los atributos consolidados se pueden verificar en el campo Detalles de Atributo.





Crear un perfil de rechazo de acceso

Este perfil se utiliza para enviar un rechazo para la administración de dispositivos, pero se puede seguir utilizando para enviar atributos junto con él. Esto se utiliza para enviar un paquete de rechazo de acceso Radius. Los pasos siguen siendo los mismos, excepto el paso uno, en el que debe elegirse Access-Reject en lugar de Access-Accept para el tipo de acceso.

Paso 5. Crear un conjunto de políticas

Los conjuntos de políticas en ISE se evalúan de arriba abajo y el primero que cumple la condición establecida en los conjuntos de políticas es responsable de la respuesta de ISE al paquete Radius Access-Request enviado por el dispositivo de red. Cisco recomienda un conjunto de políticas único para cada tipo de dispositivo. La condición para evaluar la autenticación y autorización del usuario se produce en la evaluación. Si ISE tiene orígenes de identidad externos, se puede utilizar para el tipo de autorización.

Un conjunto de políticas típico se crea de esta manera:

1. Navegue hasta Política > Conjuntos de políticas > +.

2. Cambie el nombre del Nuevo conjunto de directivas 1.

3. Establezca la condición como única para este dispositivo.

4. Expanda el Conjunto de directivas.

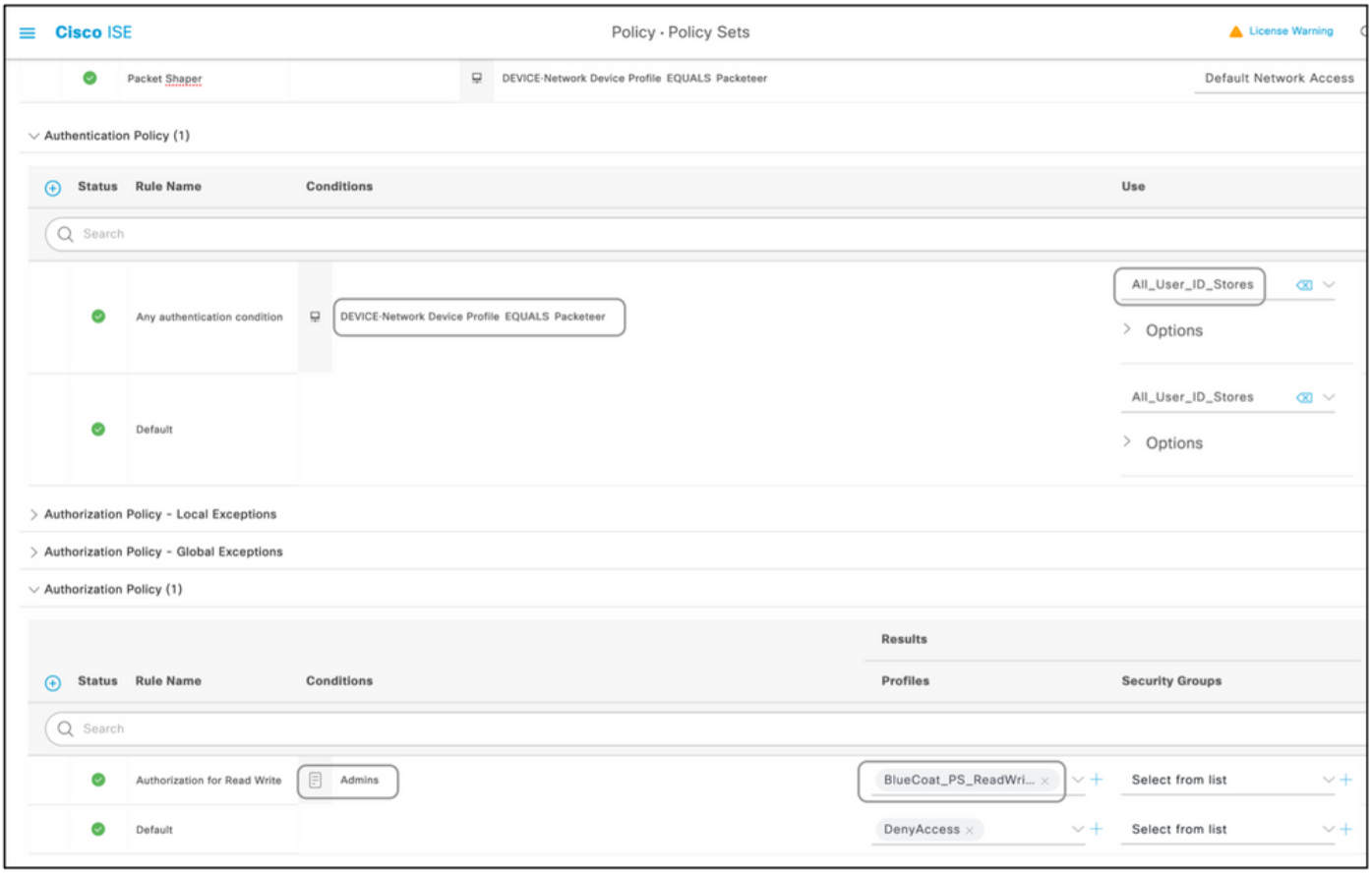
5. Expanda la política de autenticación para establecer una regla de autenticación. El origen externo o los usuarios internos son ejemplos que se pueden utilizar como una secuencia de origen de identidad en la que ISE buscaría al usuario.

6. La política de autenticación está establecida. La política se puede guardar en este punto.

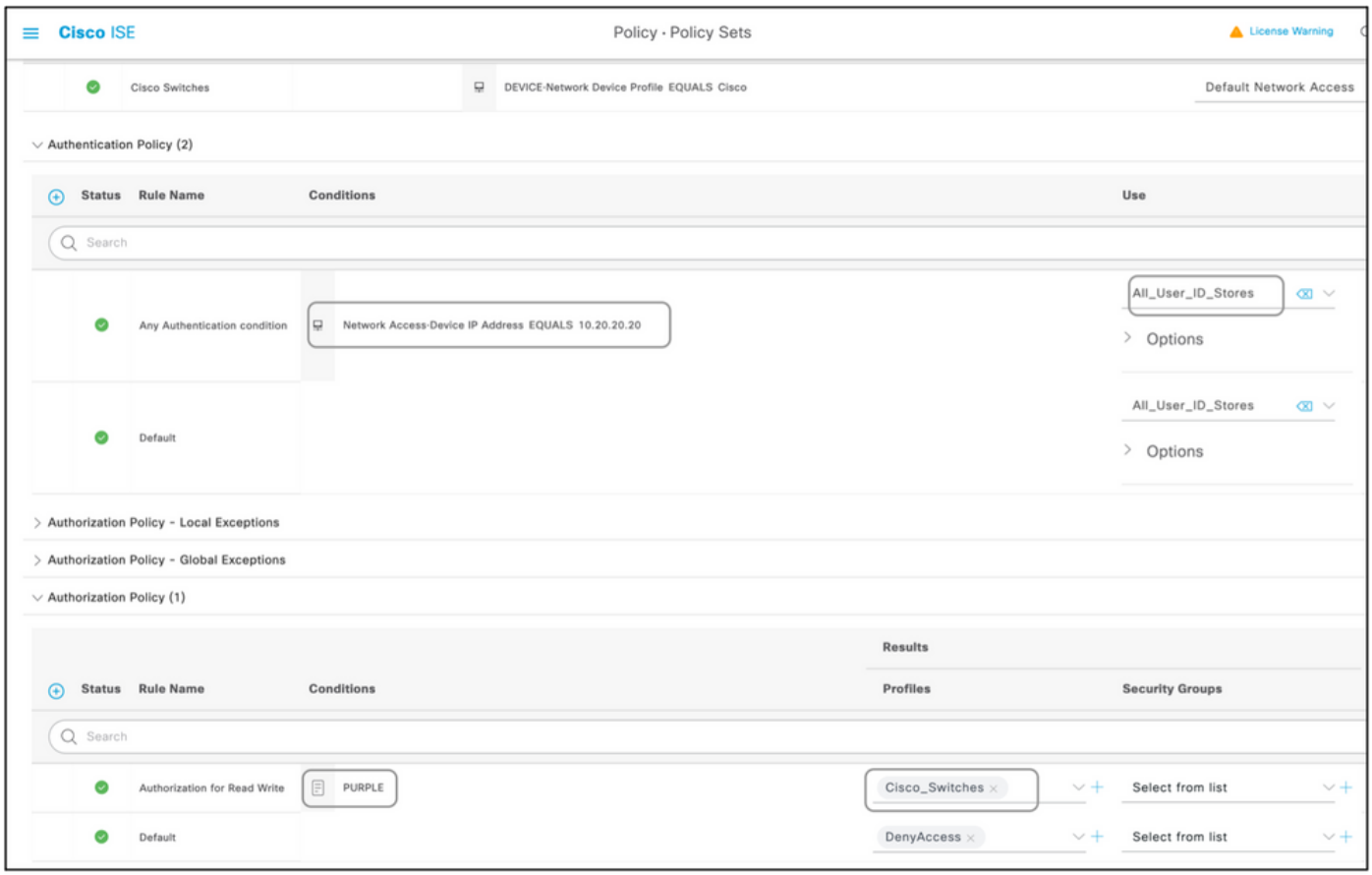
7. Expanda la directiva de autorización para agregar las condiciones de autorización de los usuarios. Un ejemplo es comprobar si hay un grupo de AD o un grupo de identidad interna de ISE determinado. Asigne a la regla el mismo nombre.

8. El resultado de la regla de autorización se puede seleccionar en la lista desplegable.

9. Cree varias reglas de autorización para los distintos tipos de acceso que admite el proveedor.


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



Lista de dispositivos

Cualquier dispositivo que admita la administración de dispositivos con Radius se puede agregar en ISE con algunas modificaciones en todos los pasos mencionados en la sección anterior. Por lo tanto, este documento tiene una lista de dispositivos que funcionan con la información provista en esta sección. La lista de atributos y valores proporcionada en este documento no es exhaustiva ni autorizada y puede cambiar en cualquier momento sin una actualización de este documento. Consulte los sitios web de los proveedores y la asistencia de los proveedores para obtener la validación.

Routers de servicios de agregación (ASR)

No es necesario crear un diccionario y VSA independientes para esto, ya que utiliza pares AV de Cisco que ya están presentes en ISE.

Atributo(s): cisco-av-pair

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

Uso: establezca los valores de<role-name>en el nombre de un rol definido localmente en el router. La jerarquía de funciones se puede describir en términos de un árbol, donde la función#root se encuentra en la parte superior del árbol y la función#sheet agrega comandos adicionales. Estas dos funciones se pueden combinar y devolver si:shell:tasks="#root,#leaf".

Los permisos también se pueden devolver en función de un proceso individual, de modo que se

pueda conceder a un usuario privilegios de lectura, escritura y ejecución para determinados procesos. Por ejemplo, para otorgar a un usuario privilegios de lectura y escritura para el proceso BGP, establezca el valor en:shell:tasks="#root,rw:bgp". El orden de los atributos no importa; el resultado es el mismo independientemente de que el valor esté establecido en shell:tasks="#root,rw:bgp"o toshell:tasks="rw:bgp,#root".

Ejemplo: agregar el atributo a un perfil de autorización.

Tipo de diccionario	Atributo RADIUS	Tipo de atributo	Valor de atributo
RADIUS-Cisco	cisco-av-pair	String (cadena)	shell:tasks="#root,#leaf,rwx:bgp,r:ospf"

Switches Cisco IOS® y Cisco IOS® XE

No es necesario crear un diccionario y VSA independientes para esto, ya que utiliza atributos RADIUS que ya están presentes en ISE.

Atributo(s):cisco-av-pair

Valor(es):shell:priv-lvl=<level>

Uso: establezca los valores de<level>en los números que son básicamente el número de privilegios que se van a enviar. Normalmente, si se envía 15, significa lectura-escritura, si se envía 7 significa sólo lectura.

Ejemplo: agregar el atributo a un perfil de autorización.

Tipo de diccionario	Atributo RADIUS	Tipo de atributo	Valor de atributo
RADIUS-Cisco	cisco-av-pair	String (cadena)	shell:priv-lvl=15

Formador de paquetes BlueCoat

Atributo(s):Packeter-AVPair

Valores:access=<level>

Uso:<level>es el nivel de acceso que se debe otorgar. El acceso táctil es equivalente a la lectura-escritura, mientras que el acceso físico es equivalente a sólo lectura.

Cree un Diccionario como se muestra en este documento con estos valores:

- Nombre: Packeter
- ID del proveedor: 2334
- Tamaño del campo de longitud del proveedor: 1
- Tamaño del campo de tipo de proveedor: 1

Introduzca los detalles del atributo:

- Atributo:Packeter-AVPair
- Descripción: Se utiliza para especificar el nivel de acceso
- ID de atributo del proveedor: 1
- Dirección: SALIDA
- Múltiple permitido: Falso
- Permitir Etiquetado: Desactivado
- Tipo de atributo: Cadena

Ejemplo: agregar el atributo a un perfil de autorización (para acceso de sólo lectura).

Tipo de diccionario	Atributo RADIUS	Tipo de atributo	Valor de atributo
RADIUS-Packeter	Packeter-AVPair	String (cadena)	access=look

Ejemplo: agregar el atributo a un perfil de autorización (para acceso de lectura y escritura).

Tipo de diccionario	Atributo RADIUS	Tipo de atributo	Valor de atributo
RADIUS-Packeter	Packeter-AVPair	String (cadena)	access=touch

Servidor proxy BlueCoat (AV/SG)

Atributo(s): Blue-Coat-Authorization

Valor(es): <level>

Uso:<level>es el nivel de acceso que se debe otorgar. 0 significa sin acceso, 1 significa acceso de solo lectura mientras que 2 significa acceso de lectura y escritura. El atributo Blue-Coat-Authorization es el responsable del nivel de acceso.

Cree un Diccionario como se muestra en este documento con estos valores:

- Nombre: BlueCoat
- ID de proveedor: 14501
- Tamaño del campo de longitud del proveedor: 1
- Tamaño del campo de tipo de proveedor: 1

Introduzca los detalles del atributo:

- Atributo: Blue-Coat-Group
- ID de atributo del proveedor: 1
- Dirección: AMBOS
- Múltiple permitido: Falso
- Permitir Etiquetado: Desactivado
- Tipo de atributo: Entero sin signo 32 (UINT32)

Introduzca los detalles del segundo atributo:

- Atributo: Blue-Coat-Authorization
- Descripción: Se utiliza para especificar el nivel de acceso
- ID de atributo del proveedor: 2
- Dirección: AMBOS
- Múltiple permitido: Falso
- Permitir Etiquetado: Desactivado
- Tipo de atributo: Entero sin signo 32 (UINT32)

Ejemplo: agregar el atributo a un perfil de autorización (sin acceso).

Tipo de diccionario	Atributo RADIUS	Tipo de atributo	Valor de atributo
RADIUS-BlueCoat	Blue-Coat-Group	UINT32	0

Ejemplo: agregar el atributo a un perfil de autorización (para acceso de sólo lectura).

Tipo de diccionario	Atributo RADIUS	Tipo de atributo	Valor de atributo
RADIUS-BlueCoat	Blue-Coat-Group	UINT32	1

Ejemplo: agregar el atributo a un perfil de autorización (para acceso de lectura y escritura).

Tipo de diccionario	Atributo RADIUS	Tipo de atributo	Valor de atributo
RADIUS-BlueCoat	Blue-Coat-Group	UINT32	2

Switches Brocade

No es necesario crear un diccionario y VSA independientes para esto, ya que utiliza atributos RADIUS que ya están presentes en ISE.

Atributo(s): Tunnel-Private-Group-ID

Valores:U:<VLAN1>; T:<VLAN2>

Uso: establezca<VLAN1>en el valor de la VLAN de datos. Establezca<VLAN2>en el valor de la VLAN de voz. En este ejemplo, la VLAN de datos es VLAN 10 y la VLAN de voz es VLAN 21.

Ejemplo: agregar el atributo a un perfil de autorización.

Tipo de diccionario	Atributo RADIUS	Tipo de atributo	Valor de atributo
RADIUS-IETF	Tunnel-Private-Group-ID	Cadena etiquetada	U:10;T:21

Infoblox

Atributo(s):Infoblox-Group-Info

Valores:<group-name>

Uso:<group-name>es el nombre del grupo con los privilegios que se le han otorgado al usuario. Este grupo debe configurarse en el dispositivo Infoblox. En este ejemplo de configuración, el

nombre del grupo es MyGroup.

Cree un Diccionario como se muestra en este documento con estos valores:

- Nombre: Infoblox
- ID del proveedor: 7779
- Tamaño del campo de longitud del proveedor: 1
- Tamaño del campo de tipo de proveedor: 1

Introduzca los detalles del atributo:

- Atributo:Infoblox-Group-Info
- ID de atributo del proveedor: 009
- Dirección: SALIDA
- Múltiple permitido: Falso
- Permitir Etiquetado: Desactivado
- Tipo de atributo: Cadena

Ejemplo: agregar el atributo a un perfil de autorización.

Tipo de diccionario	Atributo RADIUS	Tipo de atributo	Valor de atributo
RADIUS-Infoblox	Infoblox-Group-Info	String (cadena)	MiGrupo

Cisco Firepower Management Center

No es necesario crear un diccionario y VSA independientes para esto, ya que utiliza atributos RADIUS que ya están presentes en ISE.

Atributo(s):cisco-av-pair

Valores: Class-[25]=<role>

Uso: establezca los valores de <role>en los nombres de los roles definidos localmente en el FMC. Cree varias funciones, como admin y usuario de solo lectura en el FMC, y asigne los valores a los atributos de ISE que recibirá el FMC del mismo modo.

Ejemplo: agregar el atributo a un perfil de autorización.

Tipo de diccionario	Atributo RADIUS	Tipo de atributo	Valor de atributo
RADIUS-Cisco	cisco-av-pair	String (cadena)	Class-[25]=NetAdmins

Switches Nexus

No es necesario crear un diccionario y VSA independientes para esto, ya que utiliza atributos RADIUS que ya están presentes en ISE.

Atributo(s):cisco-av-pair

Valores:shell:roles="<role1> <role2>"

Uso: establezca los valores de<role1>y<role2>en los nombres de los roles definidos localmente en el switch. Cuando se crean varios roles, sepárelos con un carácter de espacio. Cuando se devuelven varias funciones del servidor AAA al switch Nexus, el resultado es que el usuario tiene acceso a los comandos definidos por la unión de las tres funciones.

Las funciones integradas se definen enConfigurar cuentas de usuario y RBAC.

Ejemplo: agregar el atributo a un perfil de autorización.

Tipo de diccionario	Atributo RADIUS	Tipo de atributo	Valor de atributo
RADIUS-Cisco	cisco-av-pair	String (cadena)	shell:roles="network-admin vdc-admin vdc-operator"

Controlador de LAN inalámbrica (WLC)

No es necesario crear un diccionario y VSA independientes para esto, ya que utiliza atributos RADIUS que ya están presentes en ISE.

Atributo(s):Service-Type

Valores:Administrativo (6) / Solicitud NAS (7)

Uso: para conceder al usuario acceso de lectura/escritura al controlador de LAN inalámbrica (WLC), el valor debe ser Administrativo; para el acceso de solo lectura, el valor debe ser Solicitud de NAS.

Para obtener más información, vea Ejemplo de configuración de autenticación de servidor RADIUS de usuarios de administración en controlador de LAN inalámbrica (WLC)

Ejemplo: agregar el atributo a un perfil de autorización (para acceso de sólo lectura).

Tipo de diccionario	Atributo RADIUS	Tipo de atributo	Valor de atributo
RADIUS-IETF	Tipo de servicio	Enumeración	NAS-Prompt

Ejemplo: agregar el atributo a un perfil de autorización (para acceso de lectura y escritura).

Tipo de diccionario	Atributo RADIUS	Tipo de atributo	Valor de atributo
RADIUS-IETF	Tipo de servicio	Enumeración	Administrativo

Data Center Network Manager (DCNM)

DCNM debe reiniciarse después de cambiar el método de autenticación. De lo contrario, puede asignar el privilegio de operador de red en lugar del de administrador de red.

No es necesario crear un diccionario y VSA independientes para esto, ya que utiliza atributos RADIUS que ya están presentes en ISE.

Atributo(s):cisco-av-pair

Valores:shell:roles=<role>

Función DCNM	Par de Cisco AV con RADIUS
Usuario	shell:roles = "network-operator"
Administrador	shell:roles = "network-admin"

Códigos de audio

Atributo(s): ACL-Auth-Level

Valores: ACL-Auth-Level = "<integer>"

Uso:<entero> es el nivel de acceso que se va a conceder. Un valor del atributo ACL-Auth-Level con el nombre ACL-Auth-UserLevel de 50 para el usuario, un valor del atributo ACL-Auth-Level con el nombre ACL-Auth-AdminLevel de valor100 para admin y un valor de ACL-Auth-Level con el nombre ACL-Auth-SecurityAdminLevel de valor 200 para admin de seguridad. Los nombres se pueden omitir y los valores de los atributos se pueden proporcionar directamente como valor para el par AV avanzado del perfil de autorización.

Cree un Diccionario como se muestra en este documento con estos valores:

- Nombre: AudioCodes
- ID del proveedor: 5003
- Tamaño del campo de longitud del proveedor: 1
- Tamaño del campo de tipo de proveedor: 1

Introduzca los detalles del atributo:

- Atributo: ACL-Auth-Level
- Descripción: Se utiliza para especificar el nivel de acceso
- ID de atributo del proveedor: 35
- Dirección: SALIDA
- Múltiple permitido: Falso
- Permitir Etiquetado: Desactivado
- Tipo de atributo: Integer

Ejemplo: agregar el atributo a un perfil de autorización (para el usuario).

Tipo de diccionario	Atributo RADIUS	Tipo de atributo	Valor de atributo
RADIUS-AudioCodes	ACL-Auth-Level	Entero	50

Ejemplo: agregar el atributo a un perfil de autorización (para admin).

Tipo de diccionario	Atributo RADIUS	Tipo de atributo	Valor de atributo
RADIUS-AudioCodes	ACL-Auth-Level	Entero	100

Ejemplo: agregar el atributo a un perfil de autorización (para administración de seguridad).

Tipo de diccionario	Atributo RADIUS	Tipo de atributo	Valor de atributo
RADIUS-AudioCodes	ACL-Auth-Level	Entero	200

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).