

Radius- und TACACS-basierte Benutzerauthentifizierung und -autorisierung für vEdge und Controller mit ISE

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Radius-Based User Authentication and Authorization for vEdge and Controllers](#)

[TACACS-basierte Benutzerauthentifizierung und -autorisierung für vEdge und Controller](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird beschrieben, wie RADIUS- und TACACS-basierte Benutzerauthentifizierung und -autorisierung für vEdge und Controller mit Identity Service Engine (ISE) konfiguriert wird.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Für die Demonstration wurde ISE Version 2.6 verwendet. vEdge-Cloud und Controller mit 19.2.1

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Die Viptela-Software enthält drei feste Benutzergruppennamen: **Basic**, **netadmin** und **operator**. Sie müssen den Benutzer mindestens einer Gruppe zuweisen. Der Benutzer Default TACACS/Radius wird automatisch in die Grundgruppe eingefügt.

Radius-Based User Authentication and Authorization for vEdge and Controllers

Schritt 1: Erstellen Sie ein Viptela-Radius-Wörterbuch für die ISE. Erstellen Sie dazu eine Textdatei mit dem Inhalt:

```
# -*- text -*-
#
# dictionary.viptela
#
#
# Version:      $Id$
#
VENDOR          Viptela                      41916

BEGIN-VENDOR    Viptela

ATTRIBUTE       Viptela-Group-Name          1      string
```

Schritt 2: Wörterbuch auf ISE hochladen Navigieren Sie zu **Richtlinien > Richtlinienelemente > Wörterbücher**. Navigieren Sie in der Liste der Wörterbücher zu **Radius > Radius Vendors** und klicken Sie dann auf **Importieren**, wie im Bild gezeigt.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The breadcrumb navigation path is: **Dictionaries > Conditions > Results > Policy Elements > Policy > Administration > Work Centers**. The 'RADIUS Vendors' page is displayed, showing a table of vendors with columns for Name, Vendor ID, and Description. The 'Import' button is highlighted with a red box.

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
H3C	25506	Dictionary for Vendor H3C
HP	11	Dictionary for Vendor HP
Juniper	2636	Dictionary for Vendor Juniper
Microsoft	311	Dictionary for Vendor Microsoft
Motorola-Symbol	388	Dictionary for Vendor Motorola-Symbol
Ruckus	25053	Dictionary for Vendor Ruckus
WISPr	14122	Dictionary for Vendor WISPr

Laden Sie jetzt die Datei hoch, die Sie in Schritt 1 erstellt haben.



Use this for to import a RADIUS Vendor. Select the file using the browser and click "Import".

* Vendor file:
 dictionary.viptela

Schritt 3: Erstellen eines Autorisierungsprofils In diesem Schritt weist das Radius-Autorisierungsprofil einem authentifizierten Benutzer beispielsweise die Ebene der Netadmin-Berechtigungen zu. Navigieren Sie hierzu zu **Richtlinien > Richtlinienelemente > Autorisierungsprofile**, und geben Sie zwei erweiterte Attribute an, wie im Bild gezeigt.

The screenshot shows the configuration page for an Authorization Profile named 'vEdge-netadmin'. The 'Advanced Attributes Settings' section is expanded, showing two attribute mappings:

- Radius:Service-Type = NAS Prompt
- Viptela:Viptela-Group-Name = netadmin

The 'Attributes Details' section shows the following values:

- Access Type = ACCESS_ACCEPT
- Service-Type = 7
- Viptela-Group-Name = netadmin

The 'Save' button is highlighted with a red box.

Schritt 4: Abhängig von Ihrer tatsächlichen Einrichtung sieht Ihr Richtlinienatz möglicherweise anders aus. Für die Demonstration in diesem Artikel wird der Richtlinieneneintrag "Terminalzugriff" wie im Bild gezeigt erstellt.

The screenshot shows the 'Policy Sets' table with the following data:

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Terminal Access						
	Radius-NAS-Port-Type EQUALS Virtual						
	Default Network Access				2		

The 'Terminal Access' policy set and the 'Default Network Access' policy set are highlighted with red boxes. A red arrow points to the right-pointing chevron icon next to the 'Default Network Access' policy set.

Klicken Sie > und der nächste Bildschirm wird angezeigt, wie im Bild gezeigt.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Policy Sets → Terminal Access Reset Pollicyset Hitcounts Reset Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Terminal Access		Radius-NAS-Port-Type EQUALS Virtual	Default Network Access * +	2

> Authentication Policy (1)
 > Authorization Policy - Local Exceptions
 > Authorization Policy - Global Exceptions
 ▼ Authorization Policy (2)

+	Status	Rule Name	Conditions	Results		Hits	Actions
				Profiles	Security Groups		
⋮	✓	vEdge-netadmin	IdentityGroup-Name EQUALS User Identity Groups:lab_admin	*vEdge-netadmin +	Select from list +	1	⚙️
	✓	Default		*DenyAccess +	Select from list +	0	⚙️

Reset Save

Diese Richtlinie stimmt mit der Benutzergruppe "lab_admin" überein und weist ein in Schritt 3 erstelltes Autorisierungsprofil zu.

Schritt 5: Definieren Sie NAS (vEdge-Router oder Controller), wie im Image gezeigt.

Identity Services Engine Administration Work Centers

System Identity Management **Network Resources** Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network Devices

Default Device

Device Security Settings

Network Devices List > vEdge-01

Network Devices

* Name

Description

IP Address * IP: /

* Device Profile

Model Name

Software Version

* Network Device Group

Location

IPSEC

Device Type

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

* Shared Secret

Use Second Shared Secret

CoA Port

RADIUS DTLS Settings

DTLS Required

Shared Secret

CoA Port

Issuer CA of ISE Certificates for CoA

DNS Name

General Settings

Enable KeyWrap

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ASCII HEXADECIMAL

Schritt 6: Konfigurieren Sie vEdge/Controller.

```

system
aaa
  auth-order      radius local
  radius
  server 10.48.87.210
    vpn 512
    key cisco
  exit
!
!

```

Schritt 7: Überprüfung. Melden Sie sich bei vEdge an, und stellen Sie sicher, dass dem Remote-Benutzer die Netadmin-Gruppe zugewiesen ist.

```
vEdgeCloud1# show users
```

SESSION	USER	CONTEXT	FROM	PROTO	AUTH GROUP	LOGIN TIME
33472	ekhabaro	cli	10.149.4.155	ssh	netadmin	2020-03-09T18:39:40+00:00

TACACS-basierte Benutzerauthentifizierung und -autorisierung für vEdge und Controller

Schritt 1: Erstellen Sie ein TACACS-Profil. In diesem Schritt wird das erstellte TACACS-Profil einem authentifizierten Benutzer zugewiesen, z. B. der Ebene der Netadmin-Berechtigungen.

- Wählen Sie **Obligatorisch** im **Custom-Attribut**-Abschnitt aus, um das Attribut wie folgt hinzuzufügen:

Typ	Name	Wert
Obligatorisch	Viptela-Gruppenname	netadmin

The screenshot displays the Cisco ISE configuration page for a TACACS profile. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > PassivelD > Policy Elements. The left sidebar shows 'TACACS Profiles' selected. The main content area is titled 'TACACS Profile' and includes a 'Name' field with the value 'vEdge_netadmin'. Below this is a 'Description' field. The 'Common Tasks' section has a 'Common Task Type' dropdown set to 'Shell'. A list of task attributes includes 'Default Privilege', 'Maximum Privilege', 'Access Control List', 'Auto Command', 'No Escape', 'Timeout', and 'Idle Time', each with a dropdown menu. The 'Custom Attributes' section contains a table with one entry: 'Mandatory' (checkbox checked), 'Viptela-Group-Name', and 'netadmin'. At the bottom right, there are 'Cancel' and 'Save' buttons.

Schritt 2: Erstellen Sie eine Gerätegruppe für SD-WAN.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network Device Groups

All Groups Choose group ▾

Refresh + Add Duplicate Edit Trash Show group members Import Export Flat Table Expand All Collapse All

Name	Description	No. of Network Devices
▾ All Device Types	All Device Types	--
<input checked="" type="checkbox"/> SD-WAN		0
<input type="checkbox"/> All Locations	All Locations	--
<input type="checkbox"/> ▸ Is IPSEC Device	Is this a RADIUS over IPSEC Device	--

Add Group



Name *

SD-WAN

Description

Parent Group *

All Device Types



Cancel

Save

Schritt 3: Konfigurieren Sie das Gerät, und weisen Sie es der SD-WAN-Gerätegruppe zu:

Network Devices

* Name

Description

IP Address * IP : /

* Device Profile

Model Name

Software Version

* Network Device Group

Location

IPSEC

Device Type

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret ⓘ

Enable Single Connect Mode

Legacy Cisco Device

TACACS Draft Compliance Single Connect Support

SNMP Settings

Advanced TrustSec Settings

Schritt 4: Definieren Sie die Gerätemanagement-Richtlinie.

Abhängig von Ihrer tatsächlichen Einrichtung sieht Ihr Richtliniensatz möglicherweise anders aus. Für die Demonstration in diesem Dokument wird die Richtlinie erstellt.

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

Network Access > Guest Access > TrustSec > BYOD > Profiler > Posture > Device Administration > PassiveID

Overview > Identities > User Identity Groups > Ext Id Sources > Network Resources > Policy Elements > Device Admin Policy Sets > Reports > Settings

Policy Sets

+	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
<input type="checkbox"/>	<input checked="" type="checkbox"/>	vEdges		DEVICE Device Type EQUALS All Device Types#SD-WAN	Default Device Admin		<input type="button" value="Settings"/> <input checked="" type="button" value="View"/>	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Default	Tacacs Default policy set		Default Device Admin	0	<input type="button" value="Settings"/> <input type="button" value="View"/>	

Klicken Sie auf > und der nächste Bildschirm wird angezeigt, wie in diesem Bild gezeigt. Diese Richtlinie stimmt mit dem Gerätetyp **SD-WAN** überein und weist dem in Schritt 1 erstellten Shell-Profil das entsprechende Shell-Profil zu.

The screenshot shows the Cisco ISE web interface for configuring Policy Sets for vEdges. The main configuration area is titled 'Policy Sets → vEdges'. A table lists the policy sets, with 'vEdges' selected. Below this, a detailed view of the 'vEdge-netadmin' rule is shown, with red boxes highlighting the rule name, the condition 'IdentityGroup-Name EQUALS User Identity Groups:lab_admin', and the result 'vEdge_netadmin'. The interface also includes buttons for 'Reset Policyset Hitcounts', 'Reset', and 'Save'.

Schritt 5: Konfigurieren Sie vEdge:

```

system
aaa
  auth-order tacacs local
!
tacacs
  server 10.48.87.210
  vpn 512
  key cisco
  exit
!
!

```

Schritt 6: Überprüfung. Melden Sie sich bei vEdge an, und stellen Sie sicher, dass der Remote-Benutzer zugewiesene Netadmin-Gruppe:

vEdgeCloud1# show users

SESSION	USER	CONTEXT	FROM	PROTO	AUTH GROUP	LOGIN TIME
33472	ekhabaro	cli	10.149.4.155	ssh	netadmin	2020-03-09T18:39:40+00:00

Schritt 5: Konfigurieren Sie vEdge:

Schritt 5: Konfigurieren Sie vEdge:

Schritt 5: Konfigurieren Sie vEdge:

Zugehörige Informationen

- Cisco ISE Device Administration-Prescriptive Deployment-Guide: <https://community.cisco.com/t5/security-documents/cisco-ise-device-administration-prescriptive-deployment-guide/ta-p/3738365#toc-hId-298630973>
- Konfigurieren von Benutzerzugriff und Authentifizierung: https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.4/02System_and_Interfaces/03Configuring_User_Access_and_Authentication