

Konfigurieren der ISE als externe Authentifizierung für die Catalyst SD-WAN-GUI

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Vorbereitungen](#)

[Konfigurieren - Verwenden von TACACS+](#)

[Konfigurieren von Catalyst SD-WAN mithilfe von TACACS+](#)

[Konfigurieren von ISE für TACACS+](#)

[Überprüfen der TACACS+-Konfiguration](#)

[Fehlerbehebung](#)

[Referenzen](#)

Einleitung

In diesem Dokument wird beschrieben, wie die Cisco Identity Services Engine (ISE) als externe Authentifizierung für die GUI-Administration der Cisco Catalyst SD-WAN konfiguriert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in den folgenden Bereichen verfügen:

- TACACS+-Protokoll
- Geräteverwaltung mit der Cisco ISE
- Cisco Catalyst SD-WAN-Verwaltung
- Cisco ISE-Richtlinienbewertung

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Identity Services Engine (ISE) Version 3.4 Patch 2
- Cisco Catalyst SD-WAN Version 20.15.3

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 kennen.

Vorbereitungen

Ab Cisco vManage Version 20.9.1 werden bei der Authentifizierung neue Tags verwendet:

- VipTela-Benutzergruppe: für Benutzergruppensdefinitionen anstelle von Viptela-Group-Name.
- Viptela-Ressourcengruppe: für Ressourcengruppen-Definitionen.

Konfigurieren - Verwenden von TACACS+

Konfigurieren von Catalyst SD-WAN mithilfe von TACACS+

Vorgehensweise

Schritt 1. (Optional) Benutzerdefinierte Rollen definieren.

Konfigurieren Sie die benutzerdefinierten Rollen, die Ihren Anforderungen entsprechen. Stattdessen können Sie die Standardbenutzerrollen verwenden. Dies ist über die Registerkarte Catalyst SD-WAN möglich: Administration > Benutzer und Zugriff > Rollen.

Erstellen Sie zwei benutzerdefinierte Rollen:

1. Administratorrolle: Superadministrator
2. Schreibgeschützte Rolle: schreibgeschützt

Dies ist über die Registerkarte Catalyst SD-WAN möglich: Administration > Benutzer und Zugriff > Rollen > klicken Sie auf > Rolle hinzufügen.

Add Custom Role



Custom Role Name

super-admin

Description (optional)

Range 1 - 32

Maximum character 100

Q Search Table

Feature	Deny	Read	Write
Alarms	☐	☐	☒
Application Monitoring	☐	☐	☒
Audit Log	☐	☐	☒
> Certificates (2)	☐	☐	☒
Cloud onRamp	☐	☐	☒
Cluster	☐	☐	☒
Colocation	☐	☐	☒
> Config Group (1)	☐	☐	☒
Cortex	☐	☐	☒
> Device Inventory (2)	☐	☐	☒
Device Monitoring	☐	☐	☒
> Device Reboot (2)	☐	☐	☒
Disaster Recovery	☐	☐	☒
Events	☐	☐	☒
> Feature Profile (28)	☐	☐	☒
Integration Management	☐	☐	☒
Interface	☐	☐	☒

Cancel Add

Administratorrolle (Super-Admin)

Add Custom Role



Custom Role Name

readonly

Range 1 - 32

Description (optional)

Maximum character 100

Q Search Table

Feature	Deny	Read	Write
Alarms	☐	☒	☐
Application Monitoring	☐	☒	☐
Audit Log	☐	☒	☐
> Certificates (2)	☐	☒	☐
Cloud onRamp	☐	☒	☐
Cluster	☐	☒	☐
Colocation	☐	☒	☐
> Config Group (1)	☐	☒	☐
Cortex	☐	☒	☐
> Device Inventory (2)	☐	☒	☐
Device Monitoring	☐	☒	☐
> Device Reboot (2)	☐	☒	☐
Disaster Recovery	☐	☒	☐
Events	☐	☒	☐
> Feature Profile (28)	☐	☒	☐
Integration Management	☐	☒	☐
Interface	☐	☒	☐

Cancel

Add

Schreibgeschützte Rolle (schreibgeschützt)

Schritt 2: Konfigurieren der externen Authentifizierung mithilfe von TACACS+ (CLI)

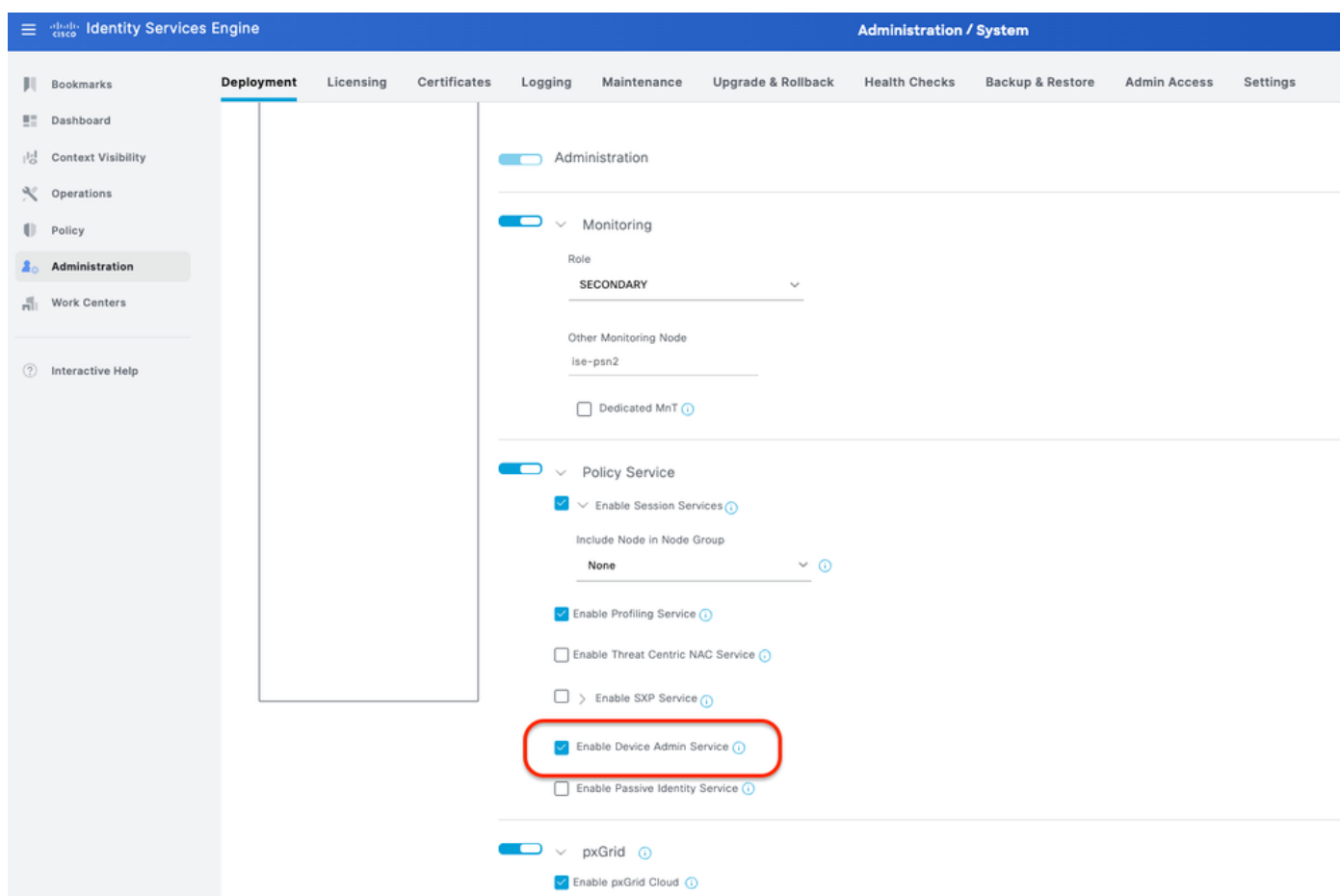
```
Entering configuration mode terminal
vmanage(config)#
vmanage(config)#
vmanage(config)# system
vmanage(config-system)# aaa
vmanage(config-aaa)# auth-order tacacs radius local
vmanage(config-aaa)# auth-fallback
vmanage(config-aaa)# commit and-quit
Commit complete.
```

vManger-CLI - TACACS+-Konfiguration

Konfigurieren von ISE für TACACS+

Schritt 1: Aktivieren Sie den Geräteverwaltungsdienst.

Dies kann über die Registerkarte Administration > System > Deployment > Edit (ISE PSN Node)>Enable Device Admin Service erfolgen.



Geräteverwaltungsdienst aktivieren

Schritt 2: Hinzufügen eines Catalyst SD-WAN als Netzwerkgerät zur ISE

Dies kann über die Registerkarte Administration > Network Resources > Network Devices

(Verwaltung > Netzwerkressourcen > Netzwerkgeräte) erfolgen.

Vorgehensweise

antwort: Definieren Sie den Namen und die IP des Netzwerkgeräts (Catalyst SD-WAN).

b. (Optional) Klassifizieren Sie den Gerätetyp für den Zustand "Policy Set".

c. Aktivieren Sie die TACACS+-Authentifizierungseinstellungen.

d. Festlegen des gemeinsamen TACACS+-Schlüssels.

ISE-Netzwerkgerät (Catalyst SD-WAN) für TACACS+

Schritt 3: Erstellen Sie für jede Catalyst SD-WAN-Rolle ein TACACS+-Profil.

Erstellen von TACACS+-Profilen:

1. Catalyst SDWAN-Administrator: Für Super-Admin-Benutzer.
2. Catalyst_SDWAN_Schreibgeschützt: Für schreibgeschützte Benutzer.

Dies kann über die Registerkarte Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles > Add erfolgen.

Identity Services Engine

Work Centers / Device Administration

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Help

Overview

Identities

User Identity Groups

Ext Id Sources

Network Resources

Policy Elements

Device Admin Policy Sets

Reports

Settings

Conditions

Network Conditions

Results

Allowed Protocols

TACACS Command Sets

TACACS Profiles

TACACS Profiles > Catalyst_SDWAN_Admin

TACACS Profile

Name

Catalyst_SDWAN_Admin

Description

Task Attribute View

Raw View

Common Tasks

Common Task Type

Shell

☐

Default Privilege

(Select 0 to 15)

☐

Maximum Privilege

(Select 0 to 15)

☐

Access Control List

☐

Auto Command

☐

No Escape

(Select true or false)

☐

Timeout

Minutes (0-9999)

☐

Idle Time

Minutes (0-9999)

Custom Attributes

Add

Trash

Edit

☐

Type

Name

Value

Mandatory

Viptela-User-Group

super-admin

✓

✕

Cancel

Save

TACACS+-Profil - (Catalyst_SDWAN_Admin)

Identity Services Engine Work Centers / Device Administration

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

Bookmarks Dashboard Context Visibility Operations Policy Administration **Work Centers** Interactive Help

Conditions > Network Conditions > Results > TACACS Profiles

TACACS Profiles > Catalyst_SDWAN_ReadOnly
TACACS Profile

Name: Catalyst_SDWAN_ReadOnly

Description:

Task Attribute View Raw View

Common Tasks

Common Task Type: Shell

☐ Default Privilege (Select 0 to 15)
☐ Maximum Privilege (Select 0 to 15)
☐ Access Control List
☐ Auto Command
☐ No Escape (Select true or false)
☐ Timeout (Minutes (0-9999))
☐ Idle Time (Minutes (0-9999))

Custom Attributes

Type	Name	Value
Mandatory	Viptela-User-Group	readonly

Cancel Save

TACACS+-Profil - (Catalyst_SDWAN_ReadOnly)

Schritt 4: Erstellen einer Benutzergruppe Hinzufügen lokaler Benutzer als Mitglied

Dies kann über die Registerkarte Work Centers > Device Administration > User Identity Groups (Arbeitszentren > Geräteverwaltung > Benutzeridentitätsgruppen) erfolgen.

Erstellen Sie zwei Benutzeridentitätsgruppen:

1. Super_Admin_Gruppe
2. Schreibgeschützte Gruppe

Identity Services Engine Administration / Identity Management

Identities **Groups** External Identity Sources Identity Source Sequences Settings

Identity Groups

User Identity Groups > Super_Admin_Group

Identity Group

* Name Super_Admin_Group

Description Catalyst SD-WAN Role (super-admin)

Member Users

Users

+ Add - Delete

Status	Email	Username	First Name	Last Name
☐	Enabled	super_user		

Benutzeridentitätsgruppe - (Super_Admin_Group)

Identity Services Engine Administration / Identity Management

Identities **Groups** External Identity Sources Identity Source Sequences Settings

Identity Groups

User Identity Groups > ReadOnly_Group

Identity Group

* Name ReadOnly_Group

Description Catalyst SD-WAN Role (readonly)

Member Users

Users

+ Add - Delete

Status	Email	Username	First Name	Last Name
☐	Enabled	readonly_user		

Benutzeridentitätsgruppe - (ReadOnly_Group)

Schritt 5: Fügen Sie optional den TACACS+-Richtliniensatz hinzu.

Dies kann über die Registerkarte Work Centers > Device Administration > Device Admin Policy Sets erfolgen.

Vorgehensweise

antwort: Klicken Sie auf Aktionen, und wählen Sie (Neue Zeile oben einfügen).

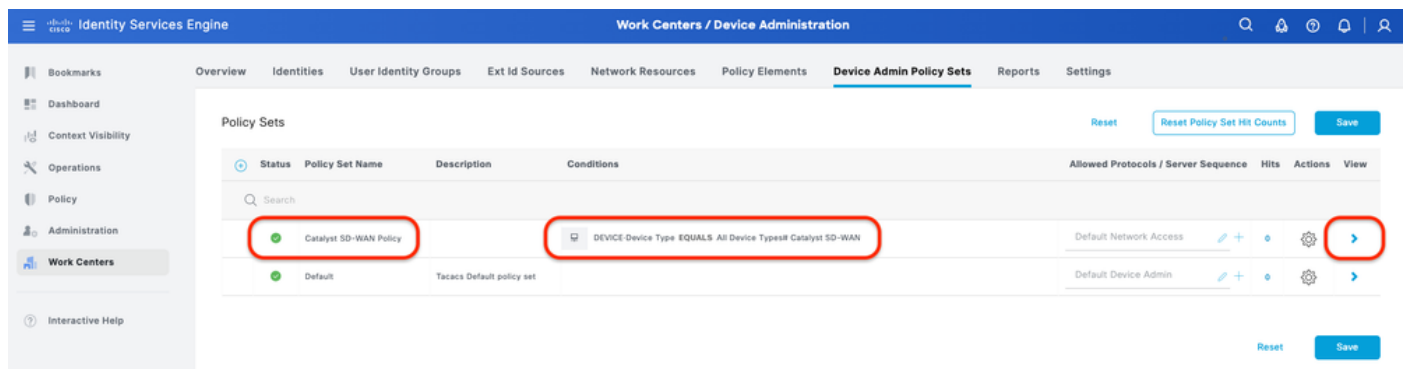
b. Definieren Sie den Namen des Richtlinienatzes.

c. Setzen Sie die Policy Set Condition auf Select Device Type (Gerätetyp auswählen), den Sie zuvor erstellt haben (Schritt 2 > b).

d. Legen Sie die zulässigen Protokolle fest.

e. Klicken Sie auf Speichern.

f. Klicken Sie auf (>) Policy Set View (Richtliniensatzansicht), um Authentifizierungs- und Autorisierungsregeln zu konfigurieren.



ISE-Richtliniensatz

Schritt 6: Konfigurieren der TACACS+-Authentifizierungsrichtlinie

Dies kann über die Registerkarte Work Centers > Device Administration > Device Admin Policy Sets > Click (>) (Work Centers > Geräteverwaltung > Gerätemanagement-Richtliniensätze) erfolgen.

Vorgehensweise

antwort: Klicken Sie auf Aktionen, und wählen Sie (Neue Zeile oben einfügen).

b. Definieren Sie den Namen der Authentifizierungsrichtlinie.

c. Legen Sie die Bedingung für die Authentifizierungsrichtlinie fest und wählen Sie den Gerätetyp aus, den Sie zuvor erstellt haben (Schritt 2 > b).

d. Legen Sie die Authentifizierungsrichtlinie Use for Identity source fest.

e. Klicken Sie auf Speichern.

The screenshot shows the Cisco ISE Work Centers / Device Administration interface. The 'Device Admin Policy Sets' tab is active. A table lists policy sets, with 'Catalyst SD-WAN Policy' selected. Below it, the 'Authentication Policy(2)' section shows a table with two rows: 'Catalyst SD-WAN Auth' and 'Default'. The 'Catalyst SD-WAN Auth' row is highlighted with a red box. To the right of this row, the 'Internal Users' dropdown menu is open, also highlighted with a red box, showing 'Options'.

Authentifizierungsrichtlinie

Schritt 7: Konfigurieren der TACACS+-Autorisierungsrichtlinie

Dies kann über die Registerkarte Work Centers > Device Administration > Device Admin Policy Sets > Click (>) (Work Center > Geräteverwaltung > Device Admin Policy Sets > Klicken Sie auf (>) erfolgen.

In diesem Schritt werden Autorisierungsrichtlinien für jede Catalyst SD-WAN-Rolle erstellt:

- Catalyst SD-WAN-Authentifizierung (Superadministrator): Superadministrator
- Catalyst SD-WAN-Authentifizierung (schreibgeschützt): schreibgeschützt

Vorgehensweise

antwort: Klicken Sie auf Aktionen, und wählen Sie (Neue Zeile oben einfügen).

b. Definieren Sie den Namen der Autorisierungsrichtlinie.

c. Legen Sie die Autorisierungsrichtlinienbedingung fest und wählen Sie die Benutzergruppe aus, die Sie in (Schritt 4) erstellt haben.

d. Legen Sie die AutorisierungsrichtlinienShell-Profil fest, und wählen Sie das TACACS-Profil aus, das Sie in (Schritt 3) erstellt haben.

e. Klicken Sie auf Speichern.

Identity Services Engine Work Centers / Device Administration

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

Policy Sets - Catalyst SD-WAN Policy

Reset Reset Policy Set Hit Counts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
●	Catalyst SD-WAN Policy		DEVICE Device Type EQUALS All Device Types Catalyst SD-WAN	Default Network Access	0

> Authentication Policy(2)
 > Authorization Policy - Local Exceptions
 > Authorization Policy - Global Exceptions
 < Authorization Policy(3)

Status	Rule Name	Conditions	Results			Hits	Actions
			Command Sets	Shell Profiles			
●	Catalyst SD-WAN Authz (super-admin)	InternalUser IdentityGroup EQUALS User Identity Groups:Super_Admin_Group	Select from list	Catalyst_SDWAN_Admin	0		
●	Catalyst SD-WAN Authz (readonly)	InternalUser IdentityGroup EQUALS User Identity Groups:ReadOnly_Group	Select from list	Catalyst_SDWAN_ReadOnly	0		
●	Default		DenyAllCommands	Deny All Shell Profile	0		

Reset Save

Autorisierungsrichtlinie

Überprüfen der TACACS+-Konfiguration

1- Anzeigen von Catalyst SD-WAS-Benutzersitzungen Catalyst SD-WAN: Administration > Users und Access > User Sessions (Verwaltung > Benutzer und Zugriff > Benutzersitzungen).

Sie können die Liste der externen Benutzer anzeigen, die sich zum ersten Mal über RADIUS angemeldet haben. Zu den angezeigten Informationen gehören die Benutzernamen und Rollen.

Catalyst SD-WAN

Users and Access

Scope Roles Users **User Sessions**

User Sessions (2)

Search Table

0 selected Remove Session

	User Name	UUID	Source Ip	Remote Host	Tenant Domain	Tenant UUID	Raw Username	User Mode	Role	Creation Date	Last Accessed Time
☐	super_user			127.0.0.1		default	super_user	tenant	super-admin	Sep 11, 2025, 1:29:13 PM	Sep 11, 2025, 1:29:16 PM
☐	readonly_user			127.0.0.1		default	readonly_user	tenant	readonly	Sep 11, 2025, 1:22:52 PM	Sep 11, 2025, 1:24:52 PM

Items per page: 10 1 - 2 of 2 < > >>

Catalyst SD-WAAS-Benutzersitzungen

2- ISE - TACACS Live-Logs Operations > TACACS > Live-Logs.

Identity Services Engine

Operations / TACACS

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Help

Live Logs

Export To

Refresh Never

Show Latest 20 records

Within Last 5 minutes

Filter

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Shell Profile	Device Type
X			Identity	Type	Authentication Policy	Authorization Policy	Shell Profile	Device Type
Sep 11, 2025 01:36:2...			readonly_user	Authorization		Catalyst SD-WAN Policy >> Catalyst SD-WAN Authz (reado...	Catalyst_SDWAN_ReadOnly	Device Type#
Sep 11, 2025 01:36:2...			readonly_user	Authentication	Catalyst SD-WAN Policy >> Catalyst SD-WAN Auth			Device Type#
Sep 11, 2025 01:33:0...			super_user	Authorization		Catalyst SD-WAN Policy >> Catalyst SD-WAN Authz (super...	Catalyst_SDWAN_Admin	Device Type#
Sep 11, 2025 01:33:0...			super_user	Authentication	Catalyst SD-WAN Policy >> Catalyst SD-WAN Auth			Device Type#

Last Updated: Thu Sep 11 2025 13:33:45 GMT+0200 (Central European Summer Time)Records Shown: 4

Live-Protokolle

Protocol	Tacacs
Type	Authorization
Service-Argument	ppp
Protocol-Argument	ip
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
AuthenticationIdentityStore	Internal Users
AuthenticationMethod	Lookup
SelectedAccessService	Default Network Access
RequestLatency	27
IdentityGroup	User Identity Groups:ReadOnly_Group
SelectedAuthenticationIdentityStores	Internal Users
AuthenticationStatus	AuthenticationPassed
UserType	User
CPMSessionID	316584755210.127.198.7438561Authorization3165847552
IdentitySelectionMatchedRule	Catalyst SD-WAN Auth
StepLatency	1=0;2=0;3=4;4=3;5=4;6=0;7=2;8=1;9=0;10=8;11=2;12=3;13=0;14=0;15=0
TotalAuthenLatency	27
ClientLatency	0
TacacsPlusTLS	false
Network Device Profile	Cisco
IPSEC	IPSEC#Is IPSEC Device#No
EnableFlag	Enabled
Response	{Author-Reply-Status=PassAdd; AVPair=Viptela-User-Group=readonly; }

Detaillierte Live-Protokolle - (schreibgeschützt)

Protocol	Tacacs
Type	Authorization
Service-Argument	ppp
Protocol-Argument	ip
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
AuthenticationIdentityStore	Internal Users
AuthenticationMethod	Lookup
SelectedAccessService	Default Network Access
RequestLatency	30
IdentityGroup	User Identity Groups:Super_Admin_Group
SelectedAuthenticationIdentityStores	Internal Users
AuthenticationStatus	AuthenticationPassed
UserType	User
CPMSessionID	354536652810.127.198.7460535Authorization3545366528
IdentitySelectionMatchedRule	Catalyst SD-WAN Auth
StepLatency	1=1;2=0;3=3;4=3;5=3;6=0;7=2;8=0;9=0;10=10;11=4;12=4;13=0;14=1;15=0
TotalAuthenLatency	30
ClientLatency	0
TacacsPlusTLS	false
Network Device Profile	Cisco
IPSEC	IPSEC#Is IPSEC Device#No
EnableFlag	Enabled
Response	{Author-Reply-Status=PassAdd; AVPair=Viptela-User-Group=super-admin; }

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Diagnoseinformationen verfügbar.

Referenzen

- [Administratorleitfaden für die Cisco Identity Services Engine, Version 3.4](#)
- [Konfigurationsleitfaden für Cisco Catalyst SD-WAN-Systeme und -Schnittstellen, Cisco IOS XE Catalyst SD-WAN Version 17.x](#)

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.