Utilizzare RADIUS per l'amministrazione dei dispositivi con Identity Services Engine

Sommario

Introduzione

Questo documento descrive la compilazione di attributi che vari prodotti Cisco e non Cisco si aspettano di ricevere da un server AAA come Cisco ISE.

Premesse

I prodotti Cisco e non Cisco si aspettano di ricevere una compilazione di attributi da un server di autenticazione, autorizzazione e accounting (AAA). In questo caso, il server è un Cisco ISE e l'ISE restituirà questi attributi insieme a un Access-Accept come parte di un profilo di autorizzazione (RADIUS).

In questo documento vengono fornite istruzioni dettagliate su come aggiungere profili di autorizzazione degli attributi personalizzati e viene fornito un elenco di dispositivi e gli attributi RADIUS che i dispositivi si aspettano vengano restituiti dal server AAA. Tutti gli argomenti includono esempi.

L'elenco di attributi fornito in questo documento non è esaustivo né autorevole e può essere modificato in qualsiasi momento senza un aggiornamento del documento.

L'amministrazione di un dispositivo di rete viene in genere eseguita tramite il protocollo TACACS+, ma se il dispositivo di rete non supporta TACACS+ o se ISE non dispone di una licenza di amministrazione del dispositivo, è possibile eseguire questa operazione anche con RADIUS, a condizione che il dispositivo di rete supporti l'amministrazione di dispositivi RADIUS. Alcuni dispositivi supportano entrambi i protocolli e spetta all'utente decidere quale protocollo usare, ma TACACS+ può essere favorevole in quanto dispone di funzionalità quali l'autorizzazione dei comandi e l'accounting dei comandi.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti elementi:

- Cisco ISE come server Radius sulla rete di interesse
- Flusso di lavoro del protocollo Radius - RFC2865

Componenti usati

Il riferimento delle informazioni contenute in questo documento è Cisco Identity Services Engine (ISE) 3.x e versioni successive di ISE.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Passaggio 1. Creare gli attributi specifici del fornitore (VSA)

È possibile creare diversi dizionari per ogni fornitore e aggiungere attributi a ciascuno di essi. Ogni dizionario può avere più attributi che possono essere utilizzati nei profili di autorizzazione. Ogni attributo, in generale, definisce il ruolo diverso dell'amministrazione dei dispositivi che un utente potrebbe ottenere quando accede al dispositivo di rete. Tuttavia, l'attributo può essere utilizzato per scopi diversi di funzionamento o configurazione sul dispositivo di rete.

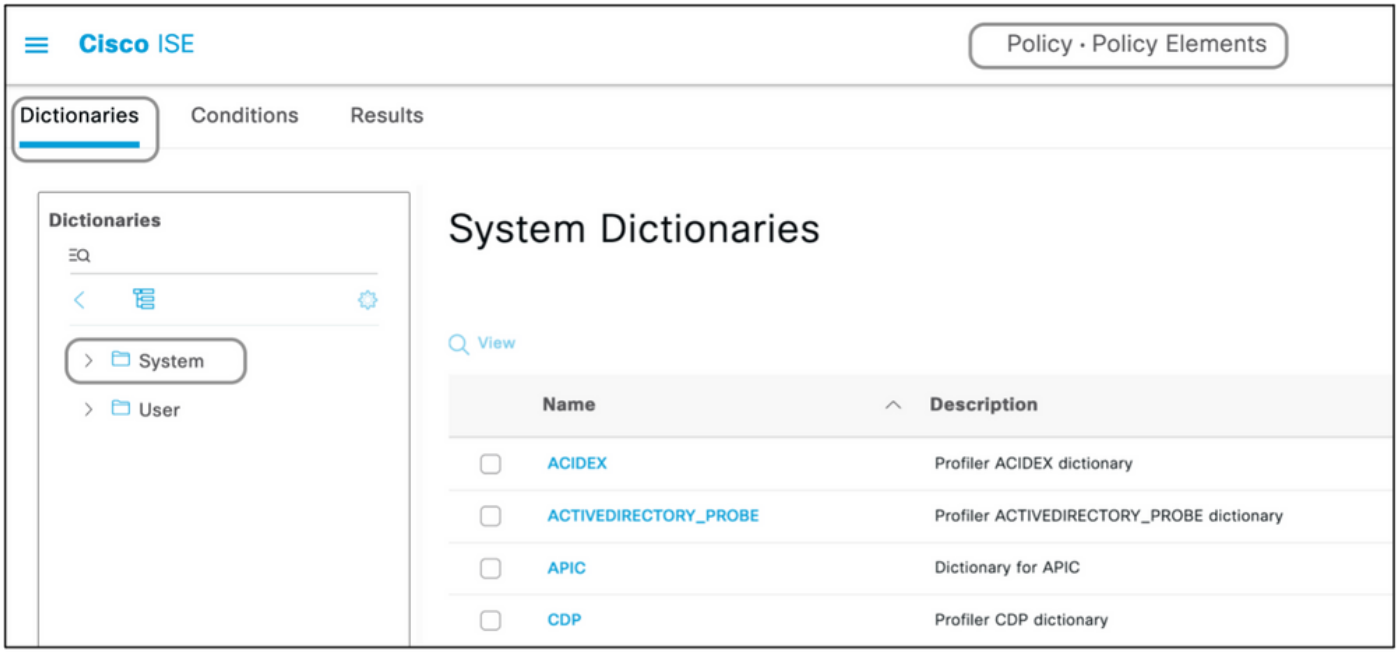
ISE viene fornito con attributi predefiniti da pochi fornitori. Se il fornitore non è presente nell'elenco, è possibile aggiungerlo come dizionario con attributi. Per alcuni dispositivi di rete, gli attributi sono configurabili e possono essere modificati per vari tipi di accesso. In questo caso, ISE deve essere configurato con gli attributi che il dispositivo di rete si aspetta per i diversi tipi di accesso.

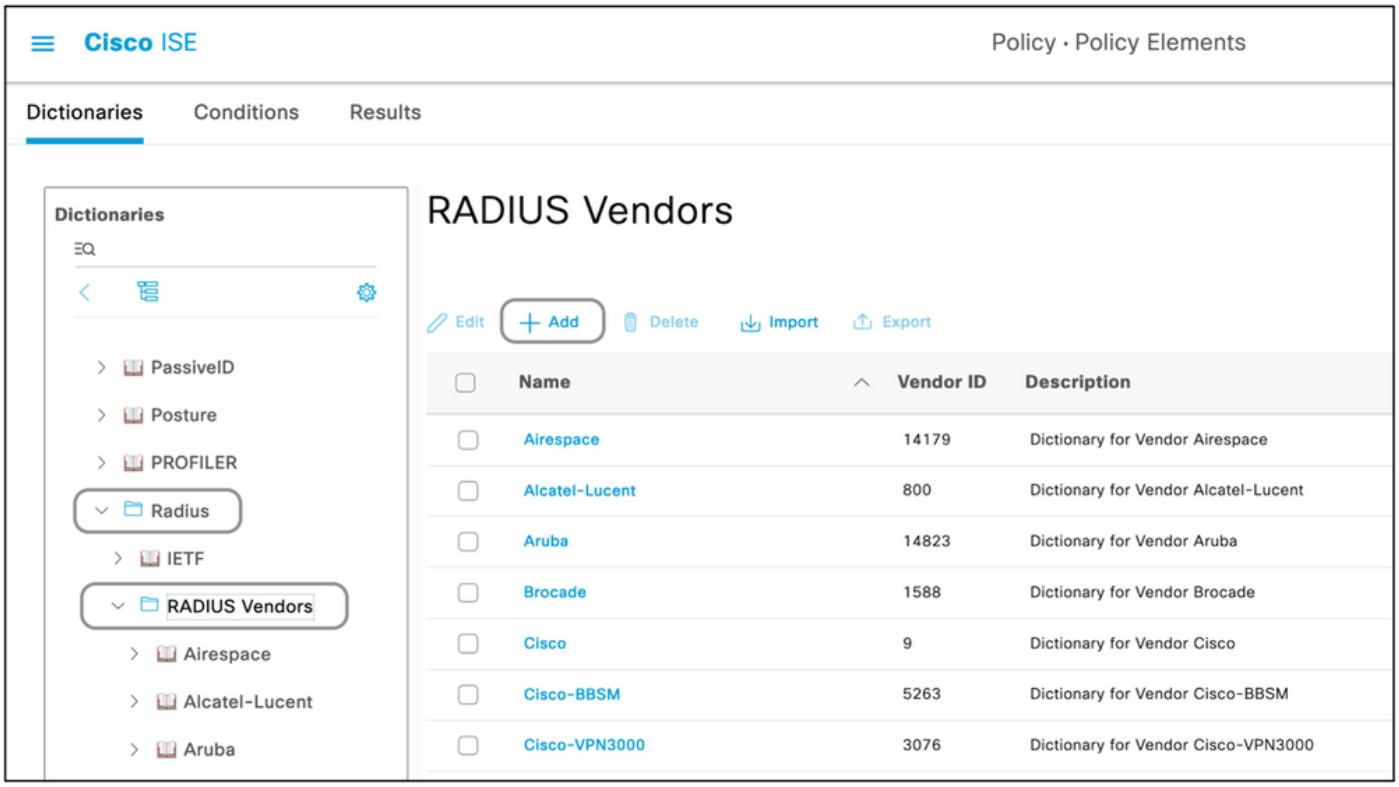
Gli attributi che devono essere inviati con un comando Radius Access-Accept sono definiti come

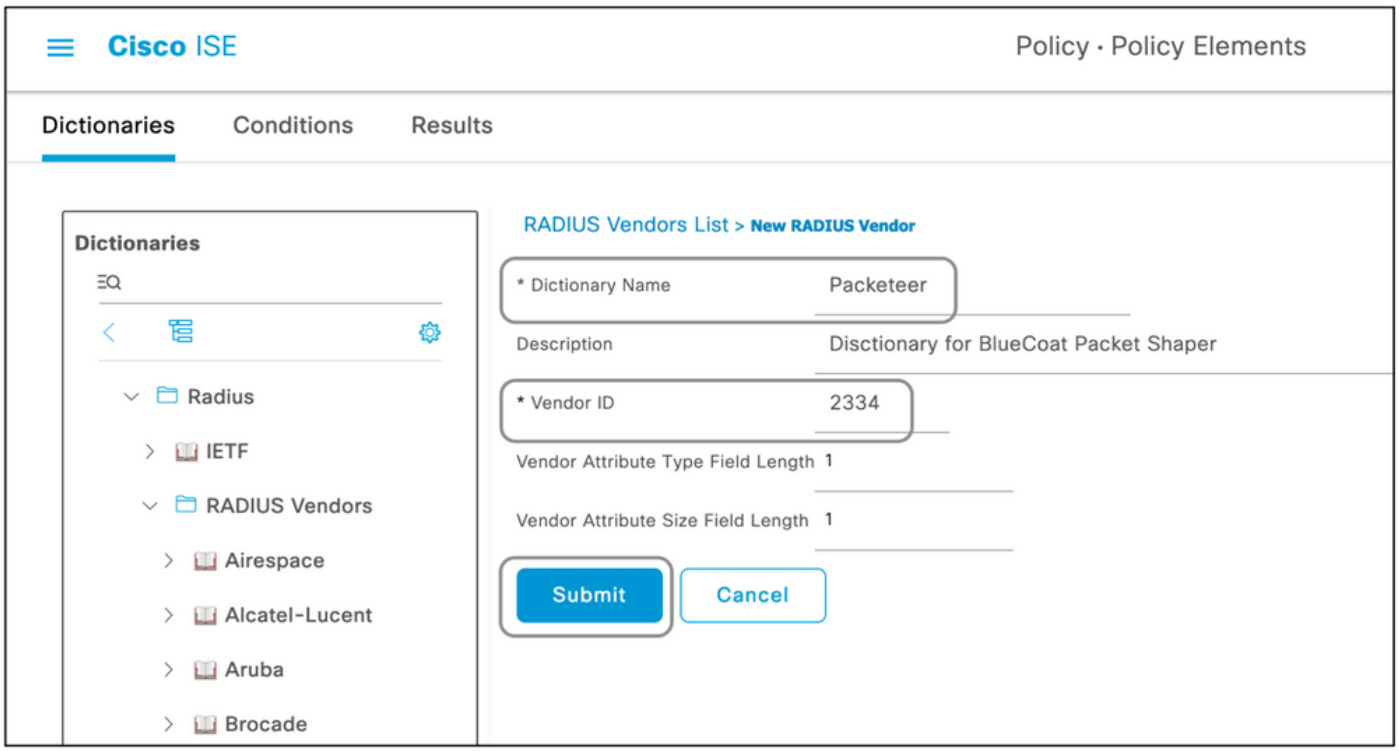
segue:

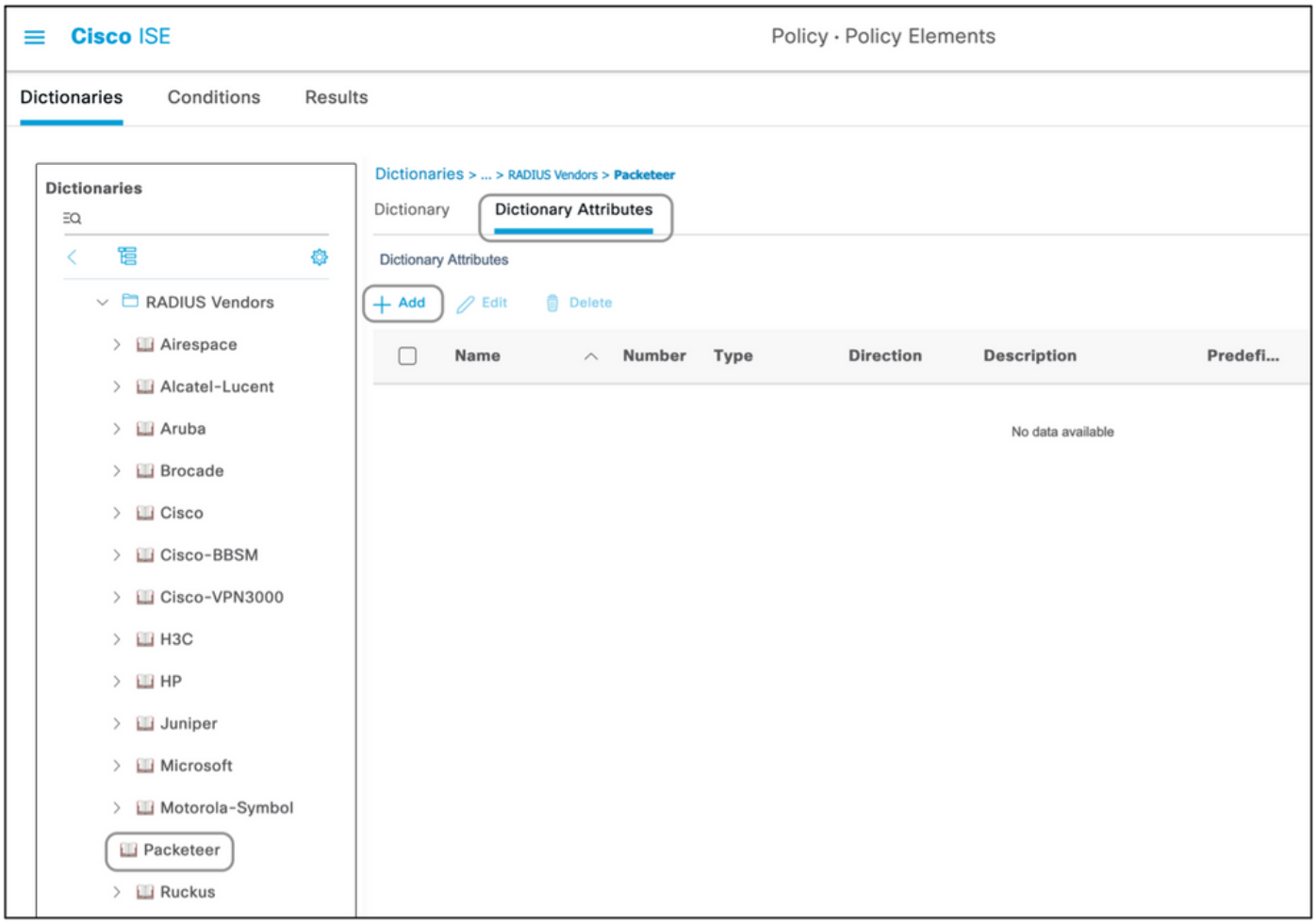
1. Selezionare Criterio > Elementi criteri > Dizionari > Sistema > Raggio > Fornitori Radius > Aggiungi.
2. Immettere e salvare il nome e gli ID fornitore.
3. Fare clic sul fornitore Radius salvato e passare a Attributi dizionario.
4. Fare clic su Add (Aggiungi) e compilare le caselle Nome attributo, Tipo di dati, Direzione e ID con distinzione tra maiuscole e minuscole.
5. Salvare l'attributo.
6. Aggiungere altri attributi nella stessa pagina se esistono più attributi da aggiungere allo stesso dizionario.

Nota: tutti i campi immessi come valori in questa sezione devono essere forniti dal fornitore stesso. È possibile visitare i siti Web dei fornitori oppure contattare il supporto dei fornitori nel caso in cui questi non siano noti.




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: non tutti i fornitori richiedono l'aggiunta di un dizionario specifico. Se il fornitore può usare gli attributi radius definiti dall'IETF, che esistono già su ISE, questo passaggio può essere saltato.

Passaggio 2. Crea profilo dispositivo di rete

Questa sezione non è obbligatoria. Un profilo di dispositivo di rete consente di separare il tipo di dispositivo di rete aggiunto e di creare profili di autorizzazione appropriati. Proprio come i dizionari radius, ISE dispone di alcuni profili predefiniti che possono essere utilizzati. Se non è già presente, è possibile creare un nuovo profilo di dispositivo.

Questa è la procedura per aggiungere un profilo di rete:

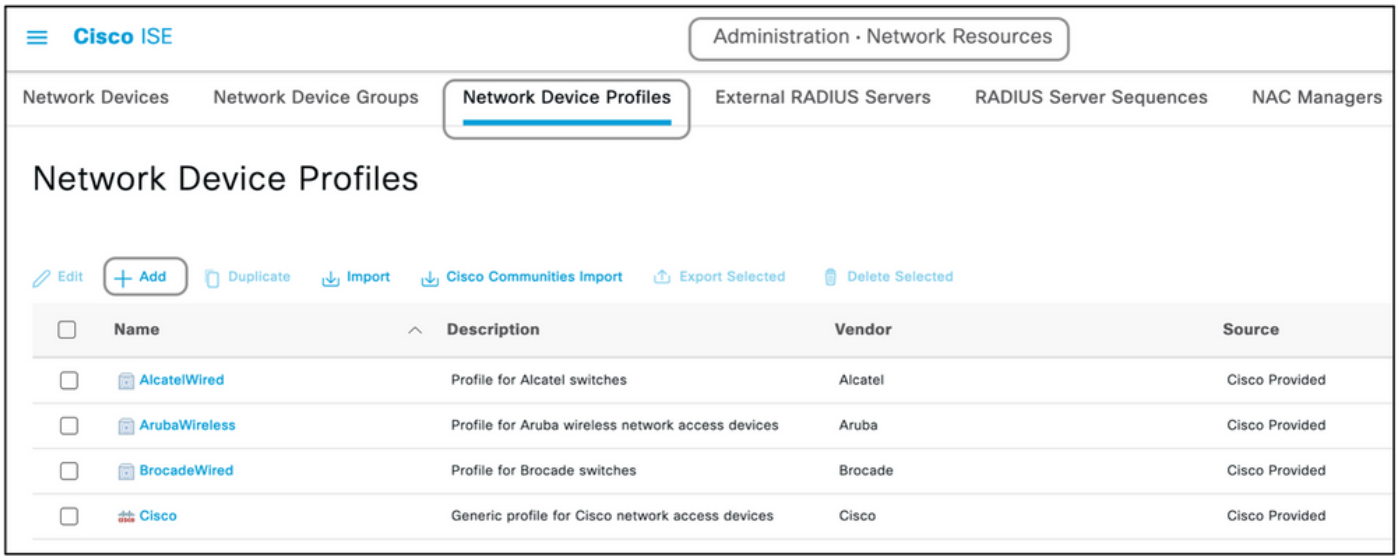
1. Selezionare Amministrazione > Risorse di rete > Profili dispositivi di rete > Aggiungi.

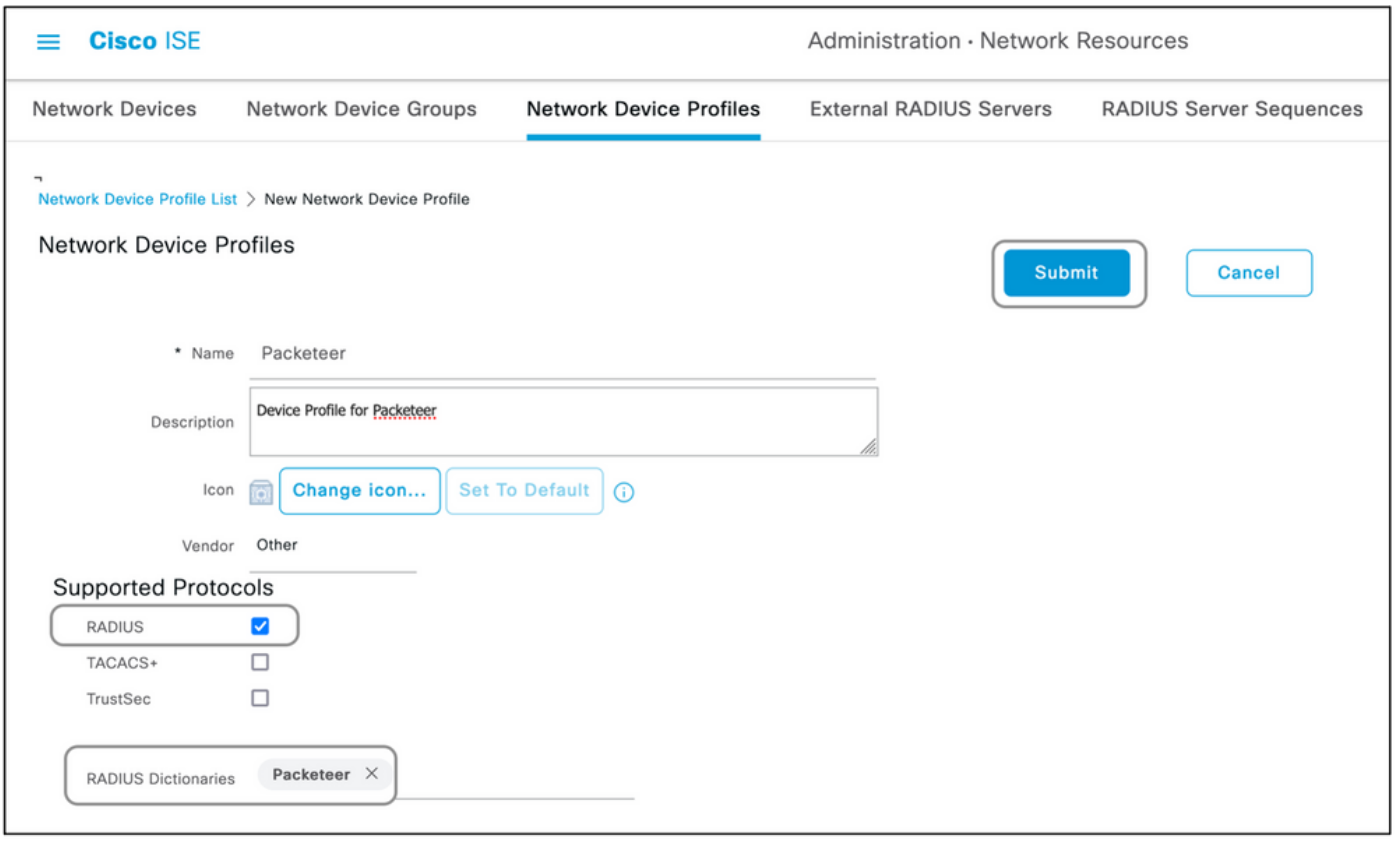
2. Assegnare un nome e selezionare la casella relativa a RADIUS.

3. In Dizionari RADIUS, selezionare il dizionario creato nella sezione precedente.

4. Se per lo stesso tipo di dispositivo sono stati creati più dizionari, è possibile selezionarli tutti in Dizionari RADIUS.

5. Salvare il profilo.





Passaggio 3. Aggiungi dispositivo di rete ad ISE

Il dispositivo di rete su cui viene eseguita l'amministrazione deve essere aggiunto ad ISE insieme a una chiave definita sul dispositivo di rete. Sul dispositivo di rete, l'ISE viene aggiunta come server AAA radius con questa chiave.

Questa è la procedura per aggiungere una periferica all'ISE:

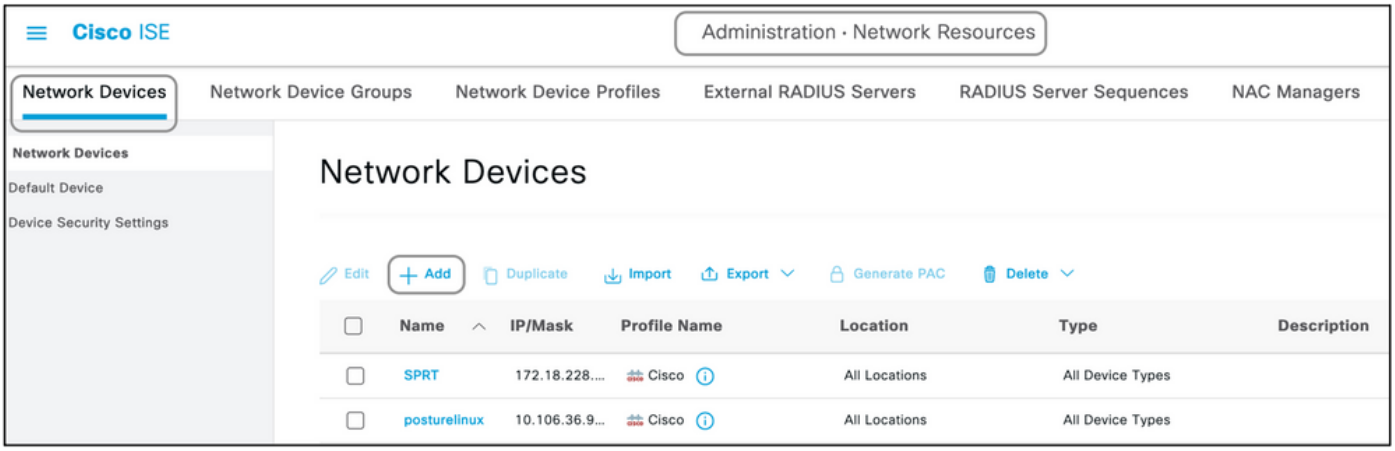
1. Selezionare Amministrazione > Risorse di rete > Dispositivi di rete > Aggiungi.

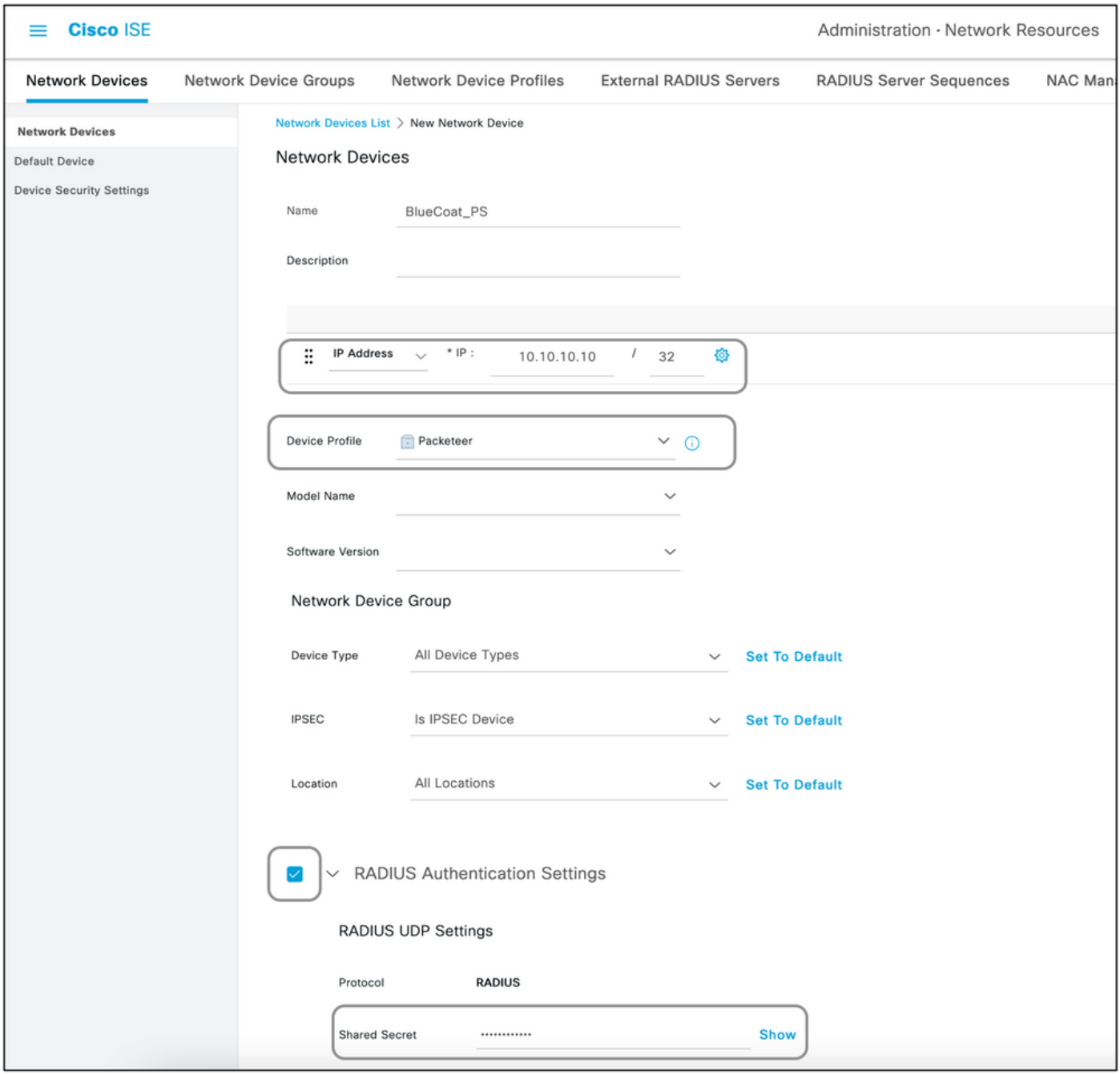
2. Assegnare un nome e l'indirizzo IP.

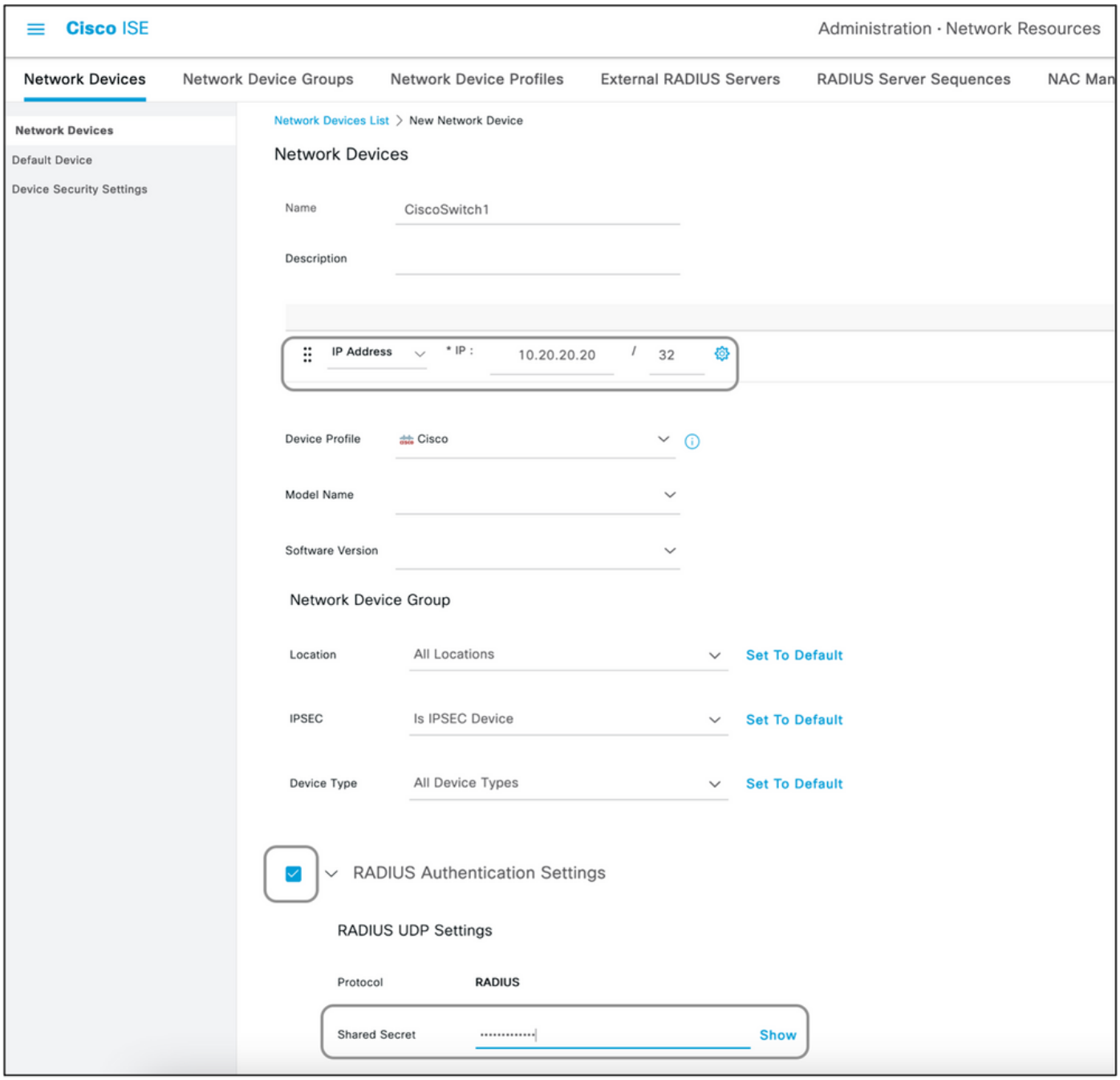
3. È possibile scegliere il profilo del dispositivo dall'elenco a discesa come definito nella sezione precedente. Se non è stato creato un profilo, è possibile utilizzare il Cisco predefinito.

4. Controllare Le Impostazioni Di Autenticazione Radius.

5. Immettere la chiave privata condivisa e salvare il 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



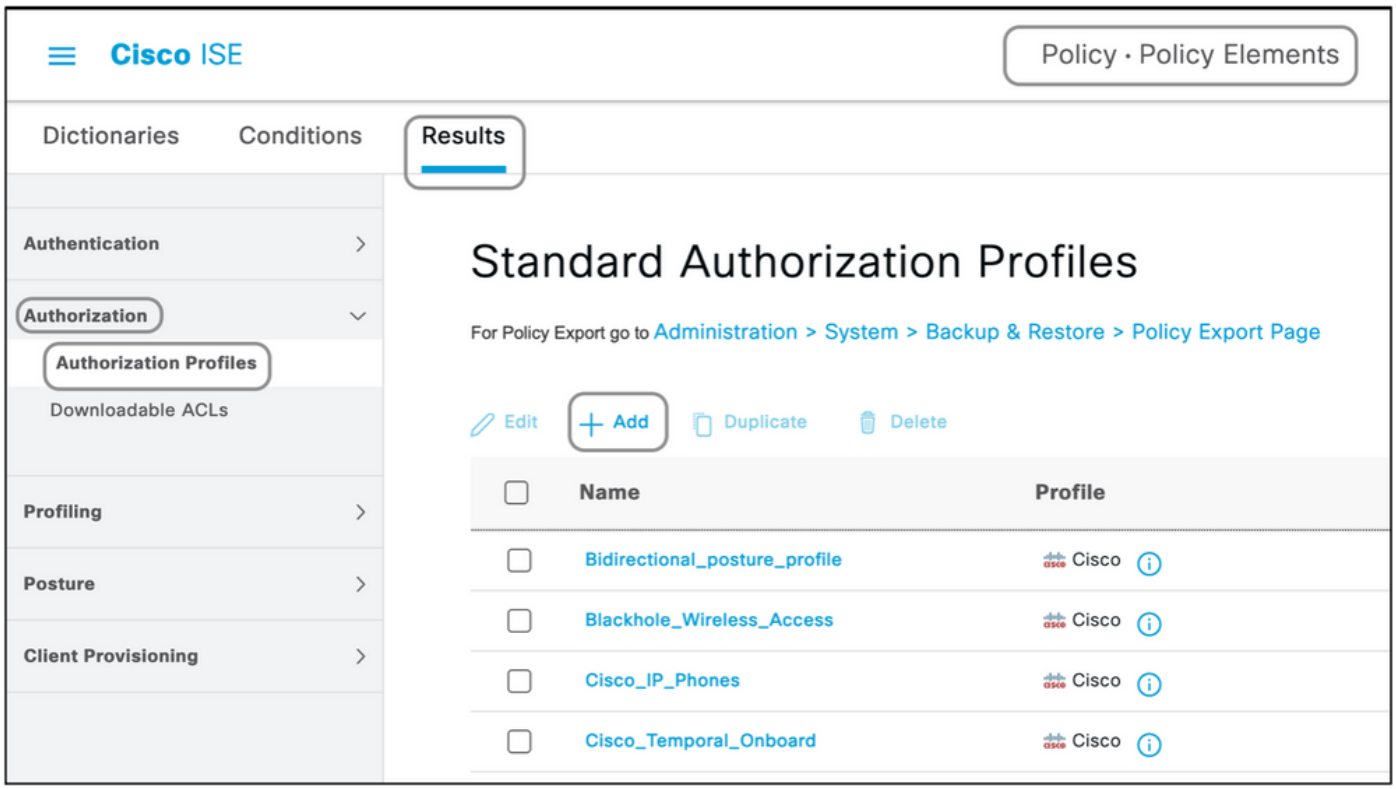
Passaggio 4. Crea profili di autorizzazione

Il risultato finale inviato da ISE come Access-Accept o Access-Reject è definito in un profilo di autorizzazione. Ogni profilo di autorizzazione può eseguire il push di attributi aggiuntivi previsti dal dispositivo di rete.

Di seguito viene riportata la procedura per creare un profilo di autorizzazione.

1. Passare a Criterio > Elementi criteri > Risultati > Autorizzazione > Profili di autorizzazione.

2. In Profili di autorizzazione standard, fare clic su Aggiungi.



I tipi di profili che è possibile aggiungere sono Accesso-Accetta e Accesso-Rifiuta.

Creazione di un profilo di accettazione dell'accesso

Questo profilo viene utilizzato per accedere al dispositivo di rete. A questo profilo possono essere associati più attributi. Di seguito sono riportati i passaggi:

1. Assegnare un nome sensibile e scegliere Tipo di accesso da Access-Accept.

2. Scegliere il profilo del dispositivo di rete creato in una delle sezioni precedenti. Se non è stato creato alcun profilo, è possibile utilizzare quello predefinito di Cisco.

3. Con diversi tipi di profili scelti, la pagina limita le opzioni di configurazione.

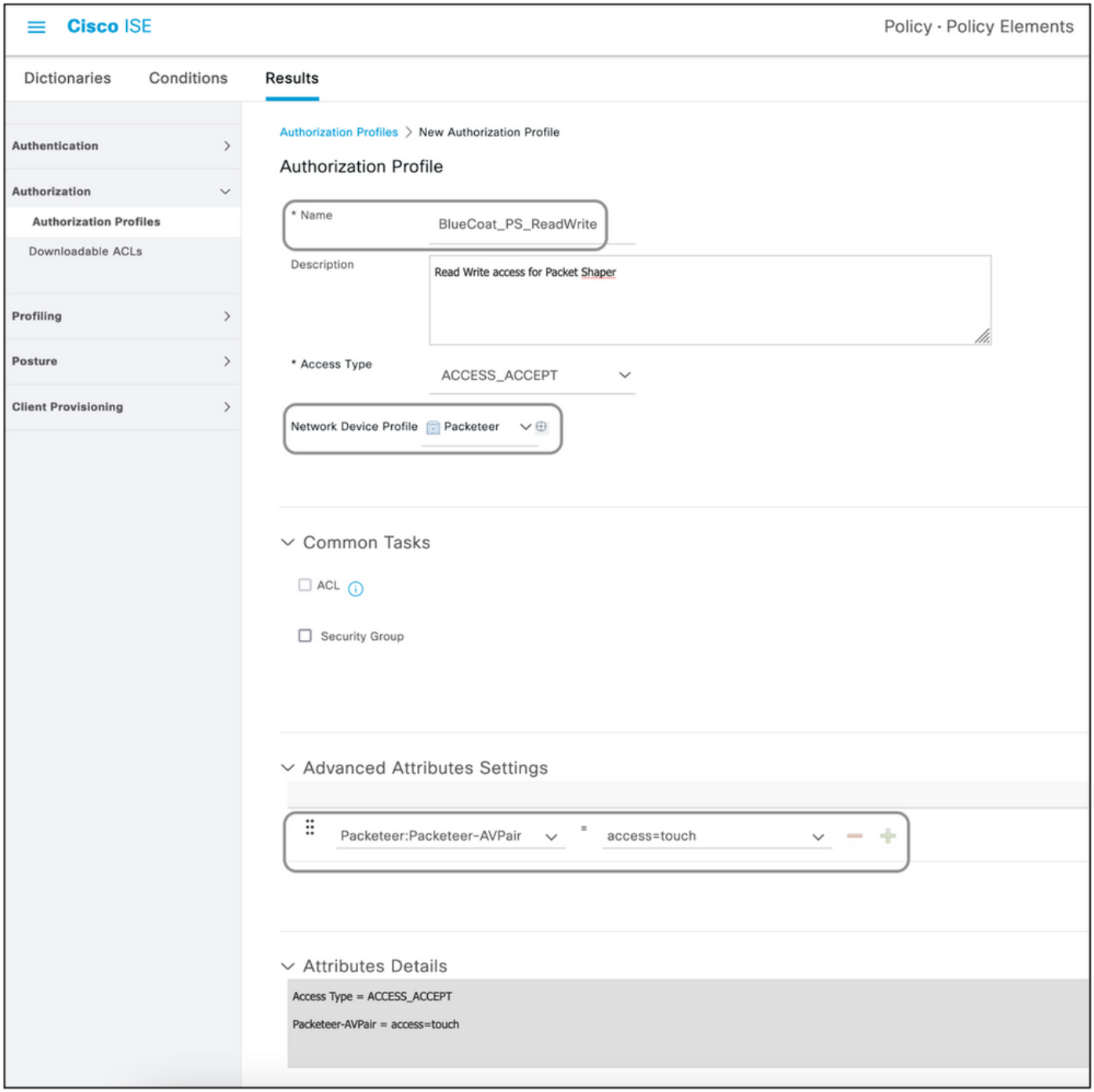
4. In Impostazioni avanzate attributi, scegliere il dizionario e l'attributo applicabile (LHS).

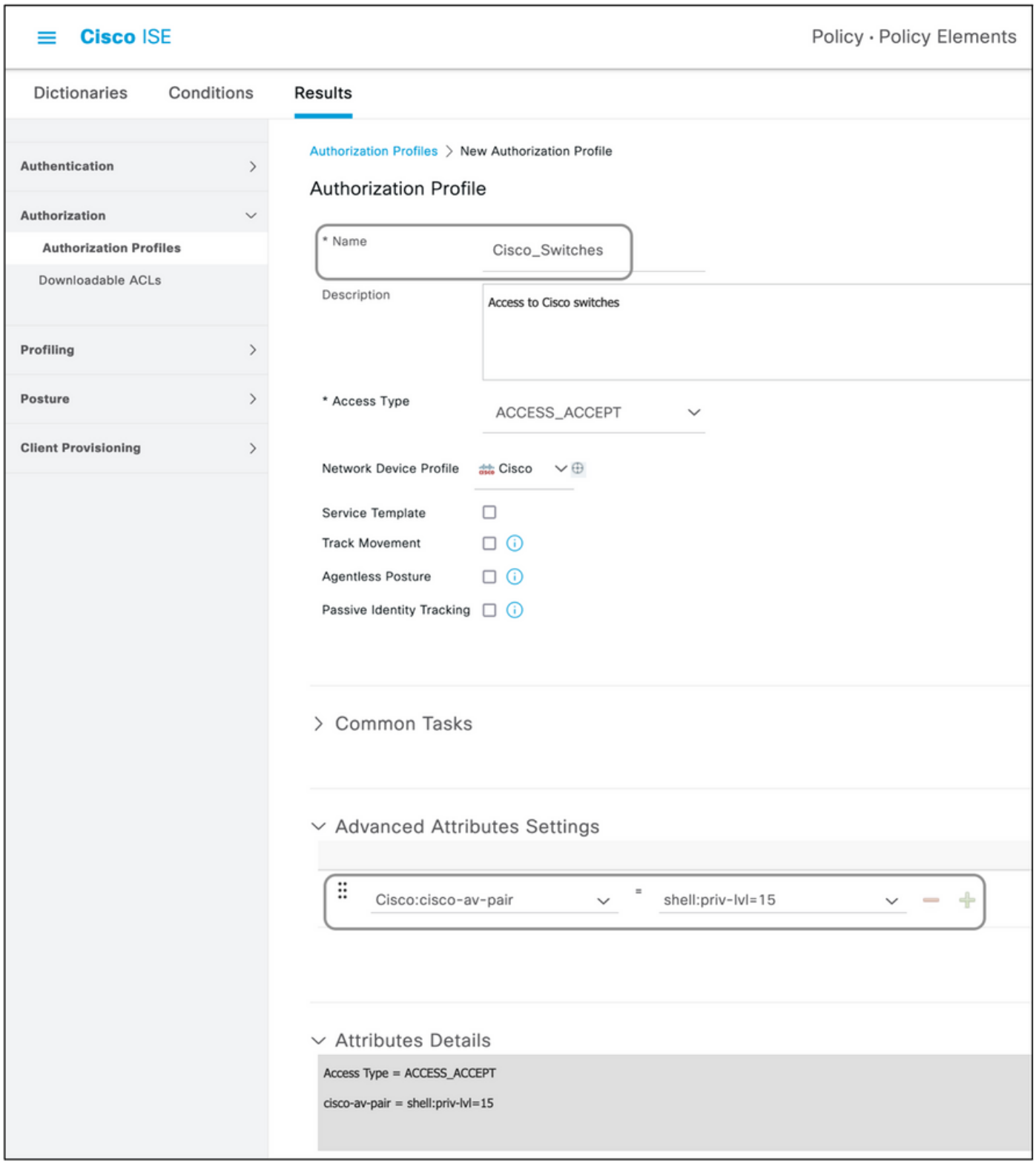
5. Assegnare un valore (RHS) all'attributo dall'elenco a discesa, se disponibile, oppure immettere il valore previsto.

6. Se sono presenti altri attributi da inviare come parte dello stesso risultato, fare clic sull'icona + e ripetere i passaggi 4 e 5.

Creazione di più profili di autorizzazione per ognuno dei risultati/ruoli/autorizzazioni che ISE deve inviare.

Nota: gli attributi consolidati possono essere verificati nel campo Dettagli attributo.


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



Creazione di un profilo di rifiuto di accesso

Questo profilo viene utilizzato per inviare un rifiuto per l'amministrazione del dispositivo, ma può comunque essere utilizzato per inviare attributi insieme ad esso. Questo comando viene usato per inviare un pacchetto Radius Access-Reject. I passaggi rimangono invariati, ad eccezione del passaggio 1, in cui è necessario scegliere Access-Reject invece di Access-Accept per il tipo di accesso.

Passaggio 5. Crea set di criteri

I set di policy sull'ISE vengono valutati dall'alto verso il basso e il primo che soddisfa la condizione impostata nei set di policy è responsabile della risposta dell'ISE al pacchetto Radius Access-Request inviato dal dispositivo di rete. Cisco consiglia di impostare criteri univoci per ciascun tipo di dispositivo. La condizione per valutare l'autenticazione e l'autorizzazione dell'utente si verifica al momento della valutazione. Se ISE dispone di fonti di identità esterne, è possibile utilizzarla per il tipo di autorizzazione.

Un set di criteri tipico viene creato nel modo seguente:

1. Passare a Criterio > Set di criteri > +.

2. Rinominare il nuovo set di criteri 1.

3. Impostare la condizione in modo che sia univoca per il dispositivo.

4. Espandere il set di criteri.

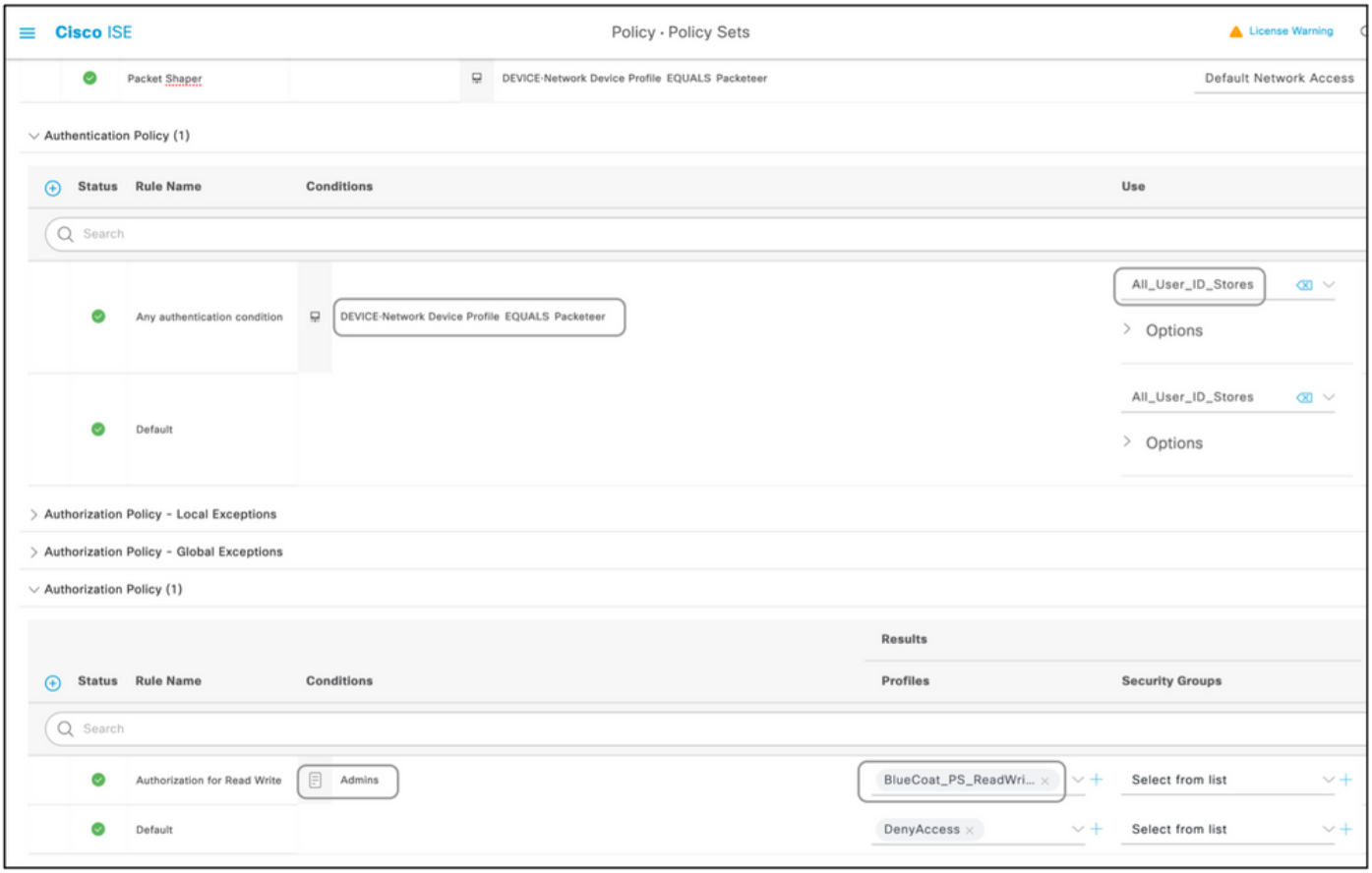
5. Espandere il criterio di autenticazione per impostare una regola di autenticazione. L'origine esterna o gli utenti interni sono esempi che possono essere utilizzati come una sequenza di origine identità in base alla quale ISE verificherebbe l'identità dell'utente.

6. Criteri di autenticazione impostati. A questo punto è possibile salvare il criterio.

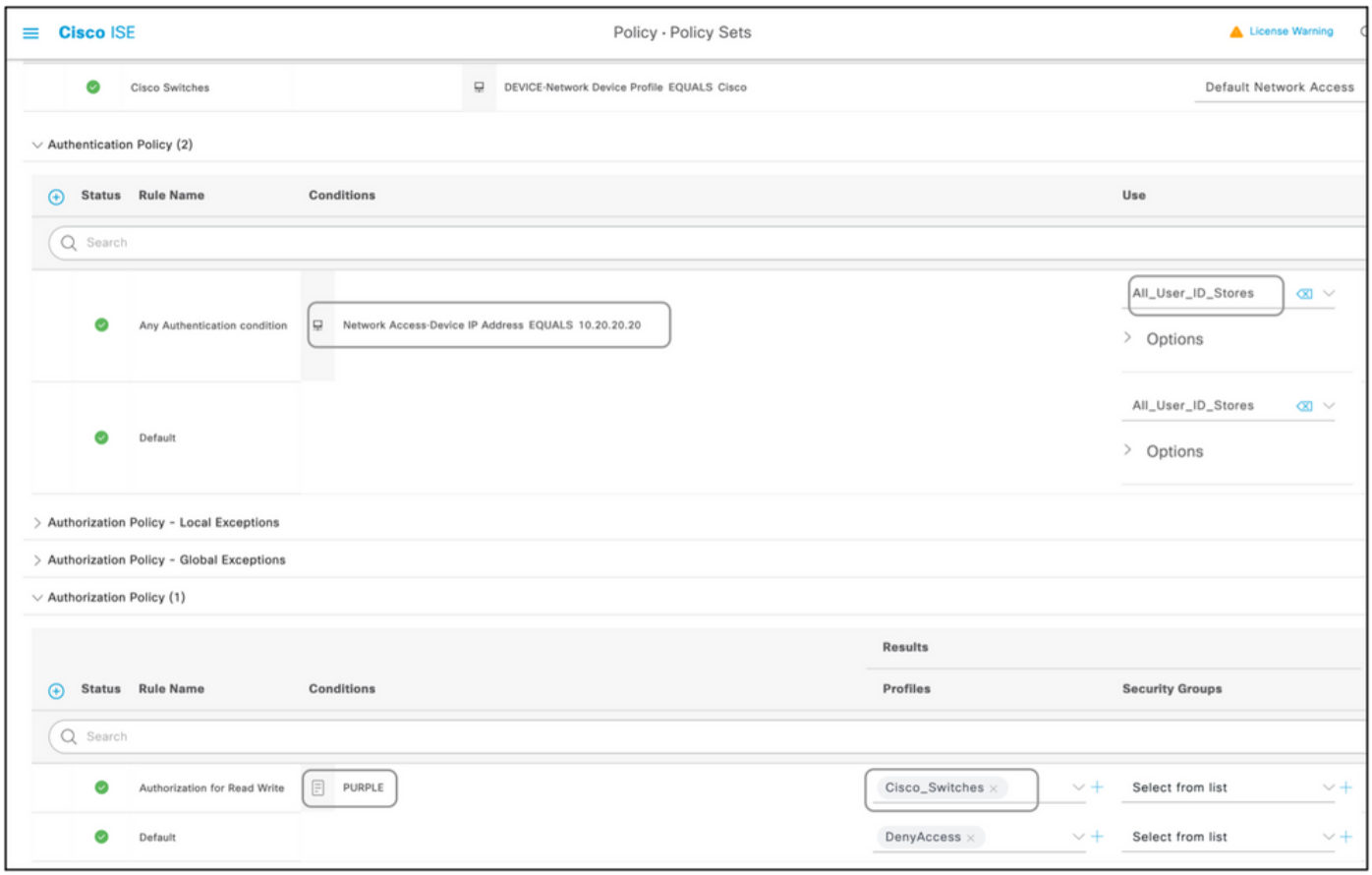
7. Espandere il criterio di autorizzazione per aggiungere le condizioni di autorizzazione per gli utenti. Ad esempio, è possibile verificare un gruppo AD specifico o un gruppo di identità interno ISE. Assegnare alla regola lo stesso nome.

8. Il risultato per la regola di autorizzazione può essere selezionato dall'elenco a discesa.

9. Creare più regole di autorizzazione per diversi tipi di accesso supportati dal fornitore.


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



Elenco dispositivi

Tutti i dispositivi che supportano l'amministrazione dei dispositivi con Radius possono essere aggiunti ad ISE con alcune modifiche a tutti i passaggi menzionati nella sezione precedente. Pertanto, questo documento contiene un elenco di dispositivi che utilizzano le informazioni fornite in questa sezione. L'elenco di attributi e valori fornito in questo documento non è esaustivo né autorevole e può essere modificato in qualsiasi momento senza un aggiornamento del documento. Consultare i siti Web e il supporto del fornitore per la convalida.

Aggregation Services Router (ASR)

Non è necessario creare dizionari separati e VSA per questo tipo di applicazione, in quanto usa coppie Cisco AV già presenti sull'ISE.

Attributo/i: cisco-av-pair

Valore/i: shell:tasks="#<nome-ruolo>,<autorizzazione>:<processo>"

Sintassi: impostare i valori di <nome-ruolo>sul nome di un ruolo definito localmente sul router. La gerarchia dei ruoli può essere descritta in termini di struttura ad albero, in cui il ruolo #radice si trova nella parte superiore della struttura ad albero e il ruolo#leafadds comandi aggiuntivi. Questi due ruoli possono essere combinati e passati se:shell:tasks="#root,#leaf".

È inoltre possibile passare le autorizzazioni a un singolo processo, in modo da concedere a un utente i privilegi di lettura, scrittura ed esecuzione per determinati processi. Ad esempio, per

concedere a un utente i privilegi di lettura e scrittura per il processo BGP, impostare il valore su:shell:tasks="#root,rw:bgp". L'ordine degli attributi è ininfluente; il risultato è lo stesso sia che il valore sia impostato su shell:tasks="#root,rw:bgp" o su toshell:tasks="rw:bgp,#root".

Esempio: aggiungere l'attributo a un profilo di autorizzazione.

Tipo di dizionario	Attributo RADIUS	Tipo di attributo	Valore attributo
RADIUS-Cisco	cisco-av-pair	Stringa	shell:tasks="#root,#leaf,rwx:bgp,r:ospf"

Switch Cisco IOS® e Cisco IOS® XE

Non è necessario creare un dizionario separato e le VSA per questo, in quanto usa attributi RADIUS già presenti su ISE.

Attributo/i:cisco-av-pair

Valore/i:shell:priv-lvl=<livello>

Sintassi: impostare i valori di <livello>sui numeri che rappresentano in pratica il numero di privilegi da inviare. In genere, se si invia 15, si tratta di lettura/scrittura, se si invia 7 si tratta di sola lettura.

Esempio: aggiungere l'attributo a un profilo di autorizzazione.

Tipo di dizionario	Attributo RADIUS	Tipo di attributo	Valore attributo
RADIUS-Cisco	cisco-av-pair	Stringa	shell:priv-lvl=15

BlueCoat Packet Shaper

Attributo/i:Packeteer-AVPair

Valore/i:access=<level>

Utilizzo:<livello>è il livello di accesso da concedere. L'accesso tramite tocco equivale alla lettura/scrittura, mentre l'accesso tramite look equivale alla sola lettura.

Creare un dizionario come mostrato nel presente documento con i seguenti valori:

- Nome: Packeteer
- ID fornitore: 2334
- Dimensione campo lunghezza fornitore: 1
- Dimensione campo tipo fornitore: 1

Immettere i dettagli dell'attributo:

- Attributo:Packeteer-AVPair

- Descrizione: utilizzato per specificare il livello di accesso.
- ID attributo fornitore: 1
- Direzione: OUT
- Multiplo consentito: False
- Consenti tag: deselezionato
- Tipo di attributo: String

Esempio: aggiungere l'attributo a un profilo di autorizzazione (per l'accesso in sola lettura).

Tipo di dizionario	Attributo RADIUS	Tipo di attributo	Valore attributo
RADIUS-Packeter	Packet-AVPair	Stringa	access=aspetto

Esempio: aggiungere l'attributo a un profilo di autorizzazione (per l'accesso in lettura/scrittura).

Tipo di dizionario	Attributo RADIUS	Tipo di attributo	Valore attributo
RADIUS-Packeter	Packet-AVPair	Stringa	access=tocco

Server proxy BlueCoat (AV/SG)

Attributo/i: autorizzazione Blue-Coat

Valore/i: <level>

Utilizzo:<livello>è il livello di accesso da concedere. 0 indica nessun accesso, 1 indica l'accesso in sola lettura, mentre 2 indica l'accesso in lettura/scrittura. L'attributo Blue-Coat-Authorization è quello responsabile del livello di accesso.

Creare un dizionario come mostrato nel presente documento con i seguenti valori:

- Nome: BlueCoat
- ID fornitore: 14501
- Dimensione campo lunghezza fornitore: 1
- Dimensione campo tipo fornitore: 1

Immettere i dettagli dell'attributo:

- Attributo: Blue-Coat-Group
- ID attributo fornitore: 1
- Direzione: BOTH
- Multiplo consentito: False
- Consenti tag: deselezionato
- Tipo di attributo: Unsigned Integer 32 (UINT32)

Immettere i dettagli del secondo attributo:

- Attributo: autorizzazione Blue-Coat
- Descrizione: utilizzato per specificare il livello di accesso.

- ID attributo fornitore: 2
- Direzione: BOTH
- Multiplo consentito: False
- Consenti tag: deselezionato
- Tipo di attributo: Unsigned Integer 32 (UINT32)

Esempio: aggiungere l'attributo a un profilo di autorizzazione (per nessun accesso).

Tipo di dizionario	Attributo RADIUS	Tipo di attributo	Valore attributo
RADIUS-BlueCoat	Blue-Coat-Group	UINT32	0

Esempio: aggiungere l'attributo a un profilo di autorizzazione (per l'accesso in sola lettura).

Tipo di dizionario	Attributo RADIUS	Tipo di attributo	Valore attributo
RADIUS-BlueCoat	Blue-Coat-Group	UINT32	1

Esempio: aggiungere l'attributo a un profilo di autorizzazione (per l'accesso in lettura/scrittura).

Tipo di dizionario	Attributo RADIUS	Tipo di attributo	Valore attributo
RADIUS-BlueCoat	Blue-Coat-Group	UINT32	2

Switch Brocade

Non è necessario creare un dizionario separato e le VSA per questo, in quanto usa attributi RADIUS già presenti su ISE.

Attributi: Tunnel-Private-Group-ID

Valore/i:U:<VLAN1>; T:<VLAN2>

Sintassi: impostare<VLAN1>sul valore della VLAN dati. Impostare<VLAN2>sul valore della VLAN vocale. Nell'esempio, la VLAN dati è la VLAN 10 e la VLAN voce è la VLAN 21.

Esempio: aggiungere l'attributo a un profilo di autorizzazione.

Tipo di dizionario	Attributo RADIUS	Tipo di attributo	Valore attributo
RADIUS-IETF	Tunnel-Private-Group-ID	Stringa con tag	U:10;T:21

Infoblox

Attributi:Infoblox-Group-Info

Valore/i:<group-name>

Sintassi:<nome-gruppo>è il nome del gruppo con i privilegi concessi all'utente. Questo gruppo deve essere configurato nel dispositivo Infoblox. In questo esempio di configurazione, il nome del gruppo è MyGroup.

Creare un dizionario come mostrato nel presente documento con i seguenti valori:

- Nome: Infoblox
- ID fornitore: 7779
- Dimensione campo lunghezza fornitore: 1
- Dimensione campo tipo fornitore: 1

Immettere i dettagli dell'attributo:

- Attributo:Infoblox-Group-Info
- ID attributo fornitore: 009
- Direzione: OUT
- Multiplo consentito: False
- Consenti tag: deselezionato
- Tipo di attributo: String

Esempio: aggiungere l'attributo a un profilo di autorizzazione.

Tipo di dizionario	Attributo RADIUS	Tipo di attributo	Valore attributo
RADIUS-Infoblox	Infoblox-Group-Info	Stringa	GruppoPersonale

Cisco Firepower Management Center

Non è necessario creare un dizionario separato e le VSA per questo, in quanto usa attributi RADIUS già presenti su ISE.

Attributo/i:cisco-av-pair

Valore/i: Class-[25]=<role>

Sintassi: impostare i valori di <ruolo>sui nomi dei ruoli definiti localmente nel CCP. Creare più ruoli, ad esempio admin e utente di sola lettura nel FMC, e assegnare i valori agli attributi nell'ISE che devono essere ricevuti dal FMC allo stesso modo.

Esempio: aggiungere l'attributo a un profilo di autorizzazione.

Tipo di dizionario	Attributo RADIUS	Tipo di attributo	Valore attributo
RADIUS-Cisco	cisco-av-pair	Stringa	Class-[25]=NetAdmins

Switch Nexus

Non è necessario creare un dizionario separato e le VSA per questo, in quanto usa attributi RADIUS già presenti su ISE.

Attributo/i:cisco-av-pair

Valore/i:shell:roles="<role1> <role2>"

Sintassi: impostare i valori di <ruolo1>e<ruolo2>sui nomi dei ruoli definiti localmente sullo switch. Quando si creano più ruoli, separarli con uno spazio. Quando più ruoli vengono passati dal server AAA allo switch Nexus, il risultato è che l'utente ha accesso ai comandi definiti dall'unione di tutti e tre i ruoli.

I ruoli predefiniti sono definiti in Configura account utente e RBAC.

Esempio: aggiungere l'attributo a un profilo di autorizzazione.

Tipo di dizionario	Attributo RADIUS	Tipo di attributo	Valore attributo
RADIUS-Cisco	cisco-av-pair	Stringa	shell:roles="network-admin vdc-admin vdc-operator"

Controller LAN wireless (WLC)

Non è necessario creare un dizionario separato e le VSA per questo, in quanto usa attributi RADIUS già presenti su ISE.

Attributo/i:Service-Type

Valore/i:amministrativi (6) / prompt NAS (7)

Uso: per concedere all'utente l'accesso in lettura/scrittura al controller WLC (Wireless LAN Controller), il valore deve essere Amministrativo; per l'accesso in sola lettura, il valore deve essere Prompt NAS.

Per i dettagli, vedereEsempio di configurazione dell'autenticazione server RADIUS degli utenti di gestione su controller WLC (Wireless LAN Controller)

Esempio: aggiungere l'attributo a un profilo di autorizzazione (per l'accesso in sola lettura).

Tipo di dizionario	Attributo RADIUS	Tipo di attributo	Valore attributo
RADIUS-IETF	Service-Type	Enumerazione	Prompt NAS

Esempio: aggiungere l'attributo a un profilo di autorizzazione (per l'accesso in lettura/scrittura).

Tipo di dizionario	Attributo RADIUS	Tipo di attributo	Valore attributo
RADIUS-IETF	Service-Type	Enumerazione	Amministrativo

DCNM (Data Center Network Manager)

Dopo aver modificato il metodo di autenticazione, è necessario riavviare DCNM. In caso contrario, può assegnare il privilegio di operatore di rete anziché quello di amministratore di rete.

Non è necessario creare un dizionario separato e le VSA per questo, in quanto usa attributi

RADIUS già presenti su ISE.

Attributo/i:cisco-av-pair

Valore/i:shell:roles=<ruolo>

Ruolo DCNM	RADIUS Cisco-AV-Pair
Utente	shell:roles = "operatore di rete"
Amministratore	shell:roles = "network-admin"

Codici audio

Attributo/i: ACL-Auth-Level

Valore/i: ACL-Auth-Level = "<integer>"

Sintassi:<integer>è il livello di accesso da concedere. Il valore dell'attributo ACL-Auth-Level con nome ACL-Auth-UserLevel pari a 50 per l'utente, il valore dell'attributo ACL-Auth-Level con nome ACL-Auth-AdminLevel pari a 100 per l'amministratore e il valore di ACL-Auth-Level con nome ACL-Auth-SecurityAdminLevel pari a 200 per l'amministratore della sicurezza. I nomi possono essere ignorati e i valori per gli attributi possono essere forniti direttamente come valore per la coppia AV avanzata del profilo di autorizzazione.

Creare un dizionario come mostrato nel presente documento con i seguenti valori:

- Nome: AudioCodes
- ID fornitore: 5003
- Dimensione campo lunghezza fornitore: 1
- Dimensione campo tipo fornitore: 1

Immettere i dettagli dell'attributo:

- Attributo: ACL-Auth-Level
- Descrizione: utilizzato per specificare il livello di accesso.
- ID attributo fornitore: 35
- Direzione: OUT
- Multiplo consentito: False
- Consenti tag: deselezionato
- Tipo di attributo: Integer

Esempio: aggiungere l'attributo a un profilo di autorizzazione (per utente).

Tipo di dizionario	Attributo RADIUS	Tipo di attributo	Valore attributo
Codici audio RADIUS	ACL-Auth-Level	Numero intero	50

Esempio: aggiungere l'attributo a un profilo di autorizzazione (per admin).

Tipo di dizionario	Attributo RADIUS	Tipo di attributo	Valore attributo

Codici audio RADIUS	ACL-Auth-Level	Numero intero	100

Esempio: aggiungere l'attributo a un profilo di autorizzazione (per l'amministratore della sicurezza).

Tipo di dizionario	Attributo RADIUS	Tipo di attributo	Valore attributo
Codici audio RADIUS	ACL-Auth-Level	Numero intero	200

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).