Configurazione dell'autorizzazione per i punti di accesso in una rete wireless unificata

Sommario

Introduzione

Questo documento descrive come configurare WLC per autorizzare l'Access Point (AP) in base all'indirizzo MAC degli AP.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di come configurare un Cisco Identity Services Engine (ISE)
- Conoscenza della configurazione dei Cisco AP e dei Cisco WLC
- Conoscenza delle soluzioni Cisco Unified Wireless Security

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- WLC con software AireOS 8.8.11.0AP Wave1: 1700/2700/3700 e 3500 (1600/2600/3600 sono ancora supportati, ma il supporto per AireOS termina con la versione 8.5.x)AP Wave2: 1800/2800/3800/4800, 1540 e 1560 Versione ISE 2.3.0.298

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Autorizzazione Lightweight AP

Durante il processo di registrazione degli access point, gli access point e i WLC si autenticano reciprocamente con l'utilizzo di certificati X.509. I certificati X.509 vengono masterizzati in un flash protetto sia sull'access point che sul WLC in fabbrica da Cisco.

Nel punto di accesso, i certificati preinstallati sono denominati certificati di fabbricazione (MIC). Tutti i Cisco AP prodotti dopo il 18 luglio 2005 hanno un MIC.

Oltre a questa autenticazione reciproca che si verifica durante il processo di registrazione, i WLC possono anche limitare gli AP che si registrano con loro in base all'indirizzo MAC dell'AP.

L'assenza di una password complessa tramite l'indirizzo MAC del punto di accesso non è un problema, in quanto il controller utilizza il MIC per autenticare il punto di accesso prima di autorizzarlo tramite il server RADIUS. L'utilizzo di MIC fornisce un'autenticazione avanzata.

L'autorizzazione AP può essere eseguita in due modi:

- Uso dell'elenco delle autorizzazioni interne sul WLC
- Utilizzo del database degli indirizzi MAC su un server AAA

Il comportamento degli access point varia a seconda del certificato utilizzato:

- AP con SSC: il WLC utilizza solo l'elenco delle autorizzazioni interne e non inoltra una richiesta a un server RADIUS per questi AP
- AP con MIC: il WLC può utilizzare l'elenco delle autorizzazioni interne configurato sul WLC o un server RADIUS per autorizzare gli AP

In questo documento viene descritto come usare l'autorizzazione AP sia con l'elenco delle autorizzazioni interne che con il server AAA.

Configurazione

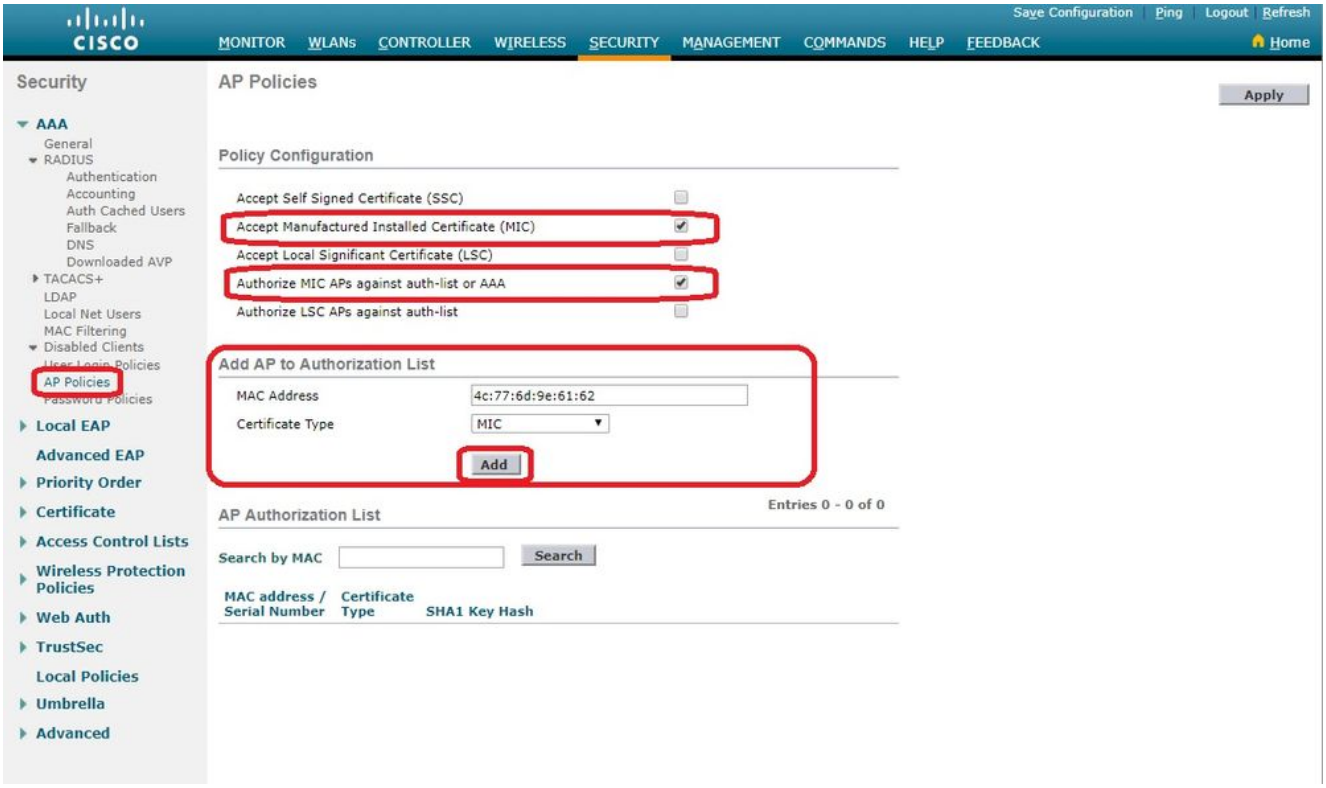
Configurazione con l'elenco delle autorizzazioni interne sul WLC

Sul WLC, usare l'elenco di autorizzazioni AP per limitare gli AP in base al loro indirizzo MAC. L'elenco di autorizzazioni AP è disponibile in **Security > AP Policies** nell'interfaccia utente del WLC.

Nell'esempio viene mostrato come aggiungere l'access point con l'indirizzo MAC **4c:77:6d:9e:61:62**.

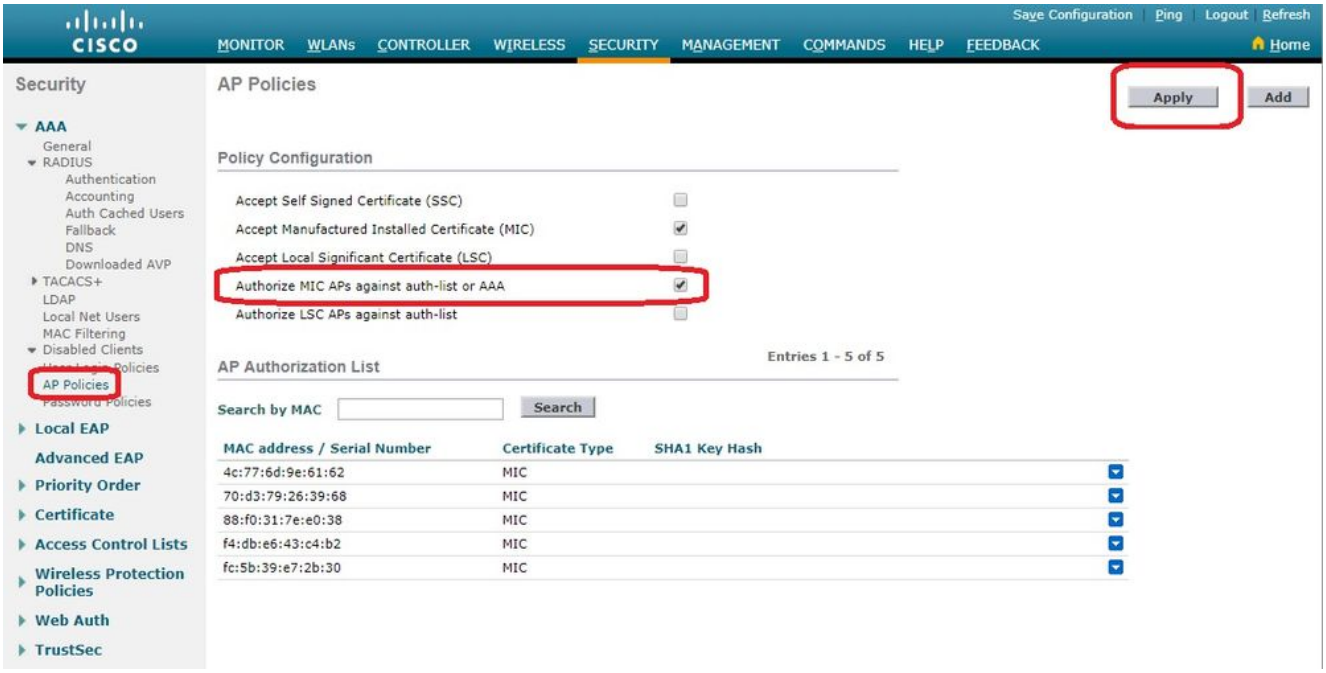
1. Dall'interfaccia utente del controller WLC, fare clic su **Security > AP Policies** e viene visualizzata la pagina Criteri PA.
2. Fare clic sul pulsante **Add** sul lato destro dello schermo.

3. Sotto **Add AP to Authorization List**, immettere il **AP MAC** (non l'indirizzo MAC della radio AP). Scegliere quindi il tipo di certificato e fare clic su **Add**.Nell'esempio, viene aggiunto un access point con un certificato MIC.**Nota:** Per gli access point con SSC, scegliere ssc in Tipo di certificato.



L'access point viene aggiunto all'elenco delle autorizzazioni dell'access point ed è elencato in **AP Authorization List**.

4. In Configurazione criteri selezionare la casella per **Authorize MIC APs against auth-list or AAA**.Quando questo parametro è selezionato, il WLC controlla prima l'elenco delle autorizzazioni locali. Se l'indirizzo MAC AP non è presente, controlla il server RADIUS.



Verifica

Per verificare questa configurazione, è necessario connettere l'access point all'indirizzo MAC **4c:77:6d:9e:61:62** alla rete e al monitor. Utilizzare il **debug capwap events/errors enable** e **debug aaa all enable** per eseguire questa operazione.

Questo output mostra i debug quando l'indirizzo MAC AP non è presente nell'elenco delle autorizzazioni AP:

> **Nota:** Alcune righe dell'output sono state spostate nella seconda riga a causa di vincoli di spazio.

```
(Cisco Controller) >debug capwap events enable
(Cisco Controller) >debug capwap errors enable
(Cisco Controller) >debug aaa all enable

*spamApTask4: Feb 27 10:15:25.592: 70:69:5a:51:4e:c0 Join Request from 192.168.79.151:5256

*spamApTask4: Feb 27 10:15:25.592: 70:69:5a:51:4e:c0 Unable to get Ap mode in Join request

*spamApTask4: Feb 27 10:15:25.592: 70:69:5a:51:4e:c0 Allocate database entry for AP
192.168.79.151:5256, already allocated index 277

*spamApTask4: Feb 27 10:15:25.592: 70:69:5a:51:4e:c0 AP Allocate request at index 277 (reserved)
*spamApTask4: Feb 27 10:15:25.593: 24:7e:12:19:41:ef Deleting AP entry 192.168.79.151:5256 from
temporary database.
*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 AP group received default-group is found in
ap group configured in wlc.

*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Dropping request or response packet to AP
:192.168.79.151 (5256) by Controller: 10.48.71.20 (5246), message Capwap_wtp_event_response,
state Capwap_no_state
```

*spamApTask4: Feb 27 10:15:25.593: **70:69:5a:51:4e:c0 In AAA state 'Idle' for AP 70:69:5a:51:4e:c0**
*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Join Request failed!

*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 State machine handler: Failed to process msg type = 3 state = 0 from 192.168.79.151:5256

*aaaQueueReader: Feb 27 10:15:25.593: **Unable to find requested user entry for 4c776d9e6162**
*aaaQueueReader: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Normal Response code for AAA Authentication : -9
*aaaQueueReader: Feb 27 10:15:25.593: ReProcessAuthentication previous proto 8, next proto 40000001
*aaaQueueReader: Feb 27 10:15:25.593: AuthenticationRequest: 0x7f01b4083638

*aaaQueueReader: Feb 27 10:15:25.593: Callback.....................................0xd6cef02166

*aaaQueueReader: Feb 27 10:15:25.593: protocolType.................................0x40000001

*aaaQueueReader: Feb 27 10:15:25.593: proxyState.....................................70:69:5A:51:4E:C0-00:00

*aaaQueueReader: Feb 27 10:15:25.593: Packet contains 9 AVPs:

*aaaQueueReader: Feb 27 10:15:25.593: AVP[01] User-Name.............................4c776d9e6162 (12 bytes)

*aaaQueueReader: Feb 27 10:15:25.593: AVP[02] Called-Station-Id.....................70-69-5a-51-4e-c0 (17 bytes)

*aaaQueueReader: Feb 27 10:15:25.593: AVP[03] Calling-Station-Id.....................4c-77-6d-9e-61-62 (17 bytes)

*aaaQueueReader: Feb 27 10:15:25.593: AVP[04] Nas-Port...............................0x00000001 (1) (4 bytes)

*aaaQueueReader: Feb 27 10:15:25.593: AVP[05] Nas-Ip-Address.........................0x0a304714 (170936084) (4 bytes)

*aaaQueueReader: Feb 27 10:15:25.593: AVP[06] NAS-Identifier.........................0x6e6f (28271) (2 bytes)

*aaaQueueReader: Feb 27 10:15:25.593: AVP[07] User-Password...........................[...]

*aaaQueueReader: Feb 27 10:15:25.593: AVP[08] Service-Type...........................0x0000000a (10) (4 bytes)

*aaaQueueReader: Feb 27 10:15:25.593: AVP[09] Message-Authenticator...................DATA (16 bytes)

*aaaQueueReader: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Error Response code for AAA Authentication : -7
*aaaQueueReader: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Returning AAA Error 'No Server' (-7) for mobile 70:69:5a:51:4e:c0 serverIdx 0
*aaaQueueReader: Feb 27 10:15:25.593: AuthorizationResponse: 0x7f017adf5770

*aaaQueueReader: Feb 27 10:15:25.593: RadiusIndexSet(0), Index(0)
*aaaQueueReader: Feb 27 10:15:25.593: resultCode.....................................-7

*aaaQueueReader: Feb 27 10:15:25.593: protocolUsed.....................................0xffffffff

*aaaQueueReader: Feb 27 10:15:25.593: proxyState.....................................70:69:5A:51:4E:C0-00:00

```
*aaaQueueReader: Feb 27 10:15:25.593: Packet contains 0 AVPs:

*aaaQueueReader: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 User entry not found in the Local FileDB
for the client.

*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Join Version: = 134770432

*spamApTask0: Feb 27 10:15:25.593: 00:00:00:00:00:00 apType = 54 apModel: AIR-AP4800-E-K

*spamApTask0: Feb 27 10:15:25.593: 00:00:00:00:00:00 apType: Ox36 bundleApImageVer: 8.8.111.0
*spamApTask0: Feb 27 10:15:25.593: 00:00:00:00:00:00 version:8 release:8 maint:111 build:0
*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Join resp: CAPWAP Maximum Msg element len =
79

*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Join Failure Response sent to 0.0.0.0:5256

*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Radius Authentication failed. Closing dtls
Connection.
*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Disconnecting DTLS Capwap-Ctrl session
0xd6f0724fd8 for AP (192:168:79:151/5256). Notify(true)
*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 CAPWAP State: Dtls tear down

*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 acDtlsPlumbControlPlaneKeys:
lrad:192.168.79.151(5256) mwar:10.48.71.20(5246)

*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 DTLS keys for Control Plane deleted
successfully for AP 192.168.79.151

*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 DTLS connection closed event receivedserver
(10.48.71.20/5246) client (192.168.79.151/5256)
*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Entry exists for AP (192.168.79.151/5256)
*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 AP Delete request
*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 AP Delete request
*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Unable to find AP 70:69:5a:51:4e:c0
*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 No AP entry exist in temporary database for
192.168.79.151:5256
```

Questo output mostra i debug quando l'indirizzo MAC LAP viene aggiunto all'elenco delle autorizzazioni dei punti di accesso:

> **Nota:** Alcune righe dell'output sono state spostate nella seconda riga a causa di vincoli di spazio.

```
(Cisco Controller) >debug capwap events enable
(Cisco Controller) >debug capwap errors enable
(Cisco Controller) >debug aaa all enable

*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 Join Request from 192.168.79.151:5256

*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 using already alloced index 274
*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 Unable to get Ap mode in Join request

*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 Allocate database entry for AP
192.168.79.151:5256, already allocated index 274

*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 AP Allocate request at index 274 (reserved)
*spamApTask4: Feb 27 09:50:25.393: 24:7e:12:19:41:ef Deleting AP entry 192.168.79.151:5256 from
temporary database.
*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 AP group received default-group is found in
ap group configured in wlc.
```

```
*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 Dropping request or response packet to AP
:192.168.79.151 (5256) by Controller: 10.48.71.20 (5246), message Capwap_wtp_event_response,
state Capwap_no_state

*spamApTask4: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Message type Capwap_wtp_event_response is
not allowed to send in state Capwap_no_state for AP 192.168.79.151

*spamApTask4: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 In AAA state 'Idle' for AP
70:69:5a:51:4e:c0
*spamApTask4: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Join Request failed!


*aaaQueueReader: Feb 27 09:50:25.394: User 4c776d9e6162 authenticated
*aaaQueueReader: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Normal Response code for AAA
Authentication : 0
*aaaQueueReader: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Returning AAA Success for mobile
70:69:5a:51:4e:c0
*aaaQueueReader: Feb 27 09:50:25.394: AuthorizationResponse: 0x7f0288a66408


*aaaQueueReader: Feb 27 09:50:25.394: structureSize.............................194

*aaaQueueReader: Feb 27 09:50:25.394: resultCode.................................0

*aaaQueueReader: Feb 27 09:50:25.394:
proxyState.................................70:69:5A:51:4E:C0-00:00

*aaaQueueReader: Feb 27 09:50:25.394: Packet contains 2 AVPs:

*aaaQueueReader: Feb 27 09:50:25.394: AVP[01] Service-
Type.........................0x00000065 (101) (4 bytes)

*aaaQueueReader: Feb 27 09:50:25.394: AVP[02] Airespace / WLAN-
Identifier.............0x00000000 (0) (4 bytes)

*aaaQueueReader: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 User authentication Success with File DB
on WLAN ID :0
*spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Join Version: = 134770432

*spamApTask0: Feb 27 09:50:25.394: 00:00:00:00:00:00 apType = 54 apModel: AIR-AP4800-E-K

*spamApTask0: Feb 27 09:50:25.394: 00:00:00:00:00:00 apType: Ox36 bundleApImageVer: 8.8.111.0
*spamApTask0: Feb 27 09:50:25.394: 00:00:00:00:00:00 version:8 release:8 maint:111 build:0
*spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Join resp: CAPWAP Maximum Msg element len =
79

*spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Join Response sent to 0.0.0.0:5256

*spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 CAPWAP State: Join

*spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 capwap_ac_platform.c:2095 - Operation State
0 ===> 4
*spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Capwap State Change Event (Reg) from
capwap_ac_platform.c 2136

*apfReceiveTask: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Register LWAPP event for AP
70:69:5a:51:4e:c0 slot 0
```

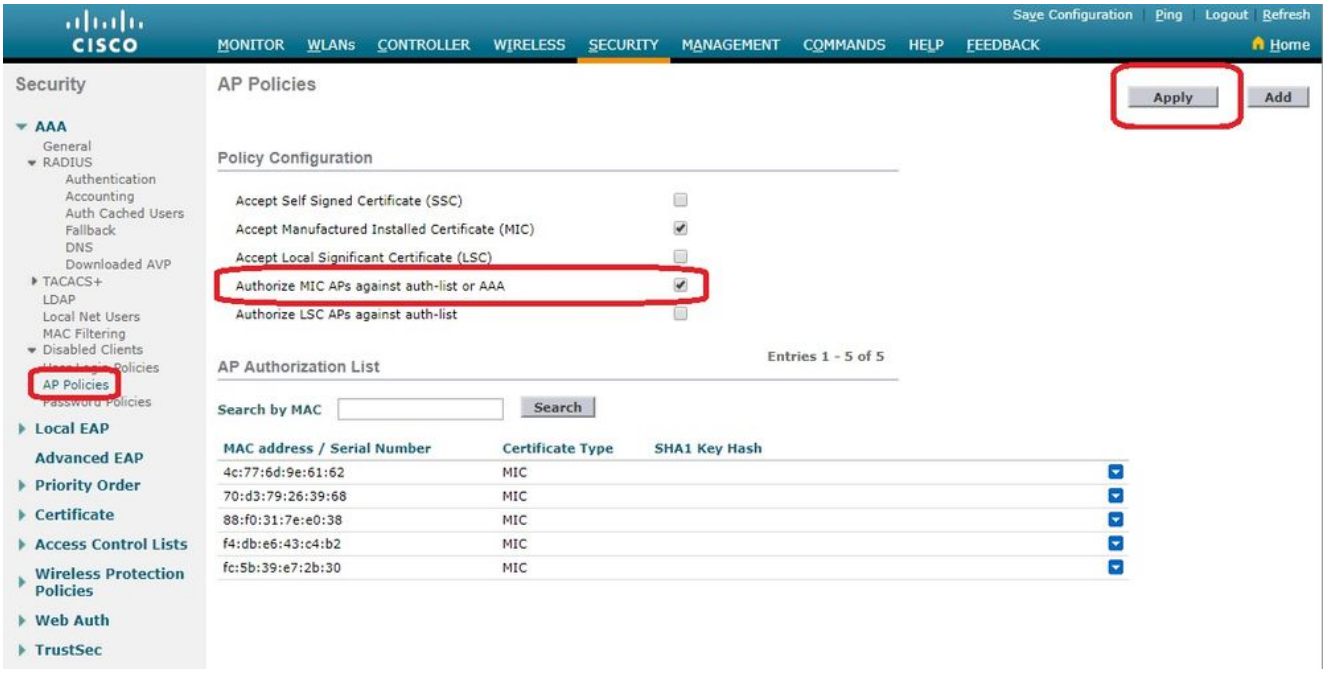
Autorizzazione AP rispetto a un server AAA

Èinoltre possibile configurare i WLC in modo che utilizzino i server RADIUS per autorizzare i punti

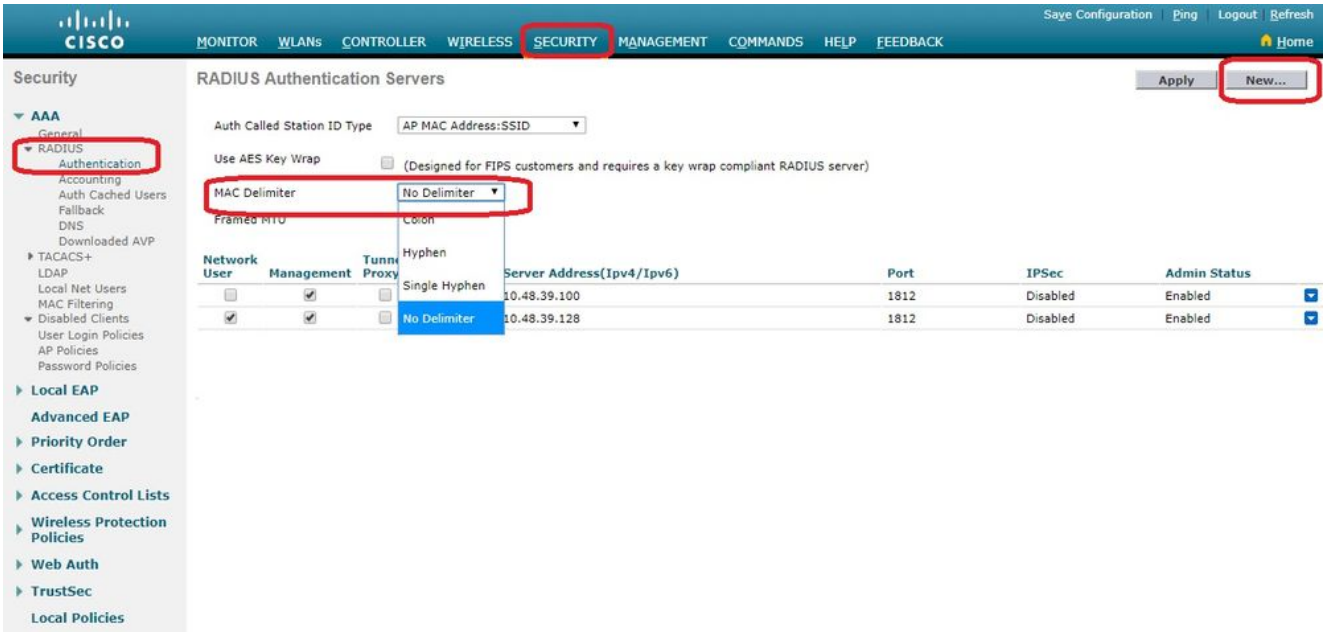
di accesso tramite i MIC. Quando invia le informazioni a un server RADIUS, il WLC utilizza un indirizzo MAC AP sia come nome utente che come password. Ad esempio, se l'indirizzo MAC dell'access point è **4c:77:6d:9e:61:62**Sia il nome utente che la password utilizzati dal controller per autorizzare l'access point sono l'indirizzo MAC specificato utilizzando il delimitatore definito.

Nell'esempio viene mostrato come configurare i WLC per autorizzare gli AP utilizzando Cisco ISE.

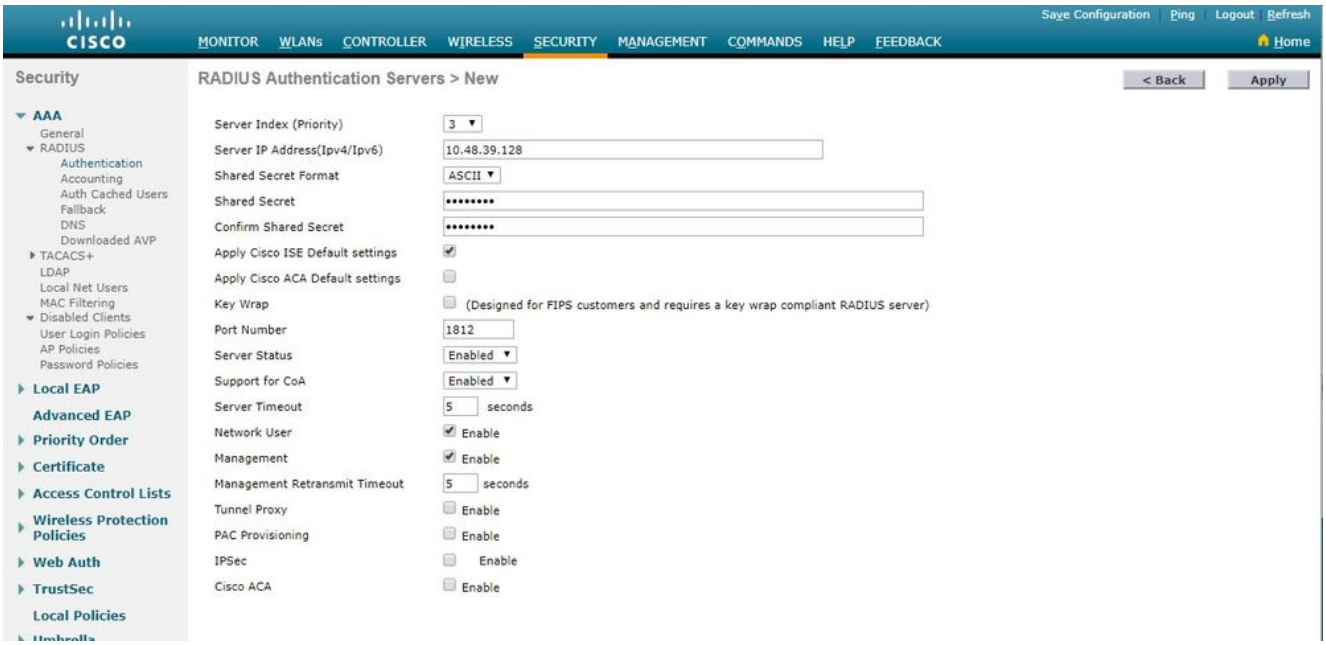
1. Dall'interfaccia utente del controller WLC, fare clic su **Security > AP Policies**. Viene visualizzata la pagina Criteri PA.
2. In Configurazione criteri selezionare la casella per **Authorize MIC APs against auth-list or AAA**.Quando si sceglie questo parametro, il WLC controlla prima l'elenco delle autorizzazioni locali. Se l'indirizzo MAC AP non è presente, controlla il server RADIUS.



3. Passa a **Security > RADIUS Authentication** dalla GUI del controller per visualizzare **RADIUS Authentication Servers** pagina. In questa pagina è possibile definire il **delimitatore MAC**. Il WLC ottiene l'indirizzo MAC dell'access point e lo invia al server Radius utilizzando il delimitatore definito qui. questo è importante affinché il nome utente corrisponda a quello configurato nel server Radius. Nell'esempio riportato di seguito **No Delimiter** viene utilizzato in modo che il nome utente sia **4c776d9e6162**.



4. Quindi, fare clic su **New** per definire un server RADIUS.



5. Definire i parametri del server RADIUS su **RADIUS Authentication Servers > New** pagina. Questi parametri includono RADIUS **Server IP Address**, **Shared Secret**, **Port Number**,e **Server Status**. Al termine, fare clic su **Apply**. In questo esempio viene usato Cisco ISE come server RADIUS con indirizzo IP 10.48.39.128.

Configurazione di Cisco ISE per l'autorizzazione degli access point

Per abilitare Cisco ISE all'autorizzazione degli access point, completare i seguenti passaggi:

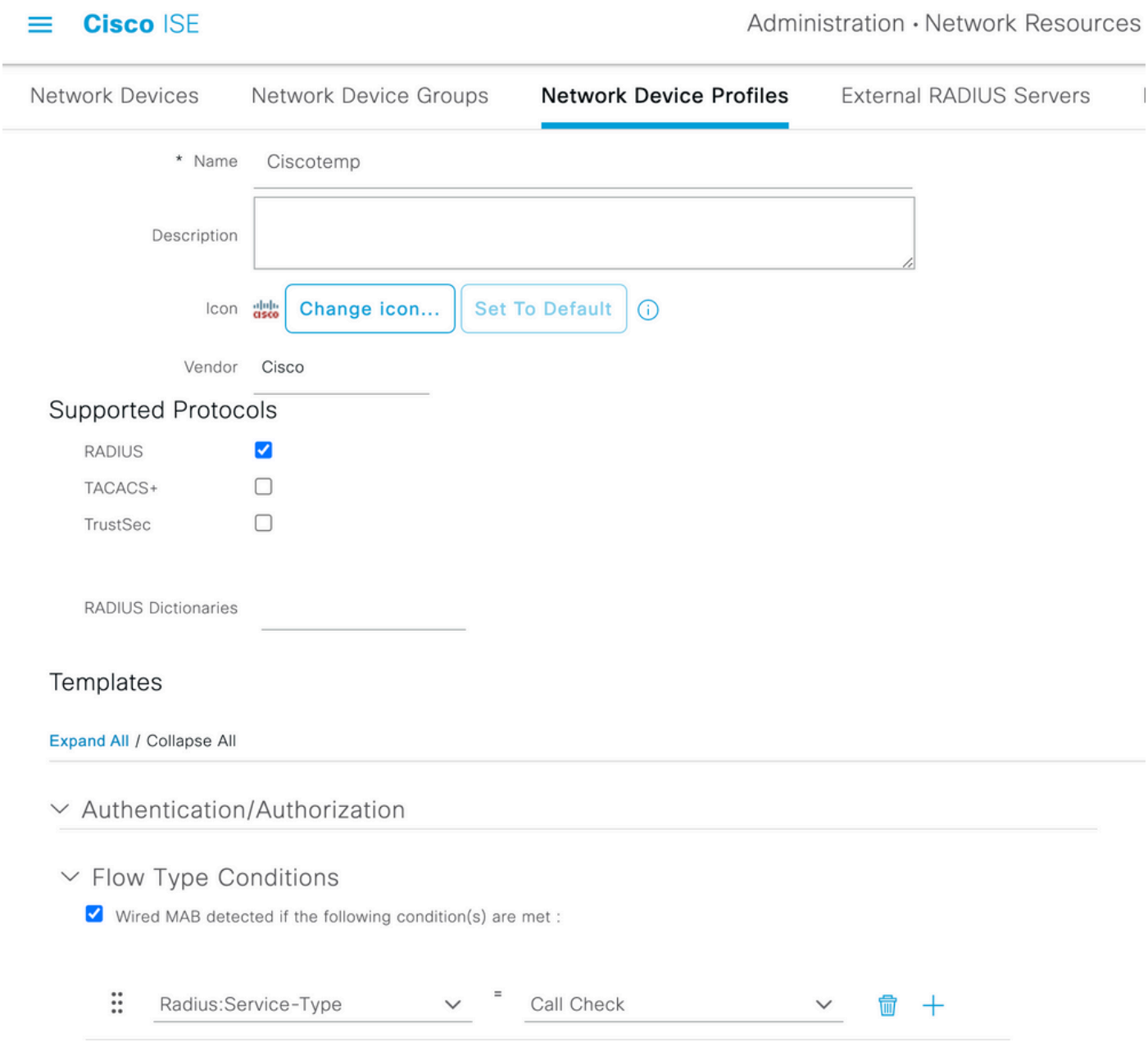
1. Configurare il WLC come client AAA su Cisco ISE.
2. Aggiungere gli indirizzi MAC AP al database su Cisco ISE.

Tuttavia, è possibile aggiungere l'indirizzo MAC AP come endpoint (il modo migliore) o come utenti (le cui password sono anche l'indirizzo MAC), ma questo richiede di ridurre i requisiti dei criteri di sicurezza delle password.

Poiché il WLC non invia l'attributo NAS-Port-Type, che è un requisito su ISE per corrispondere al flusso di lavoro MAB (Mac Address Authentication), è necessario modificare questa impostazione.

Configurazione di un nuovo profilo di dispositivo in cui MAB non richiede l'attributo NAS-Port-Type

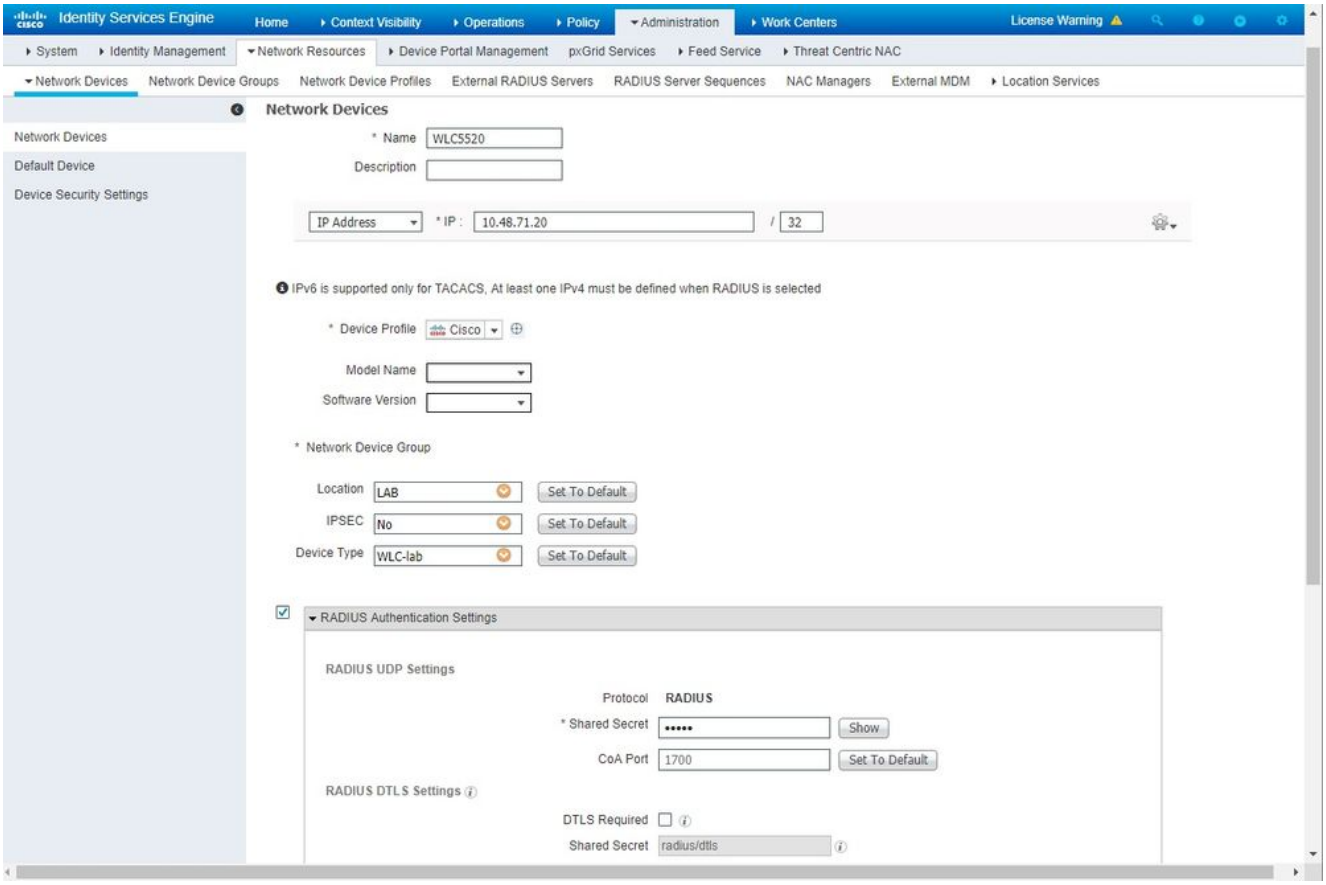
Passa a **Administration > Network device profile** e creare un nuovo profilo di dispositivo. Abilitare RADIUS e impostare il flusso MAB cablato per richiedere service-type=Call-check, come illustrato nell'immagine. È possibile copiare altre impostazioni dal profilo Cisco classico, ma l'idea è di non richiedere l'attributo 'Nas-port-type' per un flusso di lavoro Wired MAB.



Configurazione del WLC come client AAA su Cisco ISE

1. Vai a **Administration > Network Resources > Network Devices > Add**. Viene visualizzata la pagina Nuovo dispositivo di rete.
2. In questa pagina definire il WLC **Name**, Interfaccia di gestione **IP Address** e **Radius Authentications Settings** mi piace **Shared Secret**. Se si intende immettere

gli indirizzi MAC AP come endpoint, verificare di utilizzare il profilo di dispositivo personalizzato configurato in precedenza anziché quello predefinito di Cisco.



3. Clic **Submit**.

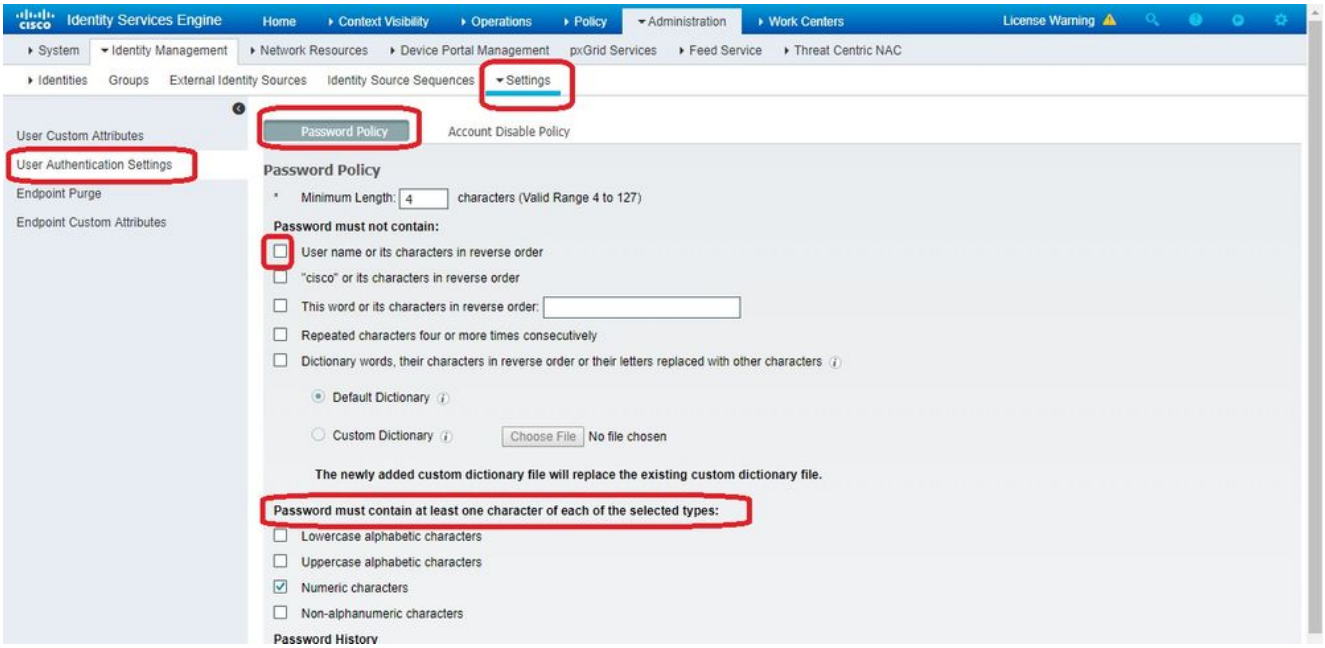
Aggiungere l'indirizzo MAC AP al database degli endpoint su Cisco ISE

Passa a **Administration > Identity Management > Identities** e aggiungere gli indirizzi MAC al database dell'endpoint.

Aggiungere l'indirizzo MAC AP al database utenti su Cisco ISE (facoltativo)

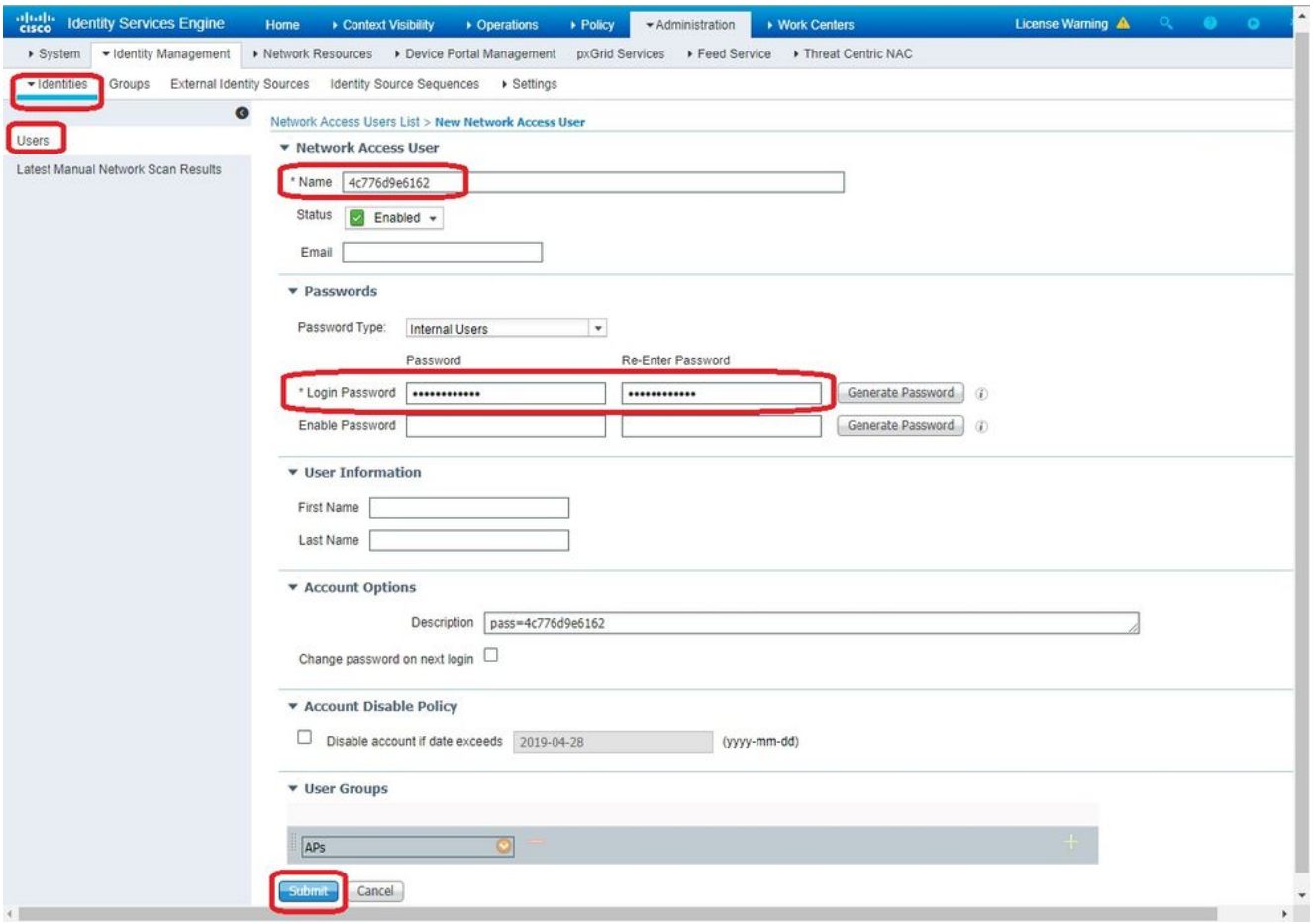
Se non si desidera modificare il profilo MAC cablato e si sceglie di impostare l'indirizzo MAC AP come utente, è necessario ridurre i requisiti dei criteri password.

1. Passa a **Administration > Identity Management**. A questo punto è necessario verificare che i criteri per la password consentano l'utilizzo del nome utente come password e che i criteri consentano anche l'utilizzo dei caratteri dell'indirizzo MAC senza la necessità di utilizzare tipi di caratteri diversi. Passa a **Settings > User Authentication Settings > Password Policy**:



2. Passare quindi a **Identities > Users** e fare clic su **Add**. Quando viene visualizzata la pagina Configurazione utente, definire il nome utente e la password per l'access point come mostrato.

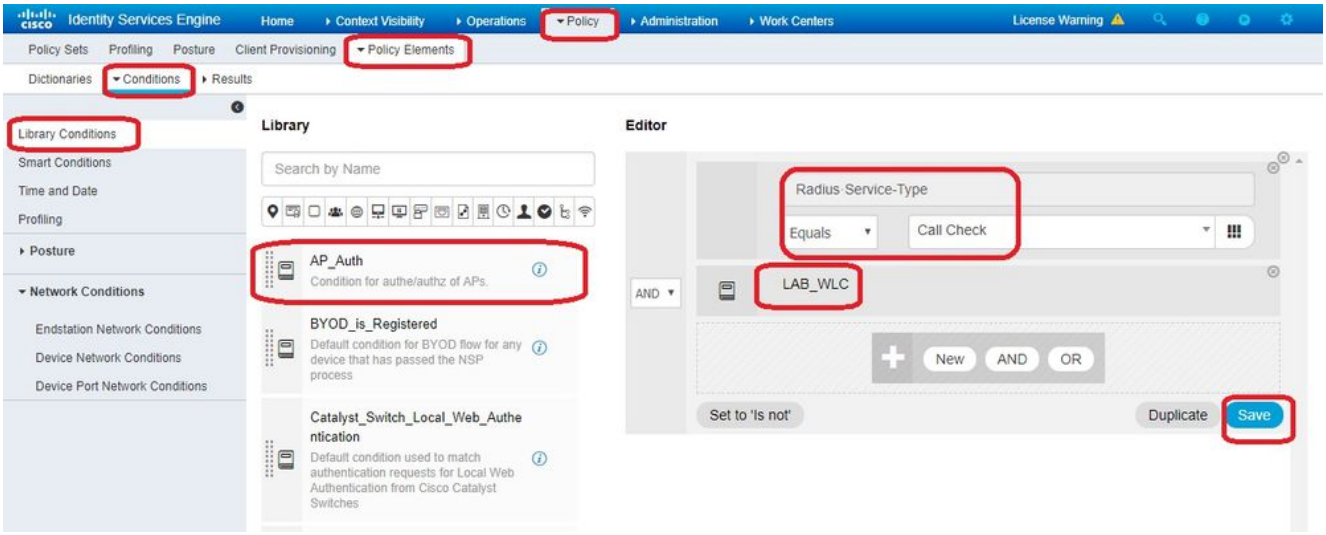
   Suggerimento: Utilizzare il **Description** per immettere la password in un secondo momento, in modo da poter identificare facilmente la password.
   La password deve essere anche l'indirizzo MAC dell'access point. In questo esempio, è **4c776d9e6162**.



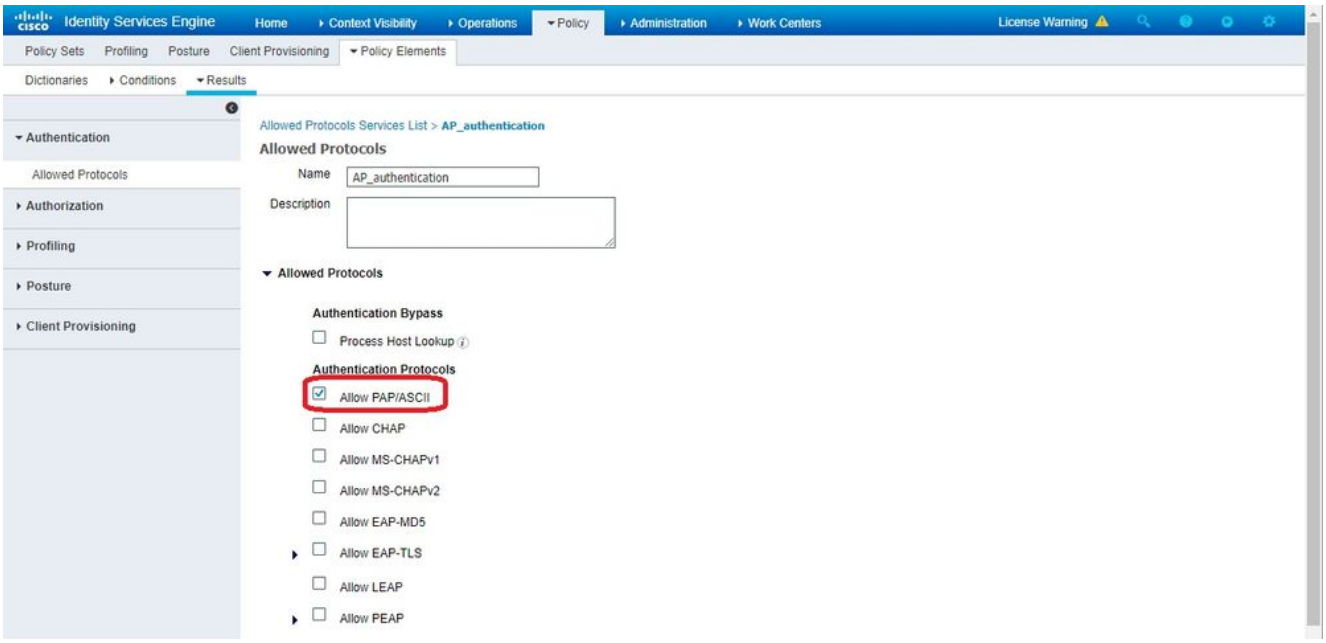
3. Clic **Submit**.

Definisci set di criteri

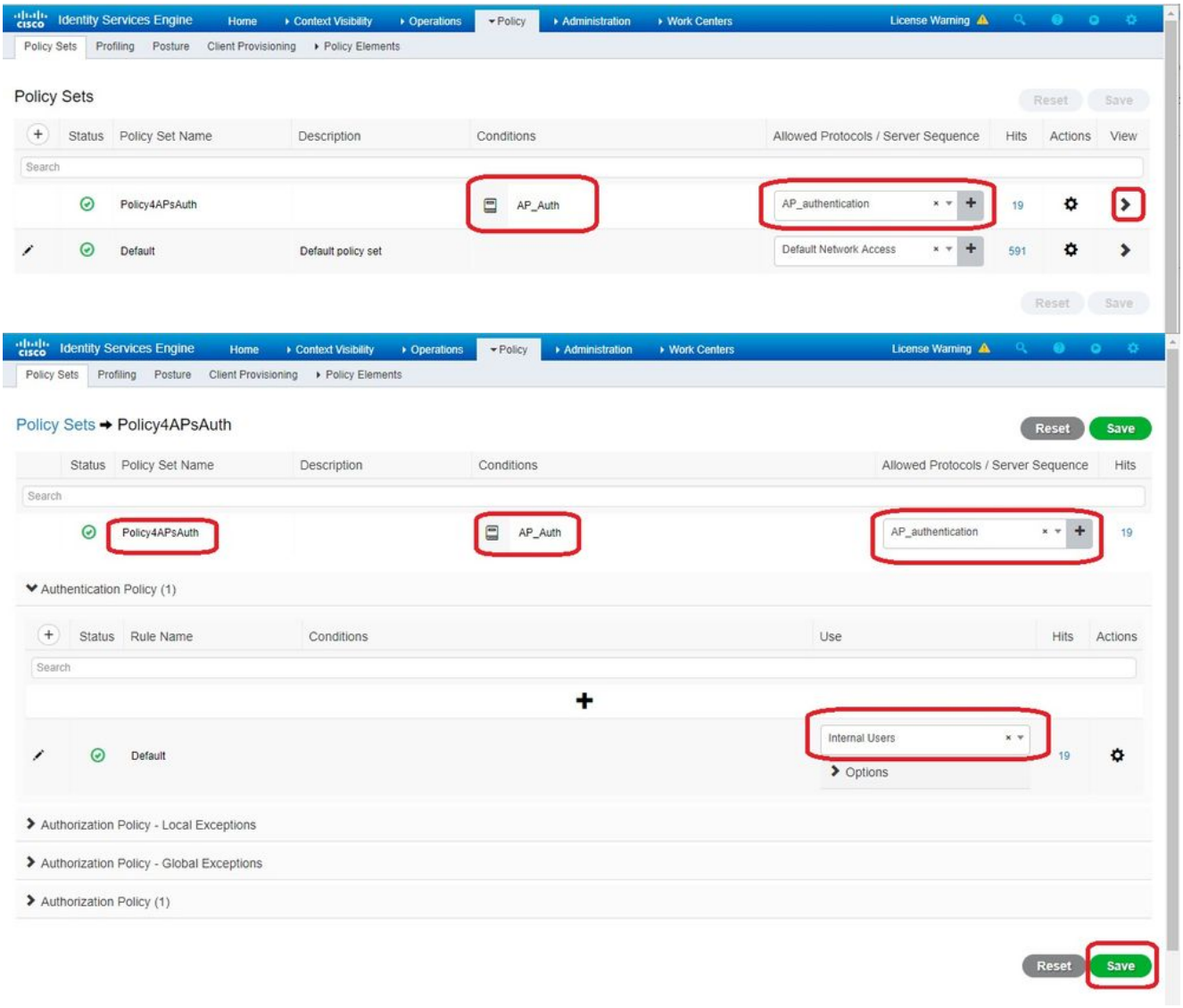
1. Ènecessario definire un **Policy Set** per soddisfare la richiesta di autenticazione proveniente dal WLC. Per prima cosa, creare una condizione passando a **Policy > Policy Elements > Conditions**e creando una nuova condizione corrispondente alla posizione WLC, in questo esempio 'LAB_WLC' e **Radius:Service-Type Equals Call Check** utilizzato per l'autenticazione Mac. La condizione è denominata 'AP_Auth'.



2. Clic **Save**.
3. Quindi crea un nuovo **Allowed Protocols Service** per l'autenticazione AP. Accertati di scegliere solo **Allow PAP/ASCII**:



4. Scegliere il servizio creato in precedenza nel **Allowed Protocols/Server Sequence**. Espandere la **View** e inferiore **Authentication Policy > Use > Internal Users** in modo che ISE cerchi nel database interno il nome utente/la password dell'access point.



5. Clic **Save**.

Verifica

Per verificare questa configurazione, è necessario connettere l'access point con indirizzo MAC 4c:77:6d:9e:61:62 alla rete e al monitor. Utilizzare
il **debug capwap events/errors enable** e **debug aaa all enable** per eseguire questa operazione.

Come si evince dai debug, il WLC ha passato l'indirizzo MAC dell'access point al server RADIUS 10.48.39.128 e il server ha autenticato correttamente l'access point. L'access point si registra quindi con il controller.

> **Nota:** Alcune righe dell'output sono state spostate nella seconda riga a causa di vincoli di spazio.

```
*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Join Request from 192.168.79.151:5248

*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 using already alloced index 437
*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Unable to get Ap mode in Join request

*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Allocate database entry for AP
```

192.168.79.151:5248, already allocated index 437

*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 AP Allocate request at index 437 (reserved)
*spamApTask4: Feb 27 14:58:07.566: 24:7e:12:19:41:ef Deleting AP entry 192.168.79.151:5248 from temporary database.
*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 AP group received default-group is found in ap group configured in wlc.

*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Dropping request or response packet to AP :192.168.79.151 (5248) by Controller: 10.48.71.20 (5246), message Capwap_wtp_event_response, state Capwap_no_state

*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Message type Capwap_wtp_event_response is not allowed to send in state Capwap_no_state for AP 192.168.79.151

*spamApTask4: Feb 27 14:58:07.566: **70:69:5a:51:4e:c0 In AAA state 'Idle' for AP 70:69:5a:51:4e:c0**
*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Join Request failed!

*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 State machine handler: Failed to process msg type = 3 state = 0 from 192.168.79.151:5248

*spamApTask4: Feb 27 14:58:07.566: 24:7e:12:19:41:ef Failed to parse CAPWAP packet from 192.168.79.151:5248

*aaaQueueReader: Feb 27 14:58:07.566: **70:69:5a:51:4e:c0 Normal Response code for AAA Authentication : -9**
*aaaQueueReader: Feb 27 14:58:07.566: ReProcessAuthentication previous proto 8, next proto 40000001
*aaaQueueReader: Feb 27 14:58:07.566: AuthenticationRequest: 0x7f01b404f0f8

*aaaQueueReader: Feb 27 14:58:07.566: Callback.....0xd6cef02166

*aaaQueueReader: Feb 27 14:58:07.566: protocolType.....0x40000001

*aaaQueueReader: Feb 27 14:58:07.566: proxyState.....70:69:5A:51:4E:C0-00:00

*aaaQueueReader: Feb 27 14:58:07.566: Packet contains 9 AVPs:

*aaaQueueReader: Feb 27 14:58:07.566: AVP[02] Called-Station-Id.....70:69:5a:51:4e:c0 (17 bytes)

*aaaQueueReader: Feb 27 14:58:07.566: AVP[03] Calling-Station-Id.....4c:77:6d:9e:61:62 (17 bytes)

*aaaQueueReader: Feb 27 14:58:07.566: AVP[04] Nas-Port.....0x00000001 (1) (4 bytes)

*aaaQueueReader: Feb 27 14:58:07.566: AVP[05] Nas-Ip-Address.....0x0a304714 (170936084) (4 bytes)

*aaaQueueReader: Feb 27 14:58:07.566: AVP[06] NAS-Identifier.....0x6e6f (28271) (2 bytes)

*aaaQueueReader: Feb 27 14:58:07.566: AVP[08] Service-Type.....0x0000000a (10) (4 bytes)

*aaaQueueReader: Feb 27 14:58:07.566: AVP[09] Message-Authenticator.....DATA (16 bytes)

*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 radiusServerFallbackPassiveStateUpdate: **RADIUS server is ready 10.48.39.128 port 1812** index 1 active 1

*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 NAI-Realm not enabled on Wlan, radius servers will be selected as usual
*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Found the radius server : 10.48.39.128 from the global server list
*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Send Radius Auth Request with pktId:185 into qid:0 of server at index:1
*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Sending the packet to v4 host 10.48.39.128:1812 of length 130
*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 **Successful transmission of Authentication Packet (pktId 185) to 10.48.39.128:1812** from server queue 0, proxy state 70:69:5a:51:4e:c0-00:00
*aaaQueueReader: Feb 27 14:58:07.566: 00000000: 01 b9 00 82 d9 c2 ef 27 f1 bb e4 9f a8 88 5a 6d ....'......Zm
*aaaQueueReader: Feb 27 14:58:07.566: 00000010: 4b 38 1a a6 01 0e 34 63 37 37 36 64 39 65 36 31 K8....4c776d9e61
*aaaQueueReader: Feb 27 14:58:07.566: 00000020: 36 32 1e 13 37 30 3a 36 39 3a 35 61 3a 35 31 3a 62..70:69:5a:51:
*aaaQueueReader: Feb 27 14:58:07.566: 00000030: 34 65 3a 63 30 1f 13 34 63 3a 37 37 3a 36 64 3a 4e:c0..4c:77:6d:
*aaaQueueReader: Feb 27 14:58:07.566: 00000040: 39 65 3a 36 31 3a 36 32 05 06 00 00 00 01 04 06 9e:61:62........
*aaaQueueReader: Feb 27 14:58:07.566: 00000050: 0a 30 47 14 20 04 6e 6f 02 12 54 46 96 61 2a 38 .0G...no..TF.a*8
*aaaQueueReader: Feb 27 14:58:07.566: 00000060: 5a 57 22 5b 41 c8 13 61 97 6c 06 06 00 00 00 0a ZW"[A..a.l......
*aaaQueueReader: Feb 27 14:58:07.566: 00000080: 15 f9 ..
*aaaQueueReader: Feb 27 14:58:07.566: **70:69:5a:51:4e:c0 User entry not found in the Local FileDB for the client.**
*radiusTransportThread: Feb 27 14:58:07.587: Vendor Specif Radius Attribute(code=26, avp_len=28, vId=9)
*radiusTransportThread: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 *** Counted VSA 150994944 AVP of length 28, code 1 atrlen 22)
*radiusTransportThread: Feb 27 14:58:07.588: Vendor Specif Radius Attribute(code=26, avp_len=28, vId=9)
*radiusTransportThread: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 AVP: VendorId: 9, vendorType: 1, vendorLen: 22

*radiusTransportThread: Feb 27 14:58:07.588: 00000000: 70 72 6f 66 69 6c 65 2d 6e 61 6d 65 3d 55 6e 6b profile-name=Unk
*radiusTransportThread: Feb 27 14:58:07.588: 00000010: 6e 6f 77 6e nown
*radiusTransportThread: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 Processed VSA 9, type 1, raw bytes 22, copied 0 bytes
*radiusTransportThread: Feb 27 14:58:07.588: **70:69:5a:51:4e:c0 Access-Accept received from RADIUS server 10.48.39.128** (qid:0) with port:1812, pktId:185
*radiusTransportThread: Feb 27 14:58:07.588: RadiusIndexSet(1), Index(1)
*radiusTransportThread: Feb 27 14:58:07.588: structureSize.....432

*radiusTransportThread: Feb 27 14:58:07.588: protocolUsed.....0x00000001

*radiusTransportThread: Feb 27 14:58:07.588: proxyState.....70:69:5A:51:4E:C0-00:00

*radiusTransportThread: Feb 27 14:58:07.588: Packet contains 4 AVPs:

*radiusTransportThread: Feb 27 14:58:07.588: **AVP[01] User-Name.....4c776d9e6162** (12 bytes)

*radiusTransportThread: Feb 27 14:58:07.588: AVP[02] State.....ReauthSession:0a302780bNEx79SKIFosJ2ioAmIYNOiRe2iDSY3drcFsHuYpChs (65 bytes)

*radiusTransportThread: Feb 27 14:58:07.588: AVP[03] Class.....DATA (83 bytes)

```
*radiusTransportThread: Feb 27 14:58:07.588: AVP[04] Message-
Authenticator.....................DATA (16 bytes)

*spamApTask0: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 Join Version: = 134770432

*spamApTask0: Feb 27 14:58:07.588: 00:00:00:00:00:00 apType = 54 apModel: AIR-AP4800-E-K

*spamApTask0: Feb 27 14:58:07.588: 00:00:00:00:00:00 apType: Ox36 bundleApImageVer: 8.8.111.0
*spamApTask0: Feb 27 14:58:07.588: 00:00:00:00:00:00 version:8 release:8 maint:111 build:0
*spamApTask0: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 Join resp: CAPWAP Maximum Msg element len =
79

*spamApTask0: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 Join Response sent to 0.0.0.0:5248

*spamApTask0: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 CAPWAP State: Join
```

Risoluzione dei problemi

Utilizzare questi comandi per risolvere i problemi relativi alla configurazione:

- debug capwap events enable- Configura il debug degli eventi LWAPP
- debug capwap packet enable— Configura il debug della traccia del pacchetto LWAPP
- debug capwap errors enable— Configura il debug degli errori del pacchetto LWAPP
- debug aaa all enable- Configura il debug di tutti i messaggi AAA

Nel caso in cui, nel registro RADIUS live, ISE restituisca il nome utente 'INVALID' nel momento in cui gli access point vengono autorizzati per ISE, significa che l'autenticazione viene verificata rispetto al database dell'endpoint e che il profilo MAB cablato non è stato modificato, come spiegato in questo documento. ISE considera non valida l'autenticazione dell'indirizzo MAC se non corrisponde al profilo MAC Wired/Wireless, che per impostazione predefinita richiede l'attributo NAS-port-type che non è inviato dal WLC.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).