

Konfigurieren des 9800-WLC-Lobby-Botschafters mit RADIUS- und TACACS+-Authentifizierung

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfiguration](#)

[Netzwerkdiagramm](#)

[RADIUS-Authentifizierung](#)

[Konfigurieren der ISE - RADIUS](#)

[TACACS+ authentifizieren](#)

[Konfigurieren von TACACS+ auf WLC](#)

[Konfigurieren der ISE - TACACS+](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[RADIUS-Authentifizierung](#)

[TACACS+ authentifizieren](#)

Einführung

Dieses Dokument beschreibt die Konfiguration der Catalyst 9800 Wireless LAN Controller für die externe RADIUS- und TACACS+-Authentifizierung von Benutzern des Lobby-Botschafters unter Verwendung der Identity Services Engine (ISE).

Voraussetzungen

Anforderungen

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

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

Verwendete Komponenten

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

- Catalyst Wireless Controller der Serie 9800 (Catalyst 9800-CL)
- Cisco IOS®-XE Gibraltar 16.12.1s
- ISE 2.3.0

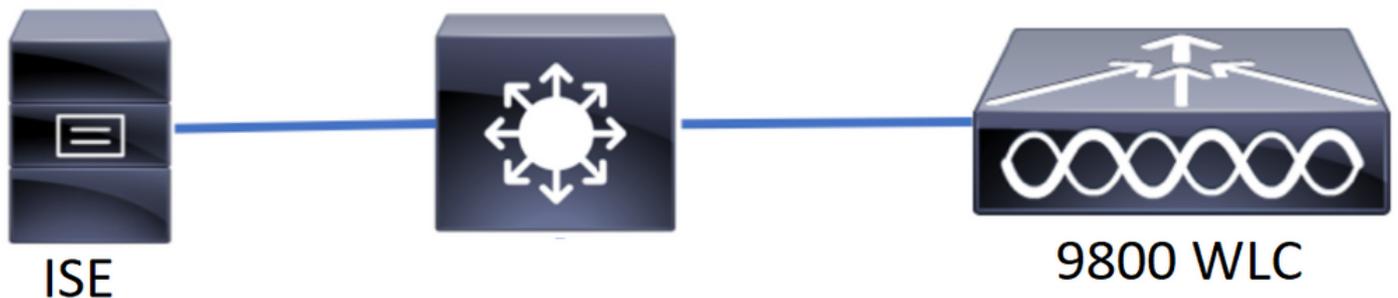
Die Informationen in diesem Dokument wurden von Geräten in einer bestimmten Laborumgebung erstellt. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Der Benutzer Lobby Ambassador wird vom Administrator des Netzwerks erstellt. Ein Benutzer von Lobby Ambassador kann den Benutzernamen, das Kennwort, die Beschreibung und die Lebensdauer eines Gastbenutzers erstellen. Außerdem kann der Gastbenutzer gelöscht werden. Der Gastbenutzer kann über GUI oder CLI erstellt werden.

Konfiguration

Netzwerkdiagramm



In diesem Beispiel werden Lobby Ambassadors "lobby" und "lobbyTac" konfiguriert. Die Lobby Ambassador "Lobby" soll gegen den RADIUS-Server authentifiziert werden und der Lobby-Botschafter "lobbyTac" wird gegen TACACS+ authentifiziert.

Die Konfiguration erfolgt zuerst für den RADIUS Lobby-Botschafter und schließlich für den TACACS+ Lobby-Botschafter. Die Konfiguration von RADIUS und TACACS+ ISE wird ebenfalls gemeinsam genutzt.

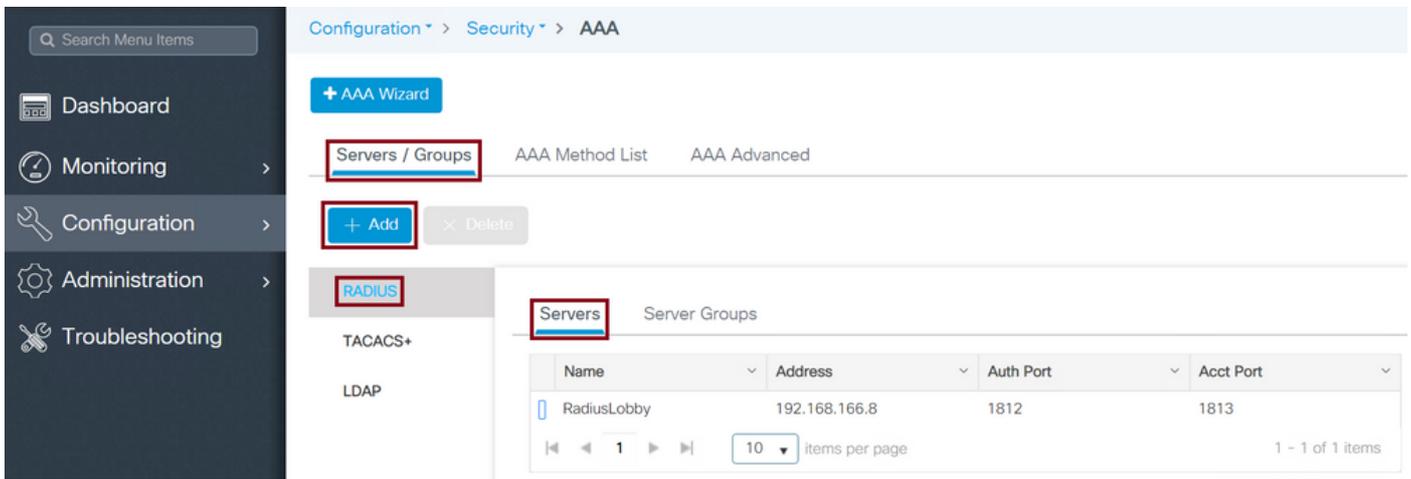
RADIUS-Authentifizierung

Konfigurieren von RADIUS auf dem Wireless LAN Controller (WLC)

Schritt 1: Deklarieren Sie den RADIUS-Server. Erstellen Sie den ISE RADIUS-Server auf dem WLC.

Benutzeroberfläche:

Navigieren Sie zu **Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add as in image (Konfiguration > Sicherheit > AAA > Server/Gruppen > RADIUS > Server > Hinzufügen)**.



Wenn das Konfigurationsfenster geöffnet wird, sind die obligatorischen Konfigurationsparameter der RADIUS-Servername (er muss nicht mit dem ISE/AAA-Systemnamen übereinstimmen), die RADIUS-Server-IP-ADRESSE und der gemeinsam genutzte geheime Schlüssel. Alle anderen Parameter können standardmäßig beibehalten oder nach Bedarf konfiguriert werden.

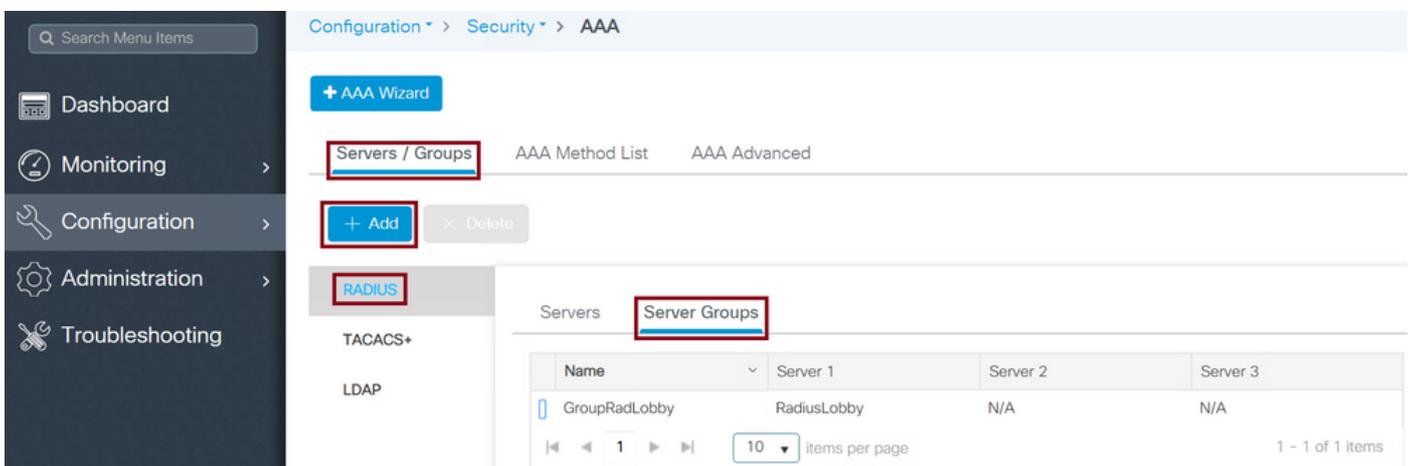
CLI:

```
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
```

Schritt 2: Fügen Sie den RADIUS-Server einer Servergruppe hinzu. Definieren Sie eine Servergruppe, und fügen Sie den konfigurierten RADIUS-Server hinzu. Dies ist der RADIUS-Server, der für die Authentifizierung des Benutzers Lobby Ambassador verwendet wird. Wenn im WLC mehrere RADIUS-Server konfiguriert sind, die für die Authentifizierung verwendet werden können, wird empfohlen, alle Radius-Server derselben Servergruppe hinzuzufügen. In diesem Fall lassen Sie die WLC-Lastverteilung der Authentifizierungen zwischen den RADIUS-Servern in der Servergruppe zu.

Benutzeroberfläche:

Navigieren Sie zu **Konfiguration > Sicherheit > AAA > Server/Groups > RADIUS > Server Groups > + Add** (wie im Bild gezeigt).



Wenn das Konfigurationsfenster geöffnet wird, um der Gruppe einen Namen zu geben, verschieben Sie die konfigurierten RADIUS-Server aus der Liste Verfügbare Server in die Liste

Zugewiesene Server.

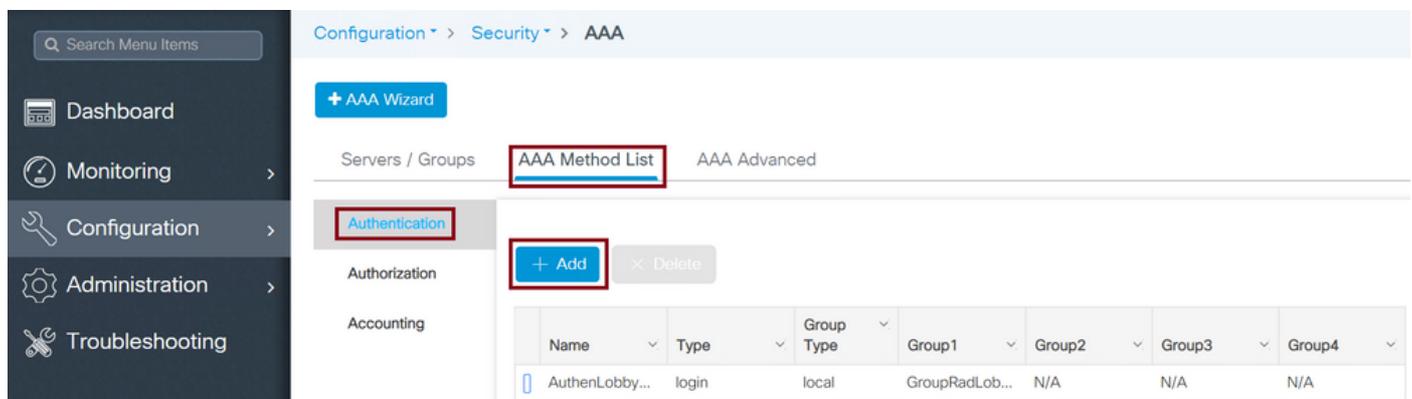
CLI:

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

Schritt 3: Erstellen einer Authentifizierungsmethodenliste. Die Authentifizierungsmethodenliste definiert den Authentifizierungstyp, den Sie suchen, und fügt diesen der von Ihnen definierten Servergruppe hinzu. Sie werden wissen, ob die Authentifizierung lokal auf dem WLC oder extern auf einem RADIUS-Server erfolgt.

Benutzeroberfläche:

Navigieren Sie zu **Konfiguration > Sicherheit > AAA > AAA-Methodenliste > Authentifizierung > + Hinzufügen**, wie im Bild gezeigt.



Wenn das Konfigurationsfenster geöffnet wird, geben Sie einen Namen ein, wählen Sie die Option Typ als **Anmelden aus**, und weisen Sie die zuvor erstellte Servergruppe zu.

Gruppentyp als lokal.

Benutzeroberfläche:

Wenn Sie "Gruppentyp" als "lokal" auswählen, prüft der WLC zunächst, ob der Benutzer in der lokalen Datenbank vorhanden ist, und greift dann nur dann auf die Servergruppe zurück, wenn der Benutzer Lobby Ambassador nicht in der lokalen Datenbank gefunden wurde.

CLI:

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

Hinweis: Bitte beachten Sie den Fehler [CSCvs87163](#), wenn Sie zuerst lokal verwenden. Dies ist in 17.3 behoben.

Gruppentyp als Gruppe.

Benutzeroberfläche:

Wenn Sie Gruppentyp als 'Gruppe' auswählen und kein Fallback zur lokalen Option aktiviert ist, prüft der WLC den Benutzer nur anhand der Servergruppe und checkt die lokale Datenbank nicht ein.

CLI:

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

Gruppentyp als Gruppe und das Fallback zur lokalen Option ist aktiviert.

Benutzeroberfläche:

Wenn Sie Gruppe Typ als 'Gruppe' auswählen und die Option Fallback to local aktiviert ist, prüft der WLC den Benutzer gegenüber der Servergruppe und fragt die lokale Datenbank nur ab, wenn der RADIUS-Server in der Antwort ein Timeout aufweist. Wenn der Server antwortet, löst der WLC keine lokale Authentifizierung aus.

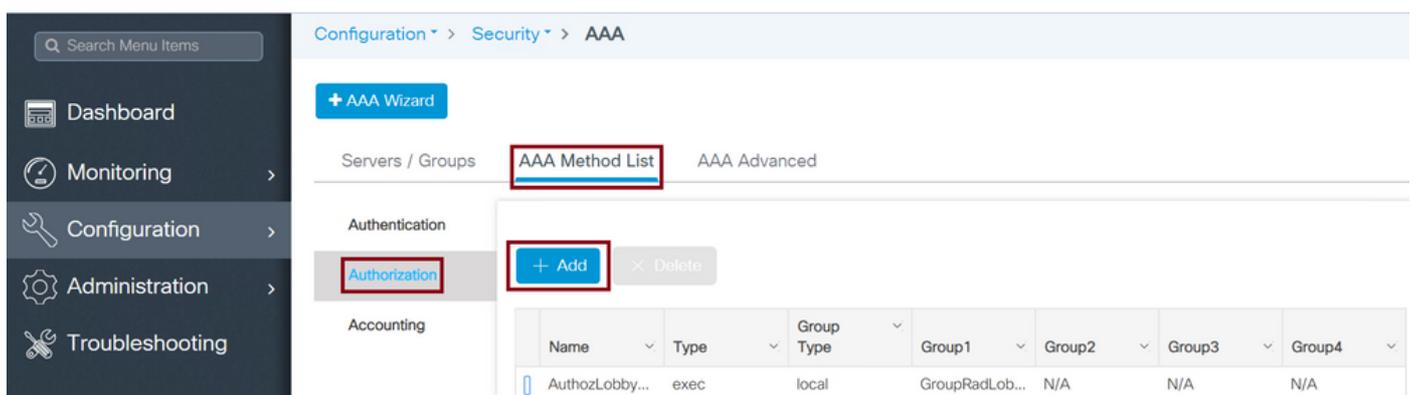
CLI:

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

Schritt 4: Erstellen einer Liste von Autorisierungsmethoden. Die Autorisierungsmethodenliste definiert den Autorisierungstyp, den Sie für den Lobby-Botschafter benötigen, der in diesem Fall "exec" ist. Sie wird auch mit derselben definierten Servergruppe verbunden. Außerdem können Sie auswählen, ob die Authentifizierung lokal auf dem WLC oder extern auf einem RADIUS-Server erfolgt.

Benutzeroberfläche:

Navigieren Sie zu **Konfiguration > Sicherheit > AAA > AAA-Methodenliste > Autorisierung > + Hinzufügen**, wie im Bild gezeigt.



The screenshot shows the configuration page for AAA Method List. The 'Authorization' tab is selected, and the '+ Add' button is highlighted. The table below shows the configuration for the 'AuthozLobby...' method.

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

Wenn das Konfigurationsfenster geöffnet wird, um einen Namen bereitzustellen, wählen Sie die Typoption als 'exec' aus, und weisen Sie die zuvor erstellte Servergruppe zu.

Beachten Sie, dass der Gruppentyp die gleiche Anwendung wie im Abschnitt Authentifizierungsmethodenliste beschrieben hat.

CLI:

Gruppentyp als lokal.

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

Gruppentyp als Gruppe.

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

Gruppentyp als Gruppe, und die Option Fallback to local ist aktiviert.

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

Schritt 5: Weisen Sie die Methoden zu. Nach der Konfiguration der Methoden müssen sie den Optionen für die Anmeldung beim WLC zugewiesen werden, um den Gastbenutzer zu erstellen, z. B. Line VTY (SSH/Telnet) oder HTTP (GUI).

Diese Schritte können nicht über die Benutzeroberfläche ausgeführt werden, daher müssen sie über die CLI ausgeführt werden.

HTTP/GUI-Authentifizierung:

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

Wenn Sie Änderungen an den HTTP-Konfigurationen durchführen, empfiehlt es sich, die HTTP- und HTTPS-Dienste neu zu starten:

```
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
```

Leitung 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
```

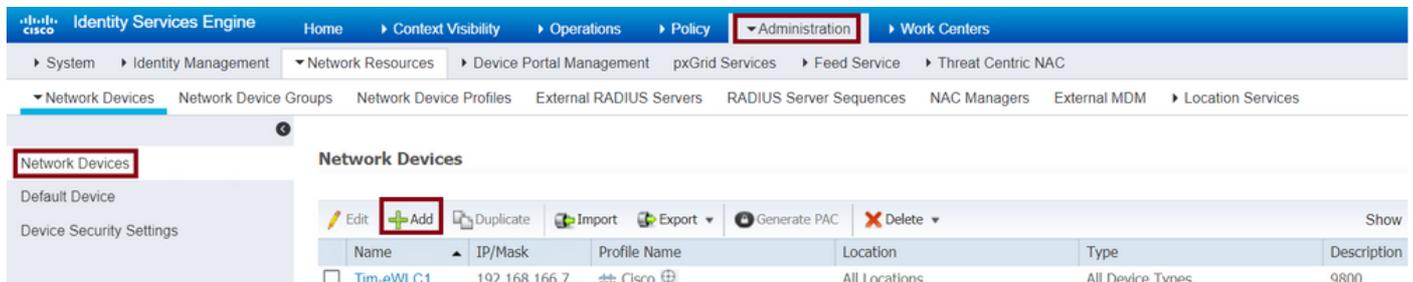
Schritt 6: Dieser Schritt ist nur in Softwareversionen vor 17.5.1 oder 17.3.3 erforderlich und ist nach den Versionen, in denen [CSCvu29748](#) enthalten ist, nicht erforderlich. wurde implementiert. Definieren Sie den Remote-Benutzer. Der auf der ISE für den Lobby-Botschafter erstellte Benutzername muss als Remote-Benutzername auf dem WLC definiert werden. Wenn der Remote-Benutzername nicht im WLC definiert ist, wird die Authentifizierung korrekt ausgeführt, aber der Benutzer erhält vollständigen Zugriff auf den WLC, anstatt nur Zugriff auf die Berechtigungen des Lobby-Botschafters zu haben. Diese Konfiguration kann nur über die CLI vorgenommen werden.

CLI:

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

Konfigurieren der ISE - RADIUS

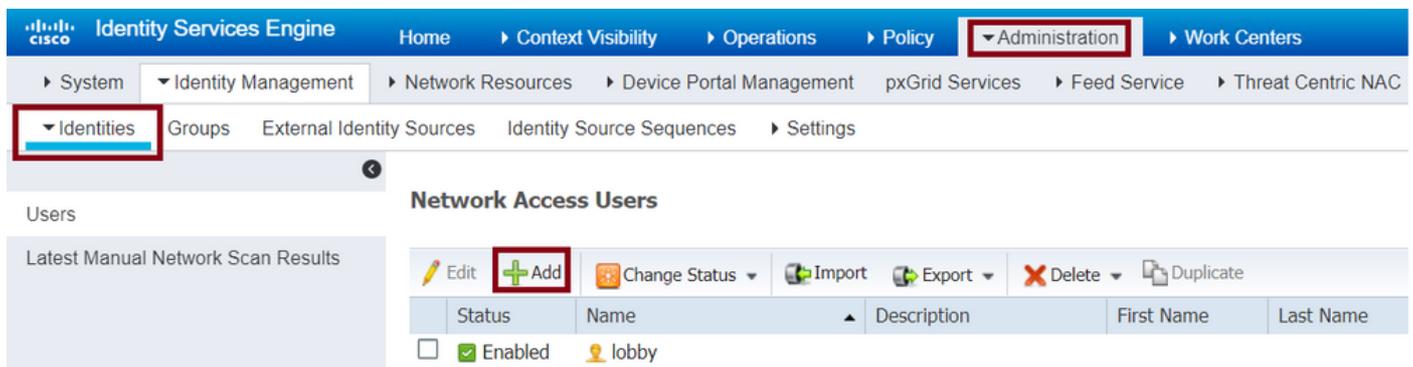
Schritt 1: Fügen Sie den WLC der ISE hinzu. Navigieren Sie zu **Administration > Network Resources > Network Devices > Add**. Der WLC muss der ISE hinzugefügt werden. Wenn Sie den WLC der ISE hinzufügen, aktivieren Sie die RADIUS-Authentifizierungseinstellungen, und konfigurieren Sie die erforderlichen Parameter, wie im Bild gezeigt.



Wenn das Konfigurationsfenster geöffnet wird, geben Sie den Namen IP ADD, RADIUS Authentication Settings (RADIUS-Authentifizierungseinstellungen) und unter Protocol Radius (Protokoll-Radius) den erforderlichen Shared Secret (Gemeinsam genutzter geheimer Schlüssel) ein.

Schritt 2: Erstellen Sie den Benutzer Lobby Ambassador auf der ISE. Navigieren Sie zu **Administration > Identity Management > Identities > Users > Add**.

Fügen Sie der ISE den Benutzernamen und das Kennwort hinzu, die dem Lobby-Botschafter zugewiesen sind, der die Gastbenutzer erstellt. Dies ist der Benutzername, den der Administrator der Lobby-Botschafterin zuweist.



Wenn das Konfigurationsfenster geöffnet wird, geben Sie den Namen und das Kennwort für den Benutzer von Lobby Ambassador an. Stellen Sie außerdem sicher, dass der Status aktiviert ist.

Schritt 3: Erstellen eines Ergebnisautorisierungsprofils. Navigieren Sie zu **Richtlinien > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofile > Hinzufügen**. Erstellen Sie ein Ergebnisautorisierungsprofil, um zum WLC und zur Access-Accept mit den erforderlichen Attributen zurückzukehren, wie im Bild gezeigt.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Policy' menu is expanded, showing 'Policy Sets', 'Profiling', 'Posture', 'Client Provisioning', and 'Policy Elements'. The 'Results' sub-menu is selected. In the left sidebar, 'Authorization Profiles' is highlighted. The main content area displays 'Standard Authorization Profiles' with a table listing profiles. The '9800RadiusLobby' profile is visible in the table.

Stellen Sie sicher, dass das Profil so konfiguriert ist, dass ein Access-Accept gesendet wird, wie im Bild gezeigt.

The screenshot shows the configuration page for the '9800RadiusLobby' Authorization Profile. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', and 'Policy'. The 'Policy Elements' menu is expanded, showing 'Policy Sets', 'Profiling', 'Posture', 'Client Provisioning', and 'Policy Elements'. The 'Results' sub-menu is selected. In the left sidebar, 'Authorization Profiles' is highlighted. The main content area displays 'Authorization Profiles > 9800RadiusLobby' and 'Authorization Profile'. The configuration fields are: '* Name' (9800RadiusLobby), 'Description' (empty), and '* Access Type' (ACCESS_ACCEPT). The '* Access Type' field is highlighted with a red box.

Sie müssen die Attribute unter Erweiterte Attributeinstellungen manuell hinzufügen. Die Attribute werden benötigt, um den Benutzer als Lobby-Botschafter zu definieren und das Privileg zu geben, damit der Lobby-Botschafter die notwendigen Änderungen vornehmen kann.

Advanced Attributes Settings

The screenshot shows two attribute entries in a list. Each entry consists of a key-value pair in a text box, followed by an equals sign and another text box for the value. The first entry is 'Cisco:cisco-av-pair' followed by '= user-type=lobby-admin'. The second entry is 'Cisco:cisco-av-pair' followed by '= shell:priv-lvl=15'. Both entries have a red border around them. There are also some icons like a plus sign and a minus sign next to the second entry.

Attributes Details

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

Schritt 4: Erstellen Sie eine Richtlinie, um die Authentifizierung zu verarbeiten. Navigieren Sie zu **Richtlinien > Richtlinienätze > Hinzufügen**. Die Bedingungen für die Konfiguration der Richtlinie hängen von der Entscheidung des Administrators ab. Network Access - Username condition und das Default Network Access Protocol werden hier verwendet.

Es muss unbedingt sichergestellt werden, dass unter der Autorisierungsrichtlinie das unter der Ergebnisautorisierung konfigurierte Profil ausgewählt ist, sodass die erforderlichen Attribute wie im Bild gezeigt an den WLC zurückgegeben werden können.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Policy' menu is highlighted. Below the navigation bar, there is a 'Policy Sets' section with a table of policy sets. The table has columns for 'Status', 'Policy Set Name', 'Description', 'Conditions', and 'Allowed Protocols / Server Sequence'. A search bar is located below the table. The first entry in the table is '9800LobbyRadius' with a status icon of a green checkmark. The 'Conditions' column for this entry shows 'Network Access UserName EQUALS lobby'. The 'Allowed Protocols / Server Sequence' column shows 'Default Network Access' with a dropdown arrow and a plus sign.

Wenn das Konfigurationsfenster geöffnet wird, konfigurieren Sie die Autorisierungsrichtlinie. Die Authentifizierungsrichtlinie kann als Standard beibehalten werden.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence
✔	9800LobbyRadius		Network Access-UserName EQUALS lobby	Default Network Access
Authentication Policy (1)				
Authorization Policy - Local Exceptions				
Authorization Policy - Global Exceptions				
Authorization Policy (2)				
✔	9800LobbyAutho		Network Access-UserName EQUALS lobby	Results Profiles Security Groups Hits

TACACS+ authentifizieren

Konfigurieren von TACACS+ auf WLC

Schritt 1: Deklarieren des TACACS+-Servers. Erstellen Sie den ISE TACACS-Server im WLC.

Benutzeroberfläche:

Navigieren Sie zu **Configuration > Security > AAA > Servers/Groups > TACACS+ > Servers > Add** as in image.

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

1 - 1 of 1 items

Wenn das Konfigurationsfenster geöffnet wird, sind die obligatorischen Konfigurationsparameter der TACACS+-Servername (er muss nicht mit dem ISE/AAA-Systemnamen übereinstimmen), die TACACS-Server-IP-ADRESSE und der Shared Secret (Gemeinsamer geheimer Schlüssel). Alle anderen Parameter können standardmäßig beibehalten oder nach Bedarf konfiguriert werden.

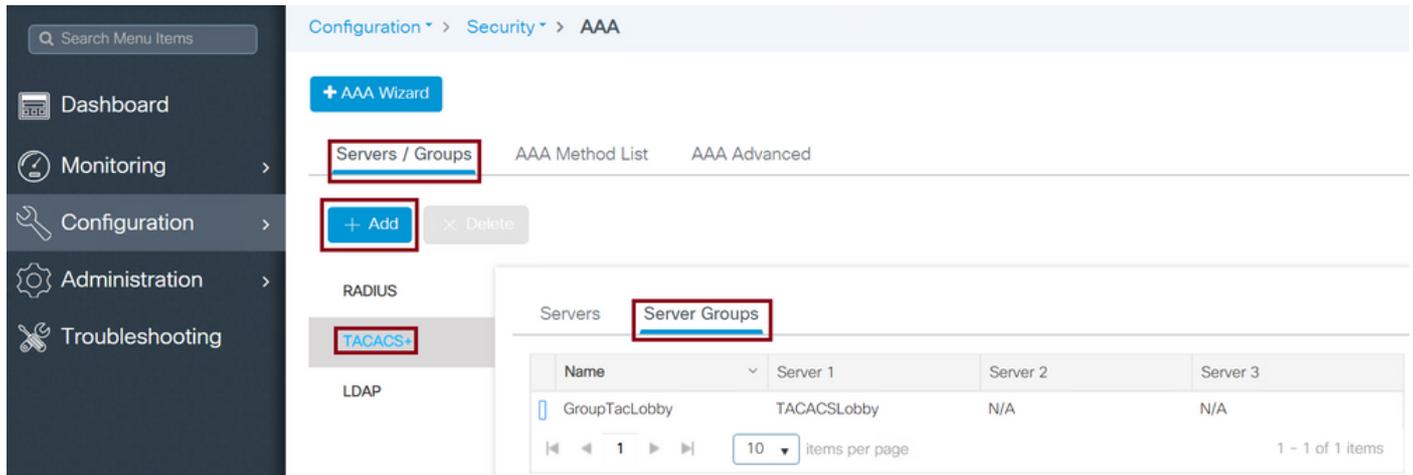
CLI:

```
Tim-eWLC1(config)#tacacs server TACACS+Lobby
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
```

Schritt 2: Fügen Sie den TACACS+-Server einer Servergruppe hinzu. Definieren Sie eine Servergruppe, und fügen Sie den konfigurierten gewünschten TACACS+-Server hinzu. Dies sind die für die Authentifizierung verwendeten TACACS+-Server.

Benutzeroberfläche:

Navigieren Sie zu **Konfiguration > Sicherheit > AAA > Server/Groups > TACACS > Server Groups > + Add** (wie im Bild gezeigt).



Wenn das Konfigurationsfenster geöffnet wird, geben Sie der Gruppe einen Namen und verschieben Sie die gewünschten TACACS+-Server aus der Liste Verfügbare Server in die Liste Zugewiesene Server.

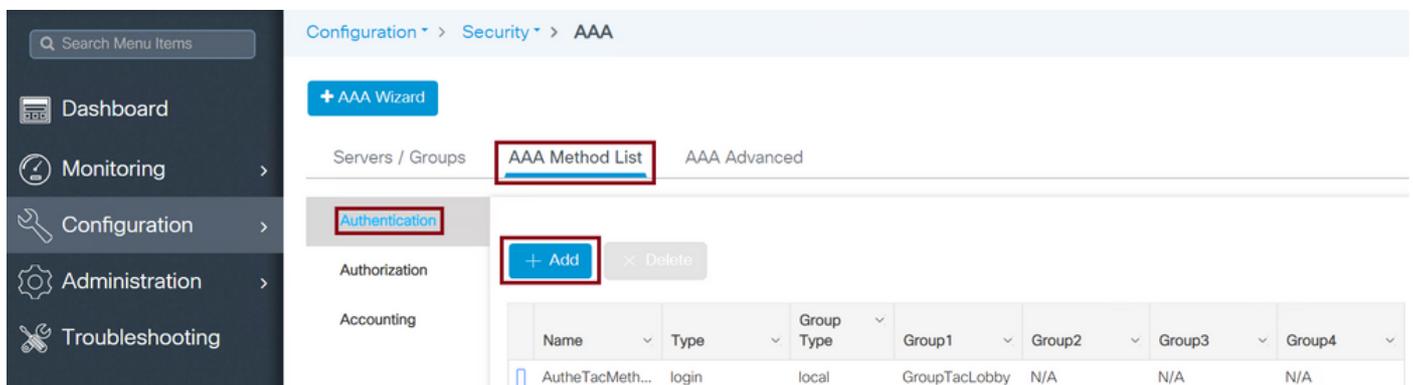
CLI:

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

Schritt 3: Erstellen einer Authentifizierungsmethodenliste. Die Authentifizierungsmethodenliste definiert den erforderlichen Authentifizierungstyp und fügt diesen der konfigurierten Servergruppe hinzu. Außerdem können Sie auswählen, ob die Authentifizierung lokal auf dem WLC oder extern auf einem TACACS+-Server erfolgen kann.

Benutzeroberfläche:

Navigieren Sie zu **Konfiguration > Sicherheit > AAA > AAA-Methodenliste > Authentifizierung > + Hinzufügen**, wie im Bild gezeigt.



Wenn das Konfigurationsfenster geöffnet wird, geben Sie einen Namen ein, wählen Sie die Option Typ als **Anmelden aus**, und weisen Sie die zuvor erstellte Servergruppe zu.

Gruppentyp als lokal.

Benutzeroberfläche:

Wenn Sie "Gruppentyp" als "lokal" auswählen, prüft der WLC zunächst, ob der Benutzer in der lokalen Datenbank vorhanden ist, und greift dann nur dann auf die Servergruppe zurück, wenn der Benutzer Lobby Ambassador nicht in der lokalen Datenbank gefunden wurde.

Hinweis: Bitte beachten Sie diesen Fehler [CSCvs87163](#) die in 17.3 festgelegt ist.

CLI:

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

Gruppentyp als Gruppe.

Benutzeroberfläche:

Wenn Sie Gruppentyp als Gruppe auswählen und kein Fallback zur lokalen Option aktiviert ist, prüft der WLC den Benutzer nur anhand der Servergruppe und checkt die lokale Datenbank nicht ein.

CLI:

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

Gruppentyp als Gruppe, und die Option Fallback to local ist aktiviert.

Benutzeroberfläche:

Wenn Sie Gruppentyp als 'Gruppe' auswählen und die Option Fallback to local aktiviert ist, prüft der WLC den Benutzer gegenüber der Servergruppe und fragt die lokale Datenbank nur ab, wenn der TACACS-Server in der Antwort ein Timeout aufweist. Wenn der Server eine Ablehnung sendet, wird der Benutzer nicht authentifiziert, auch wenn er in der lokalen Datenbank vorhanden ist.

CLI:

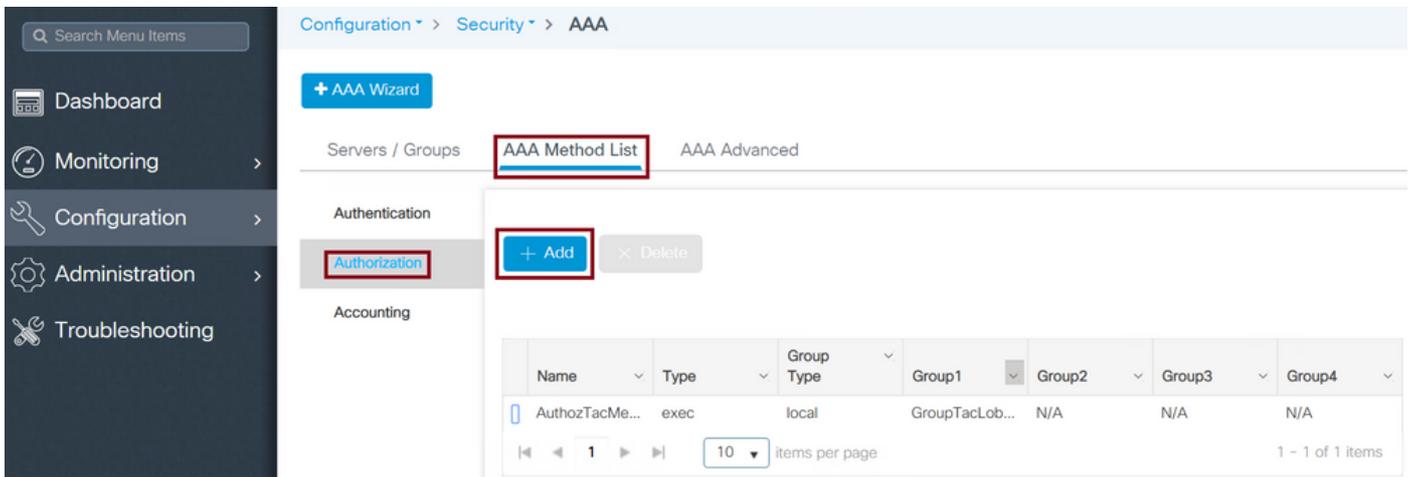
```
Tim-eWLC1(config)#aaa authentication login AutheTacMethod group GroupTacLobby local
Tim-eWLC1(config)#end
```

Schritt 4: Erstellen einer Liste von Autorisierungsmethoden.

Die Autorisierungsmethodenliste legt den Autorisierungstyp für den Lobby-Botschafter fest, der in diesem Fall exec sein wird. Sie ist auch mit derselben konfigurierten Servergruppe verbunden. Es kann auch ausgewählt werden, ob die Authentifizierung lokal auf dem WLC oder extern auf einem TACACS+-Server erfolgt.

Benutzeroberfläche:

Navigieren Sie zu **Konfiguration > Sicherheit > AAA > AAA-Methodenliste > Autorisierung > + Hinzufügen**, wie im Bild gezeigt.



Wenn das Konfigurationsfenster geöffnet wird, geben Sie einen Namen ein, wählen Sie die Option type als exec aus, und weisen Sie die zuvor erstellte Servergruppe zu.

Beachten Sie, dass der Gruppentyp auf die gleiche Weise angewendet wird wie im Abschnitt Authentifizierungsmethodenliste beschrieben.

CLI:

Gruppentyp als lokal.

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

Gruppentyp als Gruppe.

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

Gruppentyp als Gruppe und die Option Fallback an Lokal ist aktiviert.

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

Schritt 5: Weisen Sie die Methoden zu. Nachdem die Methoden konfiguriert wurden, müssen sie den Optionen zugewiesen werden, damit sie sich beim WLC anmelden können, um den Gastbenutzer wie die Leitung VTY oder HTTP (GUI) zu erstellen. Diese Schritte können nicht über die Benutzeroberfläche ausgeführt werden, daher müssen sie über die CLI ausgeführt werden.

HTTP/GUI-Authentifizierung:

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

Wenn Sie Änderungen an den HTTP-Konfigurationen vornehmen, empfiehlt es sich, die HTTP- und HTTPS-Dienste neu zu starten:

```
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
```

Leitung-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
```

Schritt 6: Definieren Sie den Remote-Benutzer. Der auf der ISE für den Lobby-Botschafter erstellte Benutzername muss als Remote-Benutzername auf dem WLC definiert werden. Wenn der Remote-Benutzername nicht im WLC definiert ist, wird die Authentifizierung korrekt ausgeführt, aber der Benutzer erhält vollständigen Zugriff auf den WLC, anstatt nur Zugriff auf die Berechtigungen des Lobby-Botschafters zu haben. Diese Konfiguration kann nur über die CLI vorgenommen werden.

CLI:

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

Konfigurieren der ISE - TACACS+

Schritt 1: Aktivieren Sie Device Admin. Navigieren Sie zu **Administration > System > Deployment**. Bevor Sie fortfahren, wählen Sie **Enable Device Admin Service** und stellen Sie sicher, dass ISE aktiviert wurde, wie im Bild gezeigt.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation path is **Administration > Deployment > Deployment Nodes List > timise23**. The **Edit Node** page is displayed, with the **General Settings** tab selected. The configuration details are as follows:

- Hostname: **timise23**
- FQDN: **timise23.cisco.com**
- IP Address: **192.168.166.8**
- Node Type: **Identity Services Engine (ISE)**
- Role: **STANDALONE** (with a **Make Primary** button)
- Administration:
- Monitoring:
 - Role: **PRIMARY** (dropdown menu)
 - Other Monitoring Node: (text input field)
- Policy Service:
 - Enable Session Services:
 - Include Node in Node Group: **None** (dropdown menu)
 - Enable Profiling Service:
 - Enable Threat Centric NAC Service:
 - Enable SXP Service:
 - Enable Device Admin Service: (highlighted with a red box)

Schritt 2: Fügen Sie den WLC der ISE hinzu. Navigieren Sie zu **Administration > Network Resources > Network Devices > Add**. Der WLC muss der ISE hinzugefügt werden. Wenn Sie den WLC der ISE hinzufügen, aktivieren Sie TACACS+-Authentifizierungseinstellungen, und konfigurieren Sie die erforderlichen Parameter, wie im Bild gezeigt.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation path is **Administration > Network Resources > Network Devices**. The **Network Devices** page is displayed, showing a table of network devices. The **Add** button is highlighted with a red box.

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

Wenn das Konfigurationsfenster geöffnet wird, um einen Namen, IP ADD, anzugeben, aktivieren Sie TACACS+ Authentication Settings, und geben Sie den erforderlichen Shared Secret ein.

Schritt 3: Erstellen Sie den Benutzer Lobby Ambassador auf der ISE. Navigieren Sie zu **Administration > Identity Management > Identities > Users > Add**. Fügen Sie der ISE den Benutzernamen und das Kennwort hinzu, die dem Lobby-Botschafter zugewiesen sind, der die Gastbenutzer erstellt. Dies ist der Benutzernamen, den der Administrator dem Lobby-Botschafter zuweist, wie im Bild gezeigt.

Identity Services Engine Administration

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Results

Network Access Users

Edit Add Change Status Import Export Delete Duplicate

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

Wenn das Konfigurationsfenster geöffnet wird, geben Sie den Namen und das Kennwort für den Benutzer von Lobby Ambassador an. Stellen Sie außerdem sicher, dass der Status aktiviert ist.

Schritt 4: Erstellen Sie ein Ergebnis-TACACS+-Profil. Navigieren Sie zu **Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles (Work Center > Device Administration > Richtlinienelemente > Ergebnisse > TACACS-Profil**, wie im Bild gezeigt. Senden Sie mit diesem Profil die erforderlichen Attribute an den WLC zurück, um den Benutzer als Lobby-Botschafter zu platzieren.

Identity Services Engine Administration

Home Context Visibility Operations Policy Administration Work Centers

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

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

Conditions

Network Conditions

Results

Allowed Protocols

TACACS Command Sets

TACACS Profiles

TACACS Profiles

0 Selected

Refresh Add Duplicate Trash Edit

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

Wenn das Konfigurationsfenster geöffnet wird, geben Sie dem Profil einen Namen ein, konfigurieren Sie auch ein Default Privileged 15 und ein Custom Attribute als Type Obligatory, Name als Benutzertyp und Wert lobby-admin. Lassen Sie außerdem den **allgemeinen Aufgabentyp** als Shell (Shell) auswählen, wie im Bild gezeigt.

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

Schritt 5: Erstellen eines Policy Set Navigieren Sie zu **Work Centers > Device Administration > Device Admin Policy Sets (Geräteadministration > Geräte-Admin-Richtliniensätze)**, wie im Bild gezeigt. Die Bedingungen für die Konfiguration der Richtlinie basieren auf der Entscheidung des Administrators. Für dieses Dokument werden der Status "Network Access - Username" (Netzwerkzugriff - Benutzername) und das Standard Device Admin-Protokoll verwendet. Es ist zwingend erforderlich, unter der Autorisierungsrichtlinie sicherzustellen, dass das unter der Ergebnisautorisierung konfigurierte Profil ausgewählt ist, sodass die erforderlichen Attribute an den WLC zurückgegeben werden können.

Policy Sets

<input type="button" value="+"/>	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
<input checked="" type="checkbox"/>	✔	9800TacacsLobby		Network Access-UserName EQUALS lobbyTac	Default Device Admin	0		

Wenn das Konfigurationsfenster geöffnet wird, konfigurieren Sie die Autorisierungsrichtlinie. Die Authentifizierungsrichtlinie kann wie im Bild gezeigt als Standard beibehalten werden.

Policy Sets → 9800TacacsLobby Reset Save

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)

+	Status	Rule Name	Conditions	Results		Hits	Actions
				Command Sets	Shell Profiles		
✔		9800TacacsAuth	Network Access-UserName EQUALS lobbyTac	Select from list	9800TacacsLobby	0	⚙️

Überprüfung

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

```
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
```

So sieht die GUI der Lobby Ambassador nach erfolgreicher Authentifizierung aus.

Search Menu Items

@ Guest User

+ Add x Delete

User Name	Description	Created By
No items to display		

⏪ 0 ⏩ 10 items per page

Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

RADIUS-Authentifizierung

Für die RADIUS-Authentifizierung können folgende Debugger verwendet werden:

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

Stellen Sie sicher, dass die richtige Methodenliste im Debuggen ausgewählt ist. Außerdem werden die erforderlichen Attribute vom ISE-Server mit dem richtigen Benutzernamen, Benutzertyp und den richtigen Berechtigungen zurückgegeben.

```
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+ authentifizieren

Für die TACACS+-Authentifizierung kann dieses Debuggen verwendet werden:

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

Stellen Sie sicher, dass die Authentifizierung mit dem richtigen Benutzernamen und ISE IP ADD verarbeitet wird. Außerdem sollte der Status "PASS" angezeigt werden. Im gleichen Debugging wird unmittelbar nach der Authentifizierungsphase der Autorisierungsprozess vorgestellt. In dieser Autorisierung stellt Phase sicher, dass der richtige Benutzername zusammen mit der richtigen ISE IP ADD verwendet wird. Ab dieser Phase sollten Sie die Attribute anzeigen können, die auf der ISE konfiguriert sind und die den WLC als Benutzer von Lobby-Botschaftern mit den richtigen Berechtigungen ausweisen.

Beispiel für die Authentifizierungsphase:

```
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)
```

Beispiel für die Autorisierungsphase:

```
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
```

Die zuvor für RADIUS und TACACS+ erwähnten Debugbeispiele enthalten die wichtigsten Schritte für eine erfolgreiche Anmeldung. Die Debug-Dateien sind ausführlicher und die Ausgabe größer. Um das Debuggen zu deaktivieren, kann der folgende Befehl verwendet werden:

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