

Konfigurieren von RADIUS & TACACS+ für GUI & CLI-Authentifizierung auf 9800-WLCs

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Schreibgeschützte Benutzereinschränkungen](#)

[Konfigurieren der RADIUS-Authentifizierung für den WLC](#)

[Konfigurieren der ISE für RADIUS](#)

[Konfigurieren von TACACS+ WLC](#)

[Konfiguration von TACACS+ ISE](#)

[Fehlerbehebung](#)

[Fehlerbehebung: Zugriff auf die WLC-GUI oder die CLI RADIUS/TACACS+ über die WLC-CLI](#)

[Fehlerbehebung: WLC-GUI oder CLITACACS+-Zugriff über die ISE-GUI](#)

Einleitung

In diesem Dokument wird die Konfiguration eines Catalyst 9800 für die externe RADIUS- oder TACACS+-Authentifizierung beschrieben.

Voraussetzungen

Anforderungen

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

- Catalyst Wireless 9800-Konfigurationsmodell
- AAA-, RADIUS- und TACACS+-Konzepte

Verwendete Komponenten

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

- C9800-CL v17.9.2
- ISE 3.2.0

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.

Hintergrundinformationen

Wenn ein Benutzer versucht, auf die CLI oder die GUI des WLC zuzugreifen, wird er aufgefordert, einen Benutzernamen und ein Kennwort einzugeben. Standardmäßig werden diese Anmeldeinformationen mit der lokalen Benutzerdatenbank verglichen, die auf dem Gerät selbst vorhanden ist. Alternativ kann der WLC angewiesen werden, die eingegebenen Anmeldedaten mit einem Remote-AAA-Server zu vergleichen: Der WLC kann entweder über RADIUS oder TACACS+ mit dem Server kommunizieren.

Konfigurieren

In diesem Beispiel werden zwei Benutzertypen auf dem AAA-Server (ISE), `adminuser` bzw. auf dem `helpdeskuser` konfiguriert. Diese Benutzer gehören jeweils zur `admin-group` und `zurhelpdesk-group` Gruppe. Es wird erwartet, dass dem Benutzer `adminuser`, der Teil der `admin-group` ist, der uneingeschränkte Zugriff auf den WLC gewährt wird. Andererseits soll dem `helpdeskuser` der `helpdesk-group` Teil der nur Monitor-Privilegien für den WLC gewährt werden. Daher besteht kein Konfigurationszugriff.

In diesem Artikel werden der WLC und die ISE zunächst für die RADIUS-Authentifizierung konfiguriert, und später wird dieselbe Konfiguration für TACACS+ durchgeführt.

Schreibgeschützte Benutzereinschränkungen

Bei Verwendung von TACACS+ oder RADIUS für die 9800 WebUI-Authentifizierung gelten folgende Einschränkungen:

- Benutzer mit der Berechtigungsstufe 0 sind vorhanden, haben aber keinen Zugriff auf die grafische Benutzeroberfläche.

-

Benutzer mit den Berechtigungsstufen 1-14 können nur die Registerkarte Monitor anzeigen (dies entspricht der Berechtigungsstufe eines schreibgeschützten, lokal authentifizierten Benutzers).

-

Benutzer mit der Berechtigungsstufe 15 haben vollen Zugriff

-

Benutzer mit der Berechtigungsstufe 15 und einem Befehlssatz, der nur bestimmte Befehle zulässt, werden nicht unterstützt. Der Benutzer kann weiterhin Konfigurationsänderungen über die WebUI ausführen.

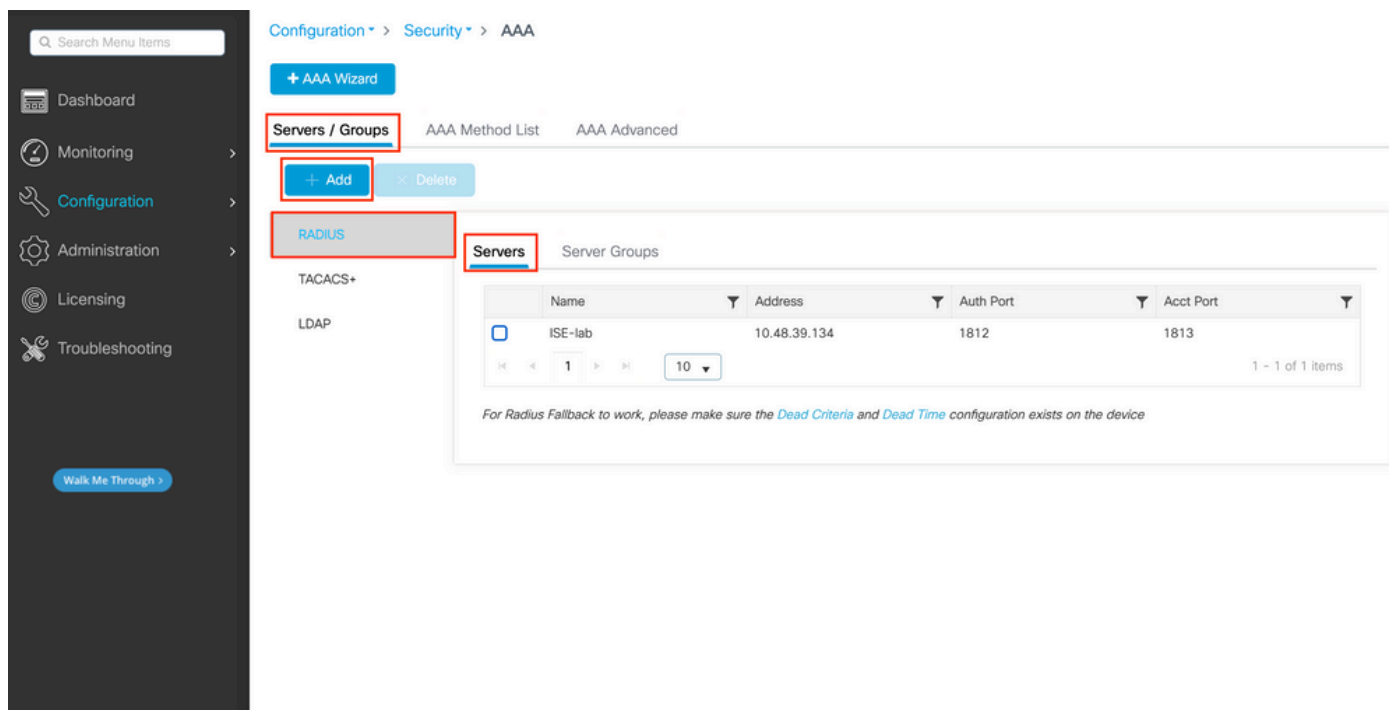
Diese Überlegungen können weder geändert noch geändert werden.

Konfigurieren der RADIUS-Authentifizierung für den WLC

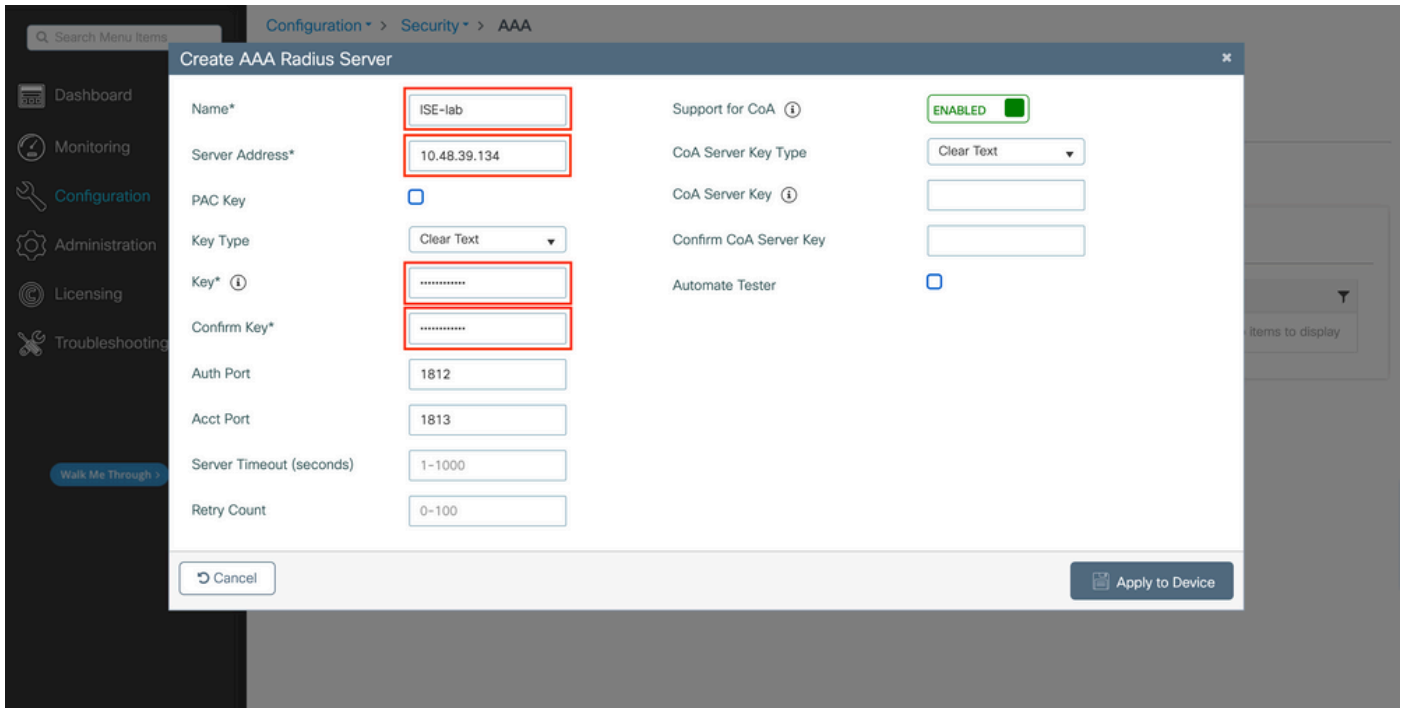
Schritt 1: Deklarieren Sie den RADIUS-Server.

Über GUI:

Erstellen Sie zunächst den ISE RADIUS-Server auf dem WLC. Dies kann über die Registerkarte Servers/Groups > RADIUS > Servers der GUI-WLC-Seite erfolgen, auf die in zugegriffen werden kann, <https://<WLC-IP>/webui/#/aaaConfiguration>Security>AAA> oder wenn Sie zu navigieren, wie in diesem Bild gezeigt.



Um einen RADIUS-Server zum WLC hinzuzufügen, klicken Sie auf die Schaltfläche Add (Hinzufügen), die im Bild rot umrahmt ist. Dadurch wird das im Screenshot dargestellte Popup-Fenster geöffnet.



In diesem Pop-up-Fenster müssen Sie Folgendes angeben:

- Der Servername (beachten Sie, dass er nicht mit dem ISE-Systemnamen übereinstimmen muss)
- Die Server-IP-Adresse
- Der gemeinsame geheime Schlüssel des WLC und des RADIUS-Servers

Es können weitere Parameter konfiguriert werden, z. B. die Ports für die Authentifizierung und die Abrechnung. Diese sind jedoch nicht obligatorisch und werden in dieser Dokumentation als Standard beibehalten.

Aus CLI:

```
<#root>
```

```
WLC-9800(config)#radius server
```

```
ISE-lab
```

```
WLC-9800(config-radius-server)#address ipv4
```

```
10.48.39.134
```

```
auth-port 1812 acct-port 1813
```

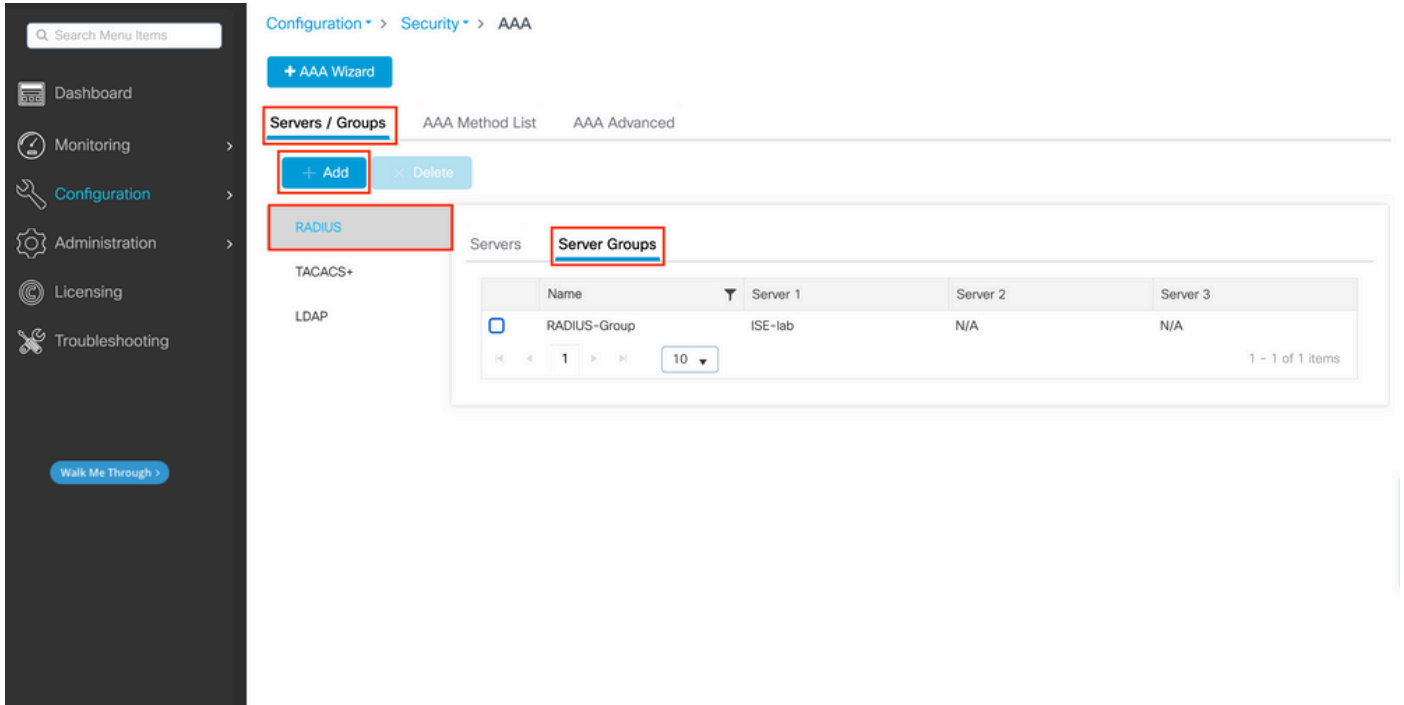
```
WLC-9800(config-radius-server)#key
```

```
Cisco123
```

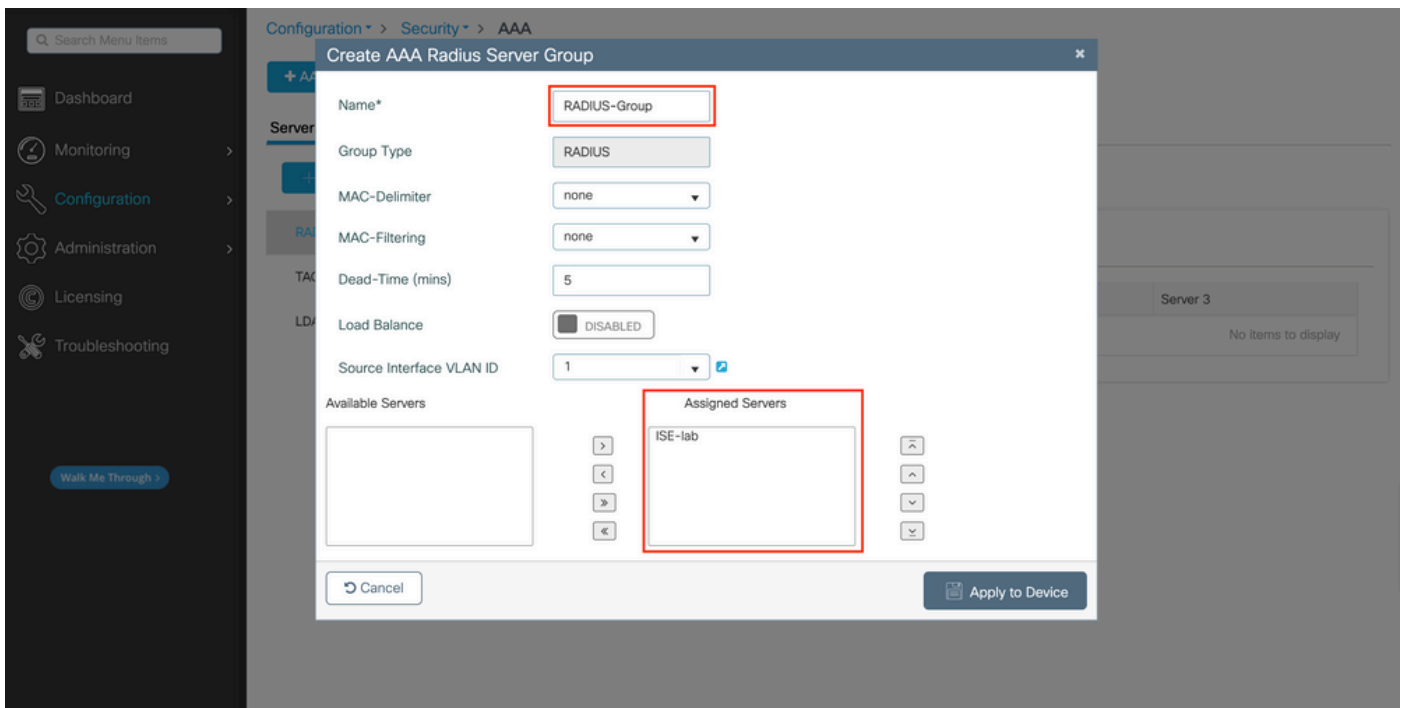
Schritt 2: Ordnen Sie den RADIUS-Server einer Servergruppe zu.

Über GUI:

Falls mehrere RADIUS-Server für die Authentifizierung verwendet werden können, wird empfohlen, alle diese Server derselben Servergruppe zuzuordnen. Der WLC sorgt für den Lastenausgleich verschiedener Authentifizierungen zwischen den Servern in der Servergruppe. RADIUS-Servergruppen werden über die Servers/Groups > RADIUS > Server Groups Registerkarte auf derselben GUI-Seite konfiguriert wie in Schritt 1. beschrieben, wie im Bild gezeigt.



Wie bei der Servererstellung wird ein Popup-Fenster angezeigt, wenn Sie auf die Schaltfläche Hinzufügen (im vorherigen Bild eingerahmt) klicken, die hier dargestellt ist.



Geben Sie im Popup-Fenster einen Namen für die Gruppe ein, und verschieben Sie die gewünschten Server in die Liste Zugewiesene Server.

Aus CLI:

```
.  
.  
.  
____<#root>
```

```
WLC-9800(config)# aaa group server radius
```

```
.  
.  
.  
RADIUS-Group
```

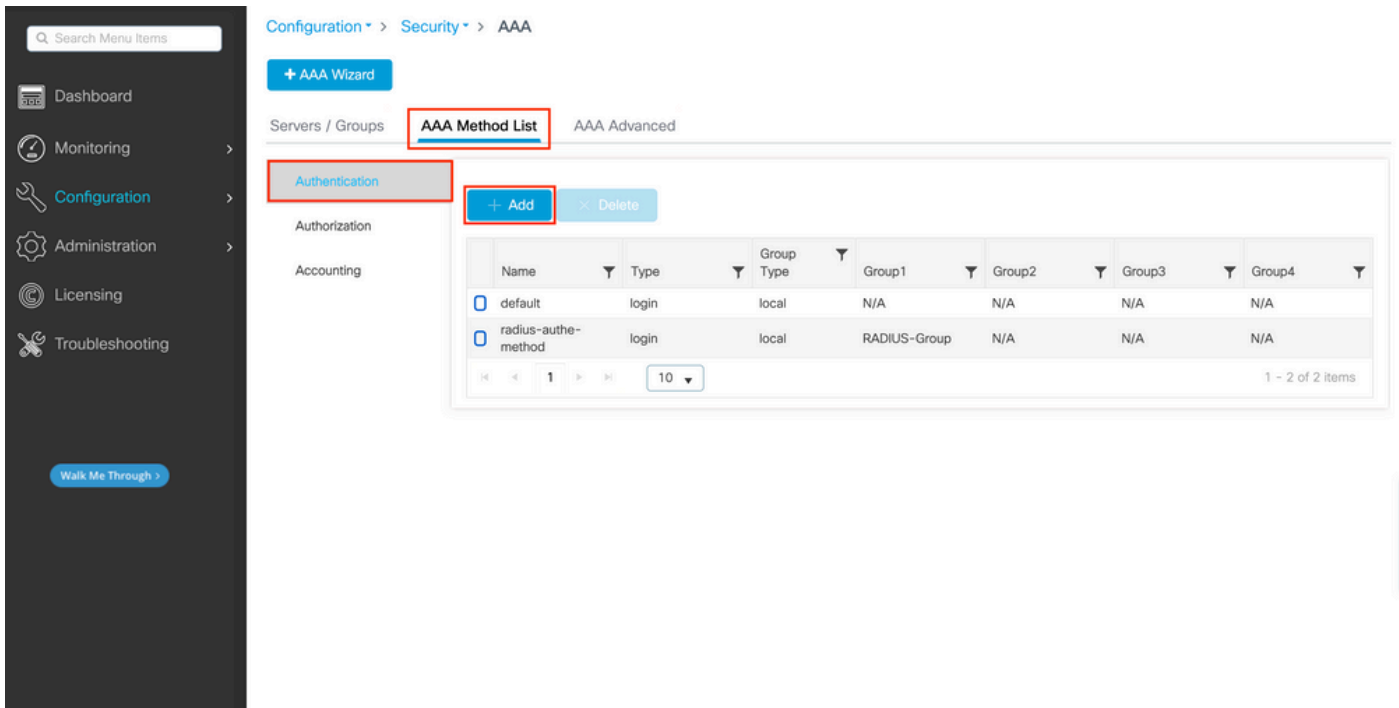
```
WLC-9800(config-sg-radius)# server name
```

```
.  
.  
.  
ISE-lab
```

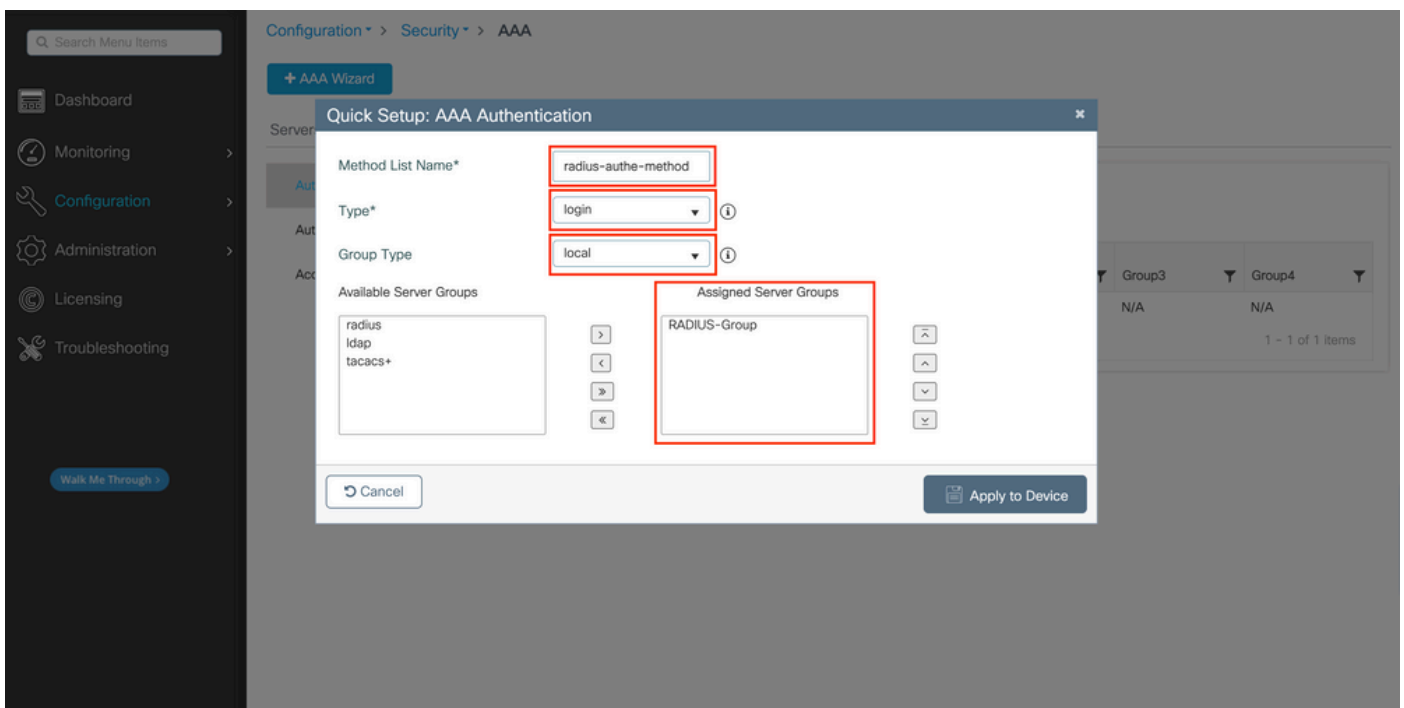
Schritt 3: Erstellen Sie eine AAA-Authentifizierungsprotokollmethode, die auf die RADIUS-Servergruppe verweist.

Über GUI:

Navigieren Sie dennoch von der GUI-Seite <https://<WLC-IP>/webui/#/aaa> zur Registerkarte, und erstellen Sie eine Authentifizierungsmethode, wie in diesem AAA Method List > Authentication Bild dargestellt.



Wenn Sie die Schaltfläche Hinzufügen verwenden, um eine Authentifizierungsmethode zu erstellen, wird wie üblich ein Popup-Fenster für die Konfiguration angezeigt, das dem in diesem Bild dargestellten Fenster ähnelt.



Geben Sie in diesem Popup-Fenster einen Namen für die Methode an. Wählen Sie Type als Anmelden aus, und fügen Sie den im vorherigen Schritt erstellten Gruppenserver zur Assigned Server Groups Liste hinzu. Für das Feld Gruppentyp sind mehrere Konfigurationen möglich.

- Wenn Sie Group Type (Gruppentyp) als local (lokal) auswählen, prüft der WLC zunächst, ob die Benutzeranmeldeinformationen lokal vorhanden sind, und greift dann auf die Servergruppe zurück.
- Wenn Sie Gruppentyp als Gruppe auswählen und nicht die Option Lokal zurückgreifen aktivieren, vergleicht der WLC lediglich die Benutzeranmeldeinformationen mit der Servergruppe.

- Wenn Sie Gruppentyp als Gruppe auswählen und die Option Fallback to local aktivieren, prüft der WLC die Benutzeranmeldeinformationen anhand der Servergruppe und fragt die lokale Datenbank nur ab, wenn der Server nicht antwortet. Wenn der Server eine Ablehnung sendet, muss der Benutzer authentifiziert werden, obwohl er in der lokalen Datenbank vorhanden sein kann.

Aus CLI:

Wenn Sie möchten, dass Benutzeranmeldeinformationen nur dann mit einer Servergruppe geprüft werden, wenn sie nicht zuerst lokal gefunden wurden, verwenden Sie Folgendes:

```
<#root>
```

```
WLC-9800(config)#aaa authentication login
```

```
radius-auth-method
```

```
local group
```

```
RADIUS-Group
```

Wenn die Benutzeranmeldeinformationen nur mit einer Servergruppe überprüft werden sollen, verwenden Sie Folgendes:

```
<#root>
```

```
WLC-9800(config)#aaa authentication login
```

```
radius-auth-method
```


group

RADIUS-Group

Wenn Sie möchten, dass die Anmeldeinformationen des Benutzers mit einer Servergruppe geprüft werden, und wenn diese letzte nicht mit einem lokalen Eintrag antwortet, verwenden Sie Folgendes:

```
<#root>
```

```
WLC-9800(config)#aaa authentication login
```

radius-authe-method

group

RADIUS-Group

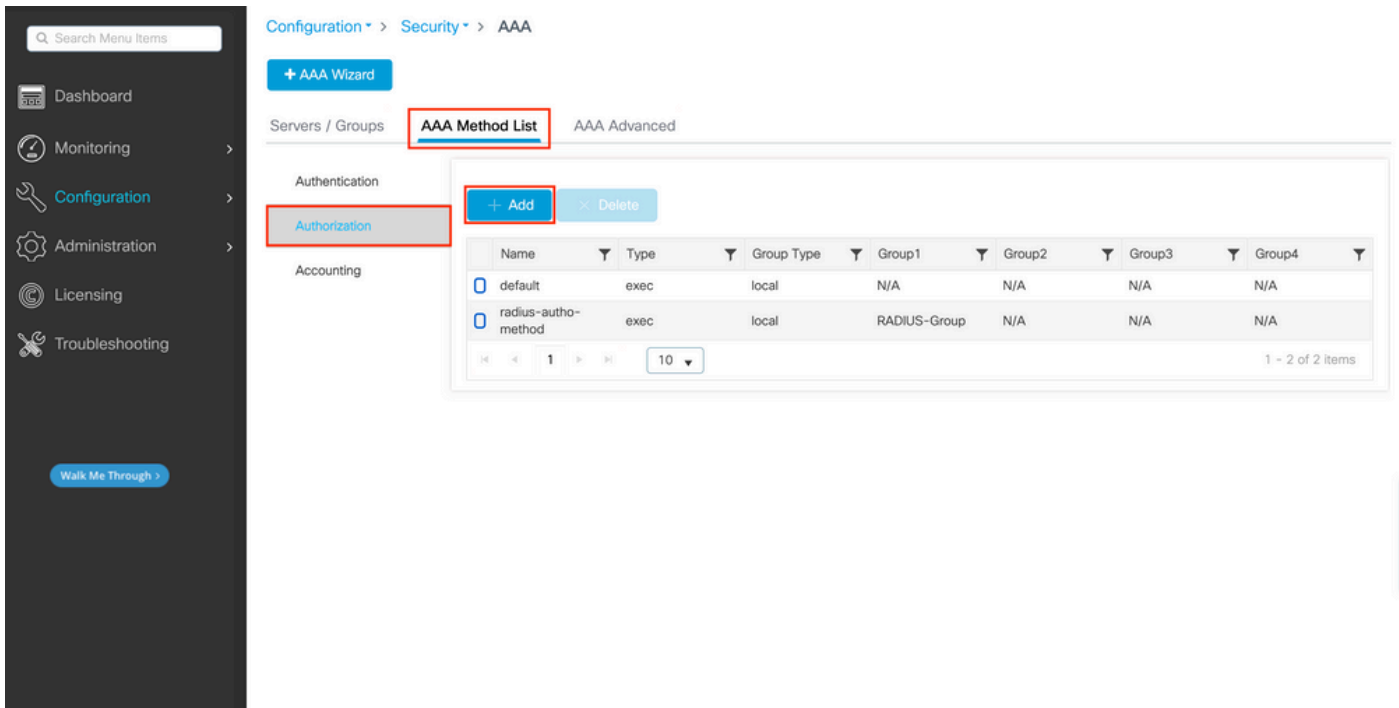
local

In dieser Beispielkonfiguration gibt es einige Benutzer, die nur lokal erstellt werden, und einige Benutzer, die nur auf dem ISE-Server arbeiten, verwenden daher die erste Option.

Schritt 4: Erstellen Sie eine exec-Methode zur AAA-Autorisierung, die auf die RADIUS-Servergruppe verweist.

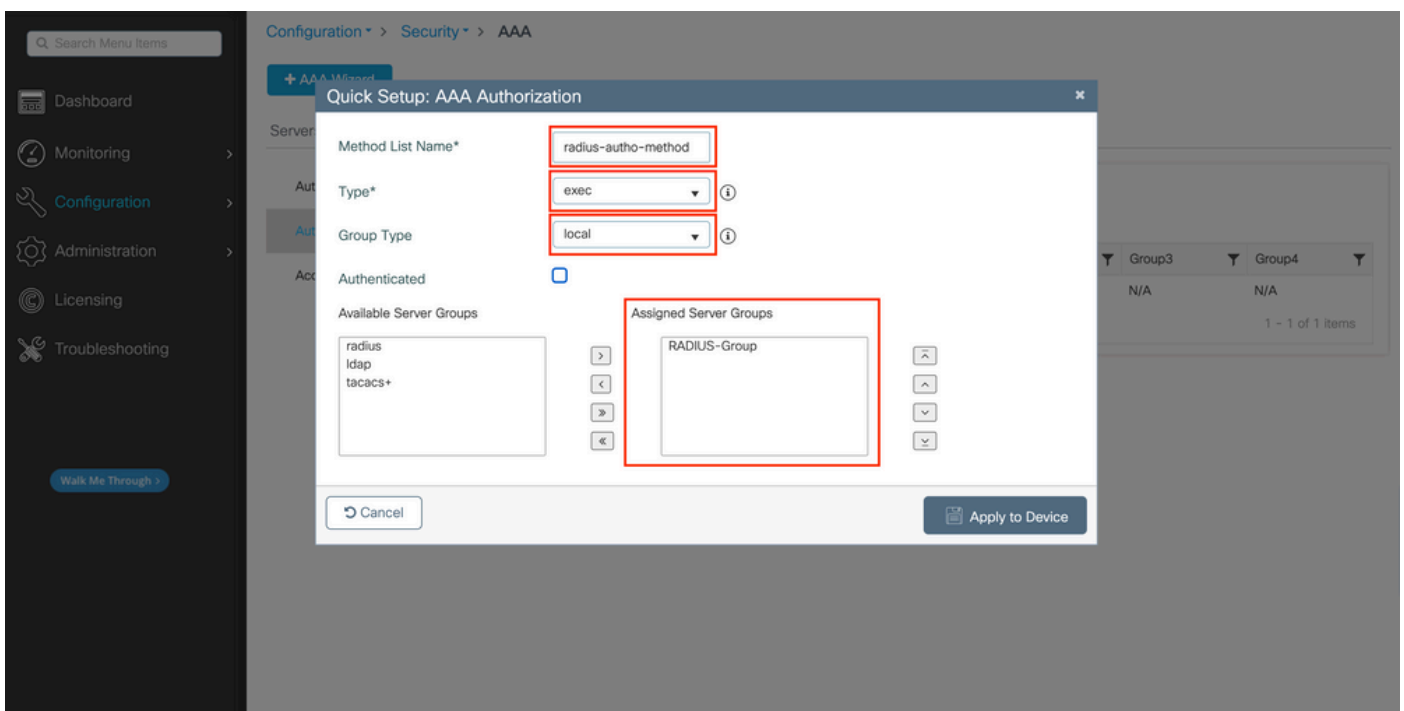
Über GUI:

Der Benutzer muss auch autorisiert werden, um Zugriff zu erhalten. Navigieren Sie dennoch von der GUI Page Configuration > Security > AAA aus zur Registerkarte, und erstellen Sie eine Autorisierungsmethode, wie in diesem AAA Method List > Authorization Bild dargestellt.



Erstellung der Autorisierungsmethode

Ein Popup-Fenster für die Konfiguration der Autorisierungsmethode, das dem abgebildeten Fenster ähnelt, wird angezeigt, wenn Sie mit der Schaltfläche Hinzufügen eine neue hinzufügen.



Geben Sie in diesem Konfigurations-Popup einen Namen für die Autorisierungsmethode an, wählen Sie den Typ als, exec und verwenden Sie die gleiche Reihenfolge von Gruppentyp wie bei der Authentifizierungsmethode in Schritt 3.

Aus CLI:

Bei der Authentifizierungsmethode wird die Autorisierung zuerst zugewiesen, um Benutzer mit lokalen Einträgen und dann mit Einträgen in einer Servergruppe zu vergleichen.

WLC-9800(config)#aaa authorization exec

radius-autho-method

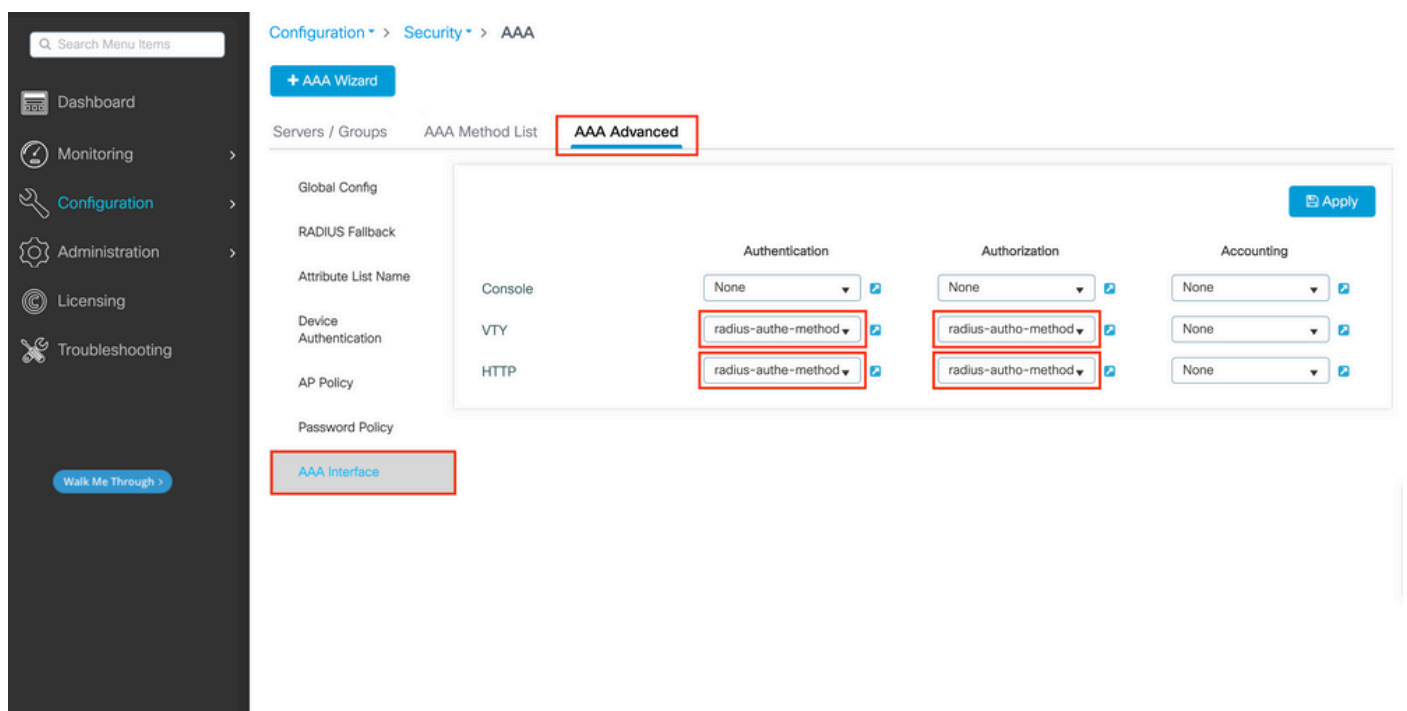
local group

RADIUS-Group

Schritt 5: Weisen Sie die Methoden den HTTP-Konfigurationen und den für Telnet/SSH verwendeten VTY-Leitungen zu.

Über GUI:

Die erstellten Authentifizierungs- und Autorisierungsmethoden können für HTTP- und/oder Telnet-/SSH-Benutzerverbindungen verwendet werden. Diese können auf der AAA Advanced > AAA Interface Registerkarte konfiguriert werden, die weiterhin auf der GUI-WLC-Seite verfügbar ist, auf die in zugegriffen werden kann, <https://<WLC-IP>/webui/#/aaa> wie in diesem Bild gezeigt:



CLI Für GUI-Authentifizierung:

<#root>

WLC-9800(config)#ip http authentication aaa login-authentication

radius-authe-method

WLC-9800(config)#ip http authentication aaa exec-authorization

radius-autho-method

CLI Für Telnet/SSH-Authentifizierung:

<#root>

WLC-9800(config)#line vty 0 15 WLC-9800(config-line)#login authentication

radius-authe-method

WLC-9800(config-line)#authorization exec

radius-autho-method

Beachten Sie, dass Sie die HTTP- und HTTPS-Dienste am besten neu starten, wenn Änderungen an den HTTP-Konfigurationen vorgenommen werden. Dies kann mithilfe der folgenden Befehle erreicht werden:

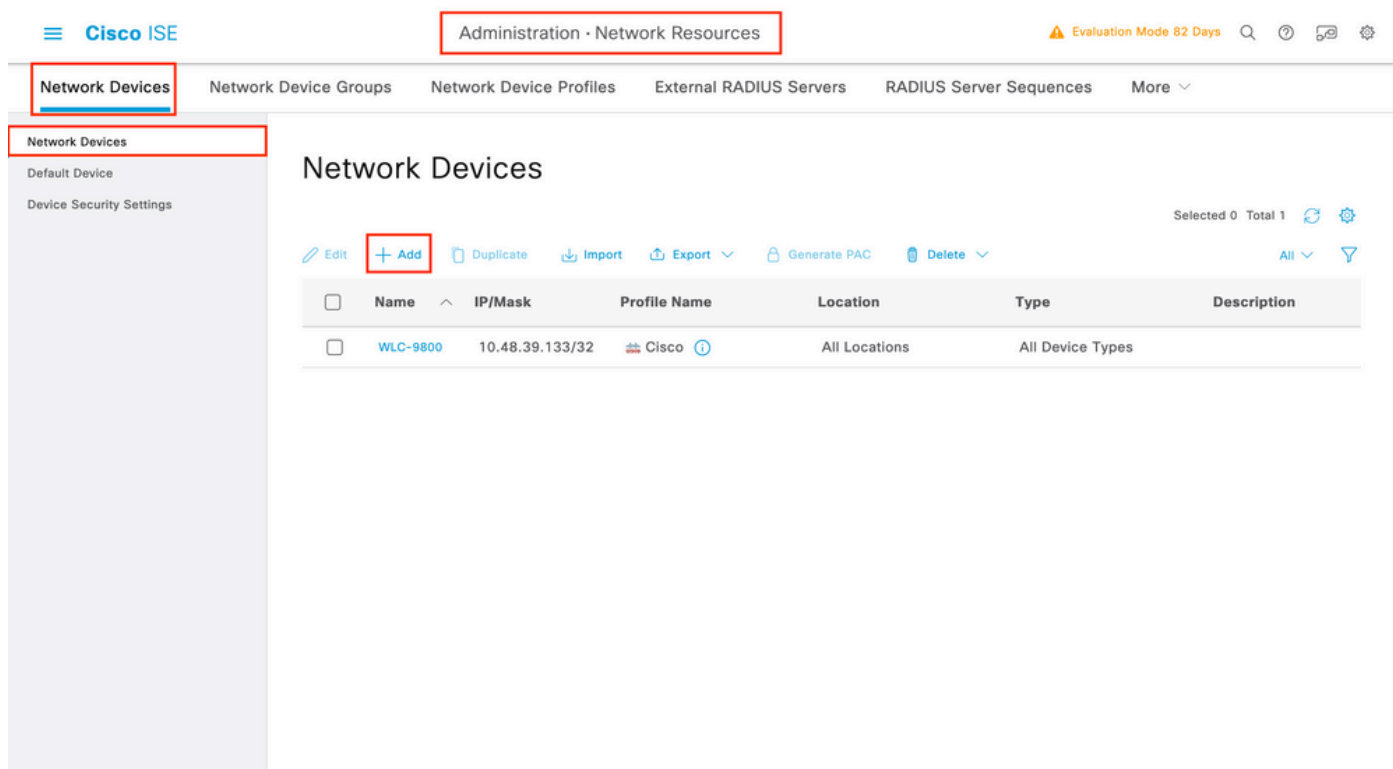
```
WLC-9800(config)#no ip http server WLC-9800(config)#no ip http secure-server WLC-9800(config)#ip http server WLC-9800(config)#ip http secure-server
```

Konfigurieren der ISE für RADIUS

Schritt 1: Konfigurieren des WLC als Netzwerkgerät für RADIUS

Über GUI:

Administration > Network Resources > Network Devices Um den im vorherigen Abschnitt verwendeten WLC als Netzwerkgerät für RADIUS in der ISE zu deklarieren, navigieren Sie zur Registerkarte Network devices (Netzwerkgeräte), und öffnen Sie diese, wie im nächsten Bild dargestellt.



Um ein Netzwerkgerät hinzuzufügen, verwenden Sie die Schaltfläche Hinzufügen, um das Konfigurationsformular für das neue Netzwerkgerät zu öffnen.

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

Location [Set To Default](#)IPSEC [Set To Default](#)Device Type [Set To Default](#) RADIUS Authentication Settings

RADIUS UDP Settings

Protocol Shared Secret [Show](#) Use Second Shared Secret [?](#)Second Shared Secret [Show](#)CoA Port [Set To Default](#)RADIUS DTLS Settings [?](#) DTLS Required [?](#)Shared Secret [?](#)

Geben Sie im neuen Fenster einen Namen für das Netzwerkgerät ein, und fügen Sie dessen IP-Adresse hinzu. Wählen Sie die RADIUS-Authentifizierungseinstellungen aus, und konfigurieren Sie den gleichen RADIUS Shared Secret wie auf dem WLC.

Schritt 2: Erstellen Sie ein Autorisierungsergebnis, um die Berechtigung zurückzugeben.

Über GUI:

Um Administratorzugriffsrechte zu erhalten, muss deradminuser über eine Privilegstufe von 15 verfügen, die den Zugriff auf die exec-Eingabeaufforderungs-Shell ermöglicht. Auf der anderen Seite benötigt derhelpdeskuser keine exec-Prompt-Shell-Zugriffsrechte und kann daher mit einer Privilegstufe unter 15 zugewiesen werden. Um Benutzern die entsprechende Berechtigungsstufe zuzuweisen, können Autorisierungsprofile verwendet werden. Diese können unter der ISE GUI Page Policy > Policy Elements > Results Registerkarte konfiguriert werden, die im nächsten Bild angezeigt wird. Authorization > Authorization Profiles.

- Dictionarys
- Conditions
- Results**
- Authentication
- Authorization
- Authorization Profiles**
- Downloadable ACLs
- Profiling
- Posture
- Client Provisioning

Standard Authorization Profiles

For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Selected 0 Total 11

[Edit](#) [+ Add](#) [Duplicate](#) [Delete](#)

All [Filter](#)

<input type="checkbox"/>	Name	Profile	Description
<input type="checkbox"/>	9800-admin-priv	Cisco	
<input type="checkbox"/>	9800-helpdesk-priv	Cisco	
<input type="checkbox"/>	Block_Wireless_Access	Cisco	Default profile used to block wireless devices. Ensure th
<input type="checkbox"/>	Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.
<input type="checkbox"/>	Cisco_Temporal_Onboard	Cisco	Onboard the device with Cisco temporal agent
<input type="checkbox"/>	Cisco_WebAuth	Cisco	Default Profile used to redirect users to the CWA portal
<input type="checkbox"/>	NSP_Onboard	Cisco	Onboard the device with Native Supplicant Provisioning
<input type="checkbox"/>	Non_Cisco_IP_Phones	Cisco	Default Profile used for Non Cisco Phones.
<input type="checkbox"/>	UDN	Cisco	Default profile used for UDN.
<input type="checkbox"/>	DenyAccess	Cisco	Default Profile with access type as Access-Reject

Verwenden Sie zum Konfigurieren eines neuen Autorisierungsprofils die Schaltfläche Hinzufügen, um das Konfigurationsformular für das neue Autorisierungsprofil zu öffnen. Dieses Formular muss speziell so aussehen, um das Profil zu konfigurieren, das dem zugewiesen istadminuser.

Dictionarys Conditions **Results**

Authentication > Authorization Profiles > New Authorization Profile

Authorization Profile

* Name 9800-admin-priv

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement ⓘ

Agentless Posture ⓘ

Passive Identity Tracking ⓘ

> Common Tasks

Advanced Attributes Settings

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

Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = shell:priv-lvl=15

Submit Cancel

Die angezeigte Konfiguration gewährt jedem Benutzer, dem sie zugeordnet ist, die Berechtigungsstufe 15. Wie bereits erwähnt, handelt es sich hierbei um das erwartete Verhalten für die Adminuser während des nächsten Schrittes erzeugten Daten. Die helpdeskuser Privilegstufe muss jedoch niedriger sein, und daher muss ein zweites Richtlinienelement erstellt werden.

Das policy-Element für helpdeskuser ist ähnlich wie das oben erstellte, mit der Ausnahme, dass die Zeichenfolge geändert werden muss shell:priv-lvl=15 muss, shell:priv-lvl=X um X durch die gewünschte Berechtigungsebene zu ersetzen. In diesem Beispiel wird 1 verwendet.

Schritt 3: Erstellen Sie Benutzergruppen auf der ISE.

Über die GUI:

ISE-Benutzergruppen werden über die Registerkarte User Identity Groups (Benutzeridentitätsgruppen) des Administration > Identity Management > Groups GUI Page erstellt, die im Screenshot angezeigt wird.

Cisco ISE Administration · Identity Management

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

Identity Groups

EQ

< [Icon] [Icon]

> Endpoint Identity Groups

> **User Identity Groups**

User Identity Groups

Selected 0 Total 10 [Refresh] [Settings]

[Edit] **+ Add** [Delete] [Import] [Export]

Name	Description
<input type="checkbox"/> helpdesk-group	This is the group containing all users with read-only privileges.
<input type="checkbox"/> admin-group	This is the group containing all users with administrator privileges.
<input type="checkbox"/> OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group
<input type="checkbox"/> GuestType_Weekly (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_SocialLogin (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Daily (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Contractor (default)	Identity group mirroring the guest type
<input type="checkbox"/> GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
<input type="checkbox"/> Employee	Default Employee User Group
<input type="checkbox"/> ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group

Um einen neuen Benutzer zu erstellen, verwenden Sie die Schaltfläche Hinzufügen. Daraufhin wird das neue Formular zur Konfiguration der Benutzeridentitätsgruppe geöffnet.

Cisco ISE Administration · Identity Management

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

Identity Groups

EQ

< [Icon] [Icon]

> Endpoint Identity Groups

> User Identity Groups

User Identity Groups > New User Identity Group

Identity Group

* Name **admin-group**

Description This is the group containing all users with administrator privileges.

Submit Cancel

Geben Sie den Namen der erstellten Gruppe an. Erstellen Sie die beiden oben genannten Benutzergruppen, nämlich die admin-group und helpdesk-group.

Schritt 4: Erstellen Sie Benutzer auf der ISE.

Über die GUI:

ISE-Benutzer werden über die Registerkarte Users of the Administration > Identity Management > Identities GUI Page erstellt, die im Screenshot angezeigt wird.

Users

Latest Manual Network Scan Res...

Network Access Users

Selected 0 Total 2

Edit **+ Add** Change Status Import Export Delete Duplicate

All

Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
<input type="checkbox"/>	Enabled	adminuser				admin-group	
<input type="checkbox"/>	Enabled	helpdeskus...				helpdesk-group	

Um einen neuen Benutzer zu erstellen, verwenden Sie die Schaltfläche Hinzufügen, um das neue Formular für die Netzwerkzugriffsbenutzerkonfiguration wie dargestellt zu öffnen.

Users

Latest Manual Network Scan Res...

Network Access Users List > New Network Access User

Network Access User

* Username **adminuser**

Status Enabled

Account Name Alias

Email

Passwords

Password Type: Internal Users

Password Lifetime:

With Expiration
Password will expire in 60 days

Never Expires

Password Re-Enter Password

* Login Password Generate Password

Enable Password Generate Password

> User Information

> Account Options

> Account Disable Policy

User Groups

admin-group

Geben Sie den Benutzern die Anmeldeinformationen (Benutzername und Kennwort) zur Authentifizierung auf dem WLC an. Stellen Sie außerdem sicher, dass der Status des Benutzers Enabled lautet. Fügen Sie abschließend den Benutzer zu seiner verwandten Gruppe hinzu, die in Schritt 4 erstellt wurde. Verwenden Sie dazu das Dropdown-Menü Benutzergruppen am Ende des Formulars.

Erstellen Sie die beiden oben genannten Benutzer, nämlich die adminuser und helpdeskuser.

Schritt 5: Benutzer authentifizieren.

Über GUI:

In diesem Szenario ermöglicht die bereits vorkonfigurierte Authentifizierungsrichtlinie der Standard-Richtliniensätze der ISE den Standard-Netzwerkzugriff. Dieser Richtliniensatz ist auf der Seite mit Policy > Policy Sets der ISE-GUI zu sehen, wie in dieser Abbildung dargestellt. Daher besteht keine Notwendigkeit, sie zu ändern.

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	0

Authentication Policy (3)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	MAB	OR Wired_MAB Wireless_MAB	Internal Endpoints > Options	0	⚙️
✓	Dot1X	OR Wired_802.1X Wireless_802.1X	All_User_ID_Stores > Options	0	⚙️
✓	Default		All_User_ID_Stores > Options	0	⚙️

Schritt 6: Autorisierung der Benutzer

Über GUI:

Nachdem der Anmeldeversuch die Authentifizierungsrichtlinie passiert hat, muss er autorisiert werden, und die ISE muss das zuvor erstellte Autorisierungsprofil zurückgeben (permit accept, zusammen mit der Berechtigungsebene).

In diesem Beispiel werden Anmeldeversuche anhand der Geräte-IP-Adresse (die die WLC-IP-Adresse ist) gefiltert, und die zu gewährende Berechtigungsstufe wird anhand der Gruppe unterschieden, zu der ein Benutzer gehört. Ein weiterer geeigneter Ansatz besteht darin, Benutzer anhand ihrer Benutzernamen zu filtern, da jede Gruppe in diesem Beispiel nur einen Benutzer enthält.

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	152

> Authentication Policy (3)

> Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions (2)

Status	Rule Name	Conditions	Results		Hits	Actions
			Profiles	Security Groups		
✔	9800 Helpdesk Users	AND Network Access-Device IP Address EQUALS 10.48.39.133 InternalUser-IdentityGroup EQUALS User Identity Groups:helpdesk-group	9800-helpdesk-priv	Select from list	1	⚙️
✔	9800 Admin Users	AND Network Access-Device IP Address EQUALS 10.48.39.133 InternalUser-IdentityGroup EQUALS User Identity Groups:admin-group	9800-admin-priv	Select from list	2	⚙️

> Authorization Policy (12)

Reset

Save

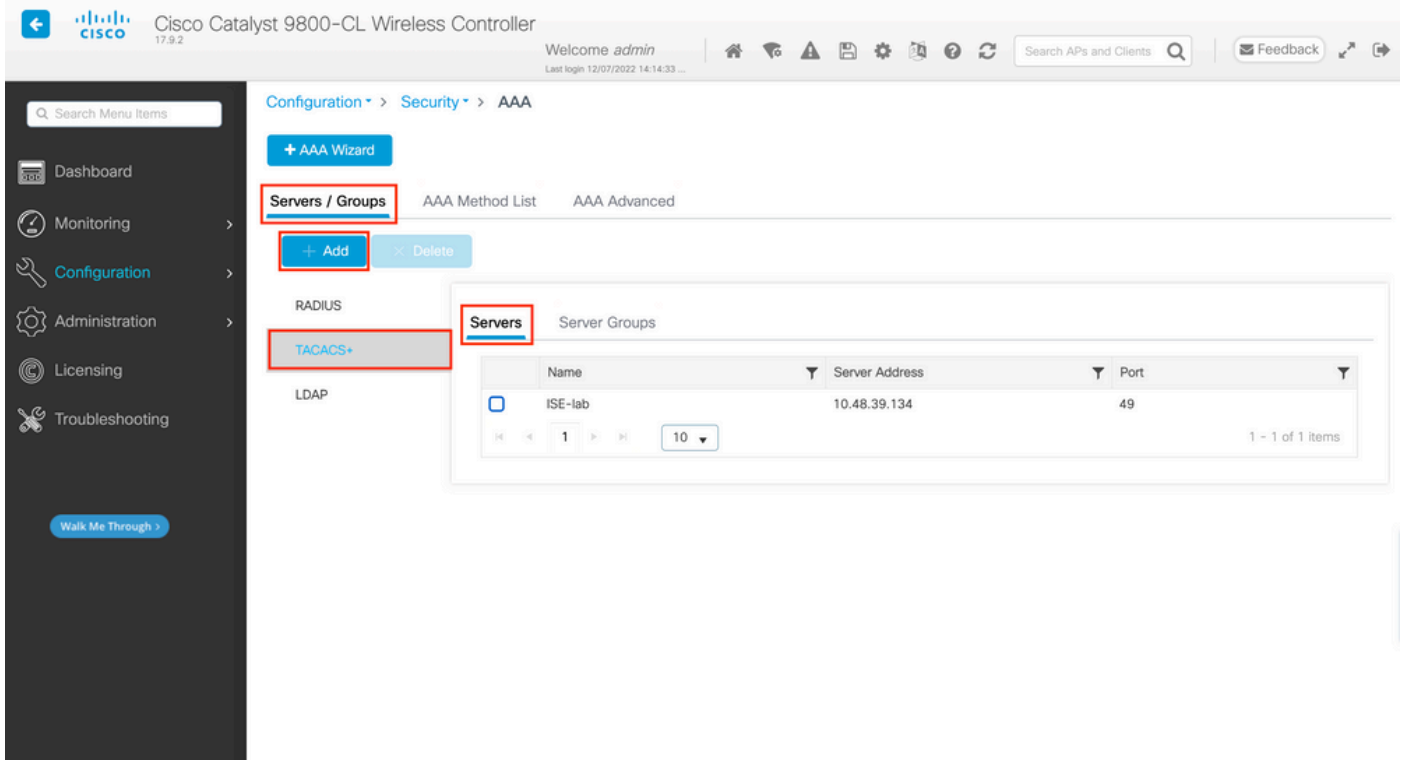
Nach Abschluss dieses Schritts können die für konfigurierten Anmeldeinformationen adminuser undhelpdesk der Benutzer zur Authentifizierung im WLC über die GUI oder über Telnet/SSH verwendet werden.

Konfigurieren von TACACS+ WLC

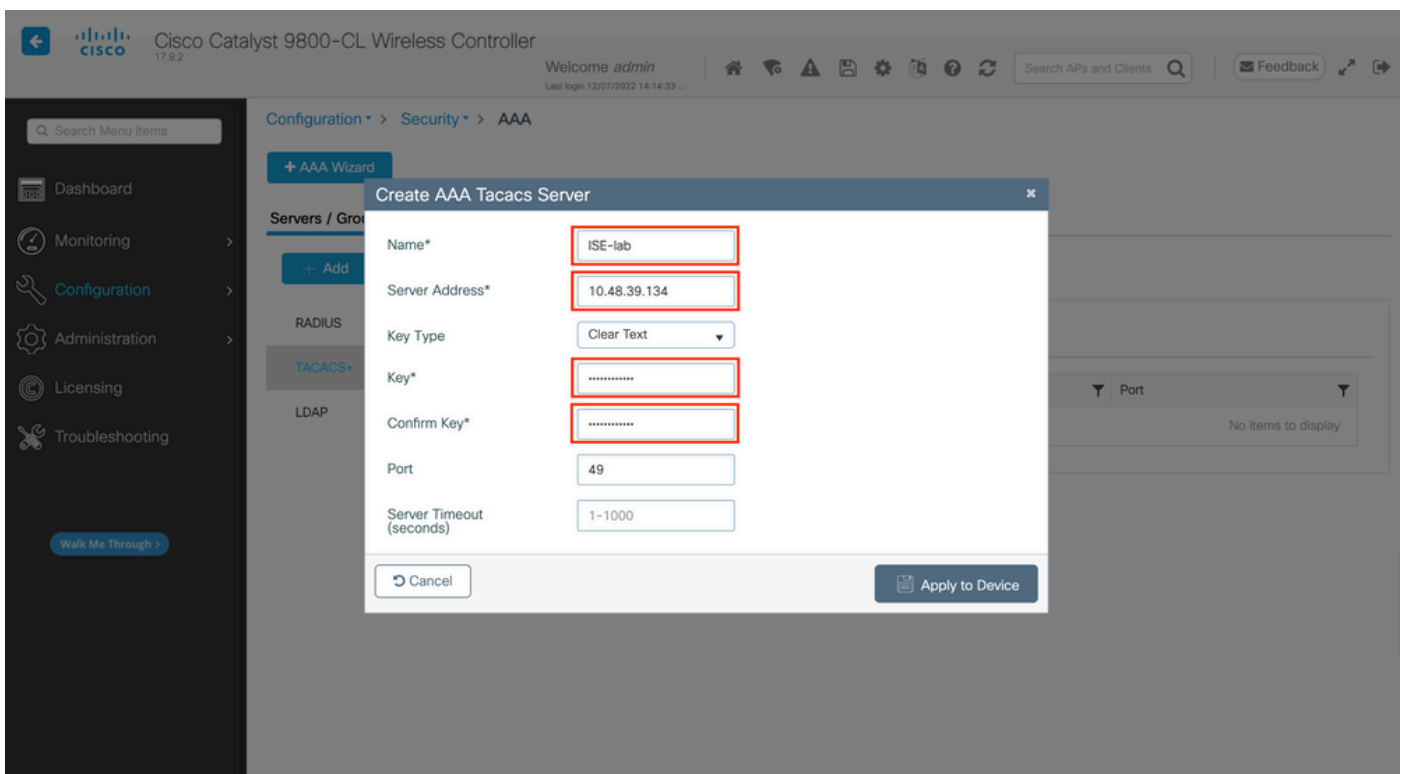
Schritt 1: Deklarieren Sie den TACACS+-Server.

Über GUI:

Erstellen Sie zunächst den TACACS+ Server ISE auf dem WLC. Dies kann über die Registerkarte Servers/Groups > TACACS+ > Servers der GUI-WLC-Seite erfolgen, auf die im zugegriffen werden kann. <https://<WLC-IP>/webui/#/aaa>Sie können auch zu der navigieren,Configuration > Security > AAA wie in diesem Bild gezeigt.



Um einen TACACS-Server zum WLC hinzuzufügen, klicken Sie auf die Schaltfläche Hinzufügen, die im obigen Bild rot umrahmt ist. Daraufhin wird das dargestellte Popup-Fenster geöffnet.



Wenn das Popup-Fenster geöffnet wird, geben Sie den Servernamen (er muss nicht mit dem ISE-Systemnamen übereinstimmen), seine IP-Adresse, den freigegebenen Schlüssel, den verwendeten Port und die Zeitüberschreitung an.

In diesem Popup-Fenster müssen Sie Folgendes angeben:

- Der Servername (beachten Sie, dass er nicht mit dem ISE-Systemnamen übereinstimmen muss)

- Die Server-IP-Adresse
- Der gemeinsame geheime Schlüssel zwischen dem WLC und dem TACACS+-Server

Es können weitere Parameter konfiguriert werden, z. B. die Ports, die für die Authentifizierung und Abrechnung verwendet werden. Diese sind jedoch nicht obligatorisch und werden in dieser Dokumentation als Standard beibehalten.

Aus CLI:

```
<#root>
```

```
WLC-9800(config)#tacacs server
```

ISE-lab

```
WLC-9800(config-server-tacacs)#address ipv4
```

```
10.48.39.134
```

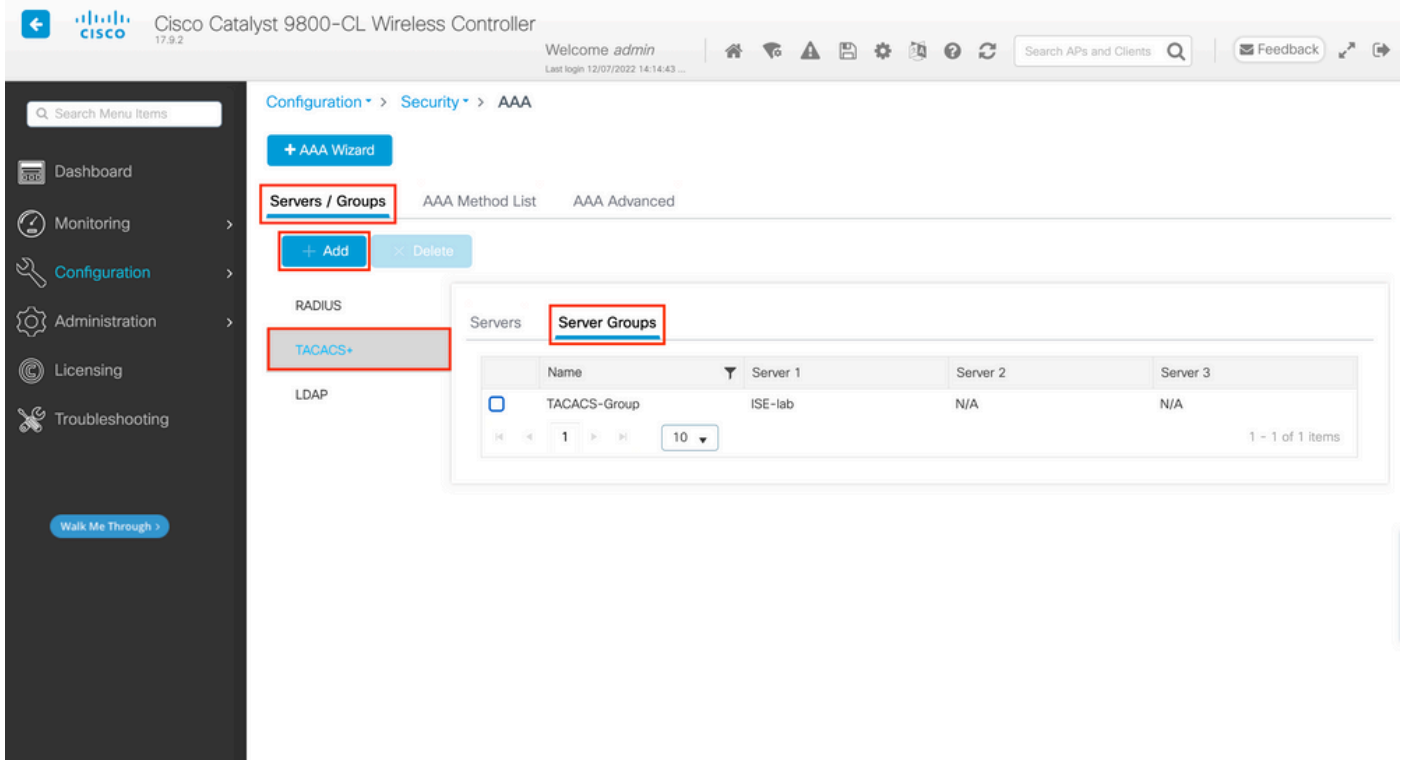
```
WLC-9800(config-server-tacacs)#key
```

Cisco123

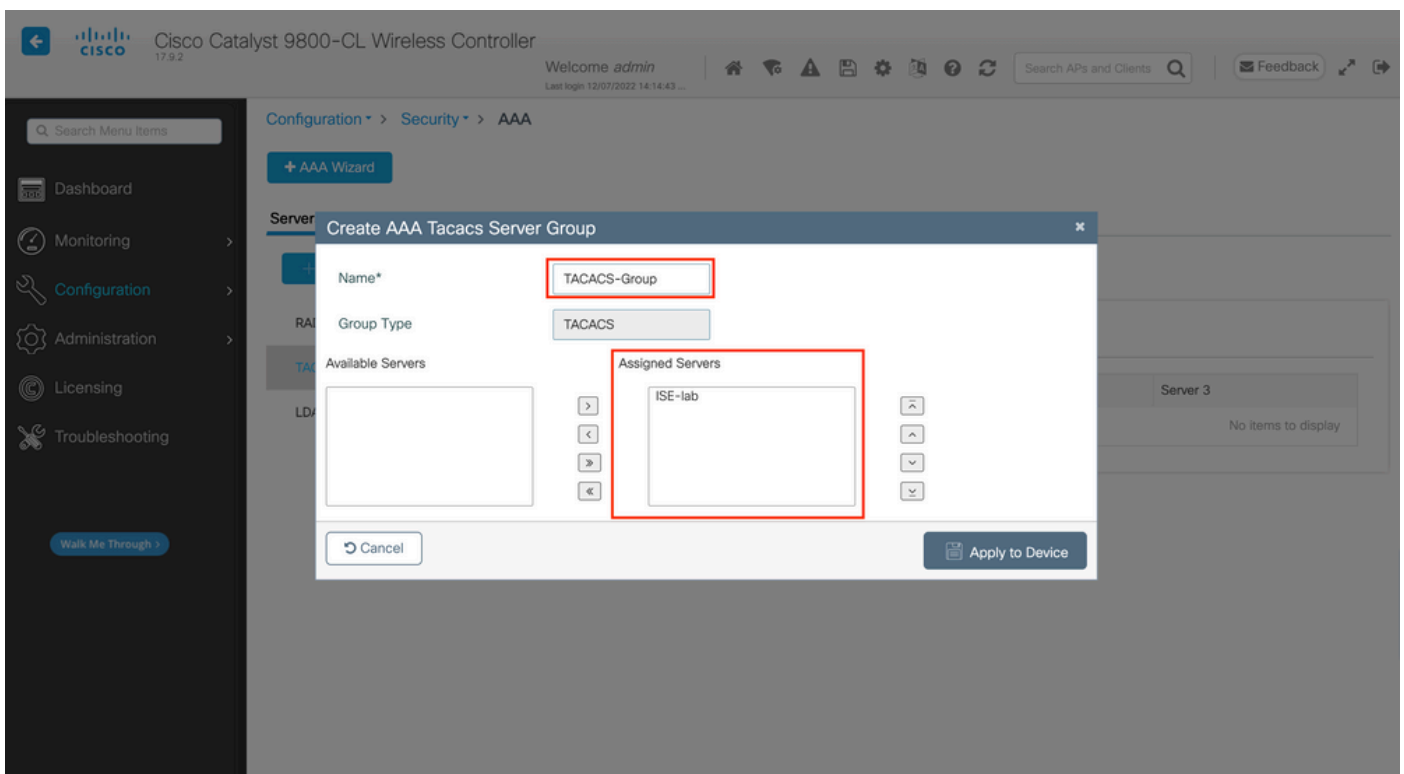
Schritt 2: Ordnen Sie den TACACS+-Server einer Servergruppe zu.

Über GUI:

Falls Sie mehrere TACACS+-Server haben, die für die Authentifizierung verwendet werden können, wird empfohlen, alle diese Server derselben Servergruppe zuzuordnen. Der WLC sorgt dann für den Lastenausgleich verschiedener Authentifizierungen zwischen den Servern in der Servergruppe. TACACS+-Servergruppen werden über die Servers/Groups > TACACS > Server Groups Registerkarte auf derselben GUI-Seite konfiguriert, die in Schritt 1. erwähnt wird, die im Bild angezeigt wird.



Wie bei der Servererstellung wird ein Popup-Fenster angezeigt, wenn Sie auf die Schaltfläche Hinzufügen klicken, die in dem zuvor im Bild dargestellten Bild eingerahmt ist.



Geben Sie im Popup-Fenster einen Namen für die Gruppe ein, und verschieben Sie die gewünschten Server in die Liste Zugewiesene Server.

Aus CLI:

<#root>

WLC-9800(config)#aaa group server tacacs+

TACACS-Group

WLC-9800(config-sg-tacacs+)#server name

ISE-lab

Schritt 3: Erstellen Sie eine AAA-Authentifizierungsmethode, die auf die TACACS+-Servergruppe verweist.

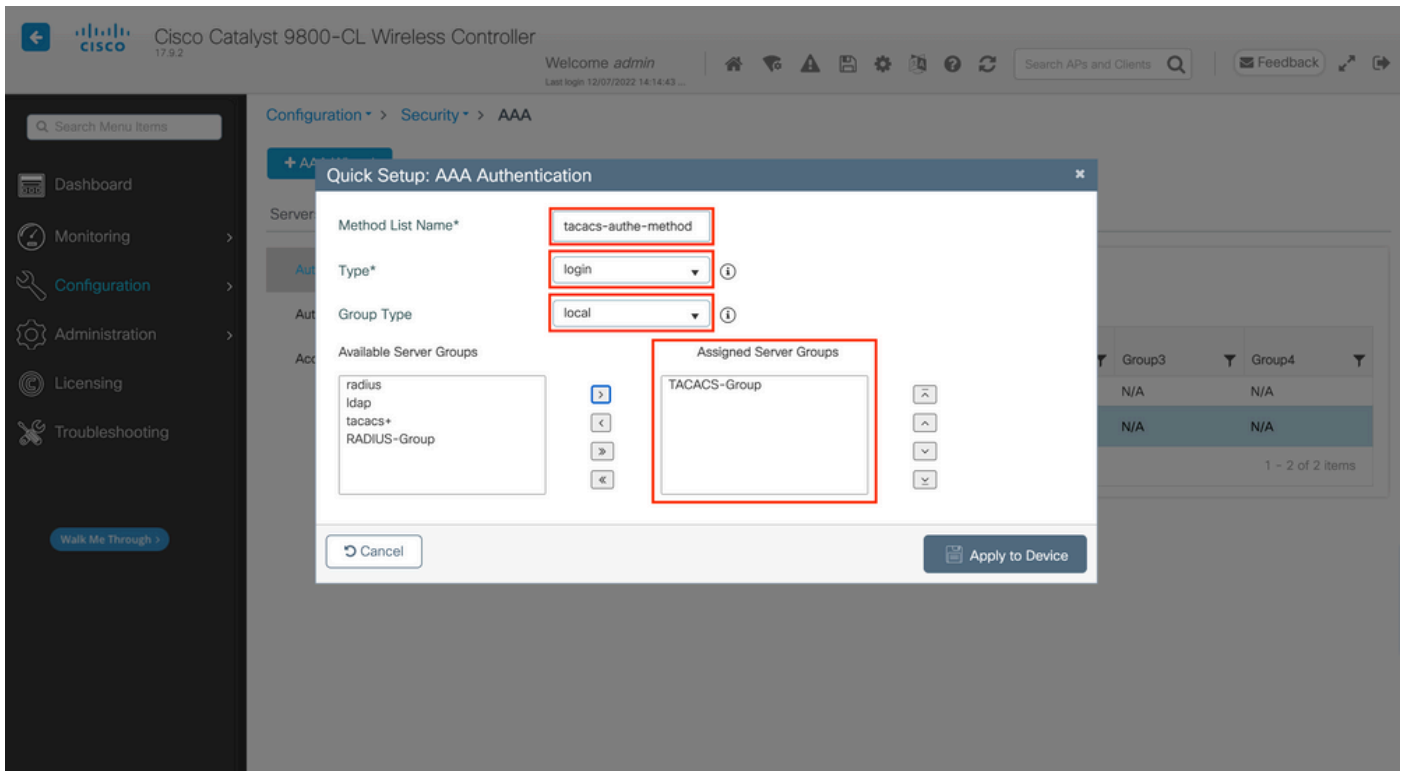
Über GUI:

Navigieren Sie auf der GUI-Seite <https://<WLC-IP>/webui/#/aaa> zur Registerkarte, AAA Method List > Authentication und erstellen Sie eine Authentifizierungsmethode, wie im Bild dargestellt.

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller GUI. The breadcrumb navigation is Configuration > Security > AAA. The 'AAA Method List' tab is active, and the 'Authentication' sub-tab is selected. A '+ Add' button is highlighted with a red box. Below it is a table with the following data:

Name	Type	Group Type	Group1	Group2	Group3	Group4
default	login	local	N/A	N/A	N/A	N/A
radius-auth-method	login	local	RADIUS-Group	N/A	N/A	N/A
tacacs-auth-method	login	local	TACACS-Group	N/A	N/A	N/A

Wenn Sie die Schaltfläche Hinzufügen verwenden, um eine Authentifizierungsmethode zu erstellen, wird wie üblich ein Popup-Fenster für die Konfiguration angezeigt, das dem in diesem Bild dargestellten Fenster ähnelt.



Geben Sie in diesem Popup-Fenster einen Namen für die Methode an, wählen Sie Type as (Typ als) aus, und fügen Sie den im vorherigen Schritt erstellten Gruppenserver der Liste Zugewiesene Servergruppen hinzu. Für das Feld Gruppentyp sind mehrere Konfigurationen möglich.

- Wenn Sie Group Type (Gruppentyp) als local (lokal) auswählen, prüft der WLC zunächst, ob die Benutzeranmeldeinformationen lokal vorhanden sind, und greift dann auf die Servergruppe zurück.
- Wenn Sie Gruppentyp als Gruppe auswählen und nicht die Option Lokal zurückgreifen aktivieren, vergleicht der WLC lediglich die Benutzeranmeldeinformationen mit der Servergruppe.
- Wenn Sie Gruppentyp als Gruppe auswählen und die Option Fallback to local aktivieren, prüft der WLC die Benutzeranmeldeinformationen anhand der Servergruppe und fragt die lokale Datenbank nur ab, wenn der Server nicht antwortet. Wenn der Server eine Ablehnung sendet, muss der Benutzer authentifiziert werden, obwohl er in der lokalen Datenbank vorhanden sein kann.

Aus CLI:

Wenn Sie möchten, dass Benutzeranmeldeinformationen nur dann mit einer Servergruppe geprüft werden, wenn sie nicht zuerst lokal gefunden wurden, verwenden Sie Folgendes:

```
<#root>
```

```
WLC-9800(config)#aaa authentication login
```

tacacs-auth-method

local group

TACACS-Group

Wenn die Benutzeranmeldeinformationen nur mit einer Servergruppe überprüft werden sollen, verwenden Sie Folgendes:

<#root>

WLC-9800(config)#aaa authentication login

tacacs-auth-method

group

TACACS-Group

Wenn Sie möchten, dass die Anmeldeinformationen des Benutzers mit einer Servergruppe geprüft werden, und wenn diese letzte nicht mit einem lokalen Eintrag antwortet, verwenden Sie Folgendes:

<#root>

WLC-9800(config)#aaa authentication login

tacacs-auth-method

group

TACACS-Group

local

In dieser Beispielkonfiguration gibt es einige Benutzer, die nur lokal erstellt werden, und einige Benutzer, die nur auf dem ISE-Server arbeiten. Daher verwenden Sie die erste Option.

Schritt 4: Erstellen Sie eine exec-Methode zur AAA-Autorisierung, die auf die TACACS+-Servergruppe verweist.

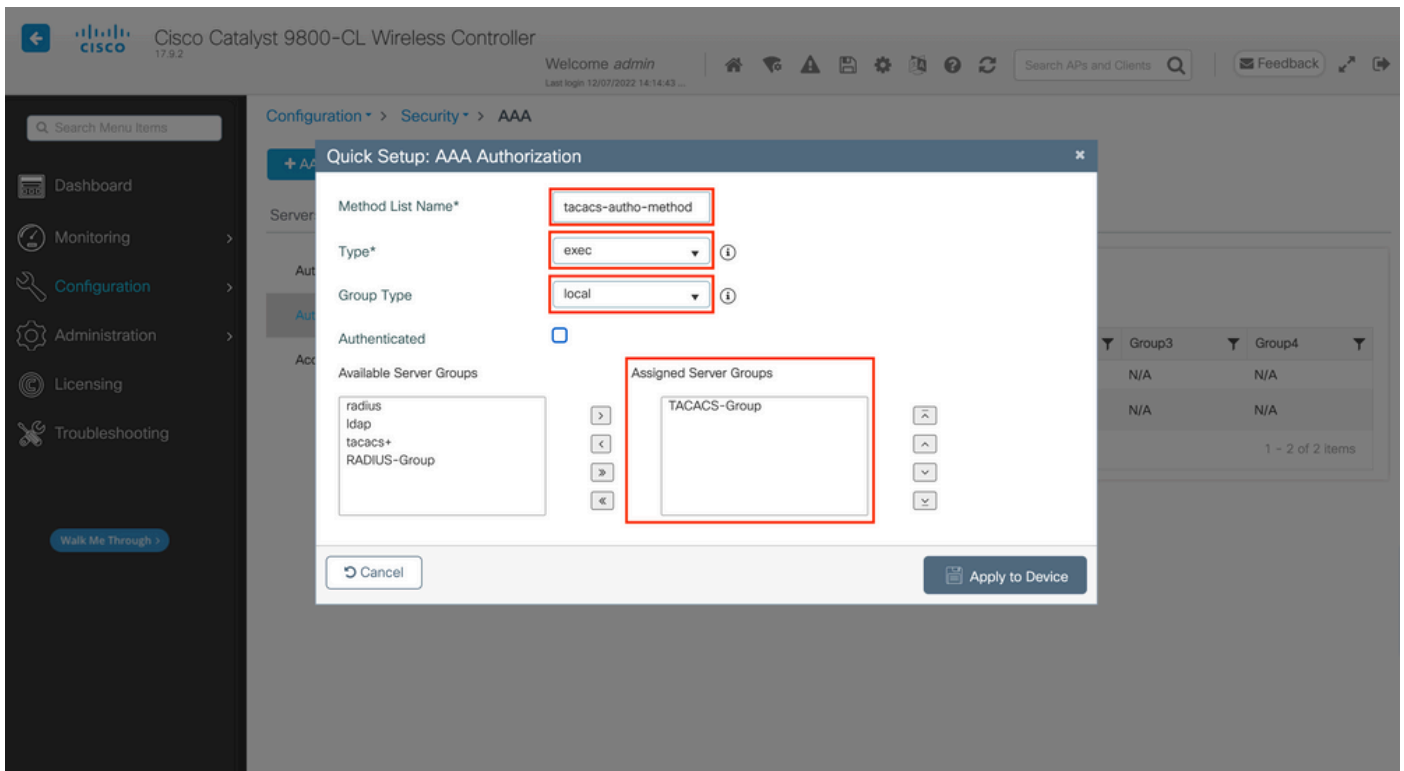
Über GUI:

Der Benutzer muss auch autorisiert werden, um Zugriff zu erhalten. Navigieren Sie auf der GUI-Seite Configuration > Security > AAA zur Registerkarte, AAA Method List > Authorization und erstellen Sie eine Autorisierungsmethode, wie im Bild dargestellt.

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller GUI. The breadcrumb navigation is Configuration > Security > AAA. The 'AAA Method List' tab is selected. The 'Authorization' sub-tab is also selected. The table below shows the configuration for the AAA Method List.

Name	Type	Group Type	Group1	Group2	Group3	Group4
default	exec	local	N/A	N/A	N/A	N/A
radius-auth-method	exec	local	RADIUS-Group	N/A	N/A	N/A
tacacs-auth-method	exec	local	TACACS-Group	N/A	N/A	N/A

Ein Popup-Fenster für die Konfiguration der Autorisierungsmethode, das dem abgebildeten Fenster ähnelt, wird angezeigt, wenn Sie mit der Schaltfläche Hinzufügen eine neue hinzufügen.



Geben Sie in diesem Konfigurations-Popup einen Namen für die Autorisierungsmethode an, wählen Sie Type as (Typ) aus, exec und verwenden Sie die gleiche Reihenfolge von Group Type (Gruppentyp) wie im vorherigen Schritt für die Authentifizierungsmethode.

Aus CLI:

```
<#root>
```

```
WLC-9800(config)#aaa authorization exec
```

```
tacacs-autho-method
```

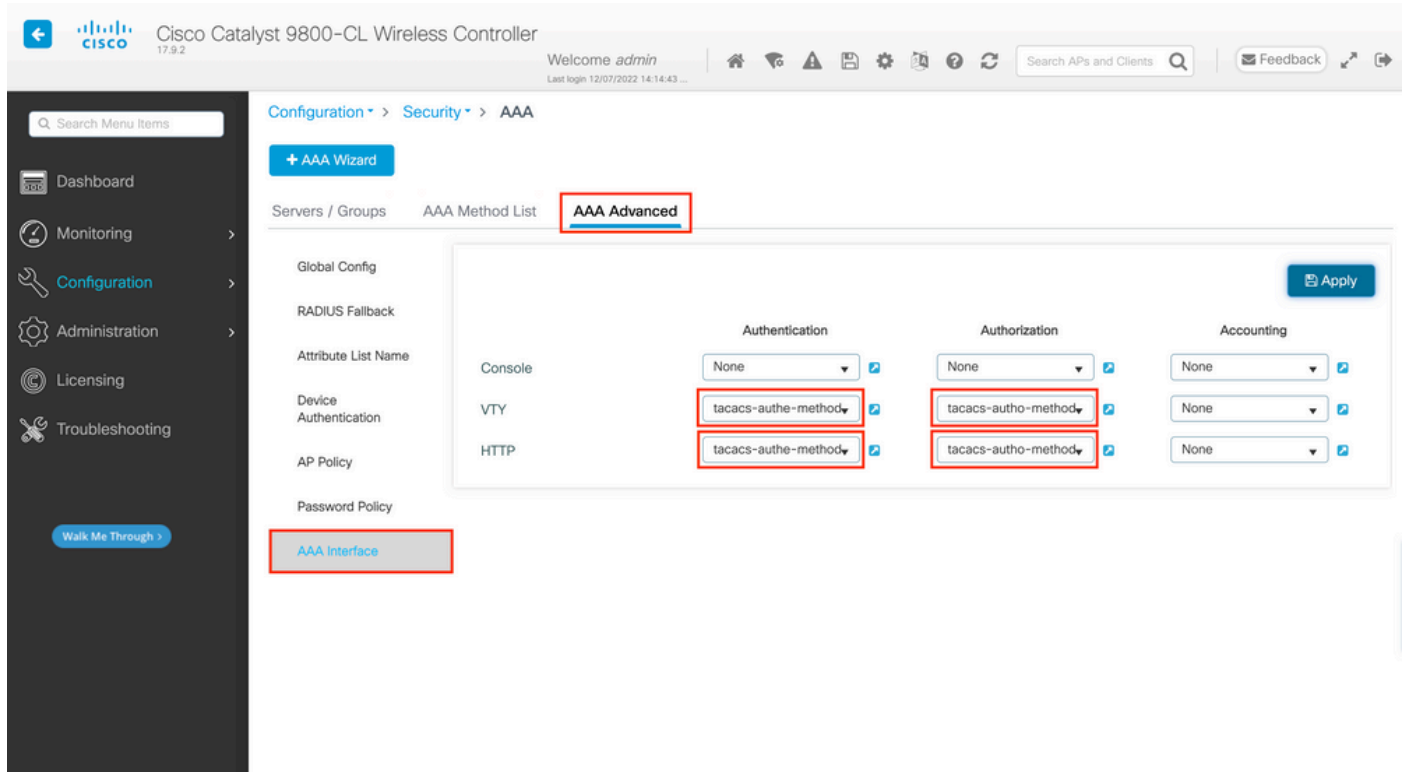
```
local group
```

```
TACACS-Group
```

Schritt 5: Weisen Sie die Methoden den HTTP-Konfigurationen und den für Telnet/SSH verwendeten VTY-Leitungen zu.

Über GUI:

AAA Advanced > AAA Interface Die erstellten Authentifizierungs- und Autorisierungsmethoden können für HTTP- und/oder Telnet-/SSH-Benutzerverbindungen verwendet werden, die über die Registerkarte konfiguriert werden können, die noch von der GUI-WLC-Seite aus zugänglich ist, <https://<WLC-IP>/webui/#/aaa> wie im Bild gezeigt.



Aus CLI:

GUI-Authentifizierung:

<#root>

WLC-9800(config)#ip http authentication aaa login-authentication

tacacs-auth-method

WLC-9800(config)#ip http authentication aaa exec-authorization

tacacs-auth-method

Für Telnet/SSH-Authentifizierung:

```
<#root>
```

```
WLC-9800(config)#line vty 0 15  
WLC-9800(config-line)#login authentication
```

```
tacacs-auth-method
```

```
WLC-9800(config-line)#authorization exec
```

```
tacacs-auth-method
```

Beachten Sie, dass Sie die HTTP- und HTTPS-Dienste am besten neu starten, wenn Änderungen an den HTTP-Konfigurationen vorgenommen werden. Dies kann mit diesen Befehlen erreicht werden.

```
WLC-9800(config)#no ip http server  
WLC-9800(config)#no ip http secure-server  
WLC-9800(config)#ip http server  
WLC-9800(config)#ip http secure-server
```

Konfiguration von TACACS+ ISE

Schritt 1: Konfigurieren des WLC als Netzwerkgerät für TACACS+

Über GUI:

Um den im vorherigen Abschnitt verwendeten WLC als Netzwerkgerät für RADIUS in der ISE zu deklarieren, navigieren Sie zur Registerkarte Network devices (Netzwerkgeräte), und öffnen Sie diese, wie in dieser Abbildung dargestellt. Sie können Administration > Network Resources > Network Devices die Registerkarte Network Devices (Netzwerkgeräte) aufrufen.

The screenshot shows the Cisco ISE Administration interface. The breadcrumb navigation at the top is 'Administration > Network Resources'. The left sidebar has 'Network Devices' selected. The main area displays a table of network devices. One device, 'WLC-9800', is selected. The 'Edit' button is visible above the table.

<input type="checkbox"/>	Name	IP/Mask	Profile Name	Location	Type	Description
<input checked="" type="checkbox"/>	WLC-9800	10.48.39....	Cisco	All Locations	All Device Types	

In diesem Beispiel wurde der WLC bereits für die RADIUS-Authentifizierung hinzugefügt (siehe Schritt 1 im Abschnitt [Konfigurieren der RADIUS-ISE](#)). Aus diesem Grund muss die Konfiguration lediglich geändert werden, um die TACACS-Authentifizierung zu konfigurieren. Dies kann geschehen, wenn Sie den WLC in der Liste der Netzwerkgeräte auswählen und auf die Schaltfläche Bearbeiten klicken. Daraufhin wird das Konfigurationsformular für Netzwerkgeräte geöffnet, wie in dieser Abbildung dargestellt.

The screenshot shows the configuration page for a network device. The 'TACACS Authentication Settings' section is expanded, and the 'Shared Secret' field is highlighted with a red box. Other settings like 'Enable KeyWrap', 'Message Authenticator Code Key', and 'Key Input Format' are also visible.

Enable KeyWrap

Key Encryption Key Show

Message Authenticator Code Key Show

Key Input Format

ASCII HEXADECIMAL

TACACS Authentication Settings

Shared Secret Show

Enable Single Connect Mode

Legacy Cisco Device

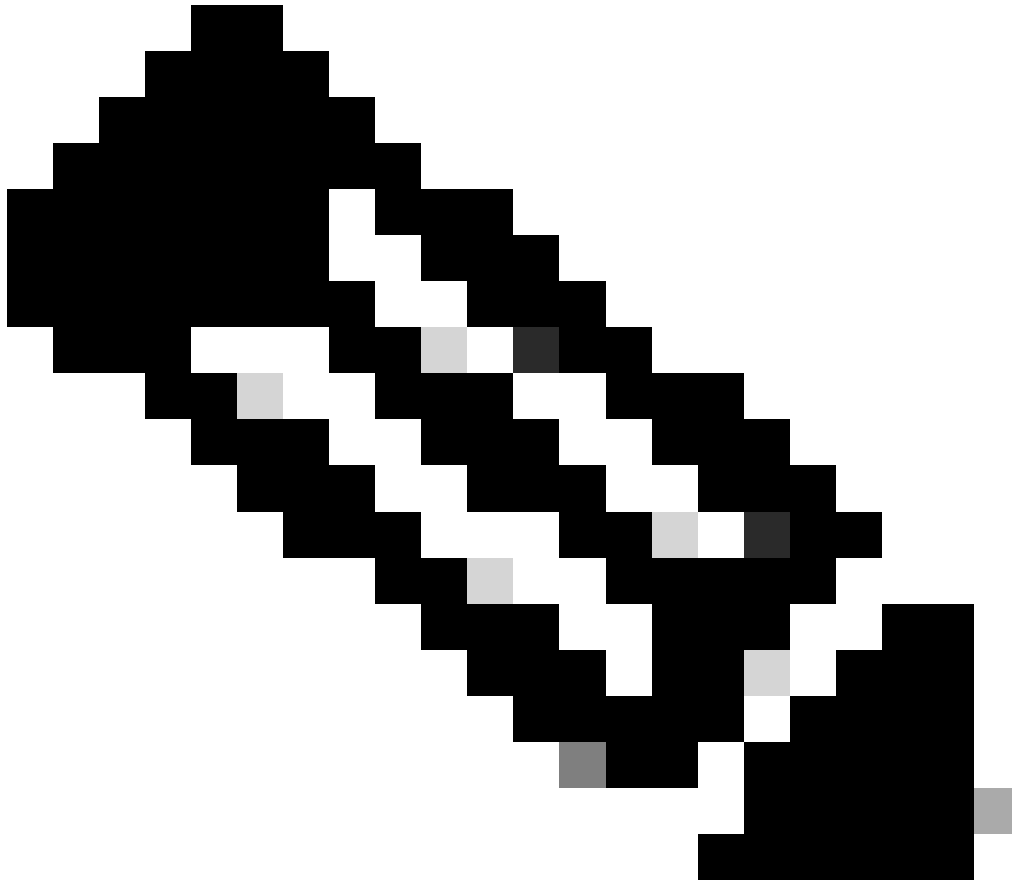
TACACS Draft Compliance Single Connect Support

SNMP Settings

Advanced TrustSec Settings

Wenn das neue Fenster geöffnet wurde, führen Sie einen Bildlauf nach unten zum Abschnitt TACACS Authentication Settings (TACACS-Authentifizierungseinstellungen) durch, aktivieren Sie diese Einstellungen, und fügen Sie den in Schritt 1 des Abschnitts [Configure TACACS+ WLC \(TACACS+ WLC konfigurieren\)](#) eingegebenen gemeinsamen geheimen Schlüssel hinzu.

Schritt 2: Aktivieren Sie die Device Admin-Funktion für den Knoten.



Hinweis: Damit Sie die ISE als TACACS+-Server verwenden können, benötigen Sie ein Device Administration-Lizenzpaket und entweder eine Base- oder eine Mobility-Lizenz.

Über GUI:

Sobald die Device Administration-Lizenzen installiert sind, müssen Sie die Device Admin-Funktion für den Knoten aktivieren, damit die ISE als TACACS+-Server verwendet werden kann. Bearbeiten Sie dazu die Konfiguration des verwendeten ISE-Bereitstellungsknotens (siehe), Administrator > Deployment und klicken Sie auf dessen Namen, oder klicken Sie auf die Edit Schaltfläche.

Deployment



Deployment

PAN Failover

Deployment Nodes

Selected 0 Total 1

Edit Register Syncup Deregister

All

<input type="checkbox"/>	Hostname	Personas	Role(s)	Services	Node Status
<input type="checkbox"/>	ise	Administration, Monitoring, Policy Service	STANDALO...	SESSION,PROFILER	<input checked="" type="checkbox"/>

Wenn das Fenster zur Knotenkonfiguration geöffnet wird, aktivieren Sie die Option Enable Device Admin Service (Geräte-Administratordienst aktivieren) im Abschnitt Policy Service (Richtliniendienst), wie in dieser Abbildung dargestellt.

Deployment

Deployment Nodes List > ise

Edit Node

General Settings Profiling Configuration

Hostname **ise**

FQDN **ise.cisco.com**

IP Address **10.48.39.134**

Node Type **Identity Services Engine (ISE)**

Role **STANDALONE** [Make Primary](#)

Administration

Monitoring

Role **PRIMARY**

Other Monitoring Node _____

Dedicated MnT ⓘ

Policy Service

Enable Session Services ⓘ

Include Node in Node Group **None**

Enable Profiling Service ⓘ

Enable Threat Centric NAC Service ⓘ

Enable SXP Service ⓘ

Enable Device Admin Service ⓘ

Enable Passive Identity Service ⓘ

pxGrid ⓘ

[Reset](#) [Save](#)

Schritt 3: Erstellen Sie TACACS-Profiles, um die Berechtigung zurückzugeben.

Über GUI:

Um Administratorzugriffsrechte zu erhalten, muss deradminuser über eine Privilegstufe von 15 verfügen, die den Zugriff auf die exec-Eingabeaufforderungs-Shell ermöglicht. Auf der anderen Seite benötigt derhelpdeskuser keine exec-Prompt-Shell-Zugriffsrechte und kann daher mit einer Privilegstufe unter 15 zugewiesen werden. Um Benutzern die entsprechende Berechtigungsstufe zuzuweisen, können Autorisierungsprofile verwendet werden. Diese können auf der ISE-GUI-Seite Work Centers > Device Administration > Policy Elements konfiguriert werden, wie im nächsten Bild unter der Registerkarte Results > TACACS Profiles dargestellt.

- Conditions
 - Library Conditions
 - Smart Conditions
- Network Conditions
- Results
 - Allowed Protocols
 - TACACS Command Sets
 - TACACS Profiles**

TACACS Profiles

Rows/Page 6 << 1 >> Go 6 Total Rows

Add Duplicate Trash Edit

<input type="checkbox"/>	Name	Type	Description
<input type="checkbox"/>	Default Shell Profile	Shell	Default Shell Profile
<input type="checkbox"/>	Deny All Shell Profile	Shell	Deny All Shell Profile
<input type="checkbox"/>	IOS Admin	Shell	Assigned to each user in the group admin-group
<input type="checkbox"/>	IOS Helpdesk	Shell	Assigned to each user in the group helpdesk-group
<input type="checkbox"/>	WLC ALL	WLC	WLC ALL
<input type="checkbox"/>	WLC MONITOR	WLC	WLC MONITOR

Um ein neues TACACS-Profil zu konfigurieren, verwenden Sie die Schaltfläche Hinzufügen, über die das neue Profilkonfigurationsformular geöffnet wird, das dem im Bild gezeigten ähnelt. Dieses Formular muss speziell so aussehen, um das Profil zu konfigurieren, das dem adminuser zugewiesen ist (d. h. mit Shell-Berechtigungen der Ebene 15).

TACACS Profiles > IOS Admin
TACACS Profile

Name
IOS Admin

Description
Assigned to each user in the group
admin-group

Task Attribute View Raw View

Common Tasks

Common Task Type Shell

<input checked="" type="checkbox"/> Default Privilege	15	(Select 0 to 15)
<input checked="" type="checkbox"/> Maximum Privilege	15	(Select 0 to 15)
<input type="checkbox"/> Access Control List		
<input type="checkbox"/> Auto Command		
<input type="checkbox"/> No Escape		(Select true or false)
<input type="checkbox"/> Timeout		Minutes (0-9999)
<input type="checkbox"/> Idle Time		Minutes (0-9999)

Custom Attributes

Add Trash Edit

Type	Name	Value
No data found.		

Cancel Save

Wiederholen Sie den Vorgang für das helpdesk Profil. Für diese letzte Option werden die Standardberechtigung und die maximale Berechtigung auf 1 festgelegt.

Schritt 4: Erstellen Sie Benutzergruppen auf der ISE.

Dies ist dasselbe wie in Schritt 3 des Abschnitts [Konfigurieren](#) der [RADIUS-ISE](#) in diesem Dokument.

Schritt 5: Erstellen Sie die Benutzer auf der ISE.

Dies ist dasselbe wie in Schritt 4 des Abschnitts [Konfigurieren](#) der [RADIUS-ISE](#) in diesem Dokument.


Schritt 6: Erstellen eines Richtlinienatzes für die Geräteadministration.

Über GUI:

Für den RADIUS-Zugriff müssen nach der Erstellung der Benutzer ihre Authentifizierungs- und Autorisierungsrichtlinien auf der ISE definiert werden, um ihnen die richtigen Zugriffsrechte zu gewähren. Für die TACACS-Authentifizierung werden zu diesem Zweck Geräte-Admin-Richtliniensätze verwendet, die wie dargestellt über das konfiguriert werden können Work Centers > Device Administration > Device Admin Policy Sets GUI Page.

Policy Sets

Reset [Reset Policyset Hitcounts](#) [Save](#)

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
							
	Search						
	WLC TACACS Authentication		 Network Access-Device IP Address EQUALS 10.48.39.133	Default Device Admin   	0		
	Default	Tacacs Default policy set		Default Device Admin   	0		

[Reset](#) [Save](#)

Um einen Richtlinienatz für die Geräteadministration zu erstellen, verwenden Sie die rot umrahmte Schaltfläche "Hinzufügen" im vorherigen Bild. Dadurch wird der Liste der Richtlinienätze ein Element hinzugefügt. Geben Sie einen Namen für den neu erstellten Satz, eine Bedingung, unter der er angewendet werden muss, und die zulässige Protokolle-/Serversequenz an (hier reicht die Default Device Admin aus). Verwenden Sie die Save Schaltfläche, um das Hinzufügen des Richtlinienatzes abzuschließen, und verwenden Sie die Pfeilspitze auf der rechten Seite, um auf die Konfigurationsseite zuzugreifen, wie es auf der abgebildeten Seite aussieht.

Policy Sets → **WLC TACACS Authentication**

Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✔	WLC TACACS Authentication		Network Access-Device IP Address EQUALS 10.48.39.133	Default Device Admin	0

Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
✔	Default		All_User_ID_Stores > Options	0	⚙️

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (3)

Status	Rule Name	Conditions	Results			Hits	Actions
			Command Sets	Shell Profiles			
✔	Helpdesk users authorization	InternalUser-IdentityGroup EQUALS User Identity Groups:helpdesk-group	AllowAllCommands	IOS Helpdesk	0	⚙️	
✔	Admin users authorization	InternalUser-IdentityGroup EQUALS User Identity Groups:admin-group	AllowAllCommands	IOS Admin	0	⚙️	
✔	Default		DenyAllCommands	Deny All Shell Profile	0	⚙️	

Reset Save

Der spezifische Richtlinienatz "WLC TACACS Authentication" in diesem Beispiel filtert Anforderungen mit der IP-Adresse, die der IP-Adresse des C9800-Beispiels entspricht.

Als Authentifizierungsrichtlinie wurde die Standardregel beibehalten, da sie den Anforderungen des Anwendungsfalls entspricht. Es wurden zwei Autorisierungsregeln festgelegt:

- Die erste wird ausgelöst, wenn der Benutzer zur definierten Gruppe admin-group gehört. Es lässt alle Befehle zu (über die StandardPermit_all-Regel) und weist Privileg 15 zu (über das definierte IOS_Admin TACACS-Profil).
- Die zweite wird ausgelöst, wenn der Benutzer zur definierten Gruppe helpdesk-group gehört. Es lässt alle Befehle zu (über die Standard-Permit_all Regel) und weist die Berechtigung 1 zu (über das definierte IOS_Helpdesk TACACS-Profil).

Nach Abschluss dieses Schritts können die für konfigurierten Anmeldeinformationen adminuser undhelpdesk Benutzer über die GUI oder mit

Telnet/SSH für die Authentifizierung im WLC verwendet werden.

Fehlerbehebung

Wenn Ihr RADIUS-Server erwartet, dass das RADIUS-Dienstattribut gesendet wird, können Sie dem WLC Folgendes hinzufügen:

```
radius-server attribute 6 on-for-login-auth
```

Fehlerbehebung bei Zugriff auf die WLC-GUI oder CLI RADIUS/TACACS+ über die WLC-CLI

Zur Fehlerbehebung beim TACACS+-Zugriff auf die WLC-GUI oder -CLI geben Sie den Befehl zusammen mit demdebug tacacs Terminal Monitor ein, und zeigen Sie die Live-Ausgabe an, wenn ein Anmeldeversuch unternommen wird.

Diese Ausgabe wird beispielsweise durch eine erfolgreiche Anmeldung und ein anschließendes Abmelden desadminuser Benutzers generiert.

```
<#root>
```

```
WLC-9800#
```

```
terminal monitor
```

```
WLC-9800#
```

```
debug tacacs
```

```
TACACS access control debugging is on
```

```
WLC-9800#
```

```
Dec 8 11:38:34.684: TPLUS: Queuing AAA Authentication request 15465 for processing
```

```
Dec 8 11:38:34.684: TPLUS(00003C69) login timer started 1020 sec timeout Dec 8 11:38:34.684: TPLUS: pro
```

Aus diesen Protokollen geht hervor, dass der TACACS+-Server die korrekten Berechtigungen zurückgibt (diese sind AV priv-lvl=15).

Wenn Sie die RADIUS-Authentifizierung durchführen, wird eine ähnliche Debugausgabe angezeigt, die den RADIUS-Datenverkehr betrifft.

Die Befehle debug aaa authentication und debug aaa authorization stattdessen zeigen, welche Methodenliste vom WLC beim Anmeldeversuch

des Benutzers ausgewählt wird.

Fehlerbehebung bei WLC-GUI- oder CLI-TACACS+-Zugriff über die ISE-GUI

Von Seite Operations > TACACS > Live Logs aus kann jede Benutzerauthentifizierung, die mit TACACS+ bis zu den letzten 24 Stunden durchgeführt wurde, angezeigt werden. Um die Details einer TACACS+-Autorisierung oder -Authentifizierung zu erweitern, verwenden Sie die Schaltfläche Details zu diesem Ereignis.

The screenshot shows the Cisco ISE interface for TACACS+ logs. The 'Live Logs' tab is selected. The table displays the following data:

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	N
Dec 08, 2022 06:51:46.1...	✓		helpdeskuser	Authorization		WLC TACACS Authentication >...	ise	W
Dec 08, 2022 06:51:46.0...	✓		helpdeskuser	Authentication	WLC TACACS Authentication >...		ise	W
Dec 08, 2022 06:38:38.2...	✓		adminuser	Authorization		WLC TACACS Authentication >...	ise	W
Dec 08, 2022 06:38:38.1...	✓		adminuser	Authentication	WLC TACACS Authentication >...		ise	W
Dec 08, 2022 06:34:54.0...	✓		adminuser	Authorization		WLC TACACS Authentication >...	ise	W
Dec 08, 2022 06:34:53.9...	✓		adminuser	Authentication	WLC TACACS Authentication >...		ise	W

Additional interface elements include: 'Operations · TACACS' breadcrumb, 'Evaluation Mode 82 Days' warning, 'Refresh Never', 'Show Latest 20 records', 'Within Last 3 hours', 'Export To' button, and 'Filter' options. The bottom status bar shows 'Last Updated: Thu Dec 08 2022 12:57:09 GMT+0100 (Central European Standard Time)' and 'Records Shown: 6'.

Bei der Erweiterung sieht ein erfolgreicher Authentifizierungsversuch für diehelpdeskuser wie folgt aus:

Overview

Request Type	Authentication
Status	Pass
Session Key	ise/459637517/243
Message Text	Passed-Authentication: Authentication succeeded
Username	helpdeskuser
Authentication Policy	WLC TACACS Authentication >> Default
Selected Authorization Profile	IOS Helpdesk

Authentication Details

Generated Time	2022-12-08 06:51:46.077000 -05:00
Logged Time	2022-12-08 06:51:46.077
Epoch Time (sec)	1670500306
ISE Node	ise
Message Text	Passed-Authentication: Authentication succeeded
Failure Reason	
Resolution	
Root Cause	
Username	helpdeskuser
Network Device Name	WLC-9800
Network Device IP	10.48.39.133
Network Device Groups	IPSEC#Is IPSEC Device#No,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	tty5
Remote Address	10.61.80.151

Steps

```

13013 Received TACACS+ Authentication START Request
15049 Evaluating Policy Group
15008 Evaluating Service Selection Policy
15048 Queried PIP - Network Access.Device IP Address
15041 Evaluating Identity Policy
22072 Selected identity source sequence - All_User_ID_Stores
15013 Selected Identity Source - Internal Users
24210 Looking up User in Internal Users IDStore
24212 Found User in Internal Users IDStore
13045 TACACS+ will use the password prompt from global
TACACS+ configuration
13015 Returned TACACS+ Authentication Reply
13014 Received TACACS+ Authentication CONTINUE Request (
🚫 Step latency=3149ms)
15041 Evaluating Identity Policy
22072 Selected identity source sequence - All_User_ID_Stores
15013 Selected Identity Source - Internal Users
24210 Looking up User in Internal Users IDStore
24212 Found User in Internal Users IDStore
22037 Authentication Passed
15036 Evaluating Authorization Policy
15048 Queried PIP - Network Access.UserName
15048 Queried PIP - InternalUser.IdentityGroup
13015 Returned TACACS+ Authentication Reply

```

Daraus können Sie erkennen, dass der Benutzer helpdeskuser mithilfe der Authentifizierungsrichtlinie erfolgreich auf dem Netzwerkgerät WLC-9800 authentifiziert wurde WLC TACACS Authentication > Default. Ferner wurde diesem Benutzer das Autorisierungsprofil IOS Helpdesk zugewiesen und ihm die Privilegstufe 1 gewährt.

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.