

Verwendung von RADIUS für die Geräteadministration mit Identity Services Engine

Inhalt

[Einleitung](#)
[Hintergrundinformationen](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Konfigurieren](#)
[Erstellen eines Access-Accept-Profiles](#)
[Erstellen eines Access-Reject-Profiles](#)
[Geräteliste](#)
[Aggregation Services Router \(ASR\)](#)
[Cisco Switches IOS® und Cisco IOS® XE](#)
[BlueCoat Packet Shaper](#)
[BlueCoat Proxy-Server \(AV/SG\)](#)
[Brocade-Switches](#)
[Infoblox](#)
[Cisco FirePOWER Management Center](#)
[Nexus Switches](#)
[Wireless LAN-Controller \(WLC\)](#)
[Data Center Network Manager \(DCNM\)](#)
[Audiocodes](#)

Einleitung

In diesem Dokument werden die Attribute beschrieben, die verschiedene Produkte von Cisco und von Drittanbietern von einem AAA-Server wie der Cisco ISE erwarten.

Hintergrundinformationen

Produkte von Cisco und anderen Anbietern erhalten eine Zusammenstellung der Attribute eines AAA-Servers (Authentication, Authorization, Accounting). In diesem Fall ist der Server eine Cisco ISE, und die ISE würde diese Attribute zusammen mit einem Access-Accept als Teil eines Autorisierungsprofils (RADIUS) zurückgeben.

Dieses Dokument enthält detaillierte Anweisungen zum Hinzufügen benutzerdefinierter Attribut-Autorisierungsprofile sowie eine Liste der Geräte und RADIUS-Attribute, die die Geräte voraussichtlich vom AAA-Server erhalten. Alle Themen enthalten Beispiele.

Die in diesem Dokument enthaltene Attributliste ist weder vollständig noch verbindlich und kann

jederzeit geändert werden, ohne dieses Dokument zu aktualisieren.

Die Geräteadministration eines Netzwerkgeräts erfolgt in der Regel mit dem Protokoll TACACS+. Wenn das Netzwerkgerät jedoch TACACS+ nicht unterstützt oder die ISE keine Geräteadministrationslizenz hat, kann sie auch mit RADIUS erfolgen, wenn das Netzwerkgerät die Verwaltung des RADIUS-Geräts unterstützt. Einige Geräte unterstützen beide Protokolle, und die Benutzer können selbst entscheiden, welches Protokoll sie verwenden möchten. TACACS+ kann jedoch von Vorteil sein, da es über Funktionen wie Befehlsautorisierung und Befehlskontoverwaltung verfügt.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über folgende Kenntnisse verfügen:

- Cisco ISE als Radius-Server im Netzwerk
- Der Workflow des Radius-Protokolls - RFC2865

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco Identity Services Engine (ISE) 3.x und höheren Versionen der ISE.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Konfigurieren

Schritt 1: Erstellen der anbieterspezifischen Attribute (VSA)

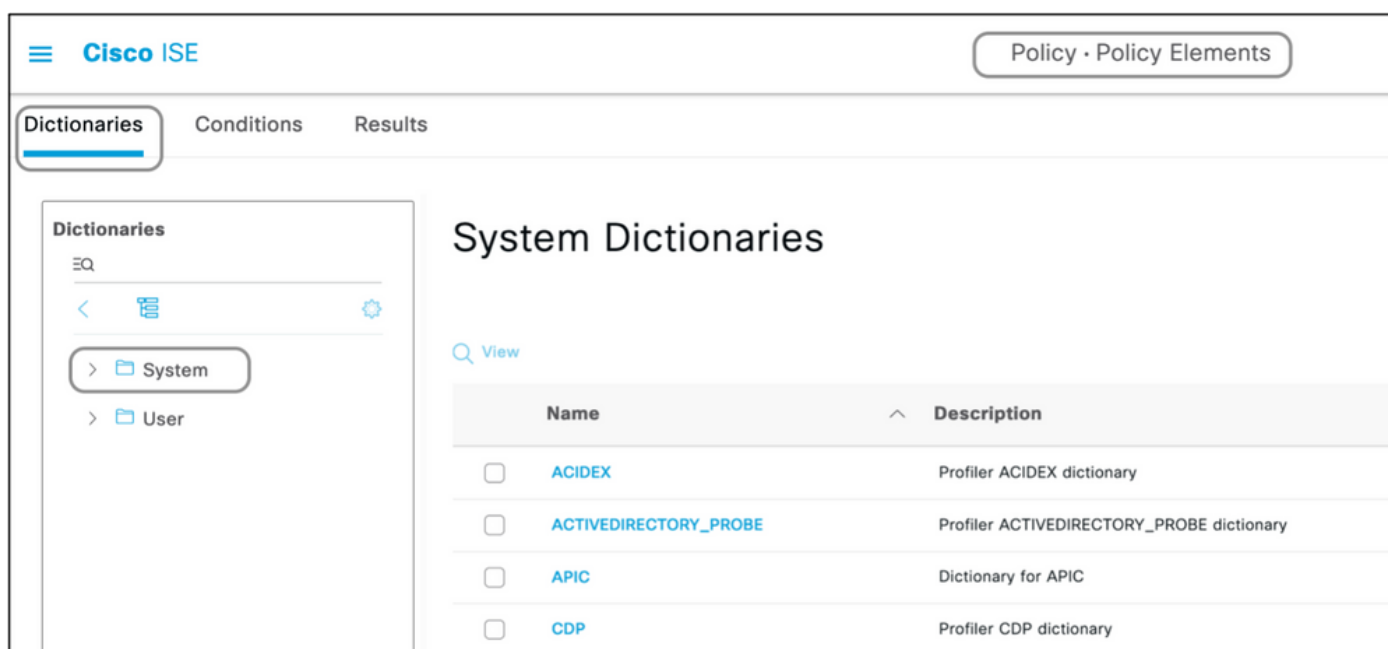
Es können für jeden der Anbieter verschiedene Wörterbücher erstellt und jedem dieser Wörterbücher Attribute hinzugefügt werden. Jedes Dictionary kann mehrere Attribute enthalten, die in den Autorisierungsprofilen verwendet werden können. Jedes Attribut definiert im Allgemeinen die unterschiedliche Rolle der Geräteverwaltung, die ein Benutzer erhalten kann, wenn er sich beim Netzwerkgerät anmeldet. Das Attribut kann jedoch für verschiedene Zwecke des Betriebs oder der Konfiguration auf dem Netzwerkgerät vorgesehen sein.

Die ISE umfasst vordefinierte Attribute für einige Anbieter. Wenn der Anbieter nicht aufgeführt ist, kann er als Wörterbuch mit Attributen hinzugefügt werden. Bei einigen Netzwerkgeräten sind die Attribute konfigurierbar und können für verschiedene Zugriffsarten geändert werden. Wenn dies der Fall ist, muss die ISE mit Attributen konfiguriert werden, die das Netzwerkgerät für verschiedene Zugriffsarten erwartet.

Die Attribute, die voraussichtlich mit einem Radius Access-Accept gesendet werden, werden wie folgt definiert:

1. Navigieren Sie zu **Richtlinie > Richtlinienelemente > Wörterbücher > System > Radius > Radius Vendors > Add**.
2. Der Name und die Anbieter-IDs sind einzugeben und zu speichern.
3. Klicken Sie auf den gespeicherten **Radius-Anbieter**, und navigieren Sie zu **Dictionary Attributes**.
4. Klicken Sie auf **Hinzufügen**, und geben Sie die Groß-/Kleinschreibung für Attributname, Datentyp, Richtung und ID ein.
5. **Speichern Sie** das Attribut.
6. Fügen Sie auf derselben Seite weitere Attribute hinzu, wenn demselben Dictionary mehrere Attribute hinzugefügt werden sollen.

Hinweis: Alle Felder, die in diesem Abschnitt als Werte eingegeben werden, sind vom Anbieter selbst bereitzustellen. Die Websites der Anbieter können besucht werden, oder der Anbieter-Support kann kontaktiert werden, falls diese nicht bekannt sind.



The screenshot shows the Cisco ISE web interface. At the top, there is a navigation bar with the Cisco ISE logo and a breadcrumb trail: Policy > Policy Elements. Below this, there are tabs for 'Dictionaries', 'Conditions', and 'Results', with 'Dictionaries' being the active tab. On the left side, there is a sidebar menu titled 'Dictionaries' with a search bar containing 'EQ'. Below the search bar, there are navigation icons and a tree view showing 'System' and 'User' folders, with 'System' selected. The main content area is titled 'System Dictionaries' and features a 'View' button. Below this is a table with the following data:

Name	Description
<input type="checkbox"/> ACIDEX	Profiler ACIDEX dictionary
<input type="checkbox"/> ACTIVEDIRECTORY_PROBE	Profiler ACTIVEDIRECTORY_PROBE dictionary
<input type="checkbox"/> APIC	Dictionary for APIC
<input type="checkbox"/> CDP	Profiler CDP dictionary

Dictionaries

EQ



- > PassiveID
- > Posture
- > PROFILER
- ▼ Radius
 - > IETF
 - ▼ RADIUS Vendors
 - > Airespace
 - > Alcatel-Lucent
 - > Aruba

RADIUS Vendors

Edit Add Delete Import Export

<input type="checkbox"/>	Name	Vendor ID	Description
<input type="checkbox"/>	Airespace	14179	Dictionary for Vendor Airespace
<input type="checkbox"/>	Alcatel-Lucent	800	Dictionary for Vendor Alcatel-Lucent
<input type="checkbox"/>	Aruba	14823	Dictionary for Vendor Aruba
<input type="checkbox"/>	Brocade	1588	Dictionary for Vendor Brocade
<input type="checkbox"/>	Cisco	9	Dictionary for Vendor Cisco
<input type="checkbox"/>	Cisco-BBSM	5263	Dictionary for Vendor Cisco-BBSM
<input type="checkbox"/>	Cisco-VPN3000	3076	Dictionary for Vendor Cisco-VPN3000

Dictionaries

EQ



- ▼ Radius
 - > IETF
 - ▼ RADIUS Vendors
 - > Airespace
 - > Alcatel-Lucent
 - > Aruba
 - > Brocade

RADIUS Vendors List > New RADIUS Vendor

* Dictionary Name

Description

* Vendor ID

Vendor Attribute Type Field Length

Vendor Attribute Size Field Length

Cisco ISE Policy · Policy Elements

Dictionaries Conditions Results

Dictionaries

Dictionary: Dictionary Attributes

Dictionary Attributes

+ Add Edit Delete

<input type="checkbox"/>	Name	Number	Type	Direction	Description	Predefi...
No data available						

Dictionaries > ... > RADIUS Vendors > Packeteer

Cisco ISE Policy · Policy Elements License Warning

Dictionaries Conditions Results

Dictionaries

Dictionary: Dictionary Attributes

** Attribute Name* Packeteer-AVPair

Description Used in order to specify Access Level

* Data Type STRING Enable MAC option

* Direction OUT

* ID 1 (0-255)

Allow Tagging

Allow multiple instances of this attribute in a profile

Submit

Hinweis: Nicht alle Anbieter erfordern das Hinzufügen eines bestimmten Wörterbuchs. Wenn der Anbieter die von der IETF definierten Radiusattribute verwenden kann, die bereits auf der ISE vorhanden sind, kann dieser Schritt übersprungen werden.

Schritt 2: Netzwerkgeräteprofil erstellen

Dieser Abschnitt ist nicht obligatorisch. Ein Netzwerkgeräteprofil hilft, den hinzugefügten Netzwerkgerätetyp zu isolieren und geeignete Autorisierungsprofile für diese Geräte zu erstellen. Wie die RADIUS-Wörterbücher verfügt auch die ISE über einige vordefinierte Profile, die

verwendet werden können. Falls noch nicht vorhanden, kann ein neues Geräteprofil erstellt werden.

So fügen Sie ein Netzwerkprofil hinzu:

1. Navigieren Sie zu **Administration > Network Resources > Network Device Profiles > Add**.
2. Geben Sie einen Namen an, und aktivieren Sie das Kontrollkästchen für **RADIUS**.
3. Wählen Sie unter **RADIUS Dictionaries** das im vorherigen Abschnitt erstellte Wörterbuch aus.
4. Wenn mehrere Wörterbücher für den gleichen Gerätetyp erstellt wurden, können alle Wörterbücher unter **RADIUS-Wörterbücher** ausgewählt werden.
5. **Speichern Sie** das Profil.

The screenshot shows the Cisco ISE interface for managing Network Device Profiles. The breadcrumb trail is Administration > Network Resources > Network Device Profiles. The page title is "Network Device Profiles". Below the title are several action buttons: Edit, Add, Duplicate, Import, Cisco Communities Import, Export Selected, and Delete Selected. A table lists existing profiles with columns for Name, Description, Vendor, and Source.

Name	Description	Vendor	Source
AlcatelWired	Profile for Alcatel switches	Alcatel	Cisco Provided
ArubaWireless	Profile for Aruba wireless network access devices	Aruba	Cisco Provided
BrocadeWired	Profile for Brocade switches	Brocade	Cisco Provided
Cisco	Generic profile for Cisco network access devices	Cisco	Cisco Provided

The screenshot shows the "New Network Device Profile" form in the Cisco ISE interface. The breadcrumb trail is Administration > Network Resources > Network Device Profiles > New Network Device Profile. The form fields are: Name (Packeteer), Description (Device Profile for Packeteer), Icon (Change icon...), Set To Default, Vendor (Other), and Supported Protocols (RADIUS checked, TACACS+ unchecked, TrustSec unchecked). A RADIUS Dictionaries dropdown menu is open, showing "Packeteer" selected.

Network Device Profile List > New Network Device Profile

Network Device Profiles

Submit Cancel

Name Packeteer

Description Device Profile for Packeteer

Icon Change icon... Set To Default

Vendor Other

Supported Protocols

RADIUS

TACACS+

TrustSec

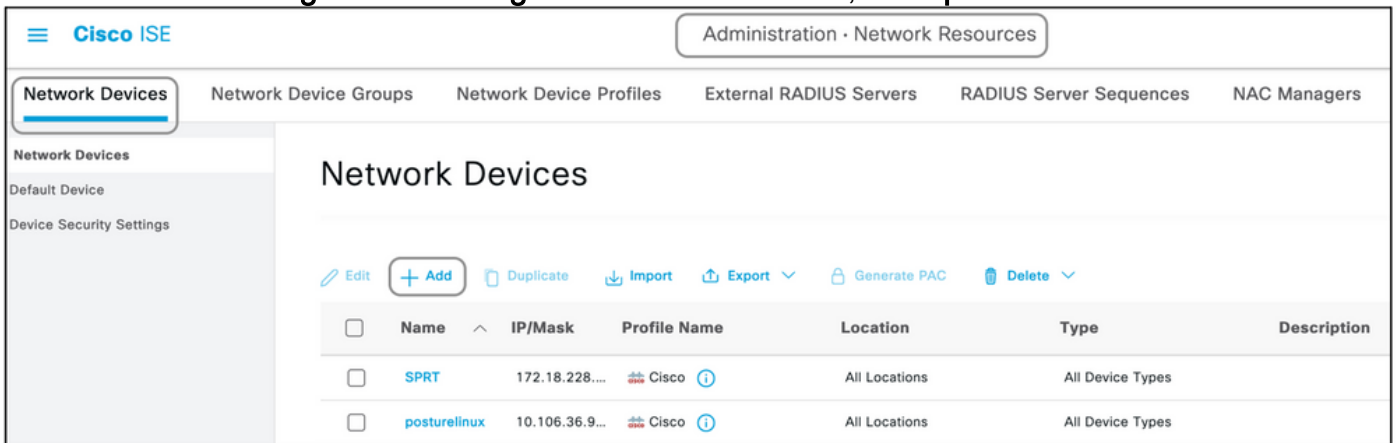
RADIUS Dictionaries Packeteer

Schritt 3: Netzwerkgerät zur ISE hinzufügen

Das Netzwerkgerät, auf dem die Geräteadministration erfolgt, muss zusammen mit einem auf dem Netzwerkgerät definierten Schlüssel der ISE hinzugefügt werden. Auf dem Netzwerkgerät wird die ISE mit diesem Schlüssel als Radius-AAA-Server hinzugefügt.

So fügen Sie ein Gerät zur ISE hinzu:

1. Navigieren Sie zu **Administration > Network Resources > Network Devices > Add**.
2. Geben Sie einen Namen und die IP-Adresse ein.
3. Sie können das Geräteprofil aus der Dropdown-Liste auswählen, um es mit dem im vorherigen Abschnitt definierten Profil zu verknüpfen. Wenn kein Profil erstellt wurde, kann der Cisco Standard verwendet werden.
4. Überprüfen Sie die RADIUS-Authentifizierungseinstellungen.
5. Geben Sie den **gemeinsamen geheimen Schlüssel ein**, und **speichern Sie** das Gerät.



The screenshot shows the Cisco ISE Administration interface. The breadcrumb navigation is 'Administration > Network Resources'. The main menu includes 'Network Devices', 'Network Device Groups', 'Network Device Profiles', 'External RADIUS Servers', 'RADIUS Server Sequences', and 'NAC Managers'. The 'Network Devices' section is active, showing a toolbar with 'Edit', '+ Add', 'Duplicate', 'Import', 'Export', 'Generate PAC', and 'Delete' buttons. Below the toolbar is a table with the following data:

<input type="checkbox"/>	Name	IP/Mask	Profile Name	Location	Type	Description
<input type="checkbox"/>	SPRT	172.18.228....	Cisco ⓘ	All Locations	All Device Types	
<input type="checkbox"/>	posturelinux	10.106.36.9...	Cisco ⓘ	All Locations	All Device Types	

Network Devices

Default Device

Device Security Settings

[Network Devices List](#) > [New Network Device](#)

Network Devices

Name

Description

IP Address /

Device Profile

Model Name

Software Version

Network Device Group

Device Type

IPSEC

Location

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol

Shared Secret

Cisco ISE Administration · Network Resources

Network Devices | Network Device Groups | Network Device Profiles | External RADIUS Servers | RADIUS Server Sequences | NAC Man

Network Devices List > New Network Device

Network Devices

Name

Description

IP Address /

Device Profile

Model Name

Software Version

Network Device Group

Location [Set To Default](#)

IPSEC [Set To Default](#)

Device Type [Set To Default](#)

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol

Shared Secret [Show](#)

Schritt 4: Autorisierungsprofile erstellen

Das Endergebnis, das von der ISE als "Access-Accept" oder "Access-Reject" weitergeleitet wird, wird in einem Autorisierungsprofil definiert. Jedes Autorisierungsprofil kann zusätzliche Attribute übertragen, die das Netzwerkgerät erwartet.

So erstellen Sie ein Autorisierungsprofil:

1. Navigieren Sie zu **Richtlinie > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofile**.
2. Klicken Sie unter **Standardautorisierungsprofile** auf **Hinzufügen**.

The screenshot shows the Cisco ISE web interface. At the top, there is a navigation bar with 'Cisco ISE' and a breadcrumb 'Policy · Policy Elements'. Below this, a menu has 'Results' selected. The left sidebar contains a tree view with 'Authentication', 'Authorization' (selected), 'Downloadable ACLs', 'Profiling', 'Posture', and 'Client Provisioning'. Under 'Authorization', 'Authorization Profiles' is selected. The main content area is titled 'Standard Authorization Profiles' and includes a link for policy export: 'For Policy Export go to Administration > System > Backup & Restore > Policy Export Page'. Below the title are action buttons: 'Edit', '+ Add', 'Duplicate', and 'Delete'. A table lists the profiles:

<input type="checkbox"/>	Name	Profile
<input type="checkbox"/>	Bidirectional_posture_profile	Cisco ⓘ
<input type="checkbox"/>	Blackhole_Wireless_Access	Cisco ⓘ
<input type="checkbox"/>	Cisco_IP_Phones	Cisco ⓘ
<input type="checkbox"/>	Cisco_Temporal_Onboard	Cisco ⓘ

Die Profiltypen, die hinzugefügt werden können, sind Access-Accept und Access-Reject.

Erstellen eines Access-Accept-Profiles

Dieses Profil wird für den Zugriff auf das Netzwerkgerät verwendet. Diesem Profil können mehrere Attribute zugeordnet werden. So gehen Sie vor:

1. Geben Sie einen sinnvollen Namen an, und wählen Sie Access Type (Zugriffstyp) als Access-Accept (Access-Accept) aus.
2. Wählen Sie das Netzwerkgeräteprofil aus, das in einem der vorherigen Abschnitte erstellt wurde. Wenn kein Profil erstellt wurde, kann die Cisco Standardeinstellung verwendet werden.
3. Bei verschiedenen Profiltypen werden auf dieser Seite die Konfigurationsoptionen eingeschränkt.
4. Wählen Sie unter **Erweiterte Attributeinstellungen** das Wörterbuch und das entsprechende Attribut (LHS) aus.
5. Weisen Sie dem Attribut einen Wert (RHS) zu, entweder aus dem Dropdown-Menü, falls verfügbar, oder geben Sie den erwarteten Wert ein.
6. Wenn mehrere Attribute als Teil desselben Ergebnisses gesendet werden sollen, klicken Sie auf das Symbol +, und wiederholen Sie die Schritte 4 und 5.

Erstellen Sie mehrere Autorisierungsprofile für jede der Ergebnisse/Rollen/Autorisierungen, die von der ISE erwartet werden.

Hinweis: Die konsolidierten Attribute können im Feld Attributdetails überprüft werden.

Dictionaryes Conditions **Results**

- Authentication >
- Authorization ▾
 - Authorization Profiles**
 - Downloadable ACLs
- Profiling >
- Posture >
- Client Provisioning >

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Common Tasks

ACL ⓘ

Security Group

Advanced Attributes Settings

Attributes Details

Access Type = ACCESS_ACCEPT

Packeteer-AVPair = access=touch

Cisco ISE Policy · Policy Elements

Dictionarys Conditions **Results**

Authentication >

Authorization >

Authorization Profiles

Downloadable ACLs

Profiling >

Posture >

Client Provisioning >

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement ⓘ

Agentless Posture ⓘ

Passive Identity Tracking ⓘ

> Common Tasks

Advanced Attributes Settings

=

Attributes Details

Access Type = ACCESS_ACCEPT

cisco-av-pair = shell:priv-lvl=15

Erstellen eines Access-Reject-Profiles

Dieses Profil wird verwendet, um eine Ablehnung für die Geräteadministration zu senden. Es kann jedoch weiterhin verwendet werden, um Attribute zusammen mit dieser zu senden. Hiermit wird ein Radius Access-Reject-Paket gesendet. Die Schritte bleiben bis auf den ersten Schritt, in dem Access-Reject (Zugriffstyp) anstelle von Access-Accept (Zugriffstyp) ausgewählt werden muss, unverändert.

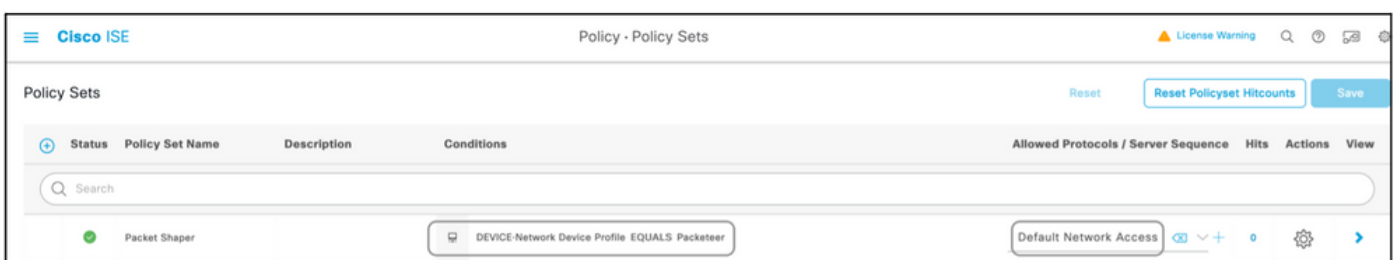
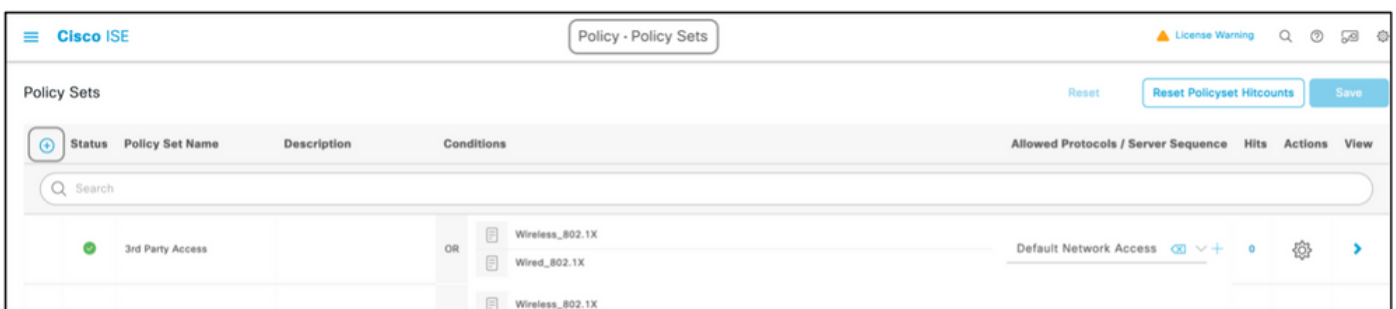
Schritt 5: Erstellen eines Policy Sets

Richtliniensätze auf der ISE werden von oben nach unten ausgewertet, und der erste, der die in

den Richtlinienätzen festgelegten Bedingungen erfüllt, ist für die Antwort der ISE auf das vom Netzwerkgerät gesendete Radius Access-Request-Paket verantwortlich. Cisco empfiehlt einen eindeutigen Richtlinienatz für jeden Gerätetyp. Die Bedingung zur Auswertung der Authentifizierung und Autorisierung des Benutzers erfolgt bei der Auswertung. Wenn die ISE über externe Identitätsquellen verfügt, kann sie für die Art der Autorisierung verwendet werden.

Ein typischer Richtlinienatz wird auf diese Weise erstellt:

1. Navigieren Sie zu **Policy > Policy Sets > +**.
2. Umbenennen des **Neuer Richtlinienatz 1**.
3. Die Bedingung für dieses Gerät als eindeutig festlegen.
4. Erweitern Sie den **Richtliniensatz**.
5. Erweitern Sie die **Authentifizierungsrichtlinie**, um eine Authentifizierungsregel festzulegen. Die externe Quelle oder die internen Benutzer sind Beispiele, die als Identitätsquellensequenz verwendet werden können, anhand derer die ISE nach dem Benutzer sucht.
6. Die Authentifizierungsrichtlinie ist festgelegt. Die Richtlinie kann an dieser Stelle gespeichert werden.
7. Erweitern Sie die **Autorisierungsrichtlinie**, um die Autorisierungsbedingungen für die Benutzer hinzuzufügen. Ein Beispiel ist die Suche nach einer bestimmten AD-Gruppe oder internen ISE-Identitätsgruppe. Geben Sie der Regel einen ähnlichen Namen.
8. Das Ergebnis für die Autorisierungsregel kann im Dropdown-Menü ausgewählt werden.
9. Erstellen Sie mehrere Autorisierungsregeln für verschiedene Arten von Zugriff, die vom Anbieter unterstützt werden.



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
✓	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)

Status	Rule Name	Conditions	Results	
			Profiles	Security Groups
✓	Authorization for Read Write	Admins	BlueCoat_PS_ReadWri... x	Select from list
✓	Default		DenyAccess x	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
✓	Cisco Switches		DEVICE Network Device Profile EQUALS Cisco	Default Network Access	0		

Geräteliste

Jedes Gerät, das die Geräteadministration mit Radius unterstützt, kann mit einigen Änderungen an allen im vorherigen Abschnitt genannten Schritten zur ISE hinzugefügt werden. Daher enthält dieses Dokument eine Liste von Geräten, die mit den in diesem Abschnitt bereitgestellten Informationen arbeiten. Die in diesem Dokument enthaltene Liste der Attribute und Werte ist weder vollständig noch verbindlich und kann jederzeit geändert werden, ohne dieses Dokument zu aktualisieren. Die Validierung finden Sie auf den Websites des jeweiligen Anbieters und im Anbietersupport.

Aggregation Services Router (ASR)

Hierfür müssen keine separaten Wörterbücher und VSAs erstellt werden, da diese Cisco AV-Paare verwenden, die bereits auf der ISE vorhanden sind.

Attribut(e): **cisco-av-pair**

Wert(e): **shell:tasks="#<Rollenname>,<Berechtigung>:<Prozess>"**

Syntax: Legen Sie die Werte von <Rollenname> auf den Namen einer Rolle fest, die lokal auf dem Router definiert ist. Die Rollenhierarchie kann in Form einer Struktur beschrieben werden, in der die Rolle #root is oben in der Struktur angezeigt wird und die Rolle #leafadd zusätzliche Befehle enthält. Diese beiden Rollen können kombiniert und zurückgegeben werden, wenn: **shell:tasks="#root,#leaf"**.

Berechtigungen können auch auf Basis einzelner Prozesse zurückgegeben werden, sodass einem Benutzer Lese-, Schreib- und Ausführungsberechtigungen für bestimmte Prozesse erteilt werden können. Um beispielsweise einem Benutzer Lese- und Schreibberechtigungen für den BGP-

Prozess zuzuweisen, setzen Sie den Wert auf: **shell:tasks="#root,rw:bgp"**. Die Reihenfolge der Attribute spielt keine Rolle. Das Ergebnis ist gleich, ob der Wert auf **"toshell:tasks="#root,rw:bgp"** oder **"toshell:tasks="rw:bgp,#root"** festgelegt ist.

Beispiel: Fügen Sie das Attribut einem Autorisierungsprofil hinzu.

Dictionary-Typ	RADIUS-Attribut	Attributtyp	Attributwert
RADIUS - Cisco	cisco-av-pair	String	shell:tasks="#root,#leaf,rwx:bgp,r:ospf"

Cisco Switches IOS® und Cisco IOS® XE

Hierfür müssen kein separates Wörterbuch und keine VSAs erstellt werden, da es RADIUS-Attribute verwendet, die bereits auf der ISE vorhanden sind.

Attribut(e): **cisco-av-pair**

Wert(e): **shell:priv-lvl=<level>**

Syntax: Legen Sie die Werte von <level> auf die Nummern fest, die im Wesentlichen die Anzahl der zu sendenden Berechtigungen sind. Wenn 15 gesendet wird, bedeutet dies in der Regel Lese-/Schreibzugriff, und wenn 7 gesendet wird, bedeutet dies schreibgeschützt.

Beispiel: Fügen Sie das Attribut einem Autorisierungsprofil hinzu.

Dictionary-Typ	RADIUS-Attribut	Attributtyp	Attributwert
RADIUS - Cisco	cisco-av-pair	String	shell:priv-lvl=15

BlueCoat Packet Shaper

Attribute: **Packeter-AVPair**

Wert(e): **access=<level>**

Nutzung: <level> ist die Ebene des zu gewährenden Zugriffs. Touch-Zugriff ist gleichbedeutend mit Lese- und Schreibzugriff, während Look-Zugriff gleichbedeutend mit Schreibzugriff ist.

Dictionary erstellen, wie in diesem Dokument gezeigt, mit folgenden Werten:

- Name: Packeteer
- Hersteller-ID: 2334
- Herstellerlänge - Feldgröße: 1
- Anbietertyp - Feldgröße: 1

Geben Sie die Details des Attributs ein:

- Attribut: Packeter-AVPair
- Beschreibung: Wird verwendet, um die Zugriffsebene anzugeben.
- Kreditorenattribut-ID: 1

- Richtung: OUT
- Mehrere zulässig: Falsch
- Tagging zulassen: deaktiviert
- Attributtyp: Zeichenfolge

Beispiel: Hinzufügen des Attributs zu einem Autorisierungsprofil (für schreibgeschützten Zugriff).

Dictionary-Typ	RADIUS-Attribut	Attributtyp	Attributwert
RADIUS-Packeter	Packeter - AVPair	String	access=look

Beispiel: Hinzufügen des Attributs zu einem Autorisierungsprofil (für Lese- und Schreibzugriff).

Dictionary-Typ	RADIUS-Attribut	Attributtyp	Attributwert
RADIUS-Packeter	Packeter - AVPair	String	access=touch

BlueCoat Proxy-Server (AV/SG)

Attribut(e): **Blue-Coat-Autorisierung**

Wert(e): **<level>**

Nutzung:<level>ist die Ebene des zu gewährenden Zugriffs. 0 bedeutet "kein Zugriff", 1 bedeutet "schreibgeschützter Zugriff", 2 bedeutet "Lese-/Schreibzugriff". Das Blue-Coat-Authorization-Attribut ist für die Zugriffsebene verantwortlich.

Dictionary erstellen, wie in diesem Dokument gezeigt, mit folgenden Werten:

- Name: BlueCoat
- Anbieter-ID: 14501
- Herstellerlänge - Feldgröße: 1
- Anbietertyp - Feldgröße: 1

Geben Sie die Details des Attributs ein:

- Attribut: Blue-Coat-Group
- Kreditorenattribut-ID: 1
- Richtung: BEIDE
- Mehrere zulässig: Falsch
- Tagging zulassen: deaktiviert
- Attributtyp: Unsigned Integer 32 (UINT32)

Geben Sie die Details des zweiten Attributs ein:

- Attribut: Blue-Coat-Autorisierung
- Beschreibung: Wird verwendet, um die Zugriffsebene anzugeben.
- Kreditorenattribut-ID: 2
- Richtung: BEIDE
- Mehrere zulässig: Falsch
- Tagging zulassen: deaktiviert
- Attributtyp: Unsigned Integer 32 (UINT32)

Beispiel: Fügen Sie das Attribut einem Autorisierungsprofil hinzu (ohne Zugriff).

Dictionary-Typ	RADIUS-Attribut	Attributtyp	Attributwert
RADIUS-BlueCoat	Blue-Coat-Gruppe	INT32	0

Beispiel: Hinzufügen des Attributs zu einem Autorisierungsprofil (für schreibgeschützten Zugriff).

Dictionary-Typ	RADIUS-Attribut	Attributtyp	Attributwert
RADIUS-BlueCoat	Blue-Coat-Gruppe	INT32	1

Beispiel: Hinzufügen des Attributs zu einem Autorisierungsprofil (für Lese- und Schreibzugriff).

Dictionary-Typ	RADIUS-Attribut	Attributtyp	Attributwert
RADIUS-BlueCoat	Blue-Coat-Gruppe	INT32	2

Brocade-Switches

Hierfür müssen kein separates Wörterbuch und keine VSAs erstellt werden, da es RADIUS-Attribute verwendet, die bereits auf der ISE vorhanden sind.

Attribut(e): **Tunnel-Private-Group-ID**

Wert(e): **U:<VLAN1>; T:<VLAN2>**

Syntax: Legen Sie <VLAN1> den Wert des Daten-VLAN fest. Legen Sie <VLAN2> den Wert des Sprach-VLANs fest. In diesem Beispiel ist das Daten-VLAN VLAN 10 und das Sprach-VLAN VLAN 21.

Beispiel: Fügen Sie das Attribut einem Autorisierungsprofil hinzu.

Dictionary-Typ	RADIUS-Attribut	Attributtyp	Attributwert
RADIUS-IETF	Tunnel-Private-Group-ID	Markierte Zeichenfolge	U:10;T:21

Infoblox

Attribut(e): **Infoblox-Group-Info**

Wert(e): **<Gruppenname>**

Syntax: <Gruppenname> ist der Name der Gruppe mit den Berechtigungen, die der Benutzer erhält. Diese Gruppe muss auf dem Infoblox-Gerät konfiguriert werden. In diesem Konfigurationsbeispiel lautet der Gruppenname MyGroup.

Dictionary erstellen, wie in diesem Dokument gezeigt, mit folgenden Werten:

- Name: Infoblox
- Anbieter-ID: 7779
- Herstellerlänge - Feldgröße: 1
- Anbietertyp - Feldgröße: 1

Geben Sie die Details des Attributs ein:

- Attribut: Infoblox-Group-Info
- Kreditorenattribut-ID: 009

- Richtung: OUT
- Mehrere zulässig: Falsch
- Tagging zulassen: deaktiviert
- Attributtyp: Zeichenfolge

Beispiel: Fügen Sie das Attribut einem Autorisierungsprofil hinzu.

Dictionary-Typ	RADIUS-Attribut	Attributtyp	Attributwert
RADIUS-Infoblox	Infoblox-Gruppe-Info	String	MeineGruppe

Cisco FirePOWER Management Center

Hierfür müssen kein separates Wörterbuch und keine VSAs erstellt werden, da es RADIUS-Attribute verwendet, die bereits auf der ISE vorhanden sind.

Attribut(e): **cisco-av-pair**

Wert(e): **Class-[25]=<Rolle>**

Syntax: Legen Sie die Werte von <Rolle> auf die Namen der Rollen fest, die lokal im FMC definiert sind. Erstellen Sie mehrere Rollen, z. B. einen Administrator und einen schreibgeschützten Benutzer, auf dem FMC, und weisen Sie die Werte den Attributen auf der ISE zu, die vom FMC ebenfalls empfangen werden sollen.

Beispiel: Fügen Sie das Attribut einem Autorisierungsprofil hinzu.

Dictionary-Typ	RADIUS-Attribut	Attributtyp	Attributwert
RADIUS - Cisco	cisco-av-pair	String	Klasse-[25]=NetAdmins

Nexus Switches

Hierfür müssen kein separates Wörterbuch und keine VSAs erstellt werden, da es RADIUS-Attribute verwendet, die bereits auf der ISE vorhanden sind.

Attribut(e): **cisco-av-pair**

Wert(e): **shell:roles="<role1> <role2>"**

Verwendung: Legen Sie die Werte von <role1> und <role2> auf die Namen der Rollen fest, die lokal auf dem Switch definiert sind. Wenn mehrere Rollen erstellt wurden, trennen Sie diese durch ein Leerzeichen. Wenn mehrere Rollen vom AAA-Server an den Nexus-Switch zurückgegeben werden, hat der Benutzer Zugriff auf Befehle, die durch die Vereinigung aller drei Rollen definiert werden.

Die integrierten Rollen werden [unter Benutzerkonten konfigurieren und RBAC](#) definiert.

Beispiel: Fügen Sie das Attribut einem Autorisierungsprofil hinzu.

Dictionary-Typ	RADIUS-Attribut	Attributtyp	Attributwert
RADIUS - Cisco	cisco-av-pair	String	shell:roles="network-admin vdc-admin vdc-operator"

Wireless LAN-Controller (WLC)

Hierfür müssen kein separates Wörterbuch und keine VSAs erstellt werden, da es RADIUS-Attribute verwendet, die bereits auf der ISE vorhanden sind.

Attribut(e): **Servicetyp**

Wert(e): **Verwaltung (6)/NAS-Aufforderung (7)**

Verwendung: Um dem Benutzer Lese-/Schreibzugriff auf den Wireless LAN Controller (WLC) zu gewähren, muss der Wert "Administrative" (Administrativ) lauten; für schreibgeschützten Zugriff muss der Wert "NAS-Prompt" (NAS-Prompt) lauten.

Weitere Informationen [finden Sie unter Konfigurationsbeispiel für die RADIUS-Serverauthentifizierung von Verwaltungsbenutzern auf dem Wireless LAN-Controller \(WLC\).](#)

Beispiel: Hinzufügen des Attributs zu einem Autorisierungsprofil (für schreibgeschützten Zugriff).

Dictionary-Typ	RADIUS-Attribut	Attributtyp	Attributwert
RADIUS-IETF	Servicetyp	Aufzählung	NAS-Aufforderung

Beispiel: Hinzufügen des Attributs zu einem Autorisierungsprofil (für Lese- und Schreibzugriff).

Dictionary-Typ	RADIUS-Attribut	Attributtyp	Attributwert
RADIUS-IETF	Servicetyp	Aufzählung	Verwaltung

Data Center Network Manager (DCNM)

DCNM muss neu gestartet werden, nachdem die Authentifizierungsmethode geändert wurde. Andernfalls kann statt network-admin eine Netzwerkbetreiberberechtigung zugewiesen werden.

Hierfür müssen kein separates Wörterbuch und keine VSAs erstellt werden, da es RADIUS-Attribute verwendet, die bereits auf der ISE vorhanden sind.

Attribut(e): **cisco-av-pair**

Wert(e): **shell:roles=<role>**

DCNM-Rolle	RADIUS Cisco-AV-Pair
Benutzer	shell:roles = "network-operator"
Administrator	shell:roles = "network-admin"

Audiocodes

Attribut(e): **ACL-Authentifizierungsebene**

Wert(e): **ACL-Auth-Level = "<Ganzzahl>"**

Syntax:<Ganzzahl> ist die Zugriffsstufe, die gewährt werden soll. Ein Wert des ACL-Auth-Level-Attributs mit dem Namen ACL-Auth-UserLevel von 50 für den Benutzer, ein Wert des ACL-Auth-Level-Attributs mit dem Namen ACL-Auth-AdminLevel von Wert100 für den Administrator und ein Wert von ACL-Auth-Level mit dem Namen ACL-Auth-SecurityAdminLevel von Wert 200 für den

Sicherheitsadministrator. Die Namen können übersprungen werden, und die Werte für Attribute können direkt als Wert für das Autorisierungsprofil Advanced AV-Paar angegeben werden.

Dictionary erstellen, wie in diesem Dokument gezeigt, mit folgenden Werten:

- Name: AudioCodes
- Hersteller-ID: 5003
- Herstellerlänge - Feldgröße: 1
- Anbietertyp - Feldgröße: 1

Geben Sie die Details des Attributs ein:

- Attribut: ACL-Authentifizierungsebene
- Beschreibung: Wird verwendet, um die Zugriffsebene anzugeben.
- Kreditorenattribut-ID: 35
- Richtung: OUT
- Mehrere zulässig: Falsch
- Tagging zulassen: deaktiviert
- Attributtyp: Integer

Beispiel: Hinzufügen des Attributs zu einem Autorisierungsprofil (für Benutzer).

Dictionary-Typ	RADIUS-Attribut	Attributtyp	Attributwert
RADIUS-Audio-Codes	ACL-Authentifizierungsebene	Ganzzahl	50

Beispiel: Fügen Sie das Attribut einem Autorisierungsprofil hinzu (für admin).

Dictionary-Typ	RADIUS-Attribut	Attributtyp	Attributwert
RADIUS-Audio-Codes	ACL-Authentifizierungsebene	Ganzzahl	100

Beispiel: Fügen Sie das Attribut einem Autorisierungsprofil hinzu (für Sicherheitsadministratoren).

Dictionary-Typ	RADIUS-Attribut	Attributtyp	Attributwert
RADIUS-Audio-Codes	ACL-Authentifizierungsebene	Ganzzahl	200

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.