

9800 WLC上でのGUI用RADIUS & TACACS+の & CLI認証の設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[読み取り専用ユーザの制限](#)

[WLC用のRADIUS認証の設定](#)

[RADIUS用のISEの設定](#)

[TACACS+ WLCの設定](#)

[TACACS+ ISEの設定](#)

[トラブルシューティング](#)

[WLC CLIを介したWLC GUIまたはCLI RADIUS/TACACS+アクセスのトラブルシューティング](#)

[ISE GUIを介したWLC GUIまたはCLITACACS+アクセスのトラブルシューティング](#)

はじめに

このドキュメントでは、RADIUSまたはTACACS+外部認証用にCatalyst 9800を設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Catalyst Wireless 9800設定モデル
- AAA、RADIUS、およびTACACS+の概念

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- C9800-CL v17.9.2
- ISE 3.2.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

ユーザがWLCのCLIまたはGUIにアクセスしようとする時、ユーザ名とパスワードの入力を求められます。デフォルトでは、これらのクレデンシャルは、デバイス自体に存在するユーザのローカルデータベースと比較されます。または、入力クレデンシャルをリモートAAAサーバと比較するようにWLCに指示することもできます。WLCは、RADIUSまたはTACACS+を使用してサーバと通信できます。

設定

この例では、AAAサーバ(ISE)上の2種類のユーザ、それぞれadminuserとhelpdeskuserが設定されます。これらのユーザは、それぞれのadmin-groupとhelpdesk-groupのグループに属しています。admin-groupの一部であるユーザadminuserには、WLCへのフルアクセス権が付与される必要があります。一方、helpdeskuserはhelpdesk-groupの一部で、WLCに対するモニタ権限のみを付与します。したがって、設定にアクセスすることはできません。

この記事では、最初にRADIUS認証用にWLCとISEを設定し、後でTACACS+用に同じ設定を行います。

読み取り専用ユーザの制限

TACACS+またはRADIUSを9800 WebUI認証に使用する場合、次の制限があります。

- 特権レベル0のユーザが存在するが、GUIにアクセスできない

-

特権レベル1 ~ 14のユーザは、Monitorタブのみを表示できます（これは、ローカルで認証された読み取り専用ユーザの特権レベルに相当します）

-

特権レベル15のユーザはフルアクセスが可能

-

特権レベル15を持ち、特定のコマンドのみを許可するコマンドセットを持つユーザはサポートされません。ユーザは、引き続きWebUIを使用して設定変更を実行できます

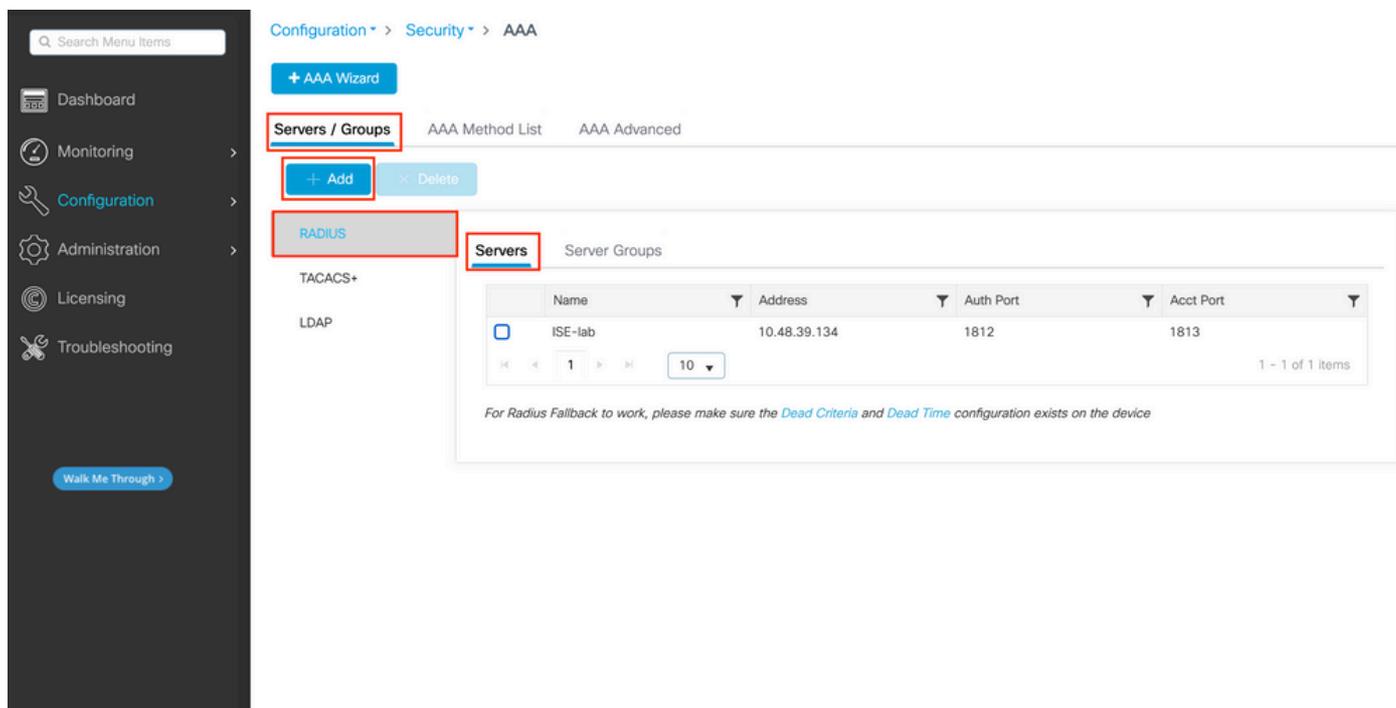
これらの考慮事項は変更または変更できません。

WLC用のRADIUS認証の設定

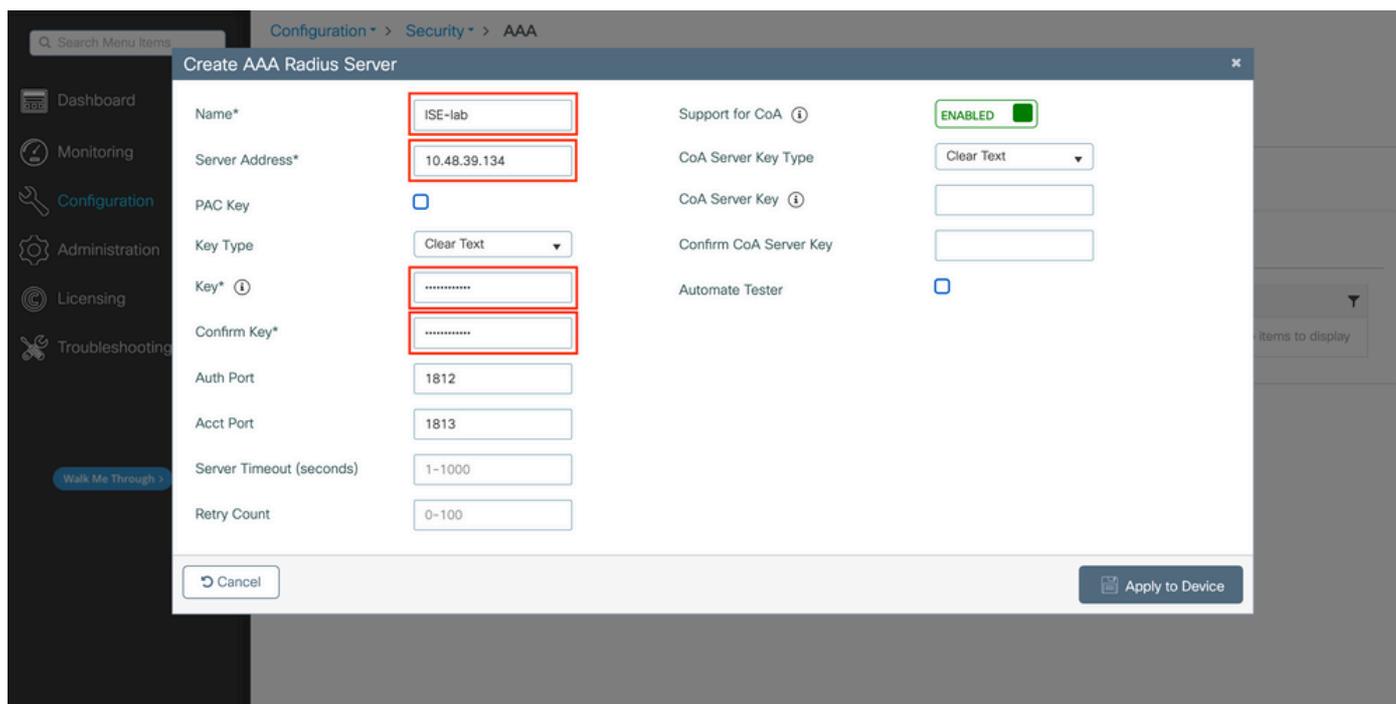
ステップ 1 : RADIUSサーバを宣言します。

GUI から :

まず、WLC上にISE RADIUSサーバを作成します。 これを行うには、<https://<WLC-IP>/webui/#/aaa>でアクセス可能なGUI WLCページのタブServers/Groups > RADIUS > Serversを使用するか、Configuration > Security > AAA(WLC)に移動します (下図参照)。



WLCにRADIUSサーバを追加するには、図の赤いフレームで囲まれたAddボタンをクリックします。これにより、スクリーンショットに示されたポップアップウィンドウが開きます。



このポップアップウィンドウでは、次の項目を指定する必要があります。

- サーバ名 (ISEシステム名と一致する必要はありません)
- サーバIPアドレス
- WLCとRADIUSサーバ間の共有秘密

認証やアカウントリングに使用されるポートなど、その他のパラメータも設定できますが、これらは必須ではなく、このドキュメントではデフォルトのままになっています。

CLI から :

<#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

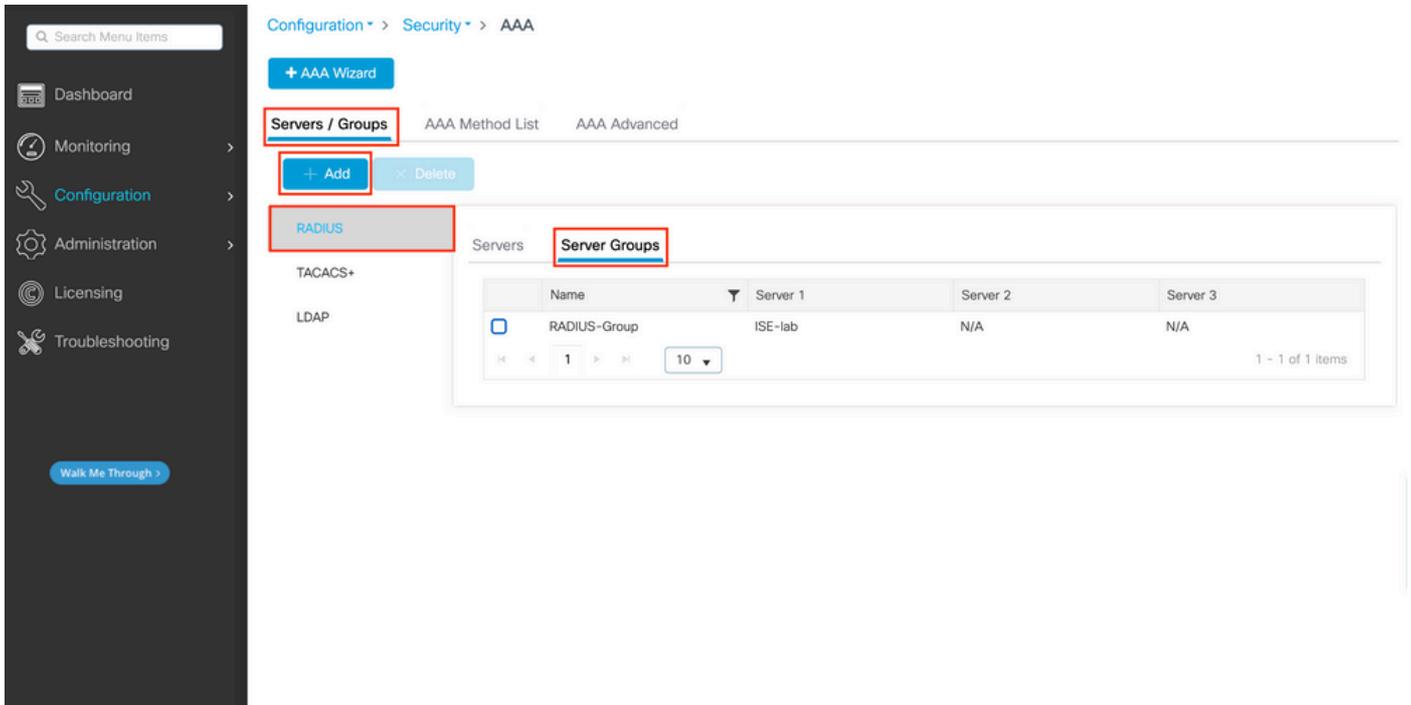
WLC-9800(config-radius-server)#key

Cisco123

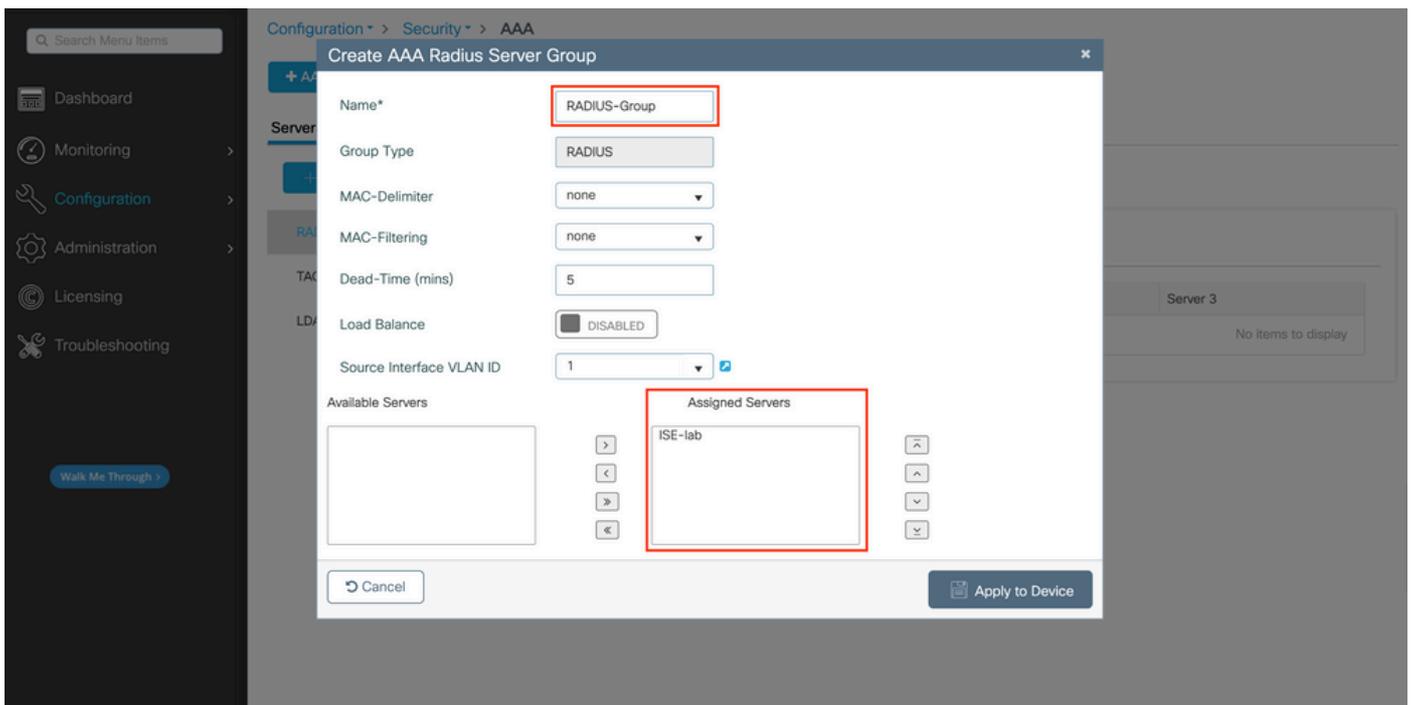
ステップ 2 : RADIUSサーバをサーバグループにマッピングします。

GUI から :

認証に使用できる複数のRADIUSサーバがある場合は、すべてのサーバを同じサーバグループにマッピングすることを推奨します。WLCは、サーバグループ内のサーバ間で異なる認証のロードバランシングを行います。RADIUSサーバグループは、図に示すように、ステップ1で説明したものと同一GUIページのServers/Groups > RADIUS > Server Groupsタブで設定します。



サーバの作成では、次に示すAddボタン（前の図でフレーム化されています）をクリックすると、ポップアップウィンドウが表示されます。



ポップアップでグループに名前を付け、目的のサーバを「割り当てられたサーバ」リストに移動します。

CLI から :

<#root>

WLC-9800(config)# aaa group server radius

RADIUS-Group

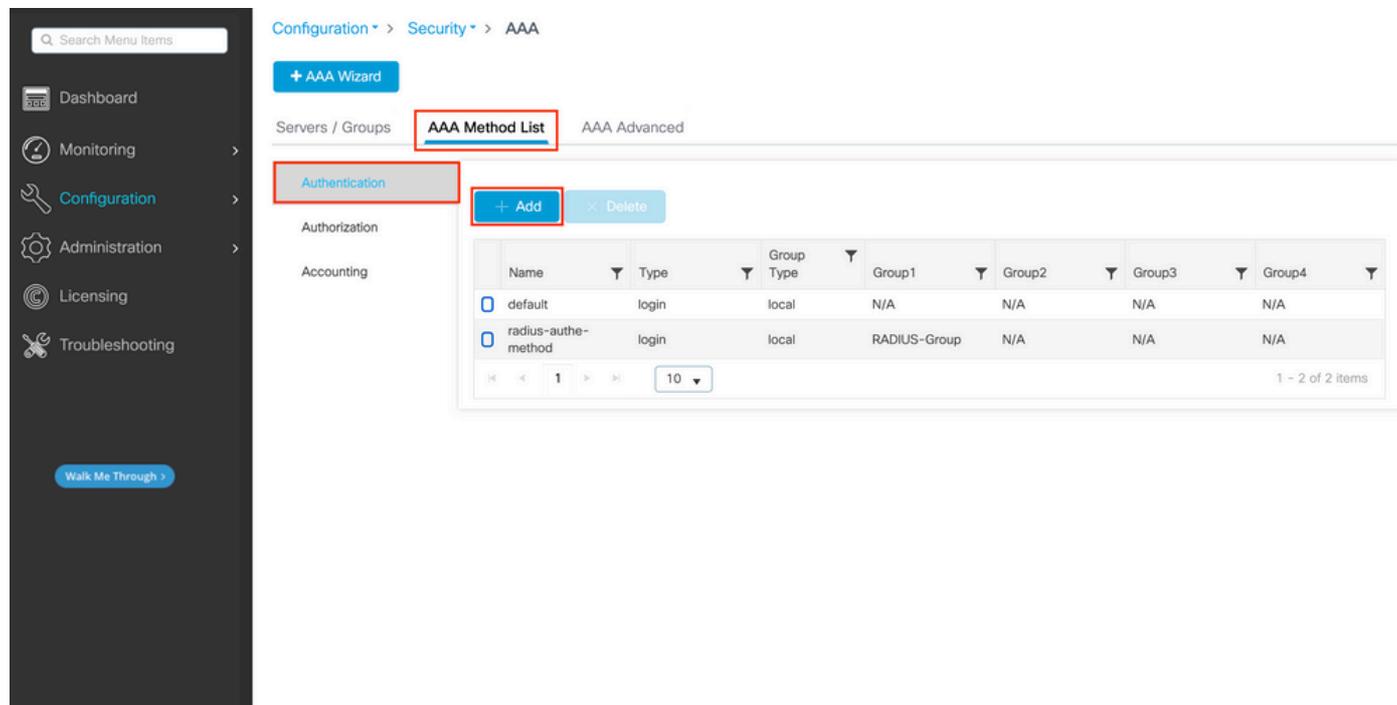
WLC-9800(config-sg-radius)# server name

ISE-lab

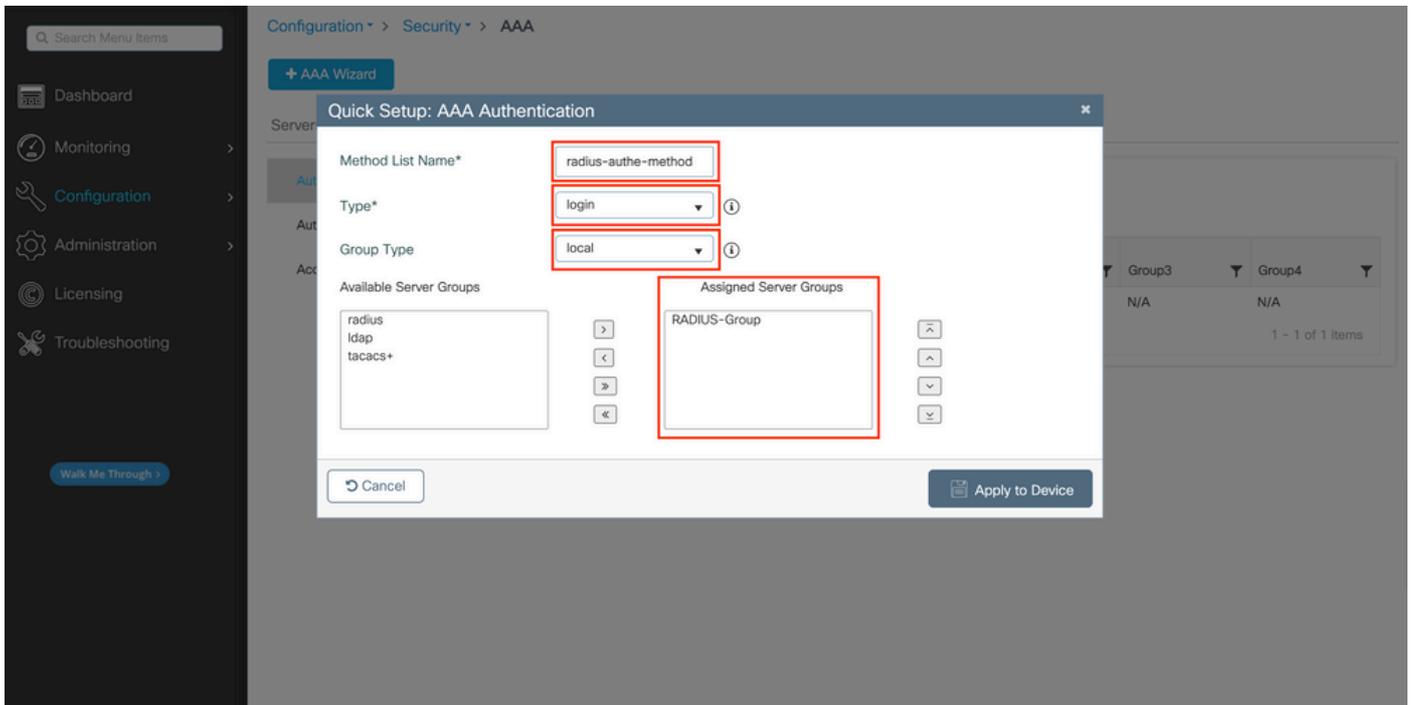
ステップ 3 : RADIUSサーバグループをポイントするAAA認証ログインメソッドを作成します。

GUI から :

引き続きGUIページから<https://<WLC-IP>/webui/#/aaa>、AAA Method List > Authenticationタブに移動し、次の図に示すように認証方式を作成します。



通常どおり、Addボタンを使用して認証方式を作成すると、次の図に示すような設定ポップアップウィンドウが表示されます。



このポップアップウィンドウで、メソッドの名前を指定します。Type as log inを選択し、前の手順で作成したグループサーバを Assigned Server Groups のリストに追加します。Group Type フィールドについては、いくつかの設定が可能です。

- グループタイプとしてローカルを選択した場合、WLCは最初にユーザクレデンシャルがローカルに存在するかどうかをチェックし、次にサーバグループにフォールバックします。
- グループとしてGroup Typeを選択し、Fall back to localオプションをチェックしない場合、WLCではサーバグループに対してユーザクレデンシャルがチェックされるだけです。
- グループとしてGroup Typeを選択し、Fallback to localオプションをチェックすると、WLCはサーバグループに対してユーザクレデンシャルをチェックし、サーバが応答しない場合にだけローカルデータベースに照会します。サーバがrejectを送信すると、ローカルデータベースに存在できるユーザであっても、そのユーザは認証されます。

CLI から :

ユーザクレデンシャルが最初にローカルで見つからない場合にのみ、サーバグループでユーザクレデンシャルをチェックするには、次のコマンドを使用します。

```
<#root>
```

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

```
radius-auth-method
```

local group

RADIUS-Group

ユーザクレデンシャルをサーバグループでのみチェックする場合は、次のコマンドを使用します。

<#root>

WLC-9800(config)#aaa authentication login

radius-auth-method

group

RADIUS-Group

ユーザクレデンシャルをサーバグループでチェックし、この最後のエントリがローカルエントリで応答しない場合は、次のコマンドを使用します。

<#root>

WLC-9800(config)#aaa authentication login

radius-auth-method

group

RADIUS-Group

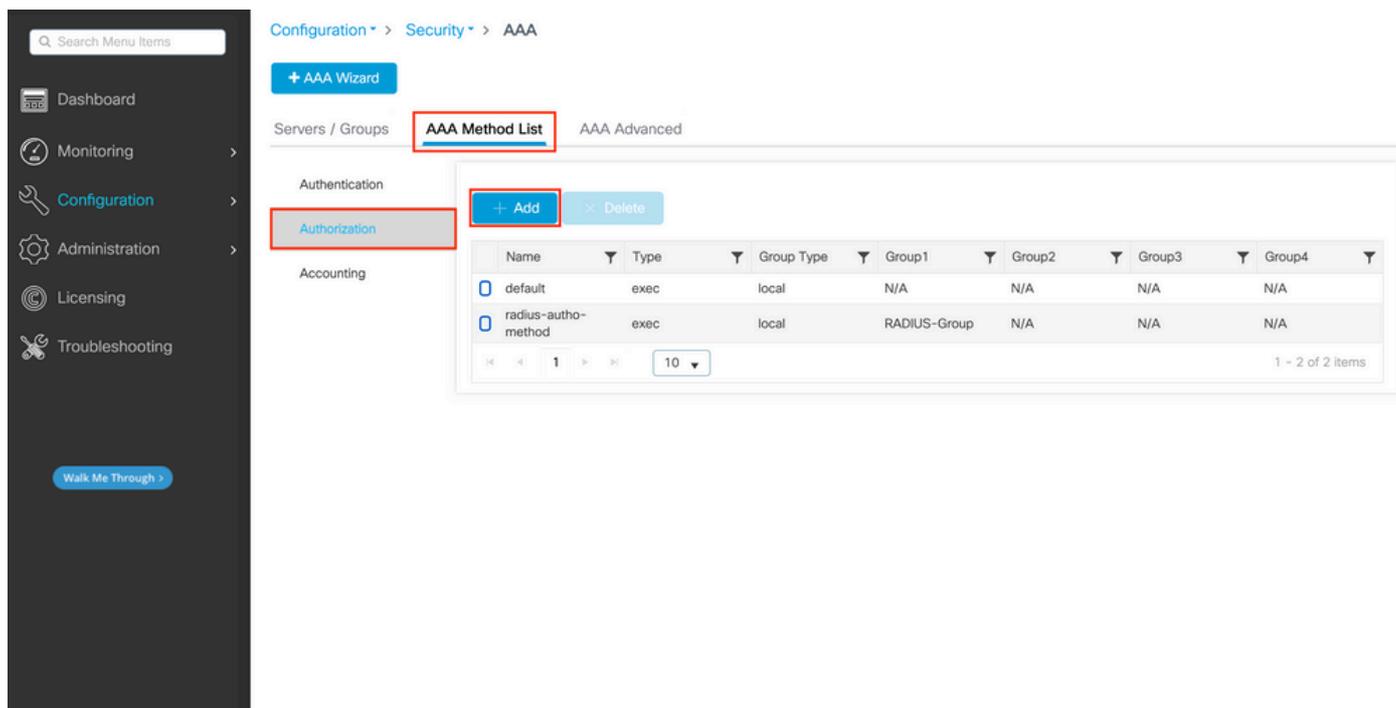
local

この設定例では、ローカルでのみ作成されるユーザとISEサーバでのみ作成されるユーザが存在するため、最初のオプションを使用します。

ステップ 4 : RADIUSサーバグループをポイントするAAA認可EXEC方式を作成します。

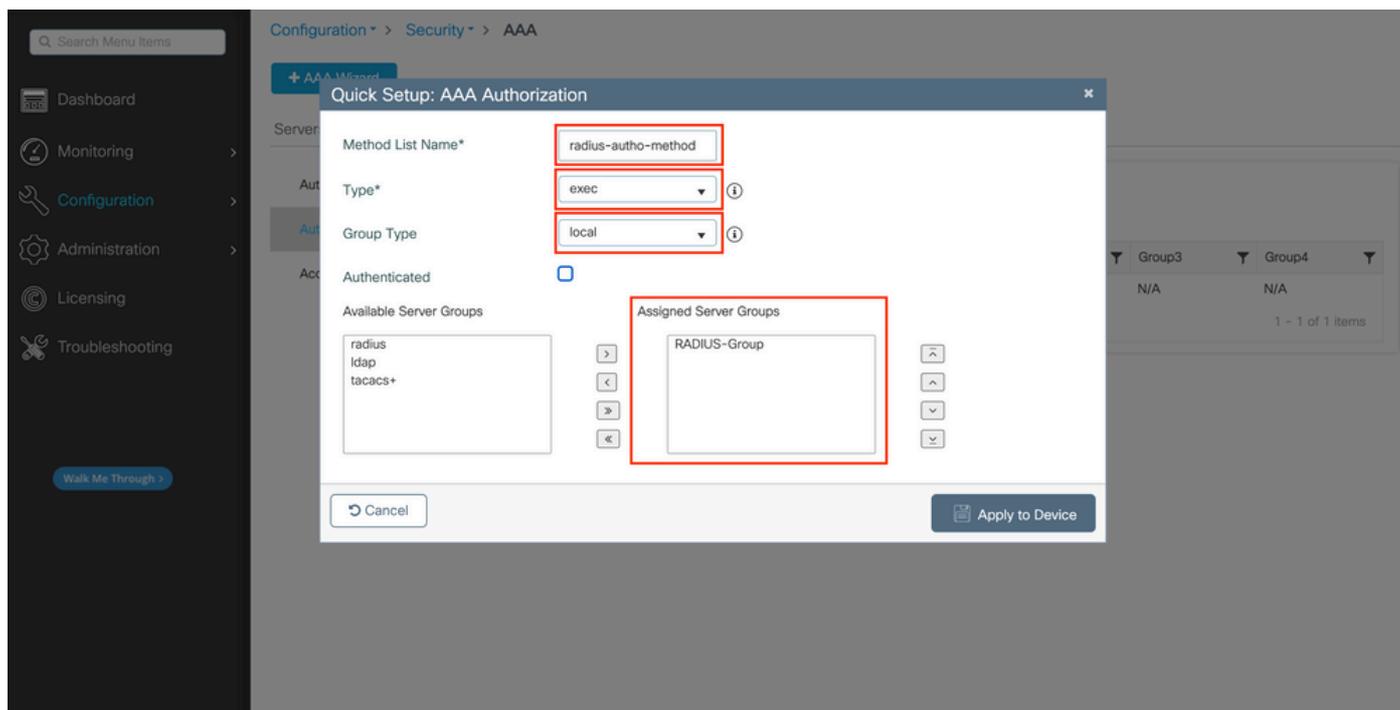
GUI から :

アクセス権を付与するには、ユーザも承認されている必要があります。引き続きGUI Page Configuration > Security > AAAから、AAA Method List > Authorizationタブに移動し、次の図に示すように認可方式を作成します。



許可方式の作成

Addボタンを使用して新しい認証方式を追加すると、図に示すような認証方式設定のポップアップが表示されます。



この設定ポップアップで、許可方式の名前を指定し、タイプとしてexecを選択し、ステップ3で認証方式に使用したものと同じグループタイプの順序を使用します。

CLI から :

認証方式では、最初に認可が割り当てられ、ユーザがローカルエントリと照合され、次にサーバグループのエントリと照合されます。

<#root>

WLC-9800(config)#aaa authorization exec

radius-autho-method

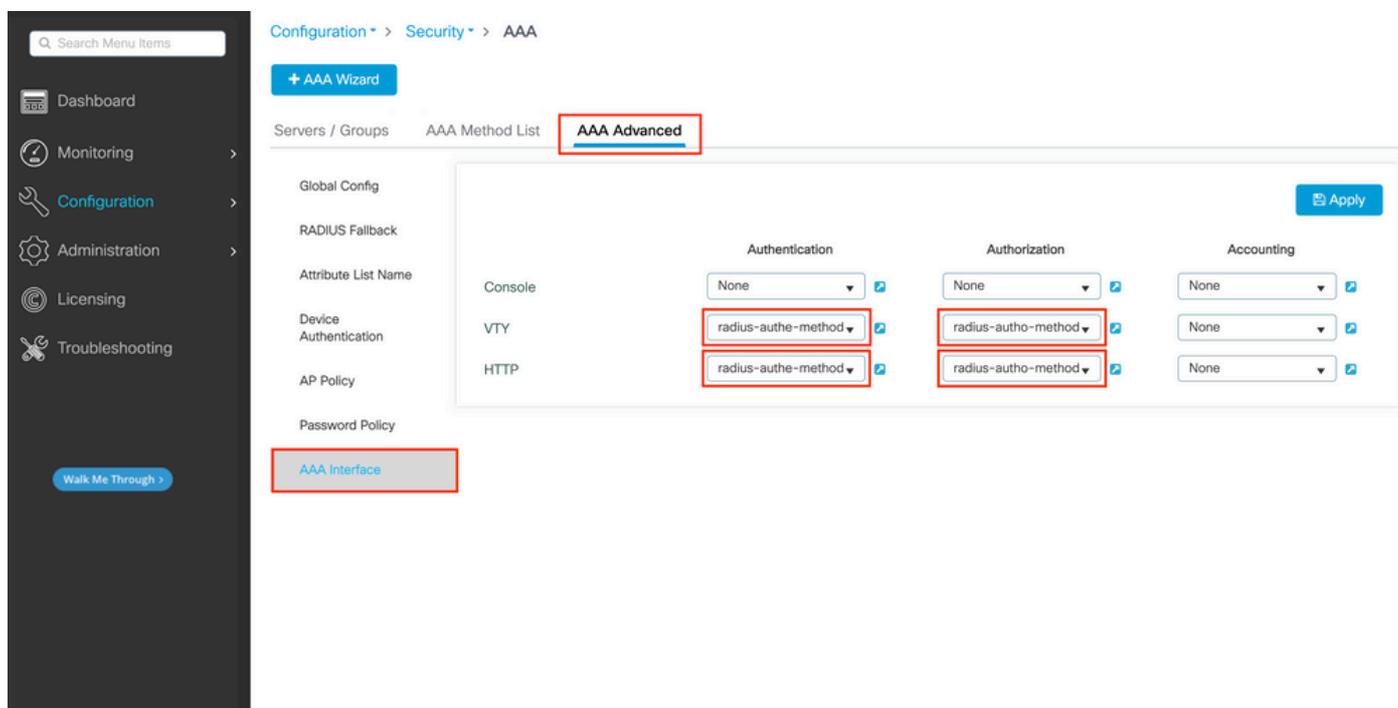
local group

RADIUS-Group

ステップ 5 : HTTP設定およびTelnet/SSHに使用するVTY回線にメソッドを割り当てます。

GUI から :

作成された認証および許可方式は、HTTPまたはTelnet/SSHユーザ接続に使用できます。これは、次の図に示すように、AAA Advanced > AAA Interfaceタブから、まだhttps://<WLC-IP>/webui/#/aaaでアクセス可能なGUI WLCページから設定できます。



GUI認証用CLI:

```
<#root>
```

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

```
radius-auth-method
```

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

```
radius-autho-method
```

Telnet/SSH認証用CLI:

```
<#root>
```

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

```
radius-auth-method
```

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

```
radius-autho-method
```

HTTP設定を変更した場合は、HTTPおよびHTTPSサービスを再起動するのが最善の方法です。これは、次のコマンドを使用して実行できます。

```
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
```

RADIUS用のISEの設定

ステップ 1 : WLCをRADIUS用のネットワークデバイスとして設定します。

GUIから :

前のセクションで使用したWLCをISEのRADIUSのネットワークデバイスとして宣言するには、次の図に示すように、Administration > Network Resources > Network Devicesに移動し、Network devicesタブを開きます。

Network Devices

Selected 0 Total 1

[Edit](#) [+ Add](#) [Duplicate](#) [Import](#) [Export](#) [Generate PAC](#) [Delete](#)

All

<input type="checkbox"/>	Name	IP/Mask	Profile Name	Location	Type	Description
<input type="checkbox"/>	WLC-9800	10.48.39.133/32	Cisco	All Locations	All Device Types	

ネットワークデバイスを追加するには、[追加]ボタンを使用して、新しいネットワークデバイス設定フォームを開きます。

Network Devices List > New Network Device

Network Devices

Name

Description

IP Address * IP:

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

新しいウィンドウで、ネットワークデバイスの名前を入力し、そのIPアドレスを追加します。RADIUS Authentication Settingsを選択し、WLCで使用されているものと同じRADIUS共有秘密を設定します。

ステップ 2 : 特権を返す許可結果を作成します。

GUI から :

管理者のアクセス権を持つには、adminuserに特権レベル15が必要です。これにより、execプロンプトシェルにアクセスできます。一方、helpdeskuserはexecプロンプトのシェルアクセスを必要としないため、15より低い特権レベルで割り当てることができます。適切な特権レベルをユーザに割り当てするには、認可プロファイルを使用できます。これらは、次の図に示すタブのISE GUI Page Policy > Policy Elements > Resultsで設定Authorization > Authorization Profilesできます。

Dictionaries 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

新しい認可プロファイルを設定するには、新しい認可プロファイル設定フォームを開くAddボタンを使用します。adminuserに割り当てられるプロファイルを設定するには、このフォームが特に次のように表示される必要があります。

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

この設定では、関連付けられているすべてのユーザに特権レベル15が付与されます。すでに説明したように、これは次の手順で作成されるadminuserの正常な動作です。ただし、helpdeskuserにはより低い特権レベルが必要なので、2番目のポリシー要素を作成する必要があります。

helpdeskuserのポリシー要素は、文字列をshell:priv-lvl=Xに変更し、Xを目的の権限レベルに置き換える必shell:priv-lvl=15 要件がある点を除き、上で作成したようなものです。この例では、1 が使用されます。

ステップ 3 : ISEでユーザグループを作成します。

GUIで次の手順を実行します。

ISEユーザグループは、画面キャプチャに示されているAdministration > Identity Management > Groups GUI PageのタブUser Identity Groupsから作成されます。

Administration · Identity Management

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

Identity Groups

EQ

< [Home] [Settings]

> Endpoint Identity Groups

> **User Identity Groups**

User Identity Groups

Selected 0 Total 10 [Refresh] [Settings]

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

All [Filter]

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

新しいユーザを作成するには、Addボタンを使用して、次に示すように新しいユーザIDグループ設定フォームを開きます。

Administration · Identity Management

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

Identity Groups

EQ

< [Home] [Settings]

> 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]

作成するグループの名前を入力します。admin-group と helpdesk-group の2つのユーザグループを作成します。

ステップ 4 : ISE でユーザを作成します。

GUI で次の手順を実行します。

ISE ユーザは、画面キャプチャに示されている Administration > Identity Management > Identities GUI Page のタブ Users から作成されます。

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	

新しいユーザを作成するには、[追加]ボタンを使用して、次に示すように新しいネットワークアクセスユーザ設定フォームを開きます。

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

ユーザのクレデンシャル (ユーザ名とパスワード) を入力します。これは、WLCでの認証に使用されます。また、ユーザのステータスがEnabledであることも確認します。最後に、手順4.で作成した関連グループにユーザを追加し、フォームの最後にUser Groupsドロップダウンメニューを表示します。

上記で説明した2人のユーザ、adminuserとhelpdeskuserを作成します。

ステップ 5 : ユーザを認証します。

GUI から :

このシナリオでは、すでに事前設定されているISEのデフォルトのポリシーセットの認証ポリシーにより、デフォルトのネットワークアクセスが許可されます。このポリシーセットは、次の図に示すように、ISE GUIページのPolicy > Policy Setsから確認できます。したがって、これを変更する必要はありません。

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	⚙️

手順 6 : ユーザを許可します。

GUI から :

ログイン試行が認証ポリシーを通過した後、認証ポリシーを承認する必要がある、ISEは以前に作成した認証プロファイル (permit accept、および特権レベル) を返す必要があります。

この例では、ログイン試行がデバイスのIPアドレス (WLCのIPアドレス) に基づいてフィルタリングされ、ユーザが属するグループに基づいて、付与される特権レベルが区別されます。この例では、各グループに1人のユーザしか含まれていないため、ユーザ名に基づいてユーザをフィルタリングするという方法も有効です。

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

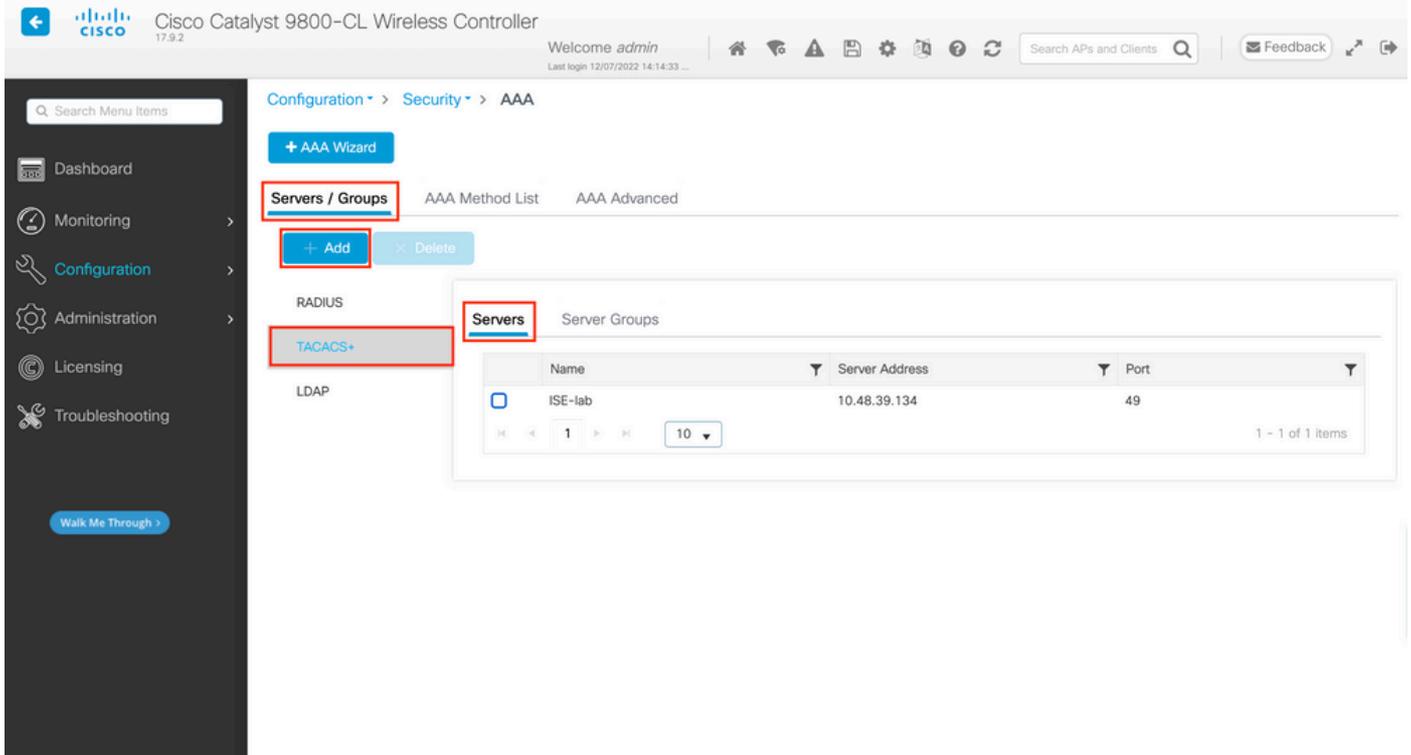
この手順が完了すると、adminuser およびhelpdeskユーザ用に設定されたクレデンシャルを使用して、GUIまたはTelnet/SSH経由でWLCで認証できます。

TACACS+ WLCの設定

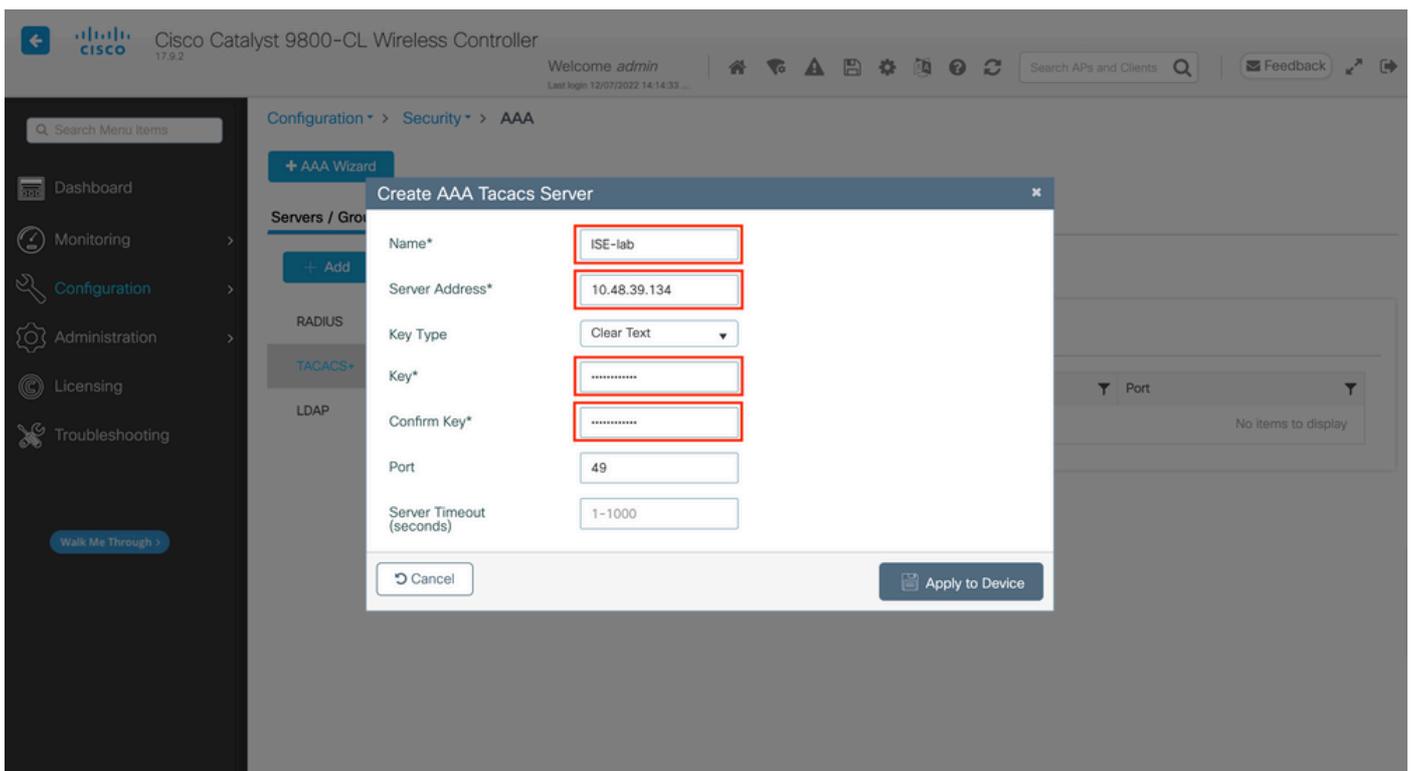
ステップ 1 : TACACS+サーバを宣言します。

GUIから :

まず、WLC上にTACACS+サーバISEを作成します。これは、Servers/Groups > TACACS+ > Serversでアクセス可能なGUIのWLCページのタブからhttps://<WLC-IP>/webui/#/aaa、またはこの図に示すようにConfiguration > Security > AAAに移動して実行できます。



WLC上にTACACSサーバを追加するには、上の図の赤いフレームで囲まれたAddボタンをクリックします。図に示すポップアップウィンドウが開きます。



ポップアップウィンドウが開いたら、サーバ名 (ISEシステム名と一致している必要はありません)、IPアドレス、共有キー、使用しているポート、タイムアウトを入力します。

このポップアップウィンドウでは、次の項目を指定する必要があります。

サーバ名 (ISEシステム名と一致する必要はありません)

- サーバIPアドレス
- WLCとTACACS+サーバ間の共有秘密

認証やアカウントリングに使用されるポートなど、その他のパラメータを設定できますが、これらは必須ではなく、このドキュメントではデフォルトのままにしておきます。

CLI から :

```
<#root>
```

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

ISE-lab

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

```
10.48.39.134
```

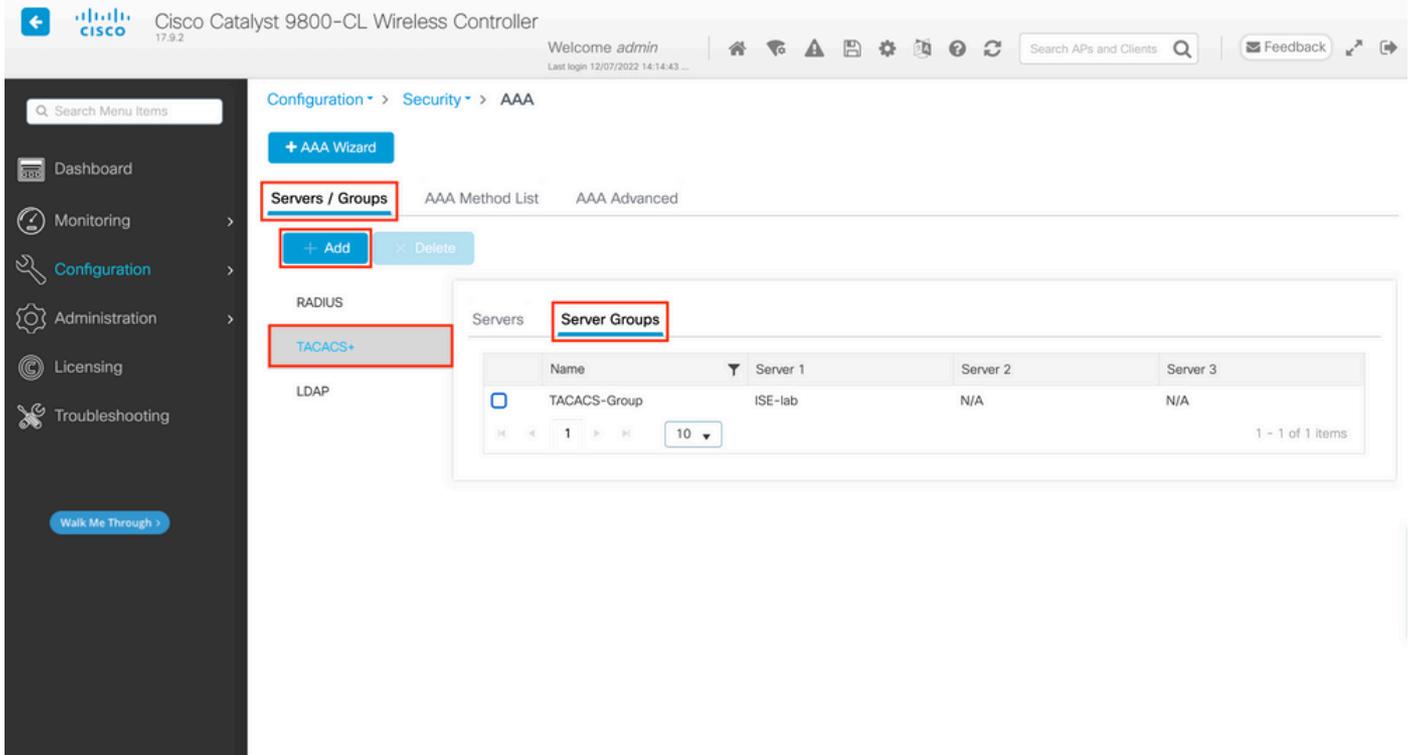
```
WLC-9800(config-server-tacacs)#key
```

Cisco123

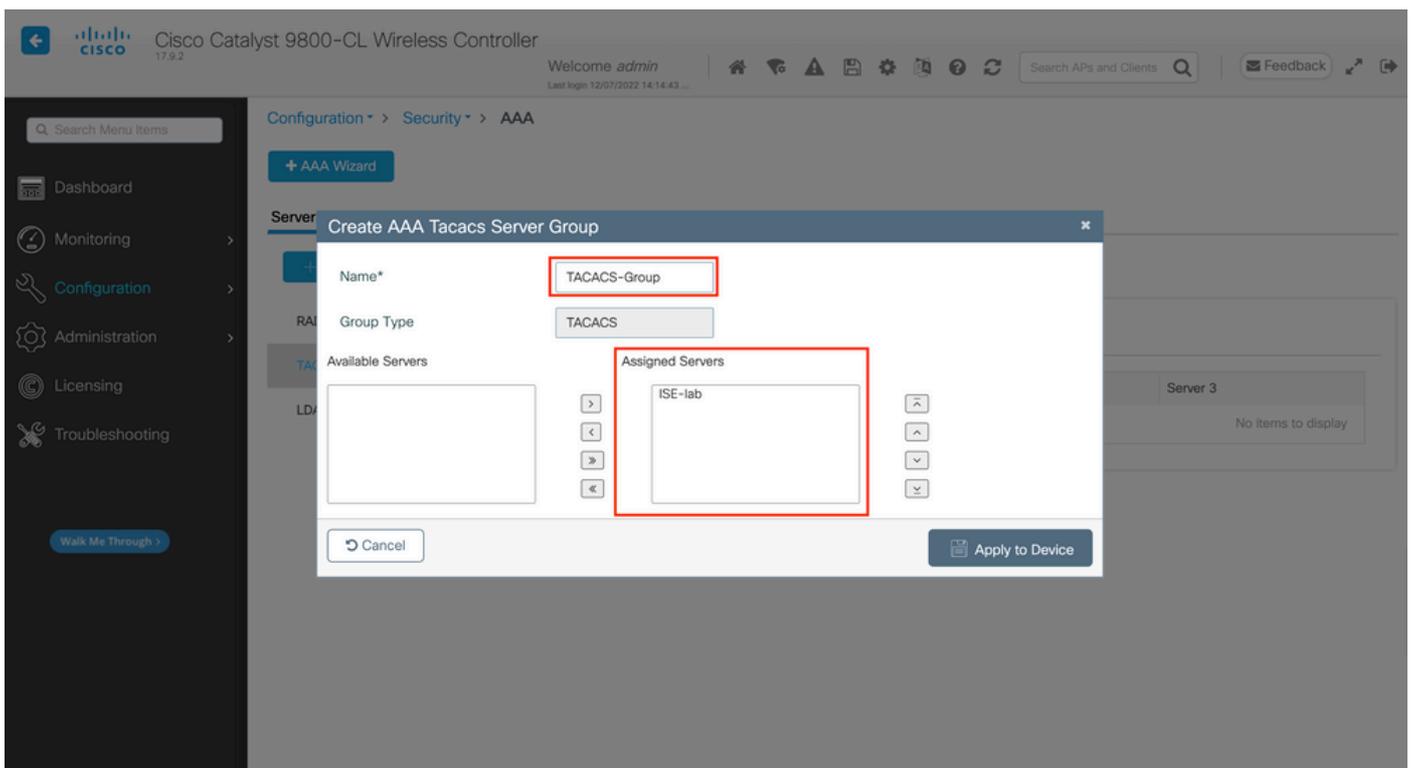
ステップ 2 : TACACS+サーバをサーバグループにマッピングします。

GUI から :

認証に使用できるTACACS+サーバが複数ある場合は、すべてのサーバを同じサーバグループにマッピングすることを推奨します。次に、WLCは、サーバグループ内のサーバ間で異なる認証のロードバランシングを行います。TACACS+サーバグループは、図に示されているステップ1で説明したGUIページと同じGUIページのServers/Groups > TACACS > Server Groupsタブで設定します。



サーバの作成では、イメージに示されている前のイメージのフレームで囲まれたAddボタンをクリックすると、ポップアップウィンドウが表示されます。



ポップアップでグループに名前を付け、目的のサーバをAssigned Serversリストに移動します。

CLI から :

<#root>

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

TACACS-Group

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

ISE-lab

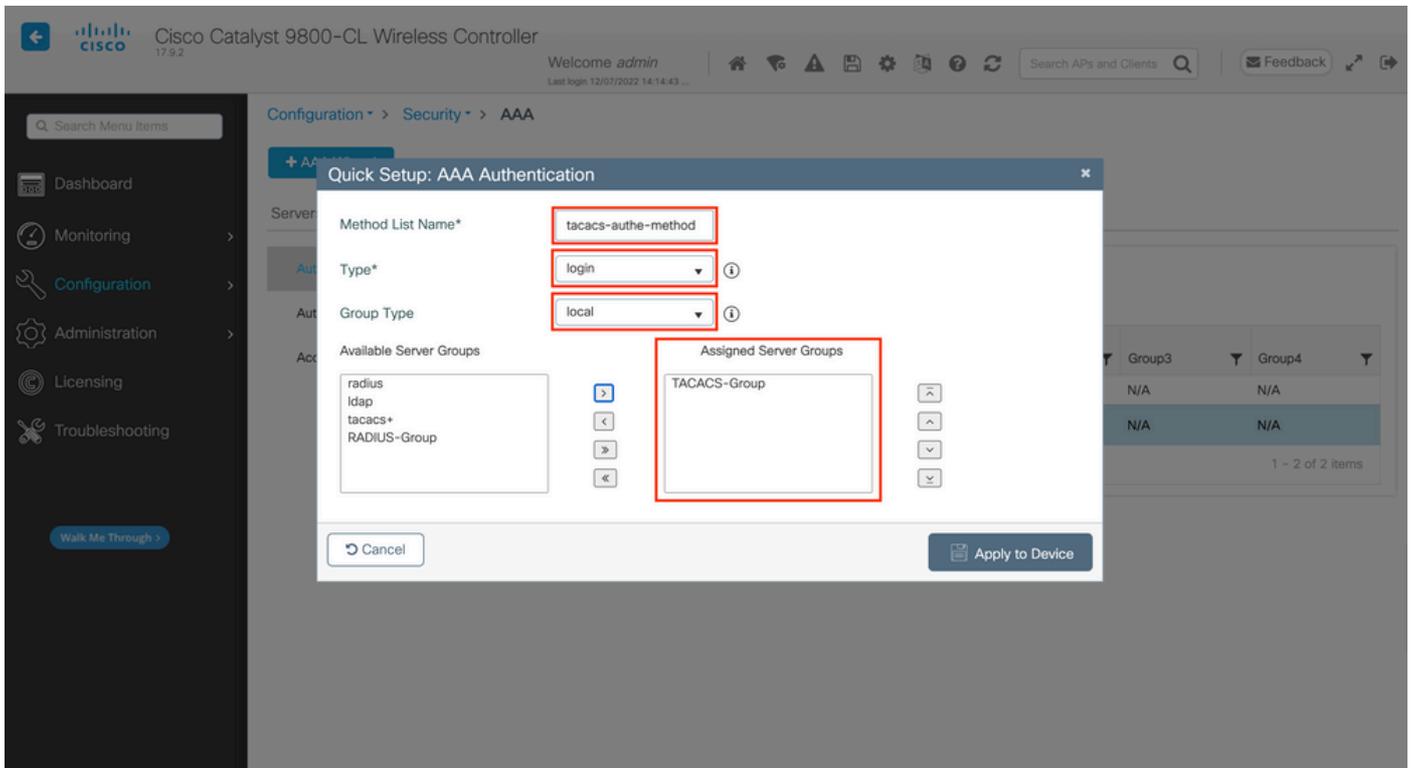
ステップ 3 : TACACS+サーバグループをポイントするAAA認証ログインメソッドを作成します。

GUI から :

引き続きGUIページから[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. 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

通常どおり、Addボタンを使用して認証方式を作成すると、次の図に示すような設定ポップアップウィンドウが表示されます。



このポップアップウィンドウで、メソッドの名前を入力し、loginとしてTypeを選択し、前の手順で作成したグループサーバをAssigned Server Groupsリストに追加します。Group Typeフィールドについては、いくつかの設定が可能です。

- グループタイプとしてローカルを選択した場合、WLCは最初にユーザクレデンシャルがローカルに存在するかどうかをチェックし、次にサーバグループにフォールバックします。
- グループとしてGroup Typeを選択し、Fall back to localオプションをチェックしない場合、WLCではサーバグループに対してユーザクレデンシャルがチェックされるだけです。
- グループとしてGroup Typeを選択し、Fallback to localオプションをチェックすると、WLCはサーバグループに対してユーザクレデンシャルをチェックし、サーバが応答しない場合にだけローカルデータベースに照会します。サーバがrejectを送信すると、ローカルデータベースに存在できるユーザであっても、そのユーザは認証されません。

CLI から :

ユーザクレデンシャルが最初にローカルで見つからない場合にのみ、サーバグループでユーザクレデンシャルをチェックするには、次のコマンドを使用します。

```
<#root>
```

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

`tacacs-auth-method`

`local group`

TACACS-Group

ユーザクレデンシャルをサーバグループでのみチェックする場合は、次のコマンドを使用します。

<#root>

WLC-9800(config)#aaa authentication login

`tacacs-auth-method`

`group`

TACACS-Group

ユーザクレデンシャルをサーバグループでチェックし、この最後のエントリがローカルエントリで応答しない場合は、次のコマンドを使用します。

<#root>

WLC-9800(config)#aaa authentication login

tacacs-auth-method

group

TACACS-Group

local

この設定例では、ローカルでのみ作成されるユーザとISEサーバでのみ作成されるユーザが存在するため、最初のオプションを使用します。

ステップ 4 : TACACS+サーバグループをポイントするAAA認可EXEC方式を作成します。

GUI から :

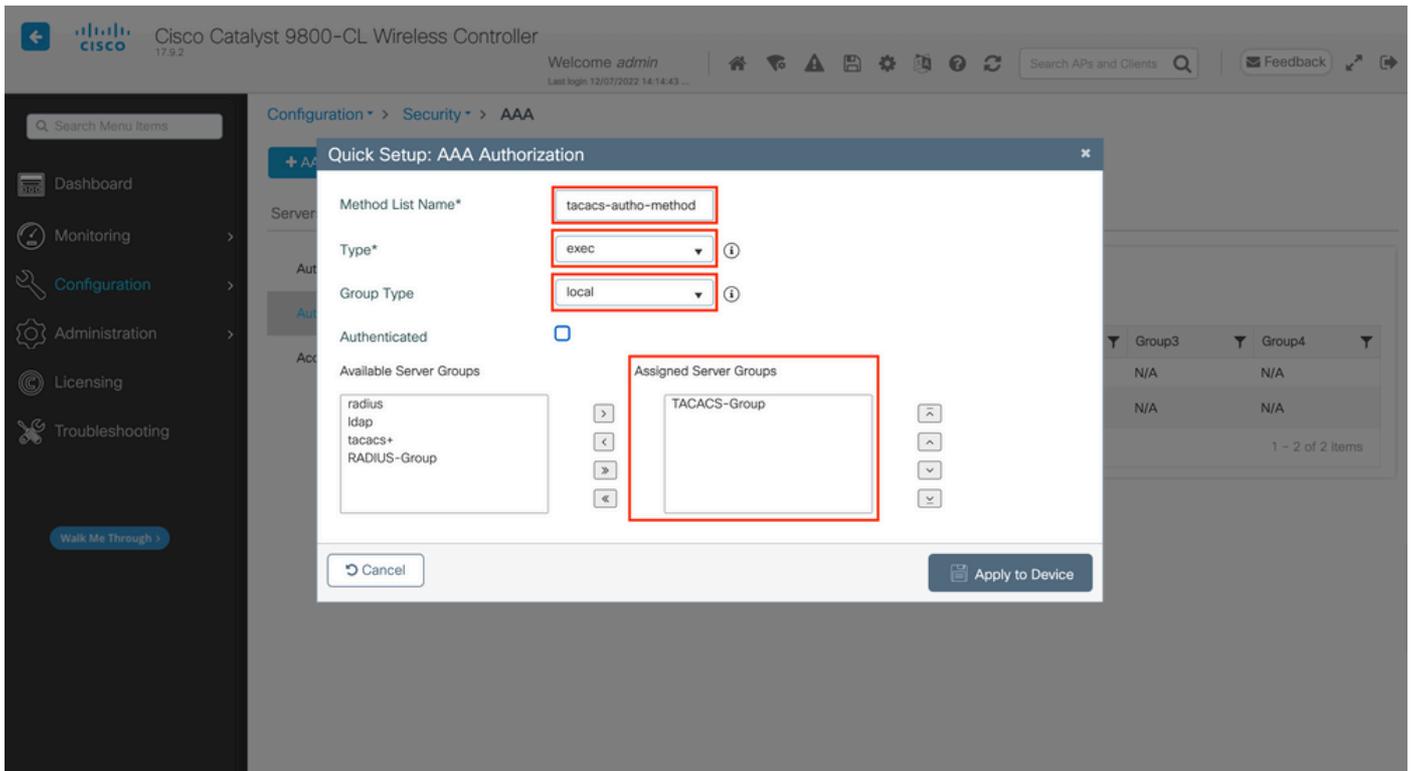
また、アクセス権を付与するには、ユーザが承認されている必要があります。引き続きGUIページからConfiguration > Security > AAAを使用してAAA Method List > Authorizationタブに移動し、図に示すように認可方式を作成します。

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 and highlighted with a red box. Below the breadcrumb, there are tabs for 'Servers / Groups', 'AAA Method List', and 'AAA Advanced'. The 'AAA Method List' tab is active. On the left sidebar, the 'Authorization' option is highlighted with a red box. The main content area shows a table with columns: Name, Type, Group Type, Group1, Group2, Group3, and Group4. There are three rows of data:

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

At the bottom of the table, there is a pagination control showing '1' of 3 items and a dropdown menu set to '10'. The 'Add' button is highlighted with a red box.

Addボタンを使用して新しい認証方式を追加すると、図に示すような認証方式設定のポップアップが表示されます。



この設定ポップアップで、認証方式の名前を指定し、execとしてTypeを選択し、前のステップで認証方式に使用したものと同一Group Typeの順序を使用します。

CLI から :

<#root>

WLC-9800(config)#aaa authorization exec

tacacs-autho-method

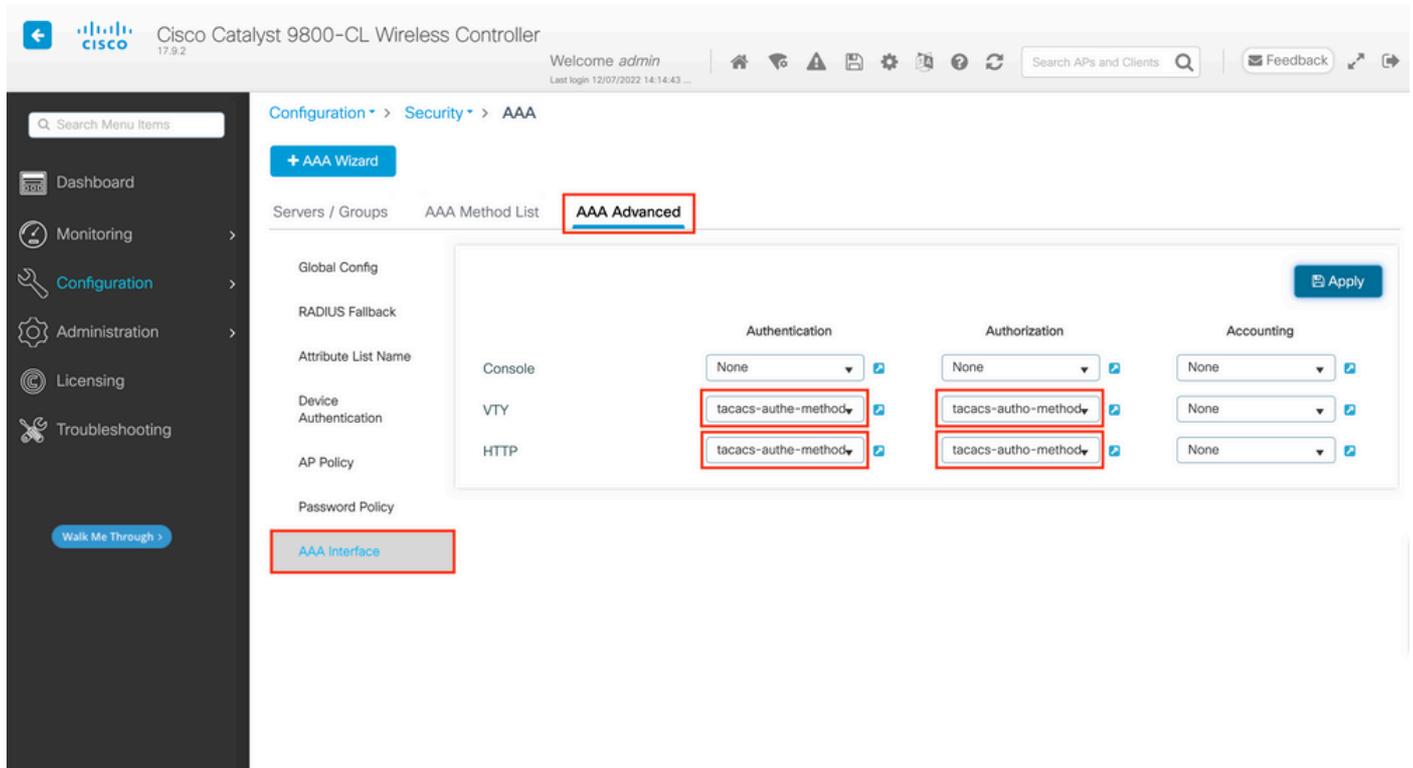
local group

TACACS-Group

ステップ 5 : HTTP設定およびTelnet/SSHに使用するVTY回線にメソッドを割り当てます。

GUI から :

作成された認証および許可方式は、HTTPおよび/またはTelnet/SSHユーザ接続に使用できます。これは、図に示すように、AAA Advanced > AAA Interfaceタブから、まだhttps://<WLC-IP>/webui/#/aaaでアクセス可能なGUI WLCページから設定できます。



CLI から :

GUI認証の場合 :

```
<#root>
```

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

```
tacacs-authe-method
```

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

```
tacacs-autho-method
```

Telnet/SSH認証の場合

```
<#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
```

HTTP設定を変更した場合は、HTTPおよびHTTPSサービスを再起動するのが最善の方法です。これは、次のコマンドを使用して実行できます。

```
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
```

TACACS+ ISEの設定

ステップ 1 : WLCをTACACS+のネットワークデバイスとして設定します。

GUIから :

前のセクションで使用したWLCをISEのRADIUSのネットワークデバイスとして宣言するには、次の図に示すように Administration > Network Resources > Network Devicesに移動し、Network devicesタブを開きます。

Administration · Network Resources

Network Devices

Network Devices

Default Device

Device Security Settings

Selected 1 Total 1

Edit + Add Duplicate Import Export Generate PAC Delete

<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	

この例では、RADIUS認証用にWLCがすでに追加されています(「[RADIUS ISEの設定](#)」セクションのステップ1を参照)。したがって、TACACS認証を設定するために設定を変更するだけで済みます。この操作は、ネットワークデバイスリストでWLCを選択してEditボタンをクリックすることで実行できます。これにより、次の図に示すネットワークデバイス設定フォームが開きます。

Administration · Network Resources

Network Devices

Network Devices

Default Device

Device Security Settings

General Settings

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

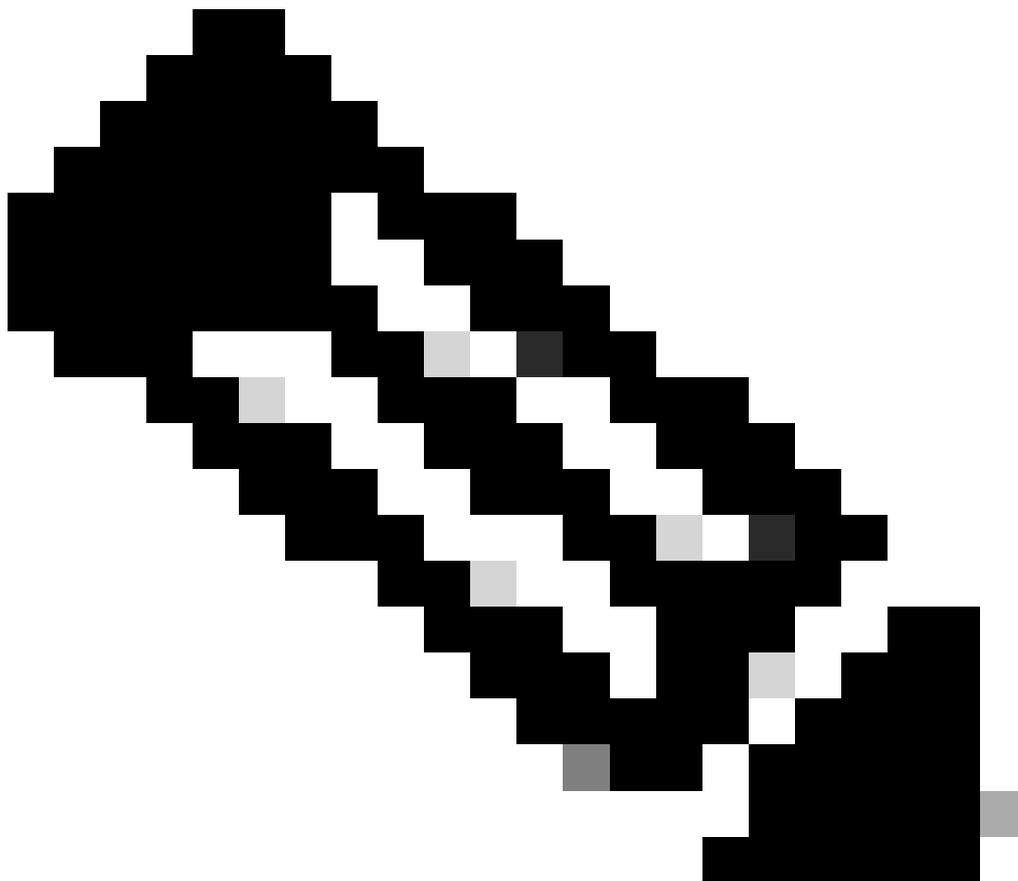
TACACS Draft Compliance Single Connect Support

SNMP Settings

Advanced TrustSec Settings

新しいウィンドウが開いたら、TACACS Authentication Settingsセクションまでスクロールダウンして、これらの設定を有効にし、[TACACS+WLCの設定](#)セクションのステップ1で入力した共有秘密を追加します。

ステップ2: ノードのデバイス管理機能を有効にします。



注:ISEをTACACS+サーバとして使用するには、デバイス管理ライセンスパッケージと、BaseまたはMobilityライセンスのいずれかが必要です。

GUIから：

デバイス管理ライセンスをインストールしたら、ISEをTACACS+サーバとして使用できるようにするために、ノードのデバイス管理機能を有効にする必要があります。そのためには、使用するISE導入ノードの設定を編集します。このノードはAdministrator > Deploymentの下にあり、名前をクリックするか、Editボタンを使用して編集します。

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"/>

ノード設定ウィンドウが開いたら、次の図に示すように、Policy Serviceセクションの下にあるEnable Device Admin Serviceオプションにチェックマークを付けます。

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](#)

ステップ 3 : 特権を返すためのTACACSプロファイルの作成。

GUI から :

管理者のアクセス権を持つには、adminuserに特権レベル15が必要です。これにより、execプロンプトシェルにアクセスできます。一方、helpdeskuserはexecプロンプトのシェルアクセスを必要としないため、15より低い特権レベルで割り当てることができます。適切な特権レベルをユーザに割り当てるには、認可プロファイルを使用できます。これらは、次の図に示すように、ISE GUIページWork Centers > Device Administration > Policy ElementsのタブResults > TACACS Profilesで設定できます。

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

TACACS Profiles

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

Add Duplicate Trash Edit

Filter

<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

新しいTACACSプロファイルを設定するには、Addボタンを使用して、図に示すような新しいプロファイル設定フォームを開きます。adminuserに割り当てられるプロファイル(つまり、シェル権限レベル15)を設定するには、このフォームが特に次のように表示される必要があります。

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

helpdeskプロフィールに対して操作を繰り返します。最後に、デフォルト権限と最大権限はどちらも1に設定されます。

ステップ 4 : ISEでユーザグループを作成します。

これは、このドキュメントの「[RADIUS ISEの設定](#)」セクションのステップ3で示したものと同じです。

ステップ 5 : ISEでユーザを作成します。

これは、このドキュメントの「[RADIUS ISEの設定](#)」セクションのステップ4で示したものと同じです。

手順 6 : デバイス管理ポリシーセットを作成します。

GUI から :

RADIUSアクセスに関しては、ユーザが作成された後も、適切なアクセス権を付与するために認証ポリシーと認可ポリシーをISEで定義する必要があります。TACACS認証は、次に示すようにWork Centers > Device Administration > Device Admin Policy Sets GUI Pageから設定できる、端末に対するデバイス管理ポリシーセットを使用します。

Policy Sets

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

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
							
	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](#)

デバイス管理ポリシーセットを作成するには、上の図の赤い枠で囲まれた追加ボタンを使用します。これにより、ポリシーセットリストに項目が追加されます。新しく作成したセットの名前、適用する必要がある条件、およびAllowed Protocols/Server Sequence(ここではDefault Device Adminで十分)を入力します。ポリシーセットの追加を完了するには、Saveボタンを使用します。また、右側の矢印を使用して、図に示すように設定ページにアクセスします。

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

この例の特定のポリシーセット「WLC TACACS Authentication」では、例のC9800 WLCのIPアドレスと同じIPアドレスを持つ要求をフィルタリングします。

認証ポリシーとして、ユーザのニーズを満たすため、デフォルトルールが残されています。次の2つの認可ルールが設定されています。

- 最初のトリガーは、ユーザが定義されたグループadmin-groupに属している場合にトリガーされます。すべてのコマンドを(デフォルトPermit_allルールを使用して)許可し、特権15を(定義されたIOS_Admin TACACSプロファイルを使用して)割り当てます。
- 2番目のトリガーは、ユーザが定義されたグループhelpdesk-groupに属している場合にトリガーされます。すべてのコマンドを(デフォルトPermit_allルールを介して)許可し、特権1を(定義されたIOS_Helpdesk TACACSプロファイルを介して)割り当てます。

この手順が完了すると、adminuserおよびhelpdeskユーザ用に設定されたクレデンシャルを使用して、GUI経由またはTelnet/SSHを通じてWLCで認証できます。

トラブルシューティング

RADIUSサーバでservice-type RADIUSアトリビュートの送信が想定されている場合は、WLCで次のコマンドを追加できます (WLCのIPアドレスを使用)。

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

WLC CLIを介したWLC GUIまたはCLI RADIUS/TACACS+アクセスのトラブルシューティング

WLCのGUIまたはCLIへのTACACS+アクセスをトラブルシューティングするには、terminal monitor 1に加えてdebug tacacsコマンドを発行し、ログインの試行時のライブ出力を確認します。

たとえば、ログインに成功した後にadminuserユーザからログアウトすると、この出力が生成されます。

```
<#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
```

これらのログから、TACACS+サーバが正しい特権(AV priv-lvl=15)を返していることがわかります。

RADIUS認証を実行すると、RADIUSトラフィックに関する同様のデバッグ出力が表示されます。

debug aaa authenticationコマンドおよびdebug aaa authorizationコマンドは、代わりに、ユーザがログインしようとするときにWLCが選択する方式リストを表示します。

ISE GUIを介したWLC GUIまたはCLI TACACS+アクセスのトラブルシューティング

ページOperations > TACACS > Live Logsから、過去24時間までにTACACS+で行われたすべてのユーザ認証を表示できます。TACACS+認可または認証の詳細を展開するには、このイベントに関連するDetailsボタンを使用します。

The screenshot shows the Cisco ISE Live Logs interface. The breadcrumb navigation is Operations > TACACS. The 'Live Logs' tab is selected. The interface includes a table of log entries with columns for Logged Time, Status, Details, Identity, Type, Authentication Policy, Authorization Policy, and Ise Node. The first row shows an Authorization event for helpdeskuser, which is highlighted with a red box. The table also includes controls for Refresh, Show (Latest 20 records), and Within (Last 3 hours). The status of all events is 'Success' (green checkmark).

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

Last Updated: Thu Dec 08 2022 12:57:09 GMT+0100 (Central European Standard Time) Records Shown: 6

展開すると、helpdeskuserの認証の試行が成功した場合は次のようになります。

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

```

この出力から、認証ポリシーWLC TACACS Authentication > Defaultを使用してユーザhelpdeskuserがネットワークデバイスWLC-9800に対して正常に認証されたことがわかります。さらに、許可プロファイルIOS Helpdeskがこのユーザに割り当てられ、特権レベル1が付与されています。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。