

Konfigurieren der externen RADIUS-Authentifizierung für DNA Center und ISE 3.1

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Überprüfung](#)

[Weitere Rollen](#)

Einleitung

In diesem Dokument wird die Konfiguration der externen RADIUS-Authentifizierung auf dem Cisco DNA Center mit einem Cisco ISE-Server mit Version 3.1 beschrieben.

Voraussetzungen

Anforderungen

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

- Cisco DNA Center und Cisco ISE sind bereits integriert, und die Integration hat den Status "Aktiv".

Verwendete Komponenten

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

- Cisco DNA Center Version 2.3.5.x
- Cisco ISE Version 3.1

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.

Konfigurieren

Schritt 1: Melden Sie sich bei der Cisco DNA Center-GUI an, und navigieren Sie zu System >

Settings > Authentication and Policy Servers.

Überprüfen Sie, ob das RADIUS-Protokoll konfiguriert ist und der ISE-Status für den ISE-Typ-Server Aktiv ist.

Settings / External Services

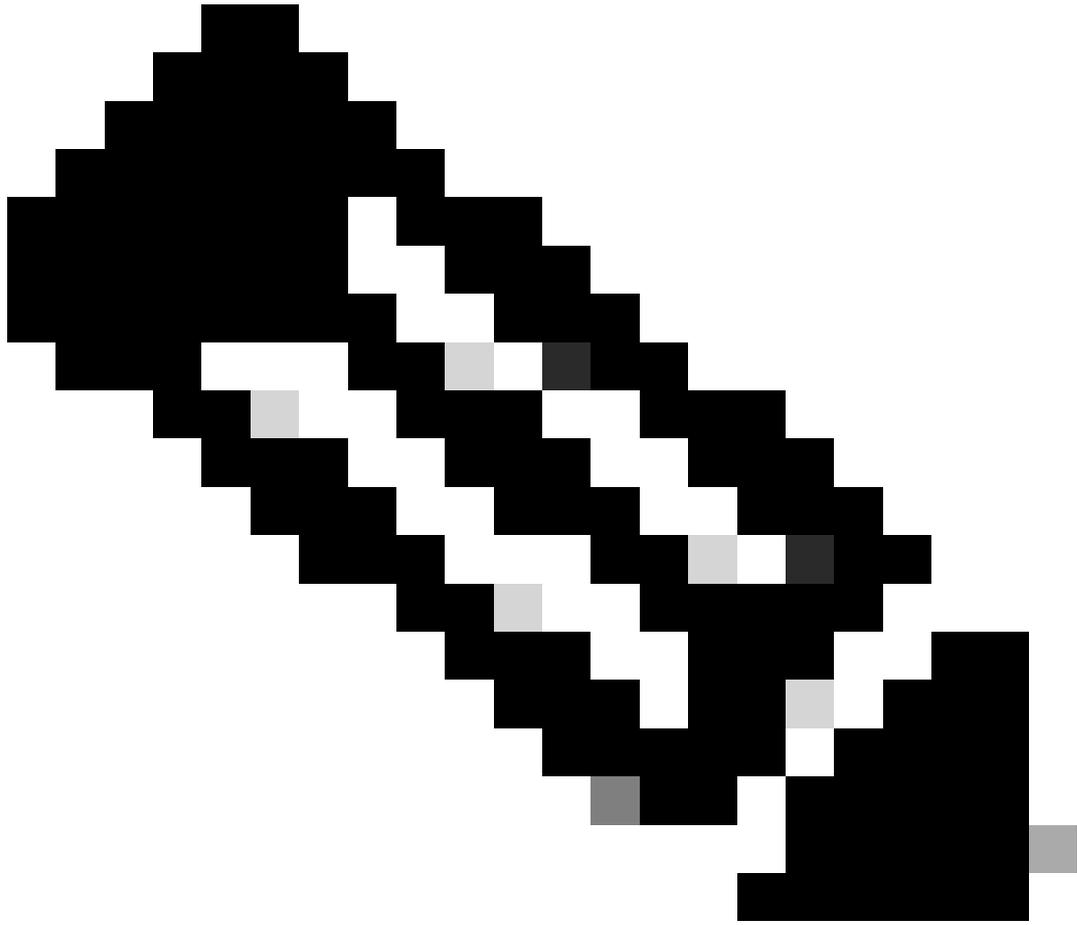
Authentication and Policy Servers

Use this form to specify the servers that authenticate Cisco DNA Center users. Cisco Identity Services Engine (ISE) servers can also supply policy and user information.

[Add](#) [Export](#)

As of: Jul 19, 2023 4:38 PM [Refresh](#)

IP Address	Protocol	Type	Status	Actions
[REDACTED]	RADIUS_TACACS	AAA	ACTIVE	...
[REDACTED]	RADIUS	ISE	ACTIVE	...
[REDACTED]	RADIUS	AAA	ACTIVE	...
[REDACTED]	RADIUS	AAA	ACTIVE	...
[REDACTED]	RADIUS_TACACS	AAA	ACTIVE	...



Hinweis: Der Protokolltyp RADIUS_TACACS funktioniert für dieses Dokument.



Warnung: Wenn sich der ISE-Server nicht im aktiven Status befindet, müssen Sie zuerst die Integration reparieren.

Schritt 2: Navigieren Sie auf dem ISE-Server zu Administration > Network Resources > Network Devices, klicken Sie auf das Filter-Symbol, schreiben Sie die Cisco DNA Center-IP-Adresse, und bestätigen Sie, ob ein Eintrag vorhanden ist. Wenn dies der Fall ist, fahren Sie mit Schritt 3 fort.

Wenn der Eintrag fehlt, muss die Meldung Keine Daten verfügbar angezeigt werden.

Network Devices

Selected 0 Total 0  

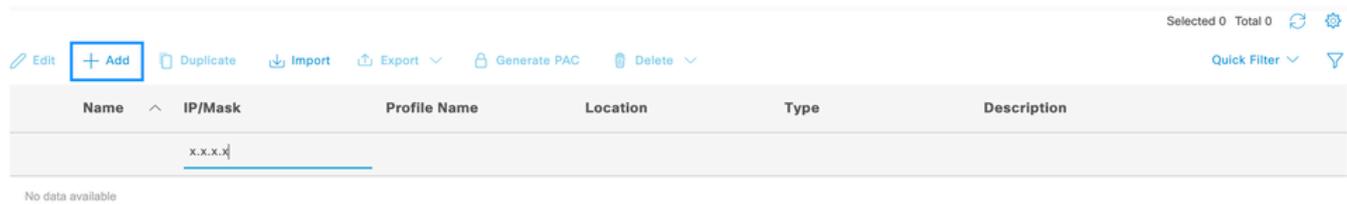
 Edit  Add  Duplicate  Import  Export  Generate PAC  Delete  Quick Filter 

Name	IP/Mask	Profile Name	Location	Type	Description
	x.x.x.x				

No data available

In diesem Fall müssen Sie ein Netzwerkgerät für Cisco DNA Center erstellen. Klicken Sie dazu auf die Schaltfläche Hinzufügen.

Network Devices



Name	IP/Mask	Profile Name	Location	Type	Description
	x.x.x.x				

No data available

Konfigurieren Sie den Namen, die Beschreibung und die IP-Adresse (oder die Adressen) von Cisco DNA Center. Alle anderen Einstellungen sind auf Standardwerte festgelegt und werden für die Zwecke dieses Dokuments nicht benötigt.

Network Devices

* Name

Description

IP Address

* Device Profile

Model Name

Software Version

* Network Device Group

Location	<input type="text" value="All Locations"/>	<input type="button" value="Set To Default"/>
IPSEC	<input type="text" value="Is IPSEC Device"/>	<input type="button" value="Set To Default"/>
Device Type	<input type="text" value="All Device Types"/>	<input type="button" value="Set To Default"/>

Blättern Sie nach unten, und aktivieren Sie die RADIUS-Authentifizierungseinstellungen, indem Sie auf das entsprechende Kontrollkästchen klicken und einen gemeinsamen geheimen Schlüssel konfigurieren.



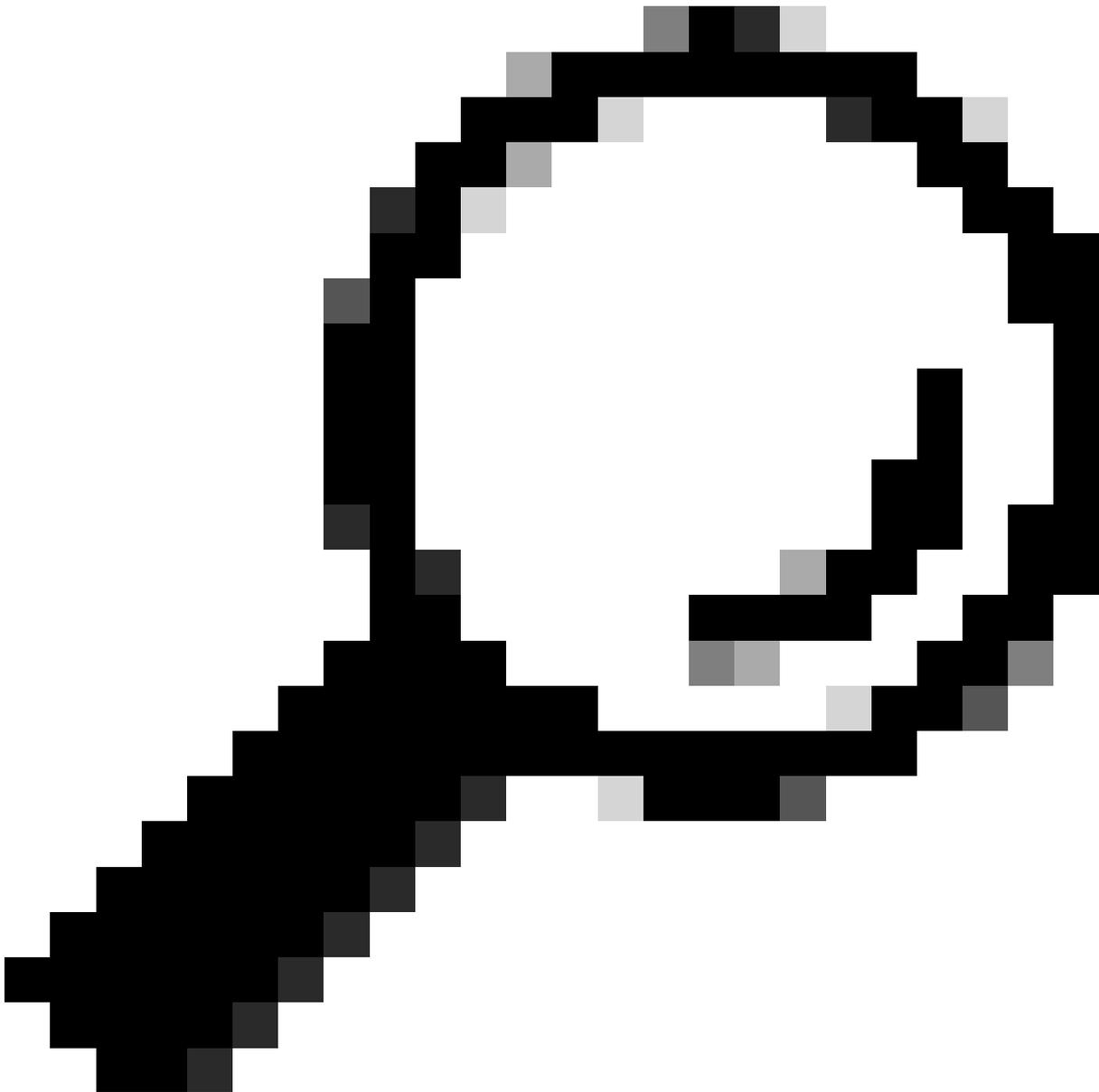
✓ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

* Shared Secret

Show

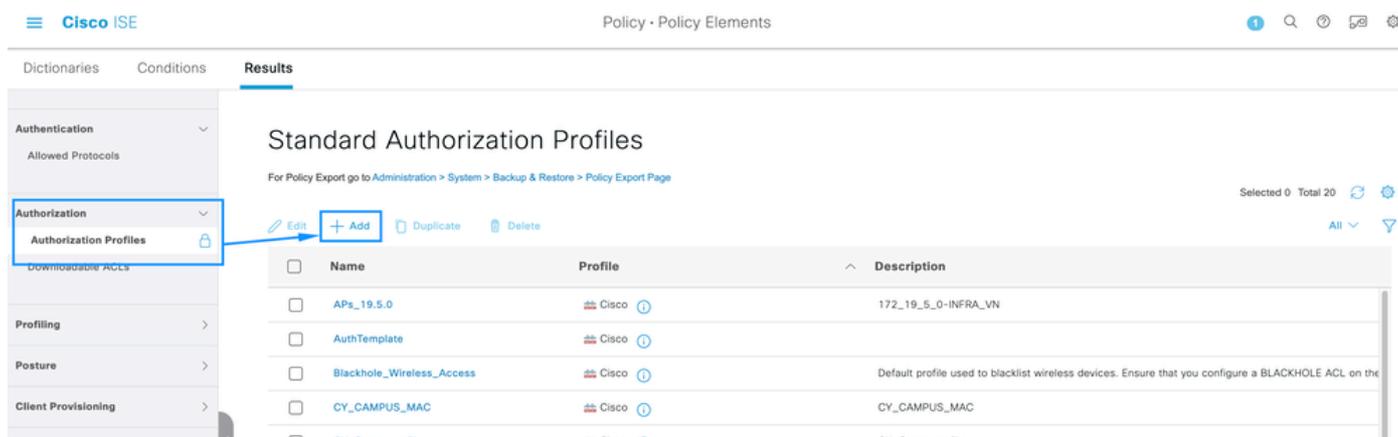


Tipp: Dieser gemeinsame geheime Schlüssel wird zu einem späteren Zeitpunkt benötigt. Speichern Sie ihn also an einer anderen Stelle.

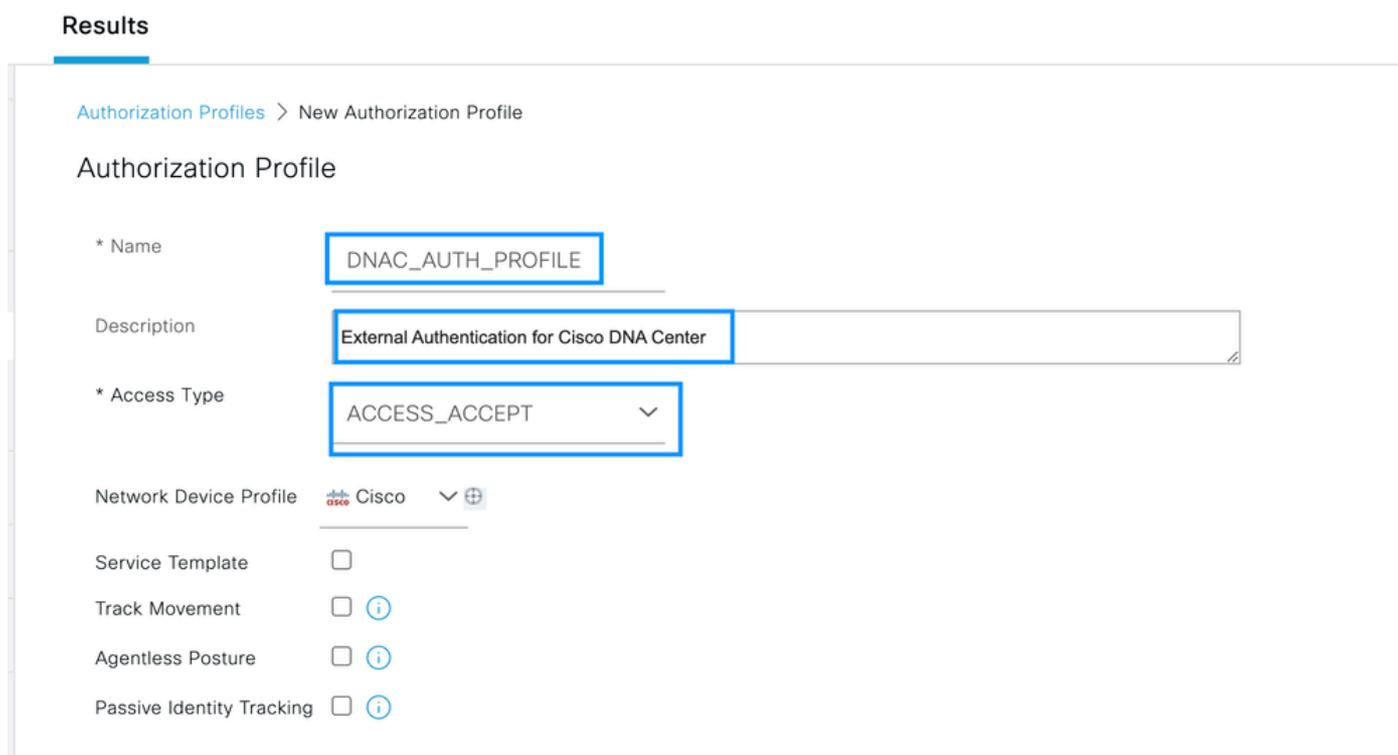
Klicken Sie dann auf Senden.

Schritt 3: Navigieren Sie auf dem ISE-Server zu Policy > Policy Elements > Results (Richtlinie > Richtlinien-elemente > Ergebnisse), um das Autorisierungsprofil zu erstellen.

Vergewissern Sie sich, dass Sie unter Autorisierung > Autorisierungsprofile sind, und wählen Sie dann die Option Hinzufügen aus.



Name konfigurieren, eine Beschreibung hinzufügen, nur um das neue Profil zu speichern und sicherzustellen, dass der Zugriffstyp auf ACCES_ACCEPT gesetzt ist.



Blättern Sie nach unten, und konfigurieren Sie die erweiterten Attributeinstellungen.

Suchen Sie in der linken Spalte nach der Option cisco-av-pair, und wählen Sie sie aus.

Geben Sie in der rechten Spalte manuell Role=SUPER-ADMIN-ROLE ein.

Sobald es wie das Bild unten aussieht, klicken Sie auf Senden.

Advanced Attributes Settings

☰ Cisco:cisco-av-pair = Role=SUPER-ADMIN-ROLE +

Attributes Details

Access Type = ACCESS_ACCEPT

cisco-av-pair = Role=SUPER-ADMIN-ROLE

Schritt 4: Navigieren Sie auf dem ISE-Server zu Work Centers > Profiler > Policy Sets, um die Authentifizierungs- und Autorisierungsrichtlinie zu konfigurieren.

Identifizieren Sie die Standard-Richtlinie, und klicken Sie auf den blauen Pfeil, um sie zu konfigurieren.

Policy Sets

Reset

Reset Policyset Hitcounts

Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
⊗	Wire-dot1x		Wired_802.1X	internal_user	0	⚙️	➔
⊗	MAB		Wired_MAB	Default Network Access	0	⚙️	➔
✅	Default	Default policy set		Default Network Access	180517	⚙️	➔

Reset Save

Erweitern Sie innerhalb des Standardrichtliniensatzes die Authentifizierungsrichtlinie, und erweitern Sie im Abschnitt Standard die Optionen, und stellen Sie sicher, dass sie mit der unten stehenden Konfiguration übereinstimmen.

Policy Sets → Default

Reset

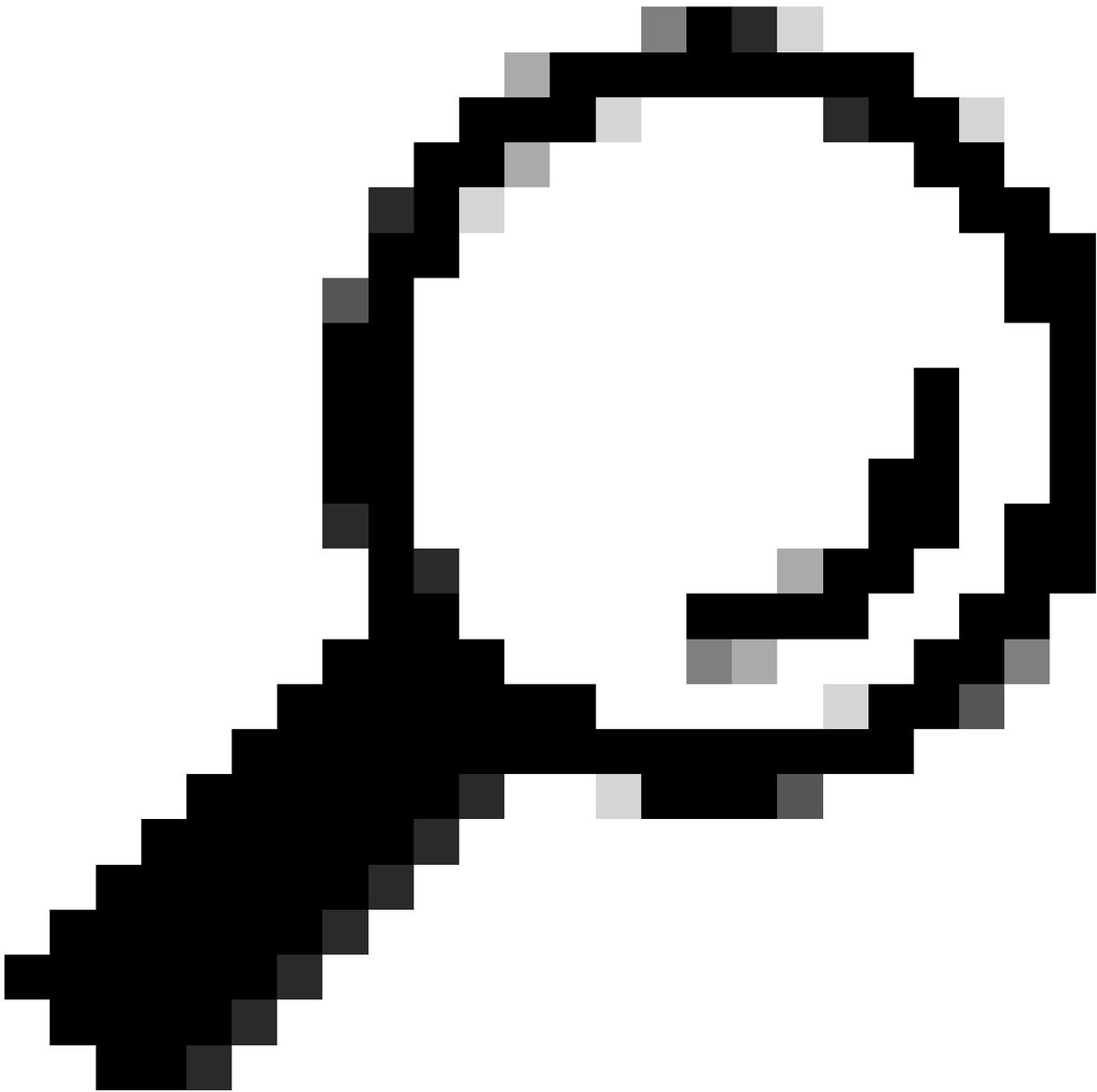
Reset Policyset Hitcounts

Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✅	Default	Default policy set		Default Network Access	180617

Authentication Policy (3)

Status	Rule Name	Conditions	Use	Hits	Actions
✅	MAB	OR Wired_MAB Wireless_MAB	Internal Endpoints > Options	4556	⚙️
✅	Dot1X	OR Wired_802.1X Wireless_802.1X	All_User_ID_Stores > Options	0	⚙️
✅	Default		All_User_ID_Stores Options If Auth fail REJECT If User not found REJECT If Process fail DROP	62816	⚙️



Tipp: REJECT, das für die 3 Optionen konfiguriert wurde, funktioniert auch

Erweitern Sie innerhalb des Standardrichtliniensatzes die Autorisierungsrichtlinie, und wählen Sie das Symbol Hinzufügen aus, um eine neue Autorisierungsbedingung zu erstellen.

Cisco ISE Work Centers - Profiler

Overview Ext Id Sources Network Devices Endpoint Classification Node Config Feeds Manual Scans Policy Elements Profiling Policies More

Policy Sets → Default Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	180617

> Authentication Policy (3)

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

Authorization Policy (25)

Status	Rule Name	Conditions	Results		Hits	Actions
			Profiles	Security Groups		
+						

Konfigurieren Sie einen Regelnamen, und klicken Sie auf das Symbol Hinzufügen, um die Bedingung zu konfigurieren.

Cisco ISE Work Centers - Profiler

Overview Ext Id Sources Network Devices Endpoint Classification Node Config Feeds Manual Scans Policy Elements Profiling Policies More

Policy Sets → Default Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	180617

> Authentication Policy (3)

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

Authorization Policy (26)

Status	Rule Name	Conditions	Results		Hits	Actions
			Profiles	Security Groups		
+	DNAC-SUPER-ADMIN-ROLE		Select from list	Select from list		

Ordnen Sie sie als Teil der Bedingung der IP-Adresse des Netzwerkgeräts zu, die in Schritt 2 konfiguriert wurde.

Conditions Studio

Library

Search by Name



- BYOD_is_Registered
- Catalyst_Switch_Local_Web_Authentication
- Compliance_Unknown_Devices
- Compliant_Devices
- CY_Campus
- CY_CAMPUS_MAC
- CY_Campus_voice
- CY_Guest
- EAP-MSCHAPv2

Editor

Network Access-Device IP Address

Equals 10.88.244.151

Set to 'Is not'

Duplicate Save

NEW | AND | OR

Close

Use

Klicken Sie auf Speichern.

Speichern Sie sie als neue Bibliotheksbedingung, und nennen Sie sie, wie Sie möchten, in diesem Fall wird sie alsDNACbenannt.



Save condition

Save as existing Library Condition (replaces current version and impact all policies that use this condition)

Select from list ▼

Save as a new Library Condition

DNAC

Description (optional)

Condition Description

Close

Save

Konfigurieren Sie abschließend das in Schritt 3 erstellte Profil.

The screenshot shows the Cisco ISE Profiler interface. The top navigation bar includes 'Cisco ISE' and 'Work Centers - Profiler'. The main menu has options like 'Overview', 'Ext Id Sources', 'Network Devices', 'Endpoint Classification', 'Node Config', 'Feeds', 'Manual Scans', 'Policy Elements', 'Profiling Policies', and 'More'. The current view is 'Policy Sets -> Default'. There are buttons for 'Reset', 'Reset Policyset Hitcounts', and 'Save'. A table lists policy sets with columns for Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, and Hits. The 'Default' policy set is highlighted. Below the table, there are expandable sections for 'Authentication Policy (3)', 'Authorization Policy - Local Exceptions', 'Authorization Policy - Global Exceptions', and 'Authorization Policy (25)'. The 'Authorization Policy (25)' section is expanded, showing a table with columns for Status, Rule Name, Conditions, Profiles, Security Groups, Hits, and Actions. The 'DNAC-SUPER-ADMIN-ROLE' rule is selected, and its 'Profiles' column shows 'DNAC_AUTH_PROFILE' with a dropdown arrow.

Klicken Sie auf Speichern.

Schritt 5: Melden Sie sich bei der Cisco DNA Center-GUI an, und navigieren Sie zu System > Users & Roles > External Authentication.

Klicken Sie auf die Option Externen Benutzer aktivieren, und legen Sie das AAA-Attribut als Cisco-

User Management

Role Based Access Control

External Authentication

External Authentication

Cisco DNA Center supports external servers for authentication and authorization of External Users. Use the fields in this window to create, update and on Cisco DNA Center is the name of the AAA attribute chosen on the AAA server. The default attribute expected is Cisco-AVPair, but if the user choo it needs to be configured here on Cisco DNA Center.

The value of the AAA attribute to be configured for authorization on AAA server would be in the format of "Role=role1". On ISE server, choose the cisc attributes list. A sample configuration inside Authorization profile would look like "cisco-av-pair= Role=SUPER-ADMIN-ROLE".

An example configuration in the case of manually defining the AAA attribute would be "Cisco-AVPair=Role=SUPER-ADMIN-ROLE".

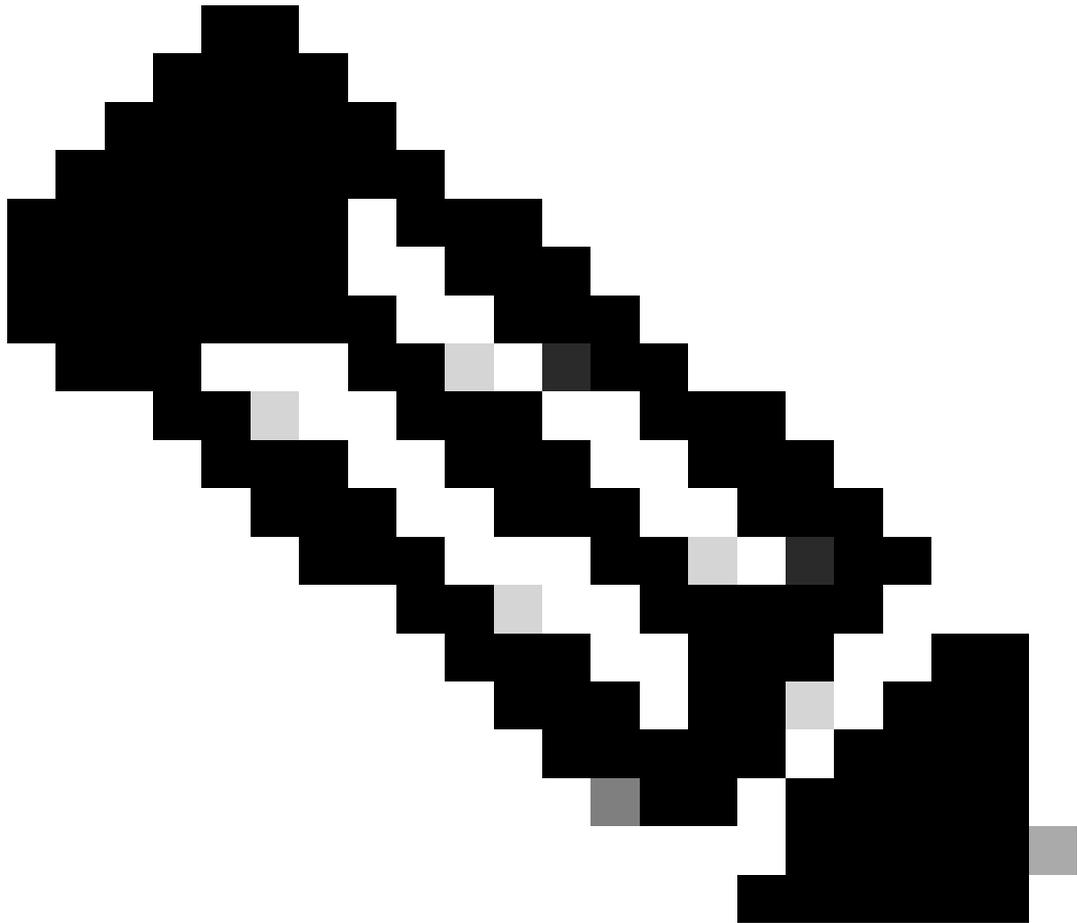
Enable External User ?

AAA Attribute

AAA Attribute
Cisco-AVPair

Reset to Default

Update



Hinweis: ISE-Server verwenden das Attribut Cisco-AVPair am Backend, sodass die Konfiguration in Schritt 3 gültig ist.

Blättern Sie nach unten, um den Konfigurationsabschnitt für AAA-Server anzuzeigen. Konfigurieren Sie die IP-Adresse des ISE-Servers in Schritt 1 und den unter Schritt 3 konfigurierten gemeinsamen geheimen Schlüssel.

Klicken Sie dann auf Erweiterte Einstellungen anzeigen.

▼ AAA Server(s)

Primary AAA Server

IP Address

10.10.10.10



Shared Secret

SHOW

Info

[View Advanced Settings](#)

Update

Secondary AAA Server

IP Address

10.10.10.10



Shared Secret

SHOW

Info

[View Advanced Settings](#)

Update

Vergewissern Sie sich, dass die RADIUS-Option aktiviert ist, und klicken Sie auf die Schaltfläche Aktualisieren auf beiden Servern.

∨ AAA Server(s)

Primary AAA Server

IP Address

██████████



Shared Secret

SHOW

Info

Hide Advanced Settings

RADIUS TACACS

Authentication Port

1812

Accounting Port

1813

Retries

3

Timeout (seconds)

4

Secondary AAA Server

IP Address

██████████



Shared Secret

SHOW

Info

Hide Advanced Settings

RADIUS TACACS

Authentication Port

1812

Accounting Port

1813

Retries

3

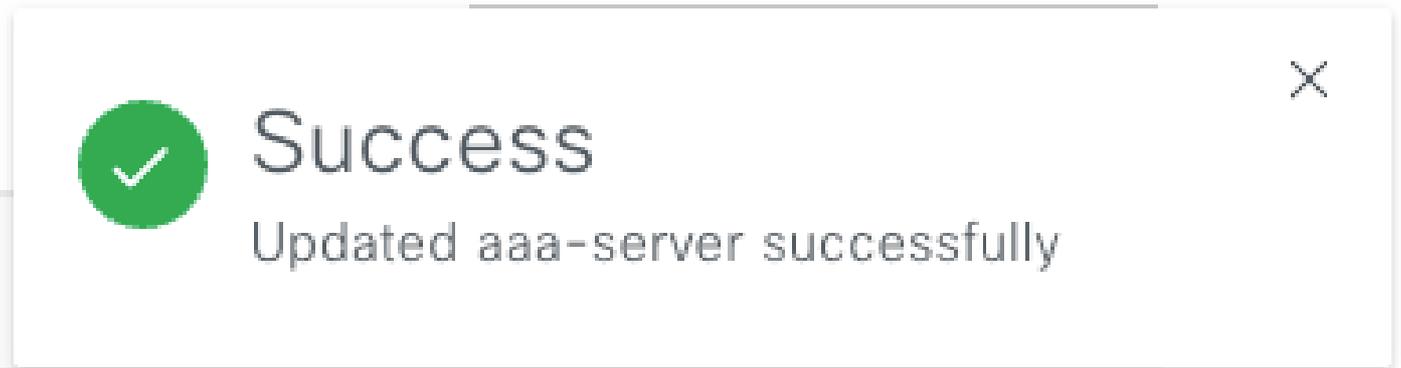
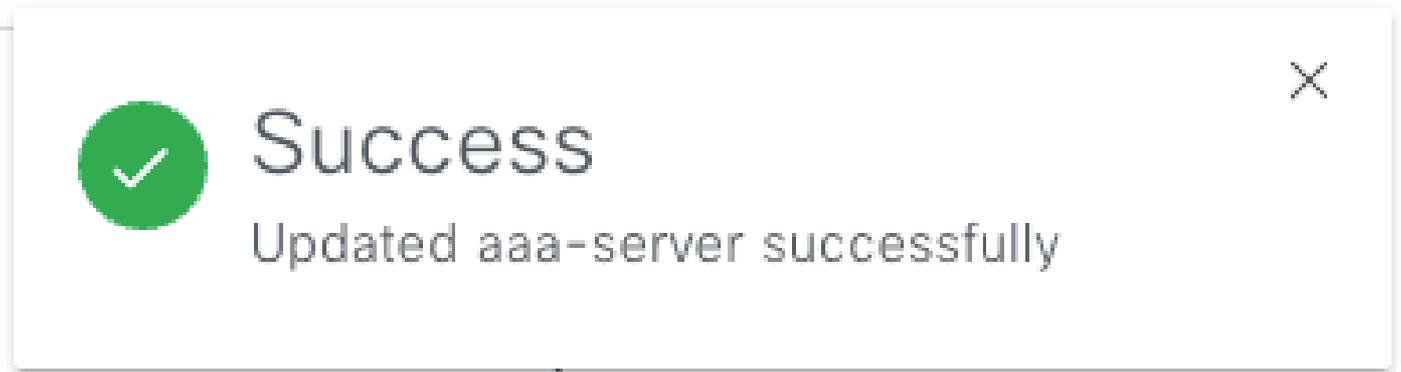
Timeout (seconds)

4

Update

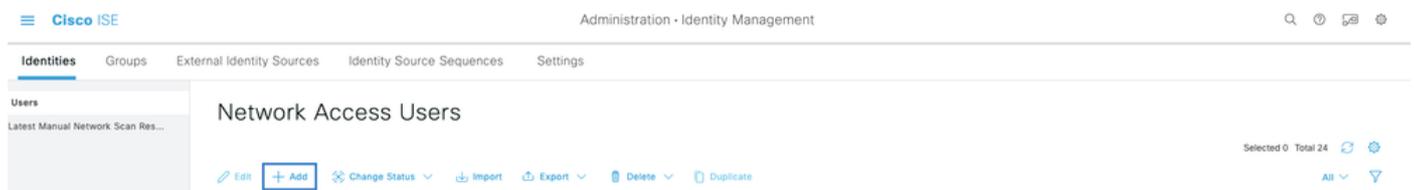
Update

Sie müssen jeweils eine Erfolgsmeldung anzeigen.



Jetzt können Sie sich mit jeder ISE-Identität anmelden, die im Menü "ISE" unter "Administration" > "Identity Management" > "Identities" > "Users" (Benutzer) erstellt wurde.

Falls Sie noch keine erstellt haben, melden Sie sich bei der ISE an, navigieren Sie zum obigen Pfad, und fügen Sie einen neuen Netzwerkzugriffsbenutzer hinzu.



Überprüfung

Laden der Benutzeroberfläche von Cisco DNA Center und melden Sie sich mit einem Benutzer von der ISE an.



Cisco DNA Center

The bridge to possible

✓ Success!

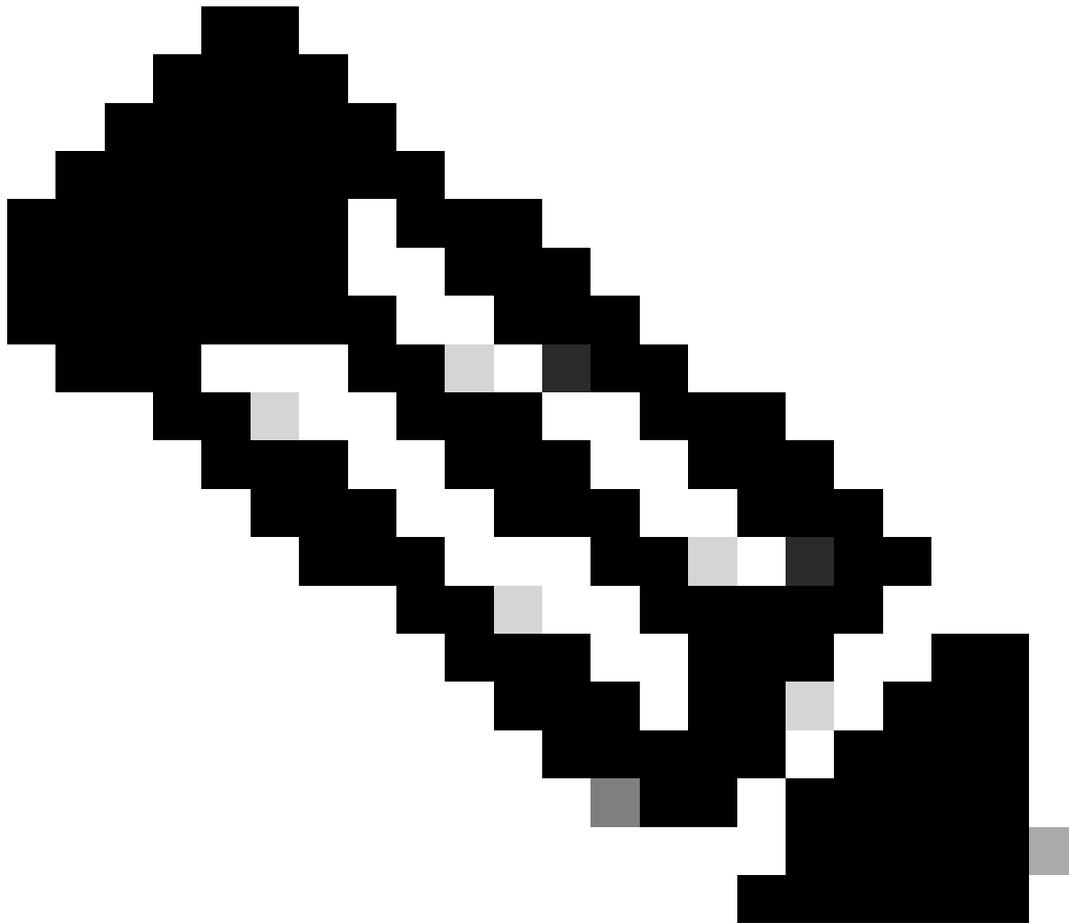
Username

test

Password

.....

Log In



Hinweis: Jeder Benutzer mit ISE-ID kann sich jetzt anmelden. Sie können die Authentifizierungsregeln auf dem ISE-Server detaillierter gestalten.

Nach erfolgreicher Anmeldung wird der Benutzername in der Cisco DNA Center-GUI angezeigt.

Welcome, test

Willkommensseite

Weitere Rollen

Sie können diese Schritte für jede Funktion im Cisco DNA Center wiederholen. Standardmäßig haben wir folgende Funktionen: SUPER-ADMIN-ROLE, NETWORK-ADMIN-ROLE und OBSERVER-ROLE.

The screenshot displays the Cisco DNA Center interface for managing user roles. The breadcrumb path is 'System / Users & Roles'. The main heading is 'User Roles', with a sub-heading 'Role Based Access Control'. Below this, there is a descriptive sentence: 'Create customized roles for your organization, grant high level access or granular functionality controls. When denying access, those aspects of Cisco DNA Center are removed from the users interface.' The interface features a 'Create a New Role' button and three role cards:

- SUPER-ADMIN-ROLE (5):** Complete control of the Cisco DNA Center deployment, all access enabled.
- NETWORK-ADMIN-ROLE (2):** General Purpose role without ability to change system configurations.
- OBSERVER-ROLE (1):** Read only access, unable to view some sensitive data in the system settings.

In diesem Dokument wird das Rollenbeispiel SUPER-ADMIN-ROLE verwendet. Sie können jedoch für jede Rolle in Cisco DNA Center ein Autorisierungsprofil auf der ISE konfigurieren. Die einzige Überlegung hierbei ist, dass die in Schritt 3 konfigurierte Rolle genau (unter Berücksichtigung der Groß-/Kleinschreibung) mit dem Rollennamen in Cisco DNA Center übereinstimmen muss.

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.