

# Differenzierung von Authentifizierungstypen auf ASA-Plattformen für Richtlinienentscheidungen auf ISE

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[RADIUS VSA 3076/150 Client-Type-Attribut](#)

[Konfigurieren](#)

[Schritt 1](#)

[Schritt 2](#)

[Überprüfen](#)

[Zugehörige Informationen](#)

## [Einführung](#)

In diesem Dokument wird beschrieben, wie die Cisco Identity Services Engine (ISE) so konfiguriert wird, dass sie das Client-Type RADIUS Vendor-Specific Attribute (VSA) verwendet, um verschiedene Authentifizierungstypen zu unterscheiden, die in der Cisco Adaptive Security Appliance (ASA) verwendet werden. Organisationen erfordern häufig Richtlinienentscheidungen, die auf der Authentifizierungsmethode des Benutzers für die ASA basieren. So können Sie auch Richtlinien auf empfangene Management-Verbindungen auf der ASA anwenden, sodass wir bei Bedarf RADIUS anstelle von TACACS+ verwenden können.

## [Voraussetzungen](#)

### [Anforderungen](#)

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- ISE-Authentifizierung und -Autorisierung
- ASA-Authentifizierungsmethoden und RADIUS-Konfiguration.

### [Verwendete Komponenten](#)

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Adaptive Security Appliance Version 8.4.3
- Cisco Identity Services Engine Version 1.1.

## Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

## RADIUS VSA 3076/150 Client-Type-Attribut

Das Client-Type-Attribut wurde in ASA Version 8.4.3 hinzugefügt. Dadurch kann die ASA den Client-Typ senden, der sich in Access-Request (and Accounting-Request)-Paketen bei der ISE authentifiziert, und die ISE kann Richtlinienentscheidungen basierend auf diesem Attribut treffen. Dieses Attribut erfordert keine Konfiguration auf der ASA und wird automatisch gesendet.

Das Client-Type-Attribut wird derzeit mit den folgenden Integer-Werten definiert:

1. Cisco VPN-Client (Internet Key Exchange Version (IKEv1))
2. SSL VPN des AnyConnect Client
3. Clientless-SSL-VPN
4. Cut-Through-Proxy
5. L2TP/IPsec SSL VPN
6. AnyConnect Client IPsec VPN (IKEv2)

## Konfigurieren

In diesem Abschnitt finden Sie die Informationen, die Sie benötigen, um die ISE für die Verwendung des in diesem Dokument beschriebenen Client-Type-Attributs zu konfigurieren.

### Schritt 1

#### Erstellen des benutzerdefinierten Attributs




Um der ISE die Client-Type-Attributwerte hinzuzufügen, erstellen Sie das Attribut, und füllen Sie seine Werte als benutzerdefiniertes Wörterbuch aus.

1. Navigieren Sie auf der ISE zu **Richtlinien > Richtlinienelemente > Wörterbücher > System**.
2. Navigieren Sie in den **System**-Wörterbüchern zu **RADIUS > RADIUS Vendors > Cisco-VPN3000**.
3. Die Anbieter-ID auf dem Bildschirm sollte 3076 lauten. Klicken Sie auf die Registerkarte **Wörterbuchattribute**. Klicken Sie auf **Hinzufügen** (siehe Abbildung 1). **Abbildung 1: Wörterbuchattribute**

Dictionary

Dictionary Attributes

## Dictionary Attributes

 Add
  Edit
  Delete

<input type="checkbox"/>	Name	Attribute Numb... ▲	Type	Direction
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	1	STRING	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	10	UINT32	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	11	UINT32	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	12	STRING	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	128	IPV4	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	129	IPV4	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	13	UINT32	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	131	IPV4	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	132	UINT32	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	133	STRING	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	134	IPV4	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	135	UINT32	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	136	UINT32	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	137	UINT32	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	15	STRING	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7x-...	150	UINT32	BOTH

Füllen Sie die Felder im benutzerdefinierten RADIUS Vendor Attribute-Formular aus, wie in Abbildung 2 gezeigt. **Abbildung 2: RADIUS-Anbieterattribut**

## ▼ RADIUS Vendor Attribute

\* Attribute Name

Description

\* Internal Name

\* Data Type

\* Direction

\* ID  (0-255)

Does this attribute support Tagging Is this a attribute allowed multiple times in Authz Profile 

## Allowed Values

+ Add - Delete

<input type="checkbox"/>	Name	Value	isDefault
<input type="checkbox"/>	Cisco VPN Client (IKEv1)	1	<input checked="" type="checkbox"/>
<input type="checkbox"/>	AnyConnect Client SSL...	2	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Clientless SSL VPN	3	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Cut-Through-Proxy	4	<input checked="" type="checkbox"/>
<input type="checkbox"/>	L2TP/IPsec SSL VPN	5	<input checked="" type="checkbox"/>
<input type="checkbox"/>	AnyConnect Client IPse...	6	<input checked="" type="checkbox"/>

Klicken Sie am unteren Bildschirmrand auf **Speichern**.

## Schritt 2

### Clienttyp-Attribut hinzufügen

Um das neue Attribut für Richtlinienentscheidungen zu verwenden, fügen Sie das Attribut einer Autorisierungsregel im Abschnitt Bedingungen hinzu.

1. Navigieren Sie in der ISE zu **Richtlinien > Autorisierung**.
2. Erstellen Sie eine neue Regel, oder ändern Sie eine vorhandene Richtlinie.
3. Erweitern Sie im Abschnitt Bedingungen der Regel den Bereich Bedingungen, und wählen Sie entweder **Neue Bedingung erstellen** (für eine neue Regel) oder **Attribut/Wert hinzufügen** (für eine bereits vorhandene Regel) aus.
4. Navigieren Sie im Feld **Attribute auswählen** zu **Cisco-VPN3000 > Cisco-VPN3000:CVPN3000/ASA/PIX7x-Client-Type**.
5. Wählen Sie den entsprechenden Operator (**Equals** oder **Not Equals**) für Ihre Umgebung aus.
6. Wählen Sie den **Authentifizierungstyp aus**, den Sie zuordnen möchten.
7. Zuweisen eines **Autorisierungsergebnisses** entsprechend Ihrer Richtlinie
8. Klicken Sie auf **Fertig**.
9. Klicken Sie auf **Speichern**.

Nach dem Erstellen der Regel sollte die Autorisierungsbedingung dem Beispiel in Abbildung 3 ähneln.

### Abbildung 3: Beispiel für eine Autorisierungsbedingung

```
if Cisco-VPN3000:CVPN3000/ASA/PIX7x-Client-Type EQUALS  
Cut-Through-Proxy
```

## Überprüfen

Um zu überprüfen, ob das Client-Type-Attribut verwendet wird, überprüfen Sie die Authentifizierungen der ASA in der ISE.

1. Navigieren Sie zu **Vorgänge > Authentifizierungen**.
2. Klicken Sie auf die Schaltfläche **Details** für die Authentifizierung von der ASA.
3. Blättern Sie nach unten zu **anderen Attributen**, und suchen Sie nach **CVPN3000/ASA/PIX7x-Client-Type=** (siehe Abbildung 4).

### **Abbildung 4: Weitere Attributdetails**

```
ConfigVersionId=4, DestinationPort=1812, Protocol=Radius, CVPN3000/ASA/PIX7x-Client-  
Type=4, CPMSessionID=0e24970b0000000051000B89, EndPointMACAddress=00-55-44-33-22-11, Device Type=Device  
Type#All Device Types, Location=Location#All Locations, Device IP Address=172.18.254.150
```

4. Das Feld **Andere Attribute** sollte den empfangenen Wert für die Authentifizierung angeben. Die Regel sollte mit der Richtlinie übereinstimmen, die in Schritt 2 des Konfigurationsabschnitts definiert wurde.

## Zugehörige Informationen

- [Cisco Identity Services Engine](#)
- [Cisco Adaptive Security Appliance Firewalls der nächsten Generation der Serie 5500](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)