Standardizzazione dell'autenticazione AP 802.1X cablata con IBNS 2.0 e modelli di interfaccia

Sommario

Introduzione

Questo documento descrive la configurazione 802.1X con i modelli di interfaccia IBNS 2.0.

Dichiarazione di problema

L'utilizzo di IEEE 802.1X per la sicurezza delle porte è una procedura consigliata comune. Oltre a migliorare la sicurezza della rete, semplifica anche le installazioni degli switch consentendo una configurazione standardizzata delle porte di accesso in tutta la rete.

In questa guida viene descritto come utilizzare una configurazione di switchport singola e

standardizzata sia per i dispositivi terminali che per i Cisco Access Point (AP). Benché ogni porta dello switch operi inizialmente come porta di accesso standard ed esegua l'autenticazione IEEE 802.1X, un access point autenticato può richiedere una modalità operativa diversa a seconda dello scenario di implementazione.

In particolare, i punti di accesso che funzionano in modalità di commutazione locale FlexConnect devono funzionare su una porta trunk perché il traffico client da più SSID viene gestito localmente. Di conseguenza, dopo un'autenticazione riuscita, l'interfaccia dello switch deve passare dinamicamente da una porta di accesso a una porta trunk.

Le porte di accesso che connettono dispositivi dell'infrastruttura anziché dispositivi terminali semplici spesso richiedono configurazioni dell'interfaccia diverse dal comportamento predefinito delle porte di accesso.

Di conseguenza, la configurazione dell'interfaccia dello switch deve essere modificata dinamicamente durante il processo di autenticazione. Nel corso degli anni, sono stati utilizzati diversi approcci per ottenere questo comportamento, tra cui le applet Auto SmartPorts e Embedded Event Manager (EEM). Attualmente, la soluzione consigliata è IBNS 2.0 [1] in combinazione con i modelli di interfaccia, che forniscono un metodo scalabile e coerente per modificare in modo dinamico la configurazione dell'interfaccia dopo l'autenticazione.

Approccio

Per un'installazione funzionante, è necessario configurare correttamente vari componenti, ovvero

- Server Radius (Identity Service Engine)
- Switch
- Access Point/Controller LAN wireless

Poiché sono disponibili documenti esistenti (vedere i riferimenti alla fine), in questo documento ci concentriamo su uno scenario particolare e facciamo riferimento alla documentazione esistente come materiale di supporto.

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Wireless Lan Controller (WLC) e Lightweight AP (LAP)

- 802.1x su switch Cisco e ISE
- Protocollo EAP (Extensible Authentication Protocol)
- RADIUS (Remote Authentication Dial-In User Service)

Componenti usati

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

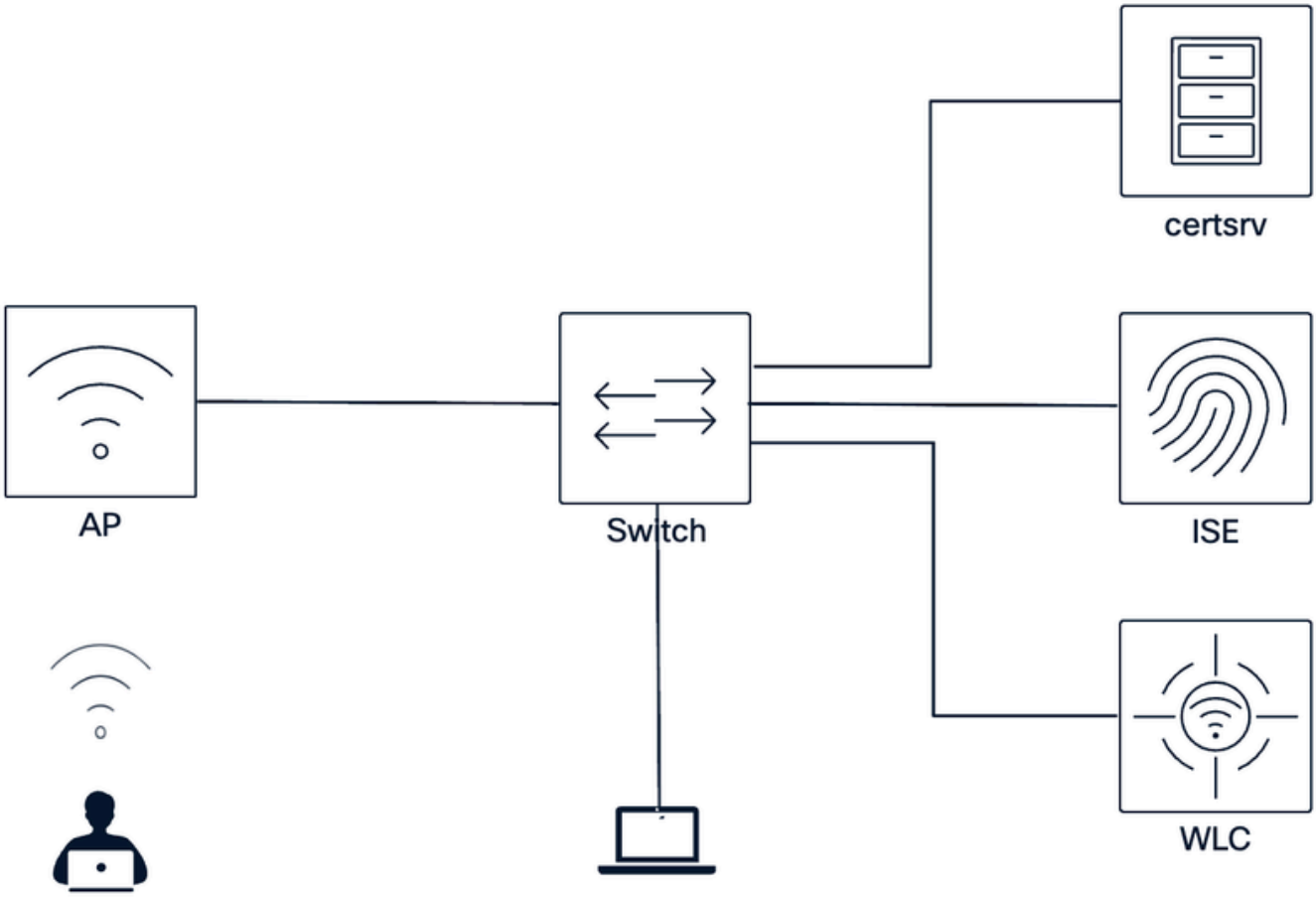
- Cisco C9350 - IOS XE 26.1.1a
- Cisco C9800-40 WLC - IOS XE 26.1.1
- Patch 1 per ISE versione 3.5
- AP CW917x, CW916x

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.

La configurazione è documentata anche in netascode.cisco.com data models for Switching e ISE per replicare facilmente l'installazione.

Configurazione

Esempio di rete



Impostazione di esempio

A questo scopo, Dell si concentra su un singolo scenario e fornisce snippet di configurazione e istruzioni dettagliate. Poiché vi sono diverse variazioni lungo il percorso, le indichiamo e facciamo riferimento alla documentazione esistente a questo scopo.

Scenario trattato in questa guida:

- AP Dot1X cablato con autenticazione EAP-FAST
- Credenziali Dot1X fornite tramite C9800 WLC
- AP in modalità di switching locale Flex Connect

In questo modello, la porta dello switch utilizza inizialmente una configurazione 802.1X in modalità chiusa comune con fallback MAB. Durante il primo caricamento, l'access point potrebbe non avere ancora le credenziali 802.1X, quindi ISE può autorizzare l'access point tramite MAB con un accesso limitato sufficiente per raggiungere il WLC o il Catalyst Center. Dopo il provisioning delle credenziali o dei certificati, l'access point esegue l'autenticazione 802.1X cablata. ISE restituisce

quindi un risultato di autorizzazione valido per il modello di interfaccia AP_FLEX_TRUNK, convertendo la porta nella configurazione del trunk FlexConnect richiesta.

Variations				
Auth Types	MAB	EAP-FAST	EAP-PEAP	EAP-TLS
Provisioning of AP Dot1x supplicant	Wireless LAN Controller	Catalyst Center		
Certificate Rollout method	SCEP	EST		

Tabella 1: Ulteriori variazioni e opzioni in una panoramica

Configurazione AP

Per utilizzare l'autenticazione Dot1x via cavo in combinazione con l'access point, è necessario distribuire prima le credenziali e/o i certificati agli access point, a seconda del metodo di autenticazione selezionato.

In generale, il supplicant Cisco Catalyst AP Dot1x supporta EAP-FAST, EAP-PEAP o EAP-TLS. Inoltre, la funzione MAB potrebbe anche essere un'opzione, soprattutto se gli access point devono raccogliere in primo luogo le credenziali o i certificati per poter eseguire l'autenticazione di tipo EAP.

- MAB
  - Non è richiesta alcuna configurazione del lato AP
  - La gestione degli indirizzi MAC hardware richiede strumenti
  - Possibilità di spoofing
  - Consente la configurazione comune delle porte

- EAP-FAST:
  - Basato su nome utente/password
  - Facile da implementare
  - Richiede l'attivazione anonima della PAC in banda su ISE

- EAP-PEAP:
  - Basato su nome utente/password
  - Richiede certificati per la convalida del server
  - Il rinnovo del certificato deve essere pianificato di conseguenza

- EAP-TLS:
  - Basato su certificato
  - Il rinnovo del certificato deve essere pianificato di conseguenza

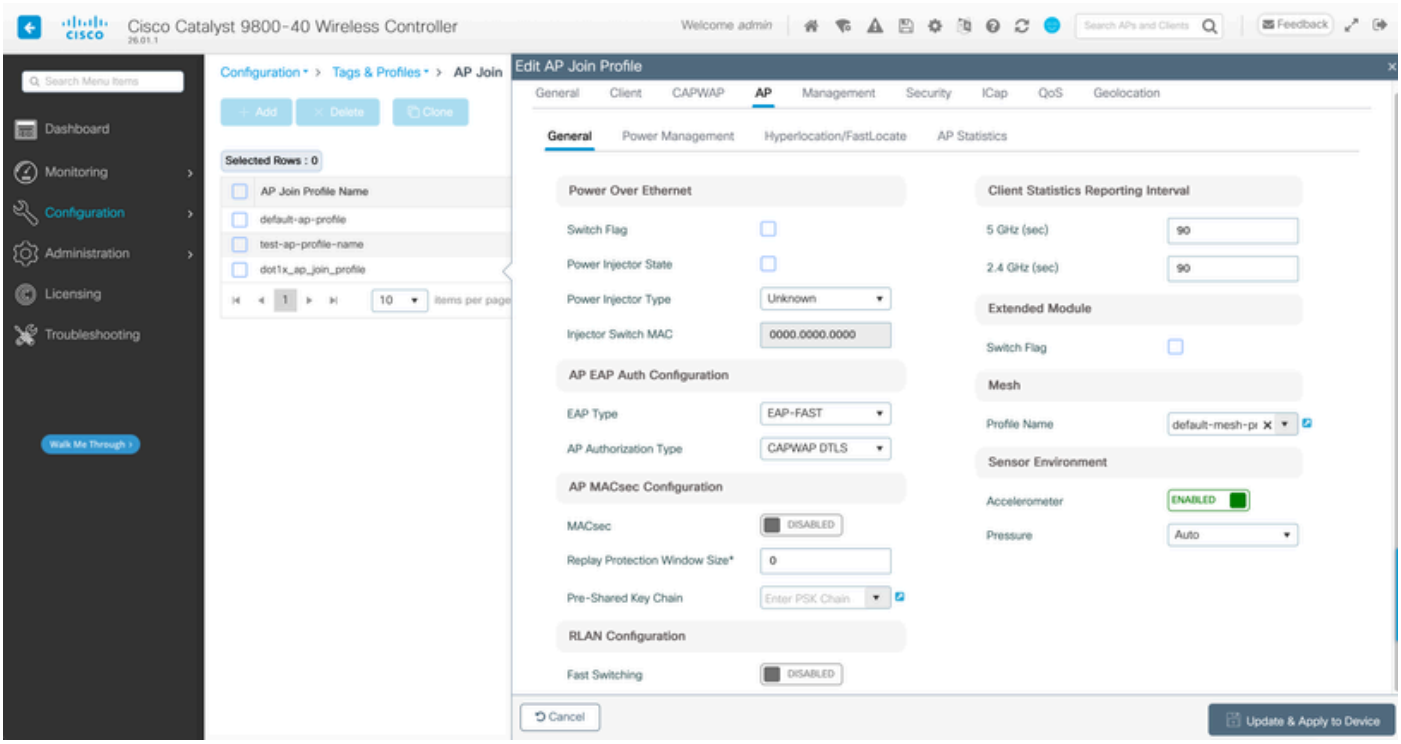
Per configurare il supplicant Dot1X cablato dell'access point sono disponibili due approcci, tramite il controller LAN wireless o Catalyst Center, descritti di seguito. Prima di entrare nei dettagli, è necessario selezionare il tipo di autenticazione da utilizzare.

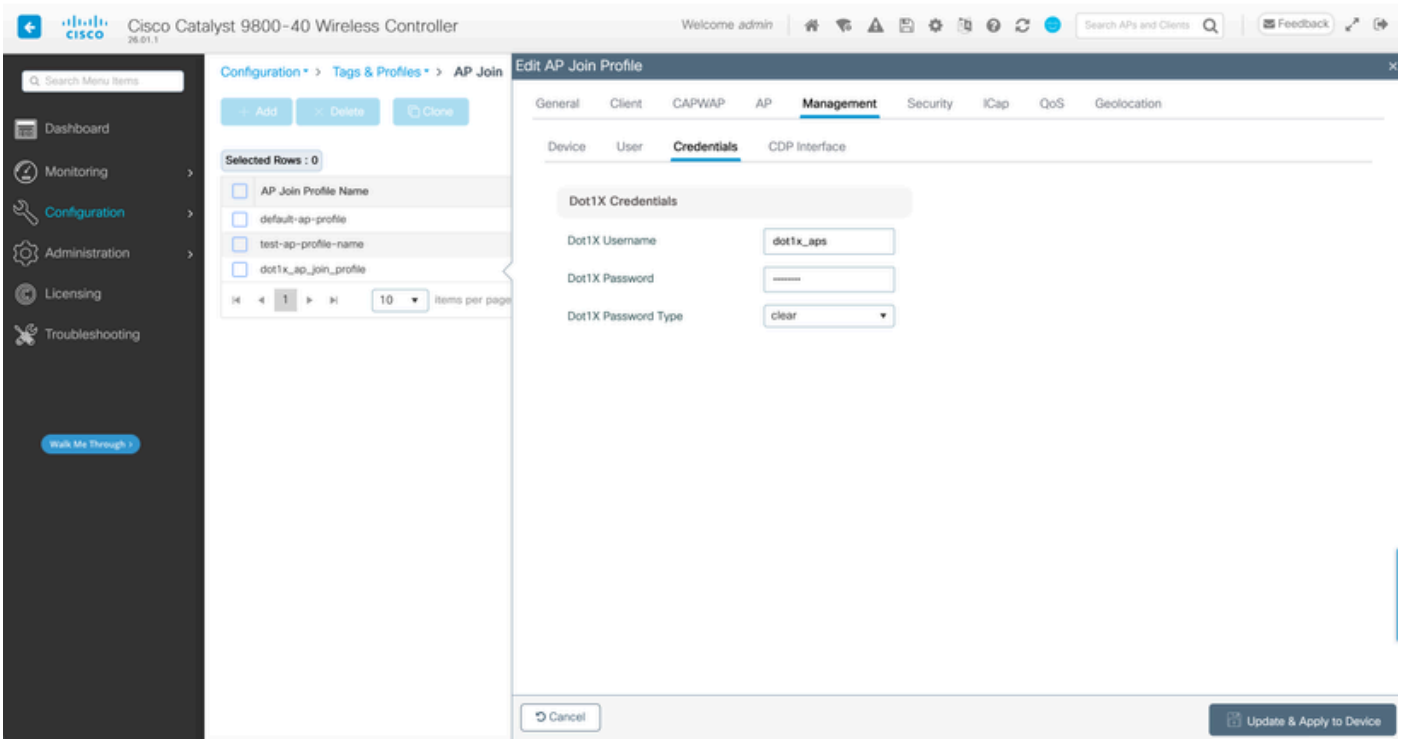
Configurazione di Dot1X cablato tramite il controller LAN wireless Cisco 9800

Se è stata selezionata un'autenticazione basata su certificato (EAP-PEAP o EAP-TLS [1]), è necessario stabilire come procedere per il rilascio dei certificati PA significativi locali (LSC, Locally Significative AP Certificate), tramite SCEP [2] o SET [3].

Quando si utilizza EAP-FAST come in questo scenario, è sufficiente generare un profilo di join AP, in cui immettere l'utente e la password Dot1X, associare il profilo di join a un tag del sito e assegnarlo agli access point.

Configurazione GUI





Configurazione dalla CLI

```
ap profile dot1x_ap_join_profile
 country DE
description dot1x_ap_join_profile
 dot1x eap-type eap-fast
 dot1x username <DOT1X_USER> password 0 <DOT1X_PASSWORD>
```

Configurazione di Dot1X cablato tramite Catalyst Center Plug and Play

Affinché PnP [4] funzioni, è necessario integrare Catalyst Center con ISE. Ciò è richiesto parzialmente a causa dei certificati che sono richiesti per poter eseguire la convalida del server dal lato AP per l'autenticazione EAP con ISE. Per il certificato sul lato dispositivo, i punti di accesso ricevono un certificato rilasciato dalla CA del Catalyst Center che per impostazione predefinita è il proprio interno o se è configurato da una CA secondaria o da un SCEP della CA corrispondente.

Il processo di installazione tramite PnP consente di fornire certificati e/o credenziali prima che il dispositivo si unisca ai WLC.

Configurazione degli switch

Oltre a costituire un meccanismo di sicurezza, l'autenticazione consente di standardizzare le configurazioni delle porte dello switch. Pertanto, queste parti descrivono gli elementi necessari per raggiungere questo obiettivo. Si tratta di una configurazione di esempio che deve essere esaminata e adattata alla configurazione. In generale, questa configurazione consente il Dot1x e il fallback MAB con la corretta gestione degli scenari Radius inattivi, la riautenticazione e così via.

Attributi globali del raggio:

```
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server attribute 31 mac format ietf upper-case
radius-server attribute 31 send nas-port-detail mac-only
radius-server dead-criteria time 5 tries 3
radius-server deadtime 3
!
ip radius source-interface <RADIUS-SOURCE-INTERFACE>
!
```

Gruppo server Radius:

```
!
radius server client-radius-server01
 address ipv4 <ISE01-PSN-IP> auth-port 1812 acct-port 1813
 timeout 10
 retransmit 1
 automate-tester username dummy ignore-acct-port probe-on key 6 <RADIUS-SECRET>
!
!
```

```
aaa group server radius client-radius-group
 server name client-radius-server01
 ip radius source-interface <RADIUS-SOURCE-INTERFACE>
!
```

Configurazione AAA:

```
!
aaa new-model
aaa session-id common
!
aaa authentication dot1x default group client-radius-group
aaa authorization network default group client-radius-group
aaa accounting Identity default start-stop group client-radius-group
aaa accounting update newinfo periodic 2880
!
aaa server radius dynamic-author
 client <ISE01-PSN-IP> server-key 6 <RADIUS-SECRET>
!
```

Mappa classi e modello di servizio IBNS2.0:

```
!
service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
 voice vlan
service-template DEFAULT_CRITICAL_DATA_TEMPLATE
service-template CRITICAL_AUTH_VLAN
 vlan <CRITICAL-AUTH-VLAN>
!
class-map type control subscriber match-all AAA_SVR_DOWN_AUTHD_HOST
 match authorization-status authorized
 match result-type aaa-timeout
!
class-map type control subscriber match-all AAA_SVR_DOWN_UNAUTHD_HOST
 match authorization-status unauthorized
 match result-type aaa-timeout
!
class-map type control subscriber match-all DOT1X
 match method dot1x
!
class-map type control subscriber match-all DOT1X_FAILED
 match method dot1x
 match result-type method dot1x authoritative
!
class-map type control subscriber match-all DOT1X_MEDIUM_PRIO
 match authorizing-method-priority gt 20
!
class-map type control subscriber match-all DOT1X_NO_RESP
 match method dot1x
 match result-type method dot1x agent-not-found
!
class-map type control subscriber match-all DOT1X_TIMEOUT
 match method dot1x
```

```
 match result-type method dot1x method-timeout
!
class-map type control subscriber match-any IN_CRITICAL_AUTH
 match activated-service-template CRITICAL_AUTH_VLAN
 match activated-service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
!
class-map type control subscriber match-all MAB
 match method mab
!
class-map type control subscriber match-all MAB_FAILED
 match method mab
 match result-type method mab authoritative
!
class-map type control subscriber match-none NOT_IN_CRITICAL_AUTH
 match activated-service-template CRITICAL_AUTH_VLAN
 match activated-service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
!
```

Policy del servizio IBNS 2.0:

```
!
policy-map type control subscriber WiredDot1xClosedAuth_1X_MAB
 event inactivity-timeout match-all
  10 class always do-until-failure
   10 clear-session
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x retries 2 retry-time 0 priority 10
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x priority 20
 event aaa-available match-all
  10 class IN_CRITICAL_AUTH do-until-failure
   10 clear-session
  20 class NOT_IN_CRITICAL_AUTH do-until-failure
   10 resume reauthentication
 event authentication-failure match-first
  10 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  20 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
   10 activate service-template CRITICAL_AUTH_VLAN
   20 activate service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
   30 authorize
   40 pause reauthentication
  30 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
   10 pause reauthentication
   20 authorize
  40 class DOT1X_NO_RESP do-until-failure
  10 terminate dot1x
  20 authenticate using mab priority 20
 50 class MAB_FAILED do-until-failure
  10 terminate mab
  20 authentication-restart 60
 60 class DOT1X_TIMEOUT do-until-failure
  10 authenticate using mab priority 20
 70 class always do-until-failure
```

```
  10 terminate dot1x
  20 terminate mab
  30 authentication-restart 60
!
```

Modelli di interfaccia:

```
!
template AP_FLEX_TRUNK
 dot1x pae authenticator
 dot1x timeout supp-timeout 7
 dot1x max-req 3
 switchport trunk native vlan <TRUNK-NATIVE-VLAN>
 switchport trunk allowed vlan <TRUNK-ALLOWED-VLANS>
 switchport mode trunk
 mab
 access-session host-mode multi-host peer
 access-session closed
 access-session port-control auto
 authentication periodic
 authentication timer reauthenticate server
 service-policy type control subscriber WiredDot1xClosedAuth_1X_MAB
!
template DEFAULT-ACCESS-PORT
 dot1x pae authenticator
 dot1x timeout supp-timeout 7
 dot1x max-req 3
 switchport mode access
 mab
 access-session host-mode multi-domain
 access-session closed
 access-session port-control auto
 authentication periodic
 authentication timer reauthenticate server
 service-policy type control subscriber WiredDot1xClosedAuth_1X_MAB
!
```

Configurazione dell'interfaccia:

```
!
interface TenGigabitEthernet1/0/1
 switchport access vlan <DEFAULT-ACCESS-VLAN>
 switchport mode access
 dot1x timeout tx-period 7
 dot1x max-reauth-req 3
 source template DEFAULT-ACCESS-PORT
 spanning-tree portfast
 spanning-tree bpduguard enable
!
```

Obbligatorio globale:

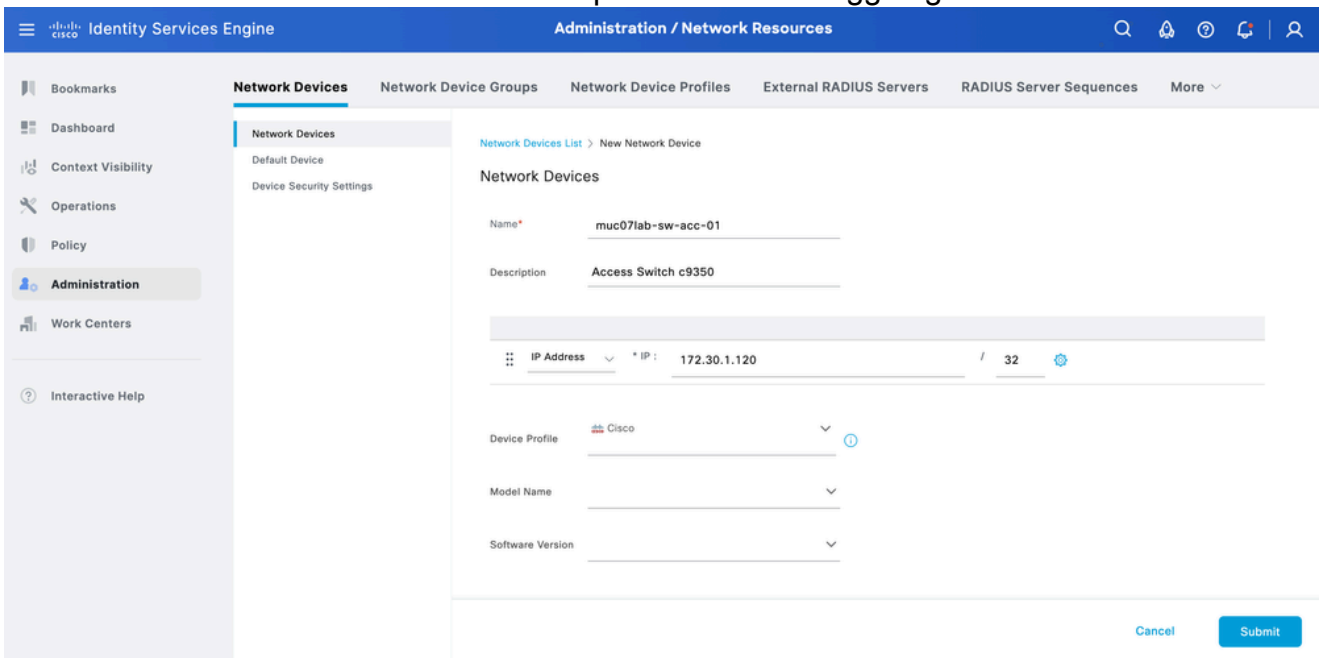
```
!
dot1x system-auth-control
!
access-session interface-template sticky timer 60
!
```

Nota: Quando si utilizza un CW9178, l'access point presenta due indirizzi MAC durante l'autenticazione. Per fare in modo che la porta dello switch non entri in stato err-disabled, inizialmente la porta deve essere configurata per la modalità host multi-auth. Se l'autenticazione 802.1X ha esito positivo, si consiglia di modificare dinamicamente la configurazione della porta in modo che host multiplo sia in modalità host.

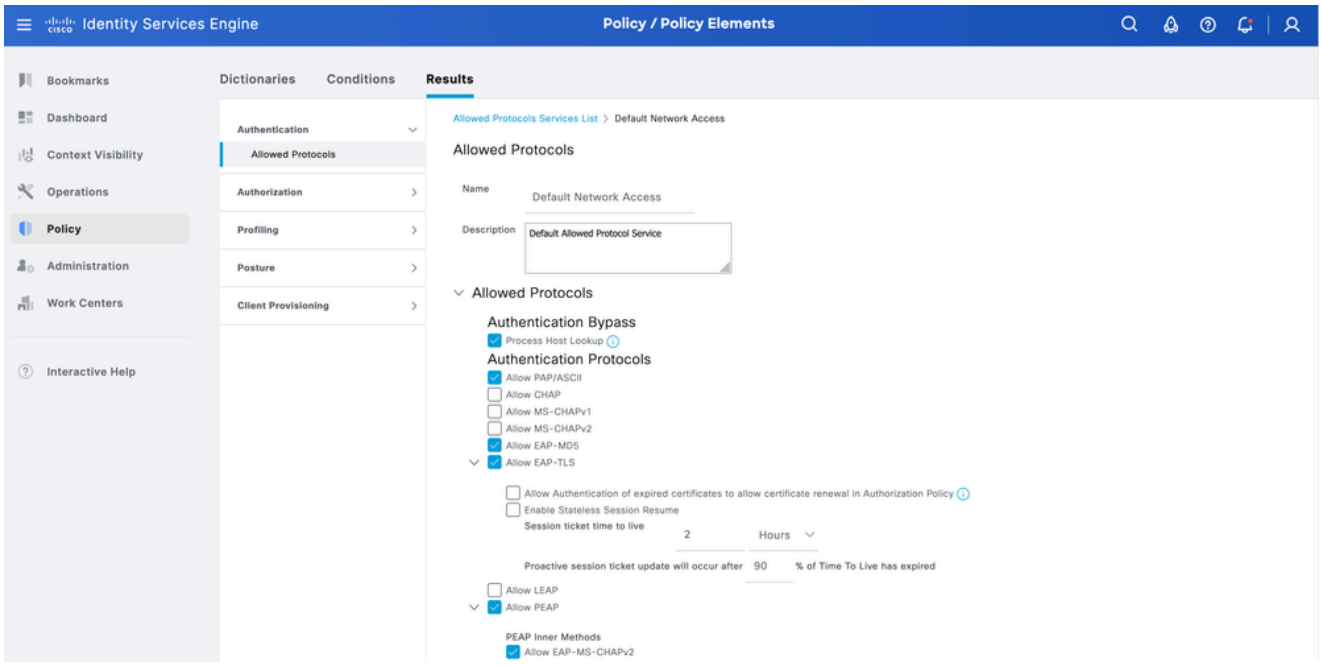
Configurazione Identity Services Engine

Infine, è necessario configurare anche il server RADIUS per consentire l'autenticazione. Per il dot1x cablato è disponibile una guida completa [5], pertanto in questo caso ci concentriamo solo sulle parti rilevanti.

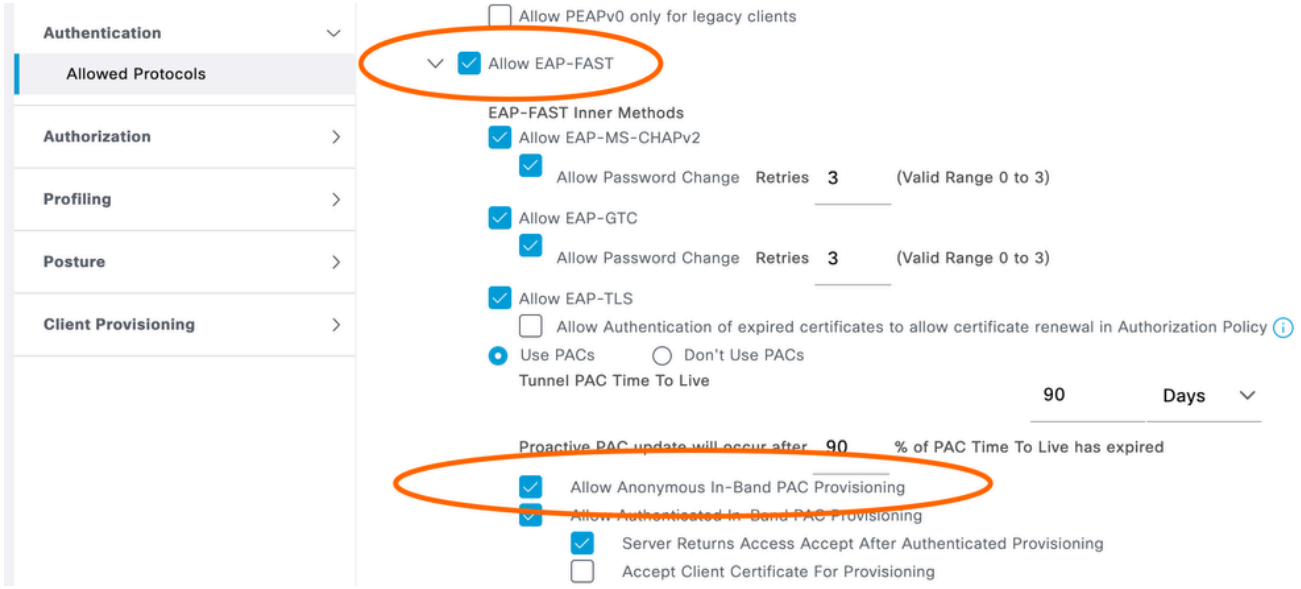
1. Aggiungere lo switch come dispositivo di accesso alla rete:
   > Amministrazione > Risorse di rete > Dispositivi di rete > Aggiungi



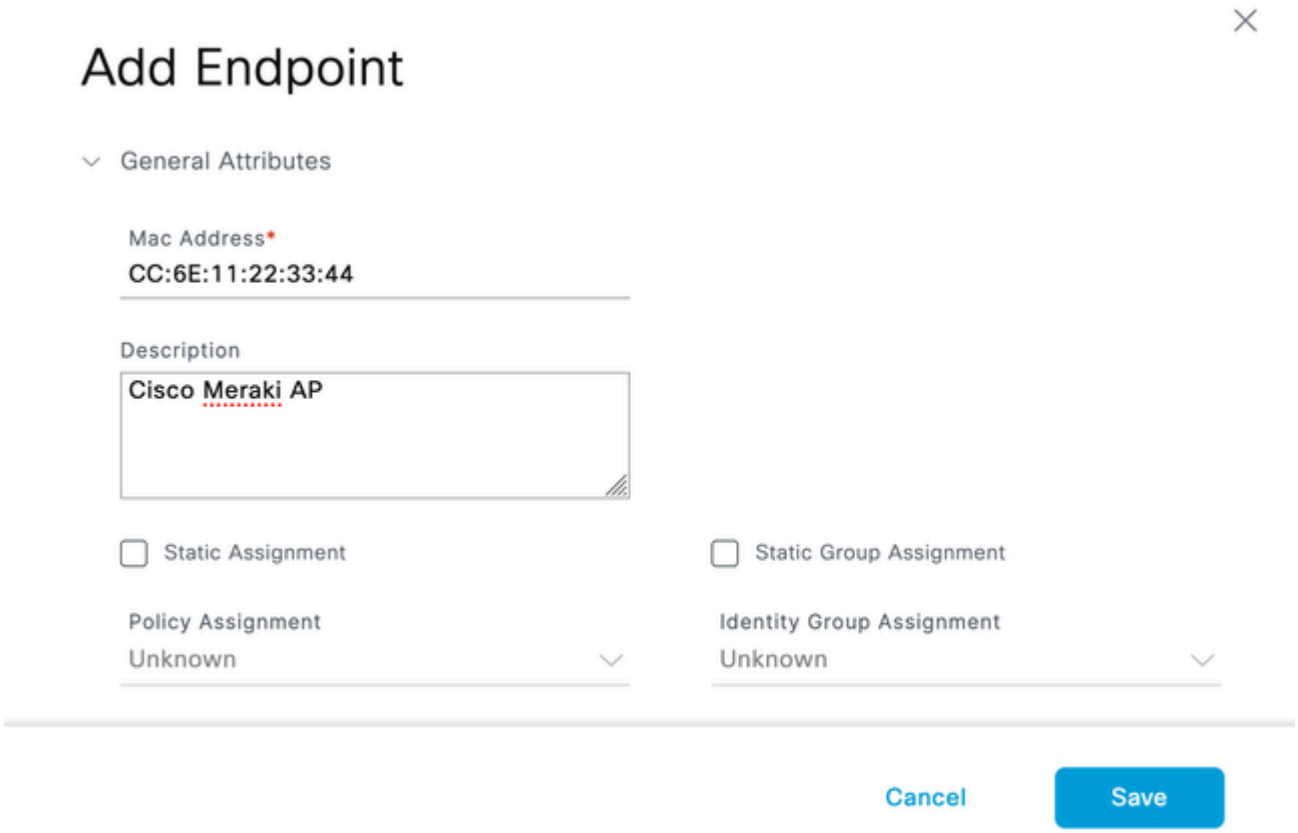
2. Abilitare il protocollo EAP in uso:
   > Policy > Elementi di policy > Risultati > Autenticazione > Protocolli consentiti



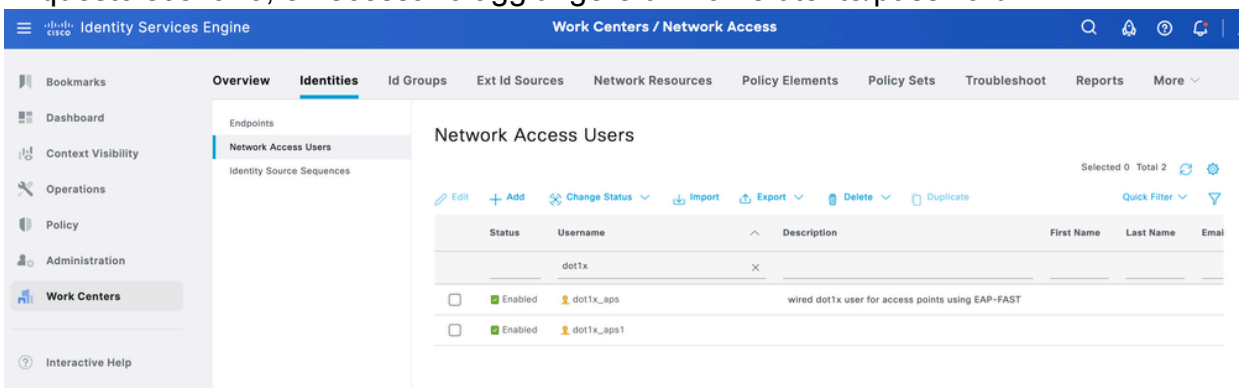
3. Per questo scenario, poiché viene utilizzato EAP-FAST, tenere presente che la funzione di "provisioning PAC in banda anonimo" deve essere abilitata:



4. Aggiungi identità
   > Centri di lavoro > Accesso alla rete > Identità
   a. Per un corretto funzionamento, il processo è in genere costituito da due passaggi. Inizialmente l'access point non dispone di credenziali e pertanto non può rispondere all'autenticazione EAP. Di conseguenza, la porta dello switch deve prima autenticare l'access point con il protocollo MAB. Può essere basato su un criterio di autorizzazione generico, un criterio basato sulla posizione o la profilatura del dispositivo. Indipendentemente dal criterio utilizzato, l'autenticazione MAB iniziale deve riuscire a consentire all'access point di ottenere le proprie credenziali, sia dal WLC tramite CAPWAP che dal Cisco Catalyst Center tramite Plug and Play (PnP).

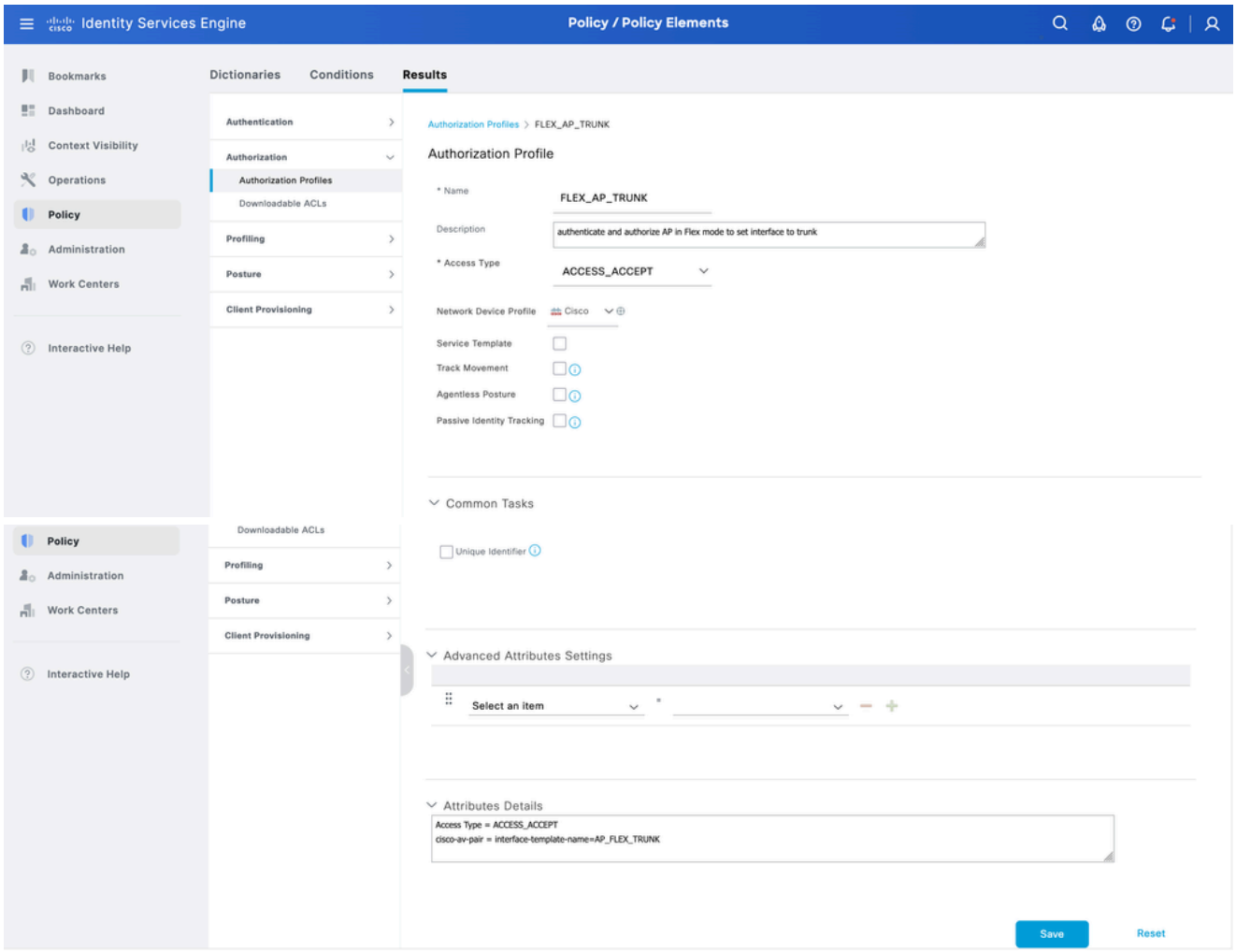


b. Dopo che l'access point ha raccolto le credenziali/il certificato, il supplicant Dot1X cablato risponde a EAPoL e Dot1X è il metodo successivo per l'autenticazione che abilita l'access point per l'accesso completo.
In questo scenario, è necessario aggiungere un nome utente/password:

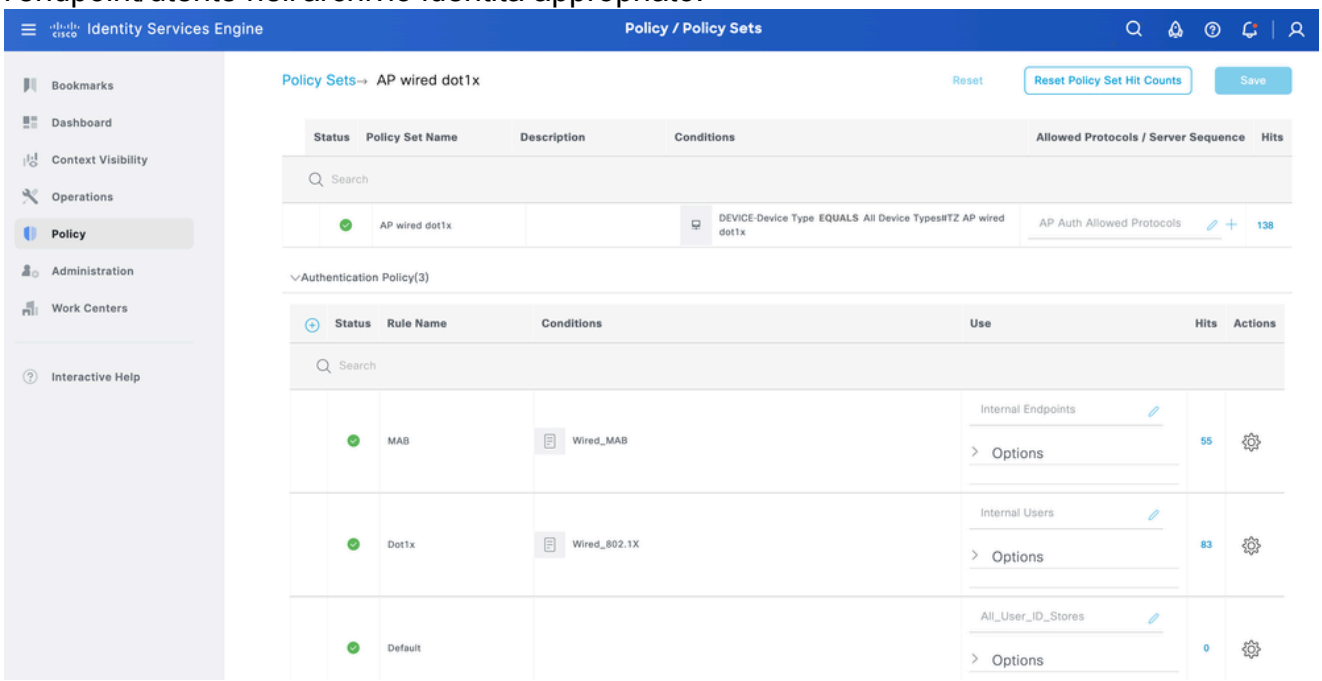


5. Creazione del profilo di autorizzazione
Il profilo di autorizzazione risponde con la coppia av richiesta. Nel nostro caso, mentre si modifica dinamicamente la porta dello switch, il modello di interfaccia deve essere configurato:
> Politica > Elementi della politica > Risultati > Autorizzazione > Profili di autorizzazione

Nome: FLEX_AP_TRUNK
Tipo di accesso: ACCETTO
Modello interfaccia: AP_FLEX_TRUNK

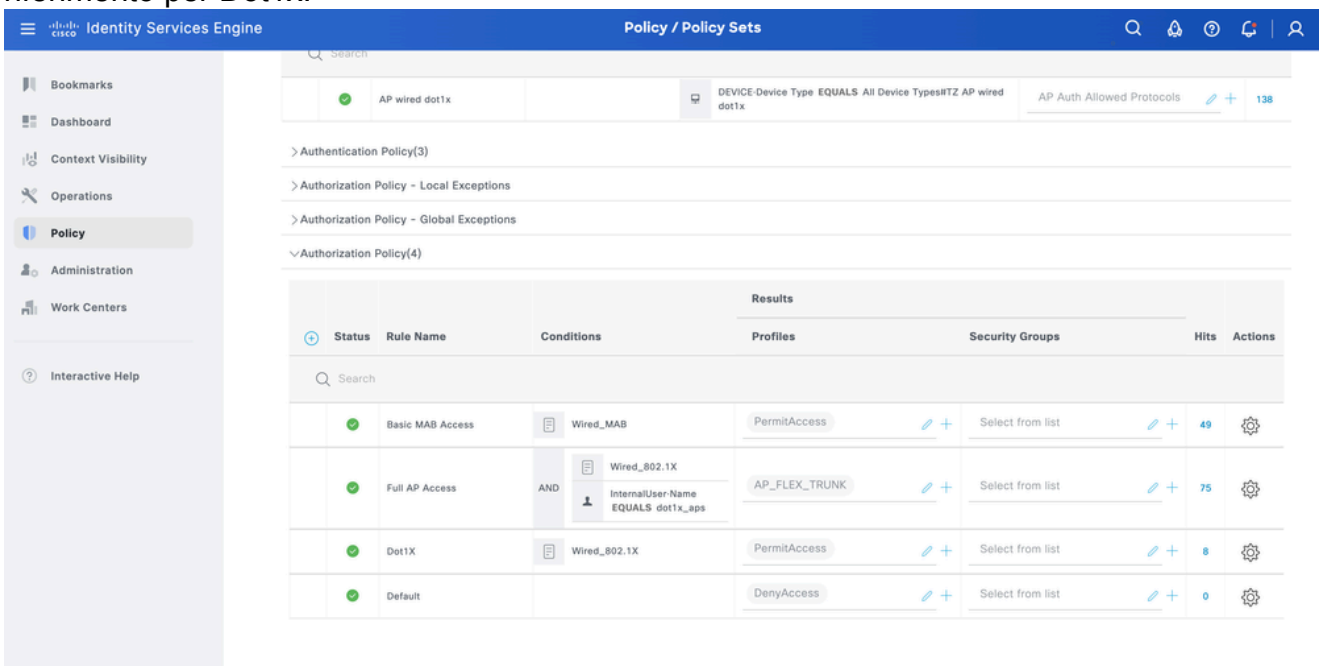


6. Crea criterio di autorizzazione
   Creare un criterio di autenticazione che consenta MAB e Dot1X cablato e cercare l'endpoint/utente nell'archivio identità appropriato.



Specificare un risultato limitato per l'autorizzazione di accesso, in base alle esigenze di MAB,

e un accesso completo all'access point, che includa la coppia av-pair modello interfaccia di riferimento per Dot1x:



Verifica

Una volta implementata la configurazione, collegare l'access point allo switch. Come prerequisito, si prevede che le impostazioni di rete predefinite, nel nostro caso un pool DHCP nella VLAN di accesso con l'opzione 43 che punta alla comunicazione WLC e CAPWAP, siano possibili per l'AP sul WLC.

Comandi AP

```
show ap authentication status
show crypto
show crypto pki trustpool
```

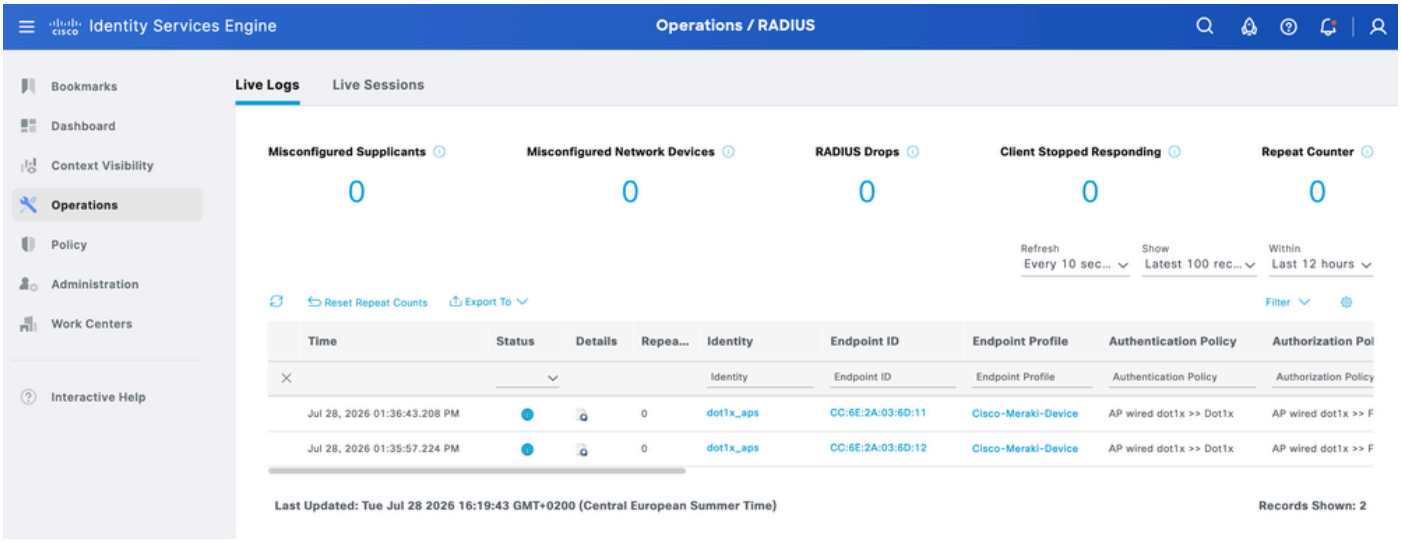
Comandi Switch

```
show access-session
show aaa servers
show access-session interface <INTERFACE> details
show template interface binding target <INTERFACE>
show derived-config interface <INTERFACE>

Sample output:
!
C9350-02-R11#show access-session interface te1/0/1
```

```
Interface MAC Address Method Domain Status Fg Session ID
---------------------------------------------------------------------------------------
Te1/0/1 6cef.1122.3344 dot1x DATA Auth 09FE1FAC000000948FF60A2F
```

ISE



Elenco di acronimi

Acronimo	Espansione
AAA	autenticazione, autorizzazione e accounting
AP	access point
AuthC	autenticazione
AuthZ	Authorization
CA	autorità di certificazione
CISP	Protocollo di segnalazione informazioni client
Punto1x	IEEE 802.1X
EAP	Extensible Authentication Protocol
EST	Iscrizione su trasporto sicuro
VELOCE	Autenticazione flessibile tramite tunneling sicuro
IBNS	Servizi Identity Based Networking
ISE	Identity Services Engine
MAB	Bypass autenticazione MAC
E	Dispositivo di accesso alla rete

PEAP	Protected Extensible Authentication Protocol
SCEP	Protocollo SCEP (Simple Certificate Enrollment Protocol)
TLS	Transport Layer Security
WLC	Controller LAN wireless

Riferimenti

[1] Configurare 802.1X sui punti di accesso per PEAP o EAP-TLS con LSC

[2] Configurare SCEP per il provisioning di certificati importanti a livello locale su 9800 WLC

[3] Cisco Wireless EST On-Prem Deployment Guide (Guida all'installazione locale di Cisco Wireless EST)

[4] Secure AP onboarding - Introduzione alla sicurezza di rete migliorata

[5] ISE Secure Wired Access Prescriptive Deployment Guide

[6] Sezione Config Guide per LSC

[7] Configurare il richiedente 802.1X per i punti di accesso con il controller 9800

[8] Proteggere una porta di switching Flexconnect AP con Dot1x

[9] Guida alla configurazione del software Cisco Catalyst serie 9800 Wireless Controller, Cisco IOS XE 17.18.x - 802.1x

[11] Cisco Catalyst Center User Guide, release 3.2.x - Configurazione delle impostazioni di gestione per un profilo AP per dispositivi Cisco IOS XE

[12] Uso dei modelli di interfaccia e IBNS 2.0 per una configurazione switchport predefinita

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).