

RADIUSおよびTACACS+認証を使用した9800 WLCロビーアンバサダーの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[RADIUSの認証](#)

[ISEの設定：RADIUS](#)

[TACACS+の認証](#)

[WLCでのTACACS+の設定](#)

[ISEの設定：TACACS+](#)

[確認](#)

[トラブルシューティング](#)

[RADIUSの認証](#)

[TACACS+の認証](#)

概要

このドキュメントでは、Identity Services Engine(ISE)を使用して、Lobby AmbassadorユーザのRADIUSおよびTACACS+外部認証用にCatalyst 9800 Wireless LAN Controller(WLC)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。

- Catalyst 9800ワイヤレスコントローラシリーズ(Catalyst 9800-CL)
- Cisco IOS®-XE Gibraltar 16.12.1s
- ISE 2.3.0

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たものです。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。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

Lobby Ambassadorユーザは、ネットワークの管理者によって作成されます。Lobby Ambassadorユーザは、ゲストユーザのユーザ名、パスワード、説明、ライフタイムを作成できます。ゲストユーザを削除する機能もあります。ゲストユーザは、GUIまたはCLIを使用して作成できます。

設定

ネットワーク図



この例では、ロビーアンバサダー「lobby」と「lobbyTac」が設定されています。ロビーアンバサダー「lobby」はRADIUSサーバに対して認証され、ロビーアンバサダー「lobbyTac」はTACACS+に対して認証されます。

設定は、まずRADIUSロビーアンバサダーに対して、最後にTACACS+ロビーアンバサダーに対して行います。RADIUSとTACACS+ ISEの設定も共有されます。

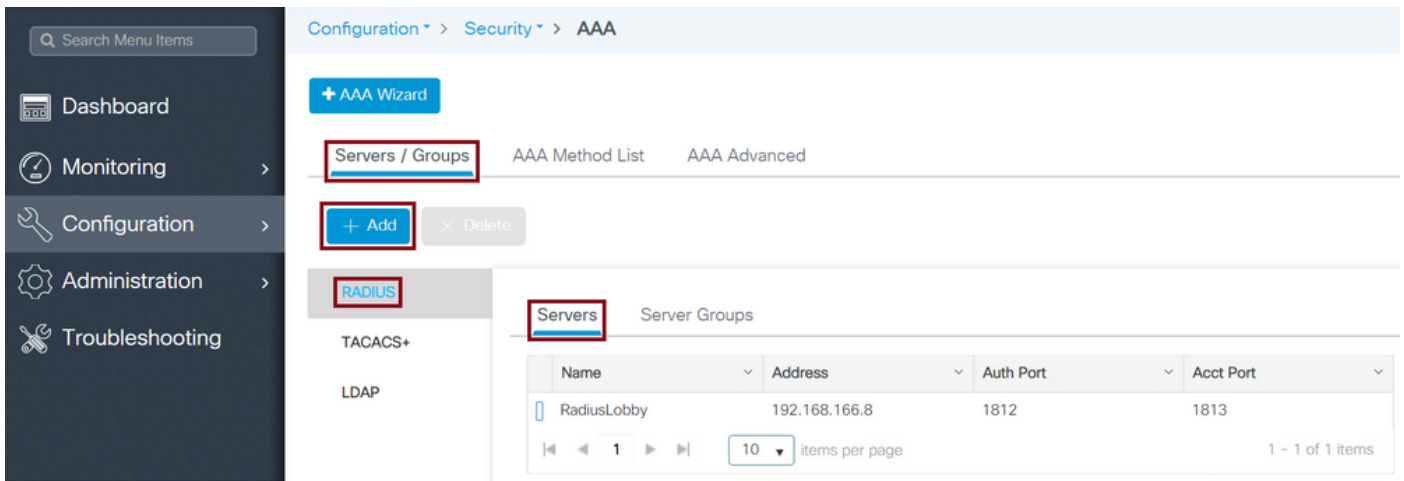
RADIUSの認証

ワイヤレスLANコントローラ(WLC)でRADIUSを設定します。

ステップ1:RADIUSサーバを宣言します。WLCでISE RADIUSサーバを作成します。

GUI :

図に示すように、[Configuration] > [Security] > [AAA] > [Servers/Groups] > [RADIUS] > [Servers] > [Add]に移動します。



設定ウィンドウが開くと、必須の設定パラメータは、RADIUSサーバ名（ISE/AAAシステム名と一致する必要はありません）、RADIUSサーバのIPアドレス、および共有秘密です。その他のパラメータは、デフォルトのままにするか、必要に応じて設定できます。

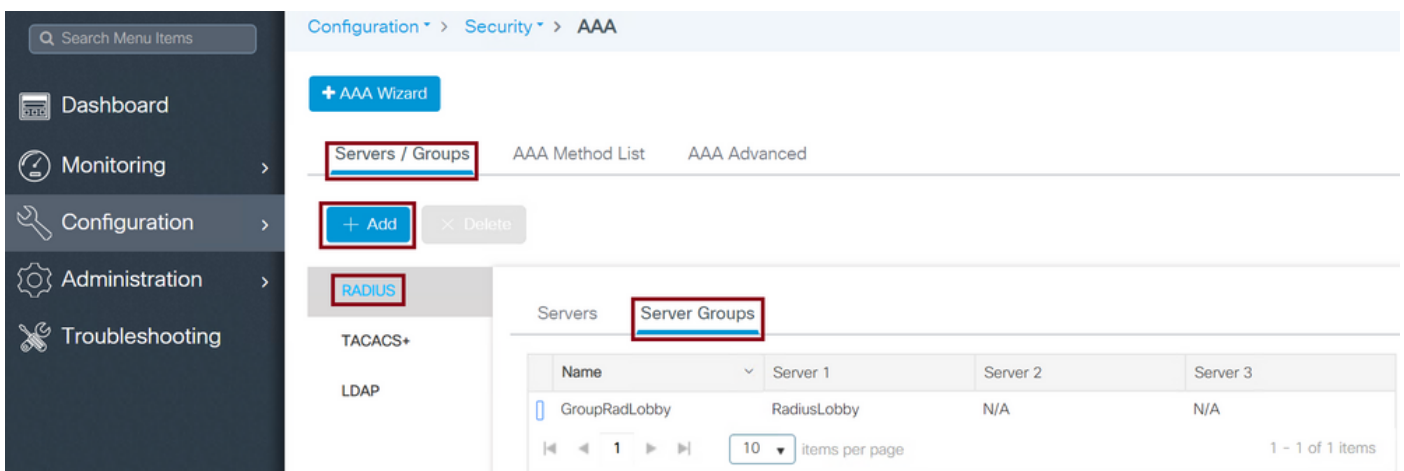
CLI :

```
Tim-eWLC1(config)#radius server RadiusLobby
Tim-eWLC1(config-radius-server)#address ipv4 192.168.166.8 auth-port 1812 acct-port 1813
Tim-eWLC1(config-radius-server)#key 0 Cisco1234
Tim-eWLC1(config)#end
```

ステップ2:RADIUSサーバをサーバグループに追加します。サーバグループを定義し、設定されたRADIUSサーバを追加します。これは、Lobby Ambassadorユーザの認証に使用されるRADIUSサーバです。認証に使用できる複数のRADIUSサーバがWLCに設定されている場合は、すべてのRADIUSサーバを同じサーバグループに追加することをお勧めします。この場合、WLCはサーバグループ内のRADIUSサーバ間の認証をロードバランシングします。

GUI :

図に示すように、[Configuration] > [Security] > [AAA] > [Servers / Groups] > [RADIUS] > [Server Groups] > [+ Add]に移動します。



グループに名前を付けるために設定ウィンドウが開いたら、設定したRADIUSサーバを[Available Servers]リストから[Assigned Servers]リストに移動します。

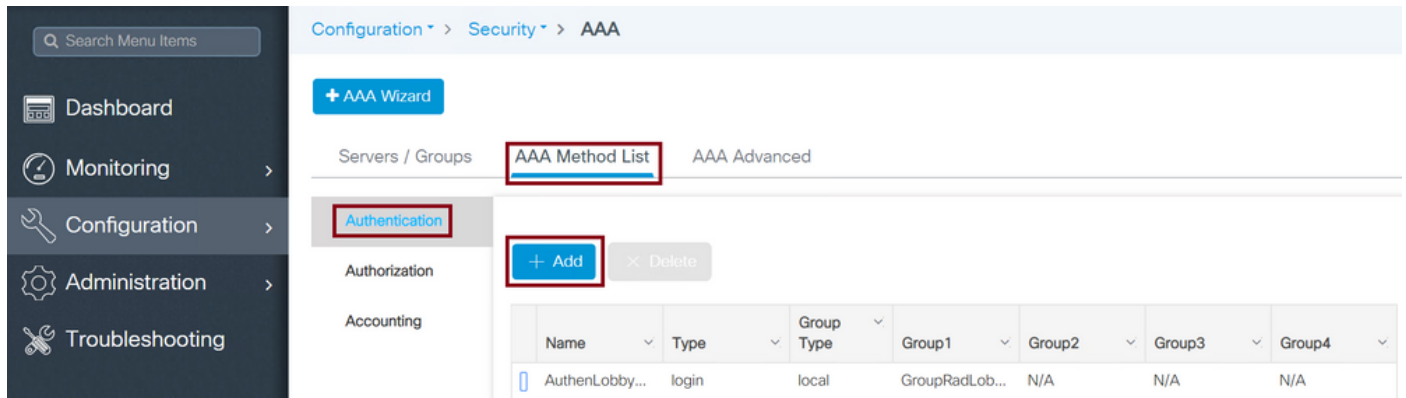
CLI :

```
Tim-eWLC1(config)#aaa group server radius GroupRadLobby
Tim-eWLC1(config-sg-radius)#server name RadiusLobby
Tim-eWLC1(config-sg-radius)#end
```

ステップ3：認証方式リストを作成します。[Authentication Method List]では、検索する認証のタイプを定義し、定義したサーバグループにも同じ認証を適用します。認証がWLCでローカルに行われるか、RADIUSサーバの外部で行われるかが確認されます。

GUI：

図に示すように、[Configuration] > [Security] > [AAA] > [AAA Method List] > [Authentication] > [+ Add]に移動します。



構成ウィンドウが開いたら、名前を入力し、タイプオプションとして[ログイン]を選択し、以前に作成したサーバグループを割り当てます。

[Group Type]を[local]に設定します。

GUI：

[Group Type]に[local]を選択すると、WLCはまずユーザがローカルデータベースに存在するかどうかを確認し、ローカルデータベースにLobby Ambassadorユーザが見つからない場合にのみサーバグループにフォールバックします。

CLI：

```
Tim-eWLC1(config)#aaa authentication login AuthenLobbyMethod local group GroupRadLobby
Tim-eWLC1(config)#end
```

注：バグCSCvs87163に注意してください [さ](#)い ローカルを最初に使用する場合。これは17.3で修正されています。

グループとしてグループタイプ。

GUI：

[Group Type]に[group]を選択し、[Fallback to local]オプションをオンにしていない場合、WLCはユーザをサーバグループに対してチェックするだけであり、ローカルデータベースはチェックしません。

CLI :

```
Tim-eWLC1(config)#aaa authentication login AuthenLobbyMethod group GroupRadLobby  
Tim-eWLC1(config)#end
```

[グループとしてグループタイプ(Group Type as a group)]と[ローカルにフォールバック(fallback to local)]オプションがオンになっています。

GUI :

[Group Type]に[group]を選択し、[fallback to local]オプションをオンにすると、WLCはユーザをサーバグループに対してチェックし、RADIUSサーバが応答でタイムアウトした場合にのみローカルデータベースを照会します。サーバが応答すると、WLCはローカル認証をトリガーしません。

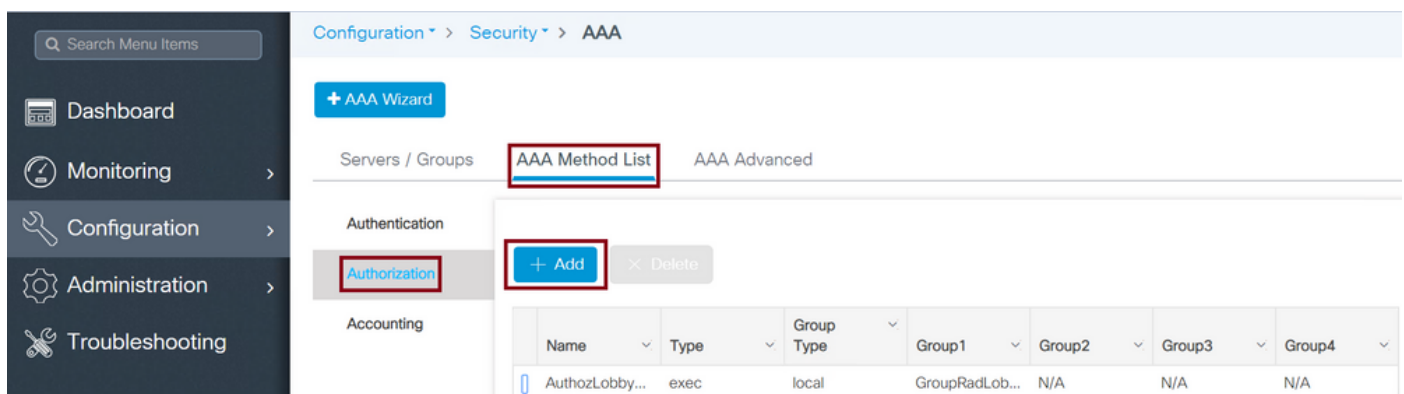
CLI :

```
Tim-eWLC1(config)#aaa authentication login AuthenLobbyMethod group GroupRadLobby local  
Tim-eWLC1(config)#end
```

ステップ4 : 許可方式リストを作成します。[Authorization Method List]では、Lobby Ambassadorに必要な認可タイプを定義します。この場合は「exec」です。また、定義されているものと同じサーバグループに接続されます。また、認証をWLCでローカルに実行するか、RADIUSサーバの外部で実行するかを選択することもできます。

GUI :

図に示すように、[Configuration] > [Security] > [AAA] > [AAA Method List] > [Authorization] > [+ Add]に移動します。



Name	Type	Group Type	Group1	Group2	Group3	Group4
AuthozLobby...	exec	local	GroupRadLob...	N/A	N/A	N/A

設定ウィンドウが開いて名前を指定したら、タイプオプションとして「exec」を選択し、以前に作成したサーバグループを割り当てます。

グループタイプは、「認証方式リスト」セクションで説明したのと同じ方法で適用されることに注意してください。

CLI :

[Group Type]を[local]に設定します。

```
Tim-eWLC1(config)#aaa authorization exec AuthozLobbyMethod local group GroupRadLobby  
Tim-eWLC1(config)#end
```

グループとしてグループタイプ。

```
Tim-eWLC1(config)#aaa authorization exec AuthozLobbyMethod group GroupRadLobby
Tim-eWLC1(config)#end
```

[Group Type as group]と[fallback to local]オプションがオンになっています。

```
Tim-eWLC1(config)#aaa authorization exec AuthozLobbyMethod group GroupRadLobby local
Tim-eWLC1(config)#end
```

ステップ5：メソッドを割り当てます。設定が完了したら、WLCにログインするオプションにメソッドを割り当てて、回線VTY(SSH/Telnet)やHTTP(GUI)などのゲストユーザを作成する必要があります。

これらの手順はGUIからは実行できないため、CLIから実行する必要があります。

HTTP/GUI認証：

```
Tim-eWLC1(config)#ip http authentication aaa login-authentication AuthenLobbyMethod
Tim-eWLC1(config)#ip http authentication aaa exec-authorization AuthozLobbyMethod
Tim-eWLC1(config)#end
```

HTTP設定を変更する場合は、HTTPおよびHTTPSサービスを再起動することをお勧めします。

```
Tim-eWLC1(config)#no ip http server
Tim-eWLC1(config)#no ip http secure-server
Tim-eWLC1(config)#ip http server
Tim-eWLC1(config)#ip http secure-server
Tim-eWLC1(config)#end
```

回線VTY。

```
Tim-eWLC1(config)#line vty 0 15
Tim-eWLC1(config-line)#login authentication AuthenLobbyMethod
Tim-eWLC1(config-line)#authorization exec AuthozLobbyMethod
Tim-eWLC1(config-line)#end
```

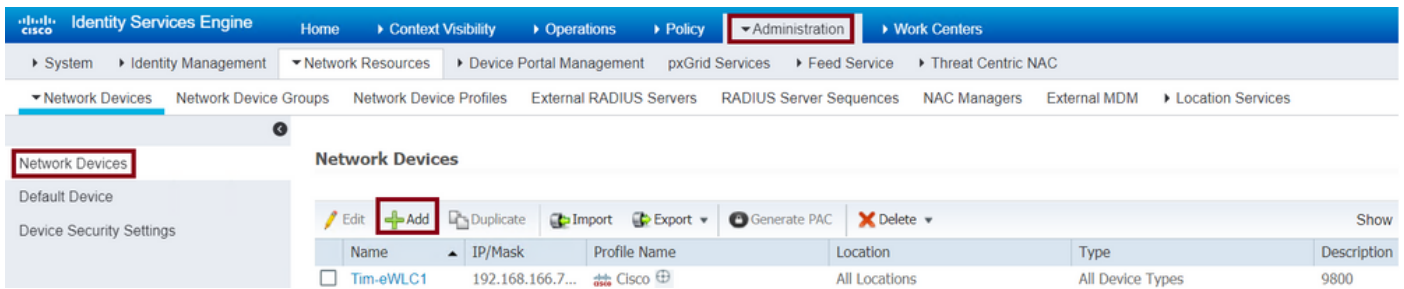
ステップ6：このステップは、17.5.1または17.3.3より前のソフトウェアバージョンでのみ必要であり、[CSCvu29748](#) が実装されました。リモートユーザを定義します。ISEでロビーアンバサダー用に作成されたユーザ名は、WLCでリモートユーザ名として定義する必要があります。リモートユーザ名がWLCで定義されていない場合、認証は正しく行われますが、ロビーアンバサダー権限へのアクセスのみではなく、WLCへのフルアクセスがユーザに付与されます。この設定は、CLIからのみ実行できます。

CLI：

```
Tim-eWLC1(config)#aaa remote username lobby
```

ISEの設定：RADIUS

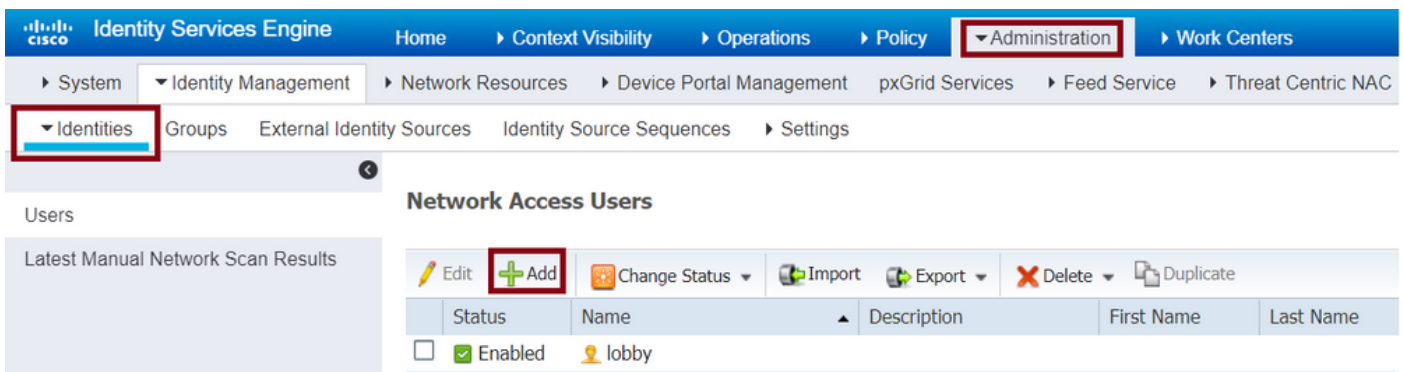
ステップ1:WLCをISEに追加します。[Administration] > [Network Resources] > [Network Devices] > [Add]に移動します。WLCをISEに追加する必要があります。WLCをISEに追加する場合は、[RADIUS Authentication Settings]を有効にし、図に示すように必要なパラメータを設定します。



設定ウィンドウが開いたら、IP ADDという名前を入力し、RADIUS Authentication Settingsを有効にし、Protocol Radiusで必要な共有秘密を入力します。

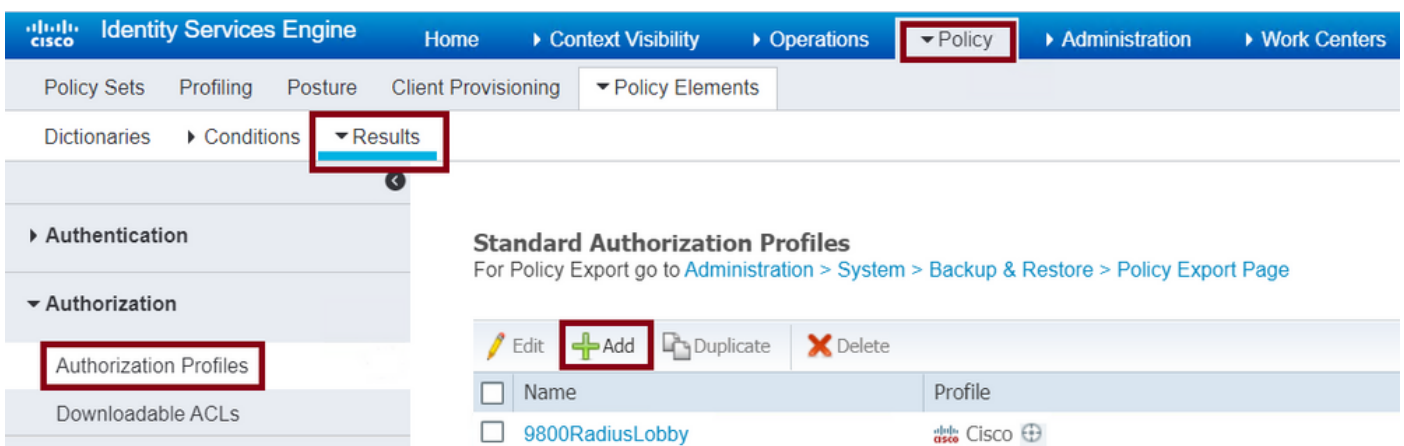
ステップ2: ISEでロビーアンバサダーユーザを作成します。[Administration] > [Identity Management] > [Identities] > [Users] > [Add]に移動します。

ゲストユーザを作成するLobby Ambassadorに割り当てられたユーザ名とパスワードをISEに追加します。これは、管理者がロビーアンバサダーに割り当てるユーザ名です。



設定ウィンドウが開いたら、Lobby Ambassadorユーザの名前とパスワードを入力します。また、[Status]が[Enabled]であることを確認します。

ステップ3: 結果の許可プロファイルを作成します。[Policy] > [Policy Elements] > [Results] > [Authorization] > [Authorization Profiles] > [Add]に移動します。図に示すように、必要な属性を持つAccess-AcceptをWLCに返すために、結果認可プロファイルを作成します。



図に示すように、プロファイルがAccess-Acceptを送信するように設定されていることを確認します。

Identity Services Engine Home Context Visibility Operations Policy

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionaries Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Authorization Profiles > 9800RadiusLobby

Authorization Profile

* Name 9800RadiusLobby

Description

* Access Type ACCESS_ACCEPT

[Advanced Attributes Settings]で属性を手動で追加する必要があります。属性は、ユーザをロビーアンバサダーとして定義し、ロビーアンバサダーが必要な変更を行えるように特権を提供するために必要です。

Advanced Attributes Settings

Cisco:cisco-av-pair = user-type=lobby-admin

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

Attributes Details

Access Type = ACCESS_ACCEPT
 cisco-av-pair = user-type=lobby-admin
 cisco-av-pair = shell:priv-lvl=15

ステップ4：認証を処理するためのポリシーを作成します。[Policy] > [Policy Sets] > [Add]に移動します。ポリシーを設定する条件は、管理者の決定に依存します。ここでは、Network Access-Username条件とDefault Network Access protocolを使用します。

[Authorization Policy]で、[Results Authorization]で設定されたプロファイルが選択されていることを確認する必要があります。これにより、図に示すように、必要な属性をWLCに返すことができます。

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence
OK	9800LobbyRadius		Network Access-UserName EQUALS lobby	Default Network Access

設定ウィンドウが開いたら、認可ポリシーを設定します。認証ポリシーはデフォルトのままにすることができます。

Policy Sets → 9800LobbyRadius

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence
OK	9800LobbyRadius		Network Access-UserName EQUALS lobby	Default Network Access

Authentication Policy (1)

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (2)

Status	Rule Name	Conditions	Results	Security Groups	Hits
OK	9800LobbyAuth	Network Access-UserName EQUALS lobby	Profiles 9800RadiusLobby	Select from list	0

TACACS+の認証

WLCでのTACACS+の設定

ステップ1:TACACS+サーバを宣言します。WLCでISE TACACSサーバを作成します。

GUI :

図に示すように、[Configuration] > [Security] > [AAA] > [Servers/Groups] > [TACACS+] > [Servers] > [Add]に移動します。

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add Delete

RADIUS

TACACS+

LDAP

Servers Server Groups

Name	Server Address	Port
TACACS Lobby	192.168.166.8	49

10 items per page 1 - 1 of 1 items

設定ウィンドウが開くと、必須の設定パラメータは、TACACS+サーバ名 (ISE/AAAシステム名と一致する必要はありません)、TACACSサーバのIPアドレス、および共有秘密です。その他のパラメータは、デフォルトのままにするか、必要に応じて設定できます。

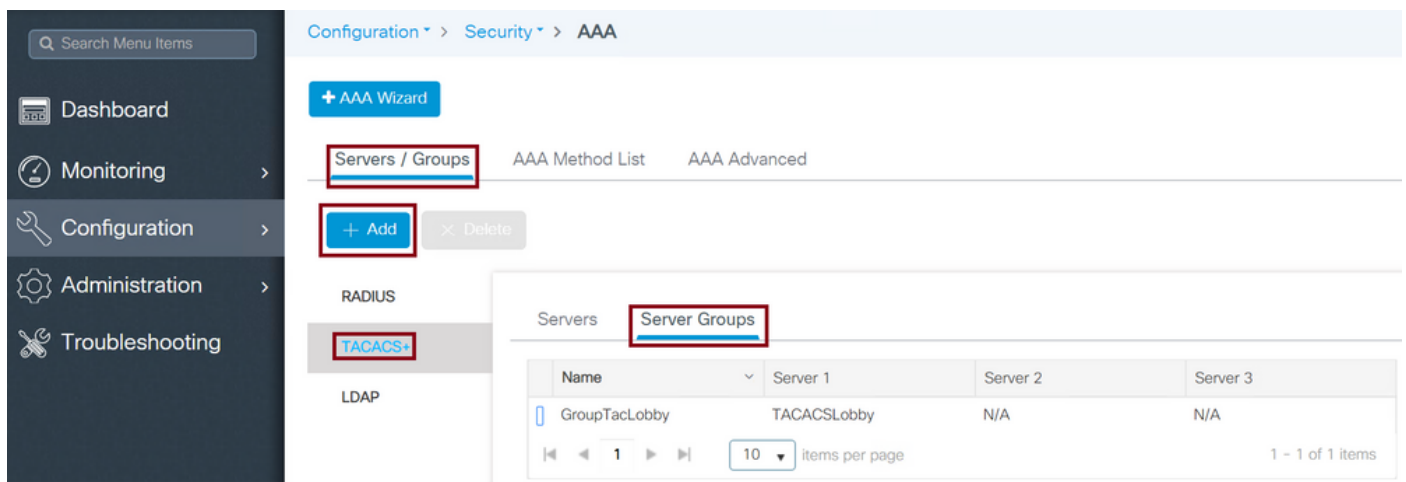
CLI :

```
Tim-eWLC1(config)#tacacs server TACACSLobby
Tim-eWLC1(config-server-tacacs)#address ipv4 192.168.166.8
Tim-eWLC1(config-server-tacacs)#key 0 Cisco123
Tim-eWLC1(config-server-tacacs)#end
```

ステップ2:TACACS+サーバをサーバグループに追加します。サーバグループを定義し、設定するTACACS+サーバを追加します。これは、認証に使用されるTACACS+サーバです。

GUI :

図に示すように、[Configuration] > [Security] > [AAA] > [Servers / Groups] > [TACACS+] > [Server Groups] > [+ Add]に移動します。



設定ウィンドウが開いたら、グループに名前を付け、目的のTACACS+サーバを[Available Servers]リストから[Assigned Servers]リストに移動します。

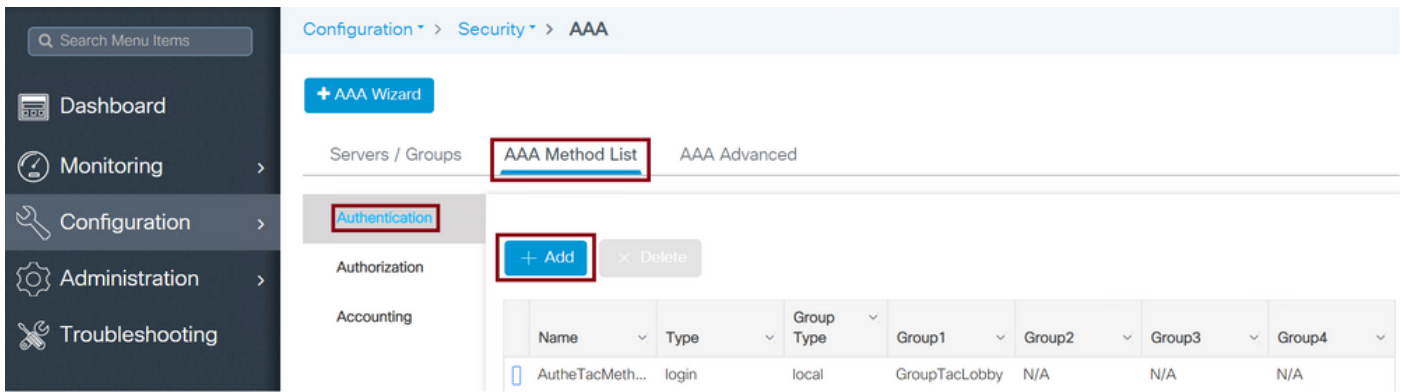
CLI :

```
Tim-eWLC1(config)#aaa group server tacacs+ GroupTacLobby
Tim-eWLC1(config-sg-tacacs+)#server name TACACSLobby
Tim-eWLC1(config-sg-tacacs+)#end
```

ステップ3: 認証方式リストを作成します。認証方式リストは、必要な認証のタイプを定義し、設定されているサーバグループにも同じ認証を割り当てます。また、WLCでローカルに認証を行うか、TACACS+サーバの外部で認証を行うかを選択することもできます。

GUI :

図に示すように、[Configuration] > [Security] > [AAA] > [AAA Method List] > [Authentication] > [+ Add]に移動します。



構成ウィンドウが開いたら、名前を入力し、タイプオプションとして[ログイン]を選択し、以前に作成したサーバーグループを割り当てます。

[Group Type]を[local]に設定します。

GUI :

[Group Type]に[local]を選択すると、WLCは最初にユーザがローカルデータベースに存在するかどうかを確認し、ローカルデータベースにLobby Ambassadorユーザが見つからない場合にのみサーバーグループにフォールバックします。

注 : このバグCSCvs87163に注意してください17.3で修正されています

CLI :

```
Tim-eWLC1(config)#aaa authentication login AutheTacMethod local group GroupTacLobby
Tim-eWLC1(config)#end
```

グループとしてグループタイプ。

GUI :

[Group Type as group]を選択し、[fallback to local]オプションをオンにしていない場合、WLCはユーザをサーバーグループに対してチェックするだけであり、ローカルデータベースはチェックしません。

CLI :

```
Tim-eWLC1(config)#aaa authentication login AutheTacMethod group GroupTacLobby
Tim-eWLC1(config)#end
```

[Group Type as group]と[fallback to local]オプションがオンになっています。

GUI :

[Group Type]に[group]を選択し、[Fallback to local]オプションをオンにすると、WLCはユーザをサーバーグループと照合し、TACACSサーバが応答でタイムアウトした場合にのみローカルデータベースを照会します。サーバが拒否を送信すると、ローカルデータベースにユーザが存在していても、ユーザは認証されません。

CLI :

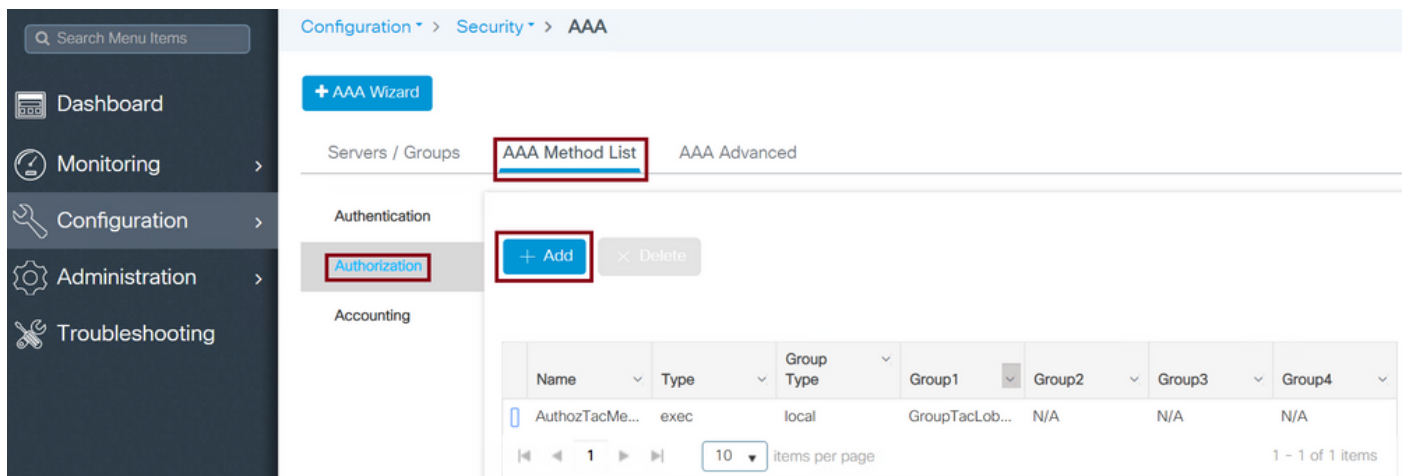
```
Tim-eWLC1(config)#aaa authentication login AutheTacMethod group GroupTacLobby local
Tim-eWLC1(config)#end
```

ステップ4：許可方式リストを作成します。

承認方式リストは、Lobby Ambassadorに必要な許可タイプを定義します。この場合はexecになります。また、設定されているものと同じサーバグループに接続されます。また、認証がWLCでローカルに行われるか、TACACS+サーバの外部で行われるかを選択することもできます。

GUI：

図に示すように、[Configuration] > [Security] > [AAA] > [AAA Method List] > [Authorization] > [+ Add]に移動します。



設定ウィンドウが開いたら、名前を入力し、execとしてタイプオプションを選択し、前に作成したサーバグループを割り当てます。

グループタイプは、[Authentication Method List]セクションで説明したのと同じ方法で適用されることに注意してください。

CLI：

[Group Type]を[local]に設定します。

```
Tim-eWLC1(config)#aaa authorization exec AuthozTacMethod local group GroupTacLobby
Tim-eWLC1(config)#end
```

グループとしてグループタイプ。

```
Tim-eWLC1(config)#aaa authorization exec AuthozTacMethod group GroupTacLobby
Tim-eWLC1(config)#end
```

[Group Type as group]および[Fallback to local]オプションがオンになっている。

```
Tim-eWLC1(config)#aaa authorization exec AuthozTacMethod group GroupTacLobby local
Tim-eWLC1(config)#end
```

ステップ5：メソッドを割り当てます。方法を設定したら、WLCにログインしてVTY回線やHTTP(GUI)などのゲストユーザを作成するために、オプションにメソッドを割り当てる必要があります。これらの手順はGUIからは実行できないため、CLIから実行する必要があります。

HTTP/GUI認証：

```
Tim-eWLC1(config)#ip http authentication aaa login-authentication AutheTacMethod
Tim-eWLC1(config)#ip http authentication aaa exec-authorization AuthozTacMethod
Tim-eWLC1(config)#end
```

HTTP設定を変更する場合は、HTTPおよびHTTPSサービスを再起動することをお勧めします。

```
Tim-eWLC1(config)#no ip http server
Tim-eWLC1(config)#no ip http secure-server
Tim-eWLC1(config)#ip http server
Tim-eWLC1(config)#ip http secure-server
Tim-eWLC1(config)#end
```

回線VTY:

```
Tim-eWLC1(config)#line vty 0 15
Tim-eWLC1(config-line)#login authentication AutheTacMethod
Tim-eWLC1(config-line)#authorization exec AuthozTacMethod
Tim-eWLC1(config-line)#end
```

ステップ6：リモートユーザを定義します。ISEでロビーアンバサダー用に作成されたユーザ名は、WLCでリモートユーザ名として定義する必要があります。リモートユーザ名がWLCで定義されていない場合、認証は正しく行われますが、ロビーアンバサダー権限へのアクセスのみではなく、WLCへのフルアクセスがユーザに付与されます。この設定は、CLIからのみ実行できます。

CLI：

```
Tim-eWLC1(config)#aaa remote username lobbyTac
```

ISEの設定：TACACS+

ステップ1:Device Adminを有効にします。[Administration] > [System] > [Deployment] を選択します。先に進む前に、[Enable Device Admin Service]を選択し、図に示すようにISEが有効になっていることを確認します。

The screenshot shows the Cisco Identity Services Engine Administration interface. The navigation menu includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. The 'Administration' menu is expanded, showing Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Backup & Restore, Admin Access, and Settings. The 'Deployment' menu is also expanded, showing Deployment and PAN Failover. The main content area displays the 'Deployment Nodes List > timise23' page, with the 'Edit Node' button highlighted. The configuration page is divided into 'General Settings' and 'Profiling Configuration' tabs. The 'General Settings' tab is active, showing the following information:

- Hostname: timise23
- FQDN: timise23.cisco.com
- IP Address: 192.168.166.8
- Node Type: Identity Services Engine (ISE)

Below the general settings, the role is set to 'STANDALONE' with a 'Make Primary' button. The 'Administration' checkbox is checked. The 'Monitoring' section is expanded, showing the 'Role' dropdown set to 'PRIMARY' and the 'Other Monitoring Node' field. The 'Policy Service' section is also expanded, showing several service options:

- Enable Session Services (i)
 - Include Node in Node Group: None (i)
- Enable Profiling Service (i)
- Enable Threat Centric NAC Service (i)
- Enable SXP Service (i)
- Enable Device Admin Service (i)

ステップ2:WLCをISEに追加します。[Administration] > [Network Resources] > [Network Devices] > [Add]に移動します。WLCをISEに追加する必要があります。WLCをISEに追加する場合は、[TACACS+ Authentication Settings]を有効にし、図に示すように必要なパラメータを設定します。

The screenshot shows the Cisco Identity Services Engine Administration interface. The navigation menu includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. The 'Administration' menu is expanded, showing Network Resources, Network Devices, Network Device Groups, Network Device Profiles, External RADIUS Servers, RADIUS Server Sequences, NAC Managers, External MDM, and Location Services. The 'Network Devices' menu is also expanded, showing Network Devices, Default Device, and Device Security Settings. The main content area displays the 'Network Devices' page, with the 'Add' button highlighted. The table below shows the following data:

Name	IP/Mask	Profile Name	Location	Type	Description
<input type="checkbox"/> Tim-eWLC1	192.168.166.7...	Cisco	All Locations	All Device Types	9800

設定ウィンドウが開き、名前IP ADDが表示されたら、TACACS+認証設定を有効にして、必要な共有秘密を入力します。

ステップ3:ISEでロビーアンバサダーユーザを作成します。[Administration] > [Identity Management] > [Identities] > [Users] > [Add]に移動します。ゲストユーザを作成するLobby Ambassadorに割り当てられたユーザ名とパスワードをISEに追加します。これは、図に示すように、管理者がロビーアンバサダーに割り当てるユーザ名です。

Identity Services Engine Administration > Network Access Users

Users

Latest Manual Network Scan Results

Status	Name	Description	First Name	Last Name
<input checked="" type="checkbox"/> Enabled	lobbyTac			

設定ウィンドウが開いたら、Lobby Ambassadorユーザの名前とパスワードを入力します。また、[Status]が[Enabled]であることを確認します。

ステップ4：結果TACACS+プロファイルを作成します。図に示すように、[Work Centers] > [Device Administration] > [Policy Elements] > [Results] > [TACACS Profiles]に移動します。このプロファイルを使用して、ユーザをロビーアンバサダーとして配置するために必要な属性をWLCに返します。

Identity Services Engine Administration > Work Centers > Policy Elements > TACACS Profiles

0 Selected

Name	Type	Description
Default Shell Profile	Shell	Default Shell Profile
Deny All Shell Profile	Shell	Deny All Shell Profile
WLC ALL	WLC	WLC ALL
WLC MONITOR	WLC	WLC MONITOR

設定ウィンドウが開いたら、プロファイルに名前を指定し、デフォルト特権15とカスタム属性をタイプ必須、名前をユーザタイプ、値lobby-adminも設定します。また、図に示すように、[Common Task Type]を[Shell]として選択します。

Task Attribute View

Raw View

Common Tasks

Common Task Type Shell

<input checked="" type="checkbox"/> Default Privilege	15	(Select 0 to 15)
<input type="checkbox"/> Maximum Privilege		(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

1 Selected

+ Add 🗑️ Trash ✎ Edit

<input checked="" type="checkbox"/>	Type	Name	Value
<input checked="" type="checkbox"/>	MANDATORY	user-type	lobby-admin

ステップ5：ポリシーセットの作成図に示すように、[Work Centers] > [Device Administration] > [Device Admin Policy Sets]に移動します。ポリシーを設定する条件は、管理者の決定に依存します。このドキュメントでは、Network Access-Username条件とDefault Device Adminプロトコルを使用します。[Results Authorization]で設定されたプロファイルが選択されていることを[Authorization Policy]で確認する必要があります。これにより、必要な属性をWLCに返すことができます。

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	9800TacacsLobby		Network Access-UserName EQUALS lobbyTac	Default Device Admin	0		

設定ウィンドウが開いたら、認可ポリシーを設定します。図に示すように、認証ポリシーはデフォルトのままにすることができます。

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
	9800TacacsLobby		Network Access-UserName EQUALS lobbyTac	Default Device Admin	0
Authentication Policy (1) Authorization Policy - Local Exceptions Authorization Policy - Global Exceptions Authorization Policy (2)					
				Results	
Status	Rule Name	Conditions	Command Sets	Shell Profiles	Hits Actions
	9800TacacsAuth	Network Access-UserName EQUALS lobbyTac	Select from list	9800TacacsLobby	0

確認

ここでは、設定が正常に機能しているかどうかを確認します。

```
show run aaa
show run | sec remote
show run | sec http
show aaa method-lists authentication
show aaa method-lists authorization
show aaa servers
show tacacs
```

認証が成功した後のLobby Ambassador GUIの外観は、次のようになります。

User Name	Description	Created By
Guest User		

0 items per page

トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

RADIUSの認証

RADIUS認証では、次のデバッグを使用できます。

```
Tim-eWLC1#debug aaa authentication
Tim-eWLC1#debug aaa authorization
Tim-eWLC1#debug aaa attr
Tim-eWLC1#terminal monitor
```

デバッグで正しい方式リストが選択されていることを確認します。また、必要な属性は、適切なユーザ名、ユーザタイプ、および権限を持つISEサーバから返されます。

```
Feb 5 02:35:27.659: AAA/AUTHEN/LOGIN (00000000): Pick method list 'AuthenLobbyMethod'
Feb 5 02:35:27.681: ADD-DELETE: AAA/ATTR(00000000): add attr: sublist(0x7FBA5500C860) index(0):
```

```
7FBA5500C870 0 00000081 username(450) 5 lobby
Feb 5 02:35:27.681: ADD-DELETE: AAA/ATTR(00000000): add attr: sublist(0x7FBA5500C860) index(1):
7FBA5500C8B0 0 00000001 user-type(1187) 4 lobby-admin
Feb 5 02:35:27.681: ADD-DELETE: AAA/ATTR(00000000): add attr: sublist(0x7FBA5500C860) index(2):
7FBA5500C8F0 0 00000001 priv-lvl(335) 4 15(F)
Feb 5 02:35:27.683: %WEBSEVER-5-LOGIN_PASSED: Chassis 1 R0/0: nginx: Login Successful from host
192.168.166.104 by user 'lobby' using crypto cipher 'ECDHE-RSA-AES128-GCM-SHA256'
```

TACACS+の認証

TACACS+認証では、次のデバッグを使用できます。

```
Tim-eWLC1#debug tacacs
Tim-eWLC1#terminal monitor
```

認証が正しいユーザ名とISE IP ADDで処理されていることを確認します。また、ステータス「PASS」が表示されます。同じデバッグでは、認証フェーズの直後に、認可プロセスが示されます。この認可では、フェーズによって正しいユーザ名が正しいISE IP ADDとともに使用されることが保証されます。このフェーズから、WLCをロビーアンバサダーユーザとして正しい権限を持つISEに設定されている属性を確認できます。

認証フェーズの例：

```
Feb 5 02:06:48.245: TPLUS: Queuing AAA Authentication request 0 for processing
Feb 5 02:06:48.245: TPLUS: Authentication start packet created for 0(lobbyTac)
Feb 5 02:06:48.245: TPLUS: Using server 192.168.166.8
Feb 5 02:06:48.250: TPLUS: Received authen response status GET_PASSWORD (8)
Feb 5 02:06:48.266: TPLUS(00000000)/0/7FB7819E2100: Processing the reply packet
Feb 5 02:06:48.266: TPLUS: Received authen response status PASS (2)
```

認証フェーズの例：

```
Feb 5 02:06:48.267: TPLUS: Queuing AAA Authorization request 0 for processing
Feb 5 02:06:48.267: TPLUS: Authorization request created for 0(lobbyTac)
Feb 5 02:06:48.267: TPLUS: Using server 192.168.166.8
Feb 5 02:06:48.279: TPLUS(00000000)/0/7FB7819E2100: Processing the reply packet
Feb 5 02:06:48.279: TPLUS: Processed AV priv-lvl=15
Feb 5 02:06:48.279: TPLUS: Processed AV user-type=lobby-admin
Feb 5 02:06:48.279: TPLUS: received authorization response for 0: PASS
```

RADIUSおよびTACACS+に関して前述したデバッグ例には、ログインを成功させるための重要な手順があります。デバッグはより詳細で、出力が大きくなります。デバッグを無効にするには、次のコマンドを使用できます。

```
Tim-eWLC1#undebug all
```