Configurazione dell'autenticazione EAP locale su Catalyst 9800 WLC

Sommario

Introduzione

Questo documento descrive la configurazione di EAP locale sui controller LAN wireless Catalyst 9800 WLC.

Prerequisiti

Requisiti

In questo documento viene descritta la configurazione del protocollo EAP (Extensible Authentication Protocol) locale sui WLC Catalyst 9800; in altre parole, il WLC funziona come server di autenticazione RADIUS per i client wireless.

In questo documento si presume che l'utente abbia familiarità con la configurazione di base di una WLAN sul WLC 9800 e si focalizza solo sul WLC che funziona come server EAP locale per client wireless.

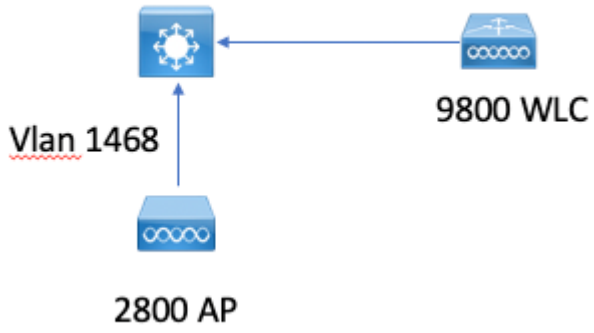
Componenti usati

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.

Catalyst 9800 sulla versione 16.12.1s

Configurazione

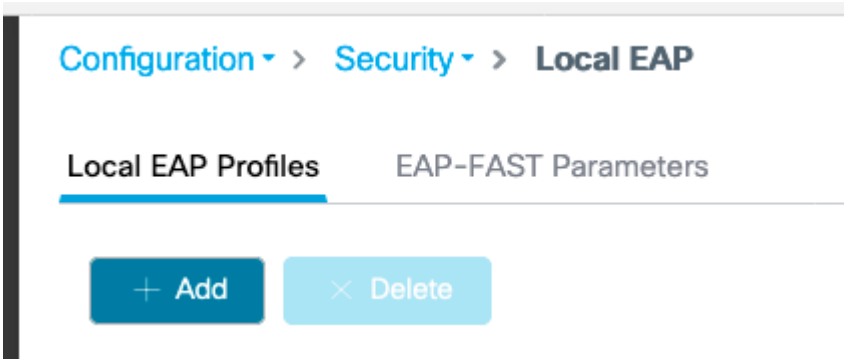
Esempio di rete



Configurazione EAP locale principale

Passaggio 1. Profilo EAP locale

Selezionare **Configurazione > Protezione > EAP locale** nell'interfaccia utente Web 9800.

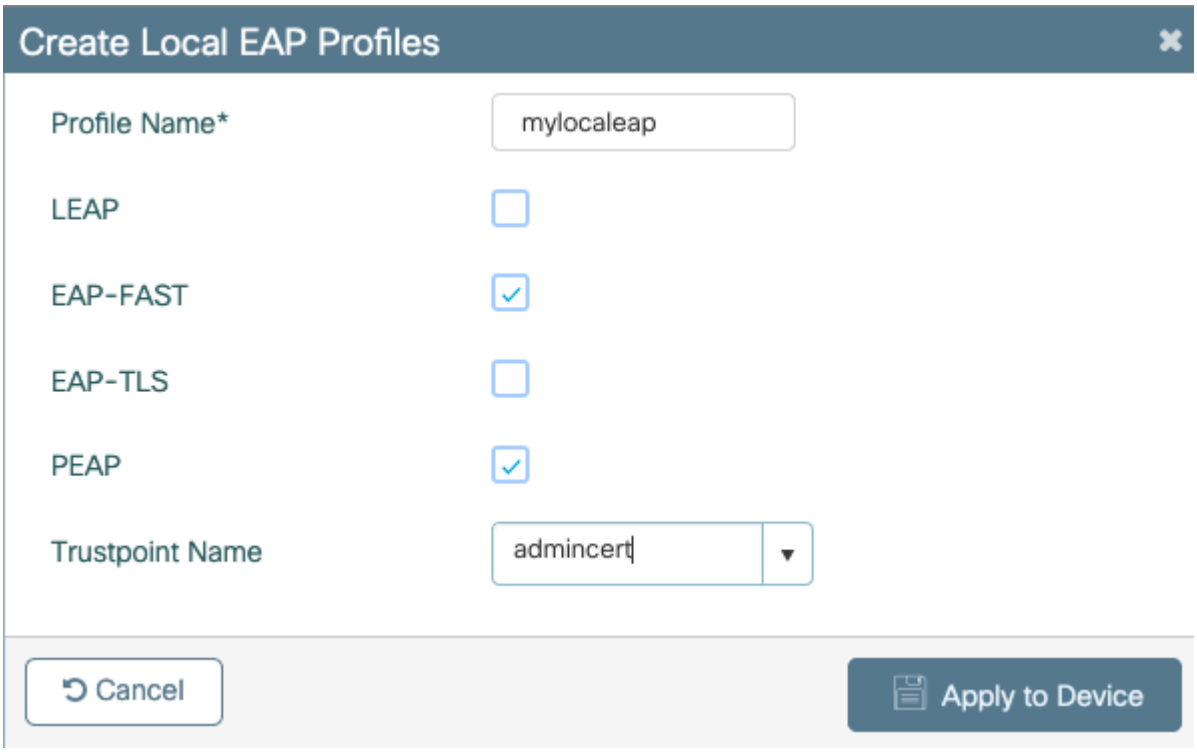


Selezionare **Aggiungi**

Immettere il nome di un profilo.

Si sconsiglia di utilizzare LEAP proprio a causa della sua sicurezza debole. Tutti gli altri 3 metodi EAP richiedono la configurazione di un trust point. Infatti, lo switch 9800, che funge da autenticatore, deve inviare un certificato affinché il client lo consideri attendibile.

Poiché i client non considerano attendibile il certificato predefinito WLC, è necessario disattivare la convalida del certificato server sul lato client (scelta non consigliata) o installare un trust point certificato sul WLC 9800 considerato attendibile dal client (oppure importarlo manualmente nell'archivio trust del client).



CLI:

```
(config)#eap profile mylocapeap
(config-eap-profile)#method peap
(config-eap-profile)#pki-trustpoint admincert
```

Passaggio 2. Metodo di autenticazione AAA

È necessario configurare un metodo AAA dot1x che punti anche localmente per utilizzare il database locale degli utenti (ma è possibile, ad esempio, utilizzare la ricerca LDAP esterna).

Selezionare **Configuration > Security > AAA** (Configurazione > Protezione > AAA) e selezionare la scheda **elenco metodi AAA** per **Authentication (Autenticazione)**. Selezionare **Aggiungi.**

Selezionare il tipo "dot1x" e il tipo di gruppo locale.

Passaggio 3. Configurare un metodo di autorizzazione AAA

Andare alla scheda secondaria **Autorizzazione** e creare un nuovo metodo per il tipo **credenziale-download** e puntarlo a locale.

Eseguire la stessa operazione per il tipo di autorizzazione di **rete**

CLI:

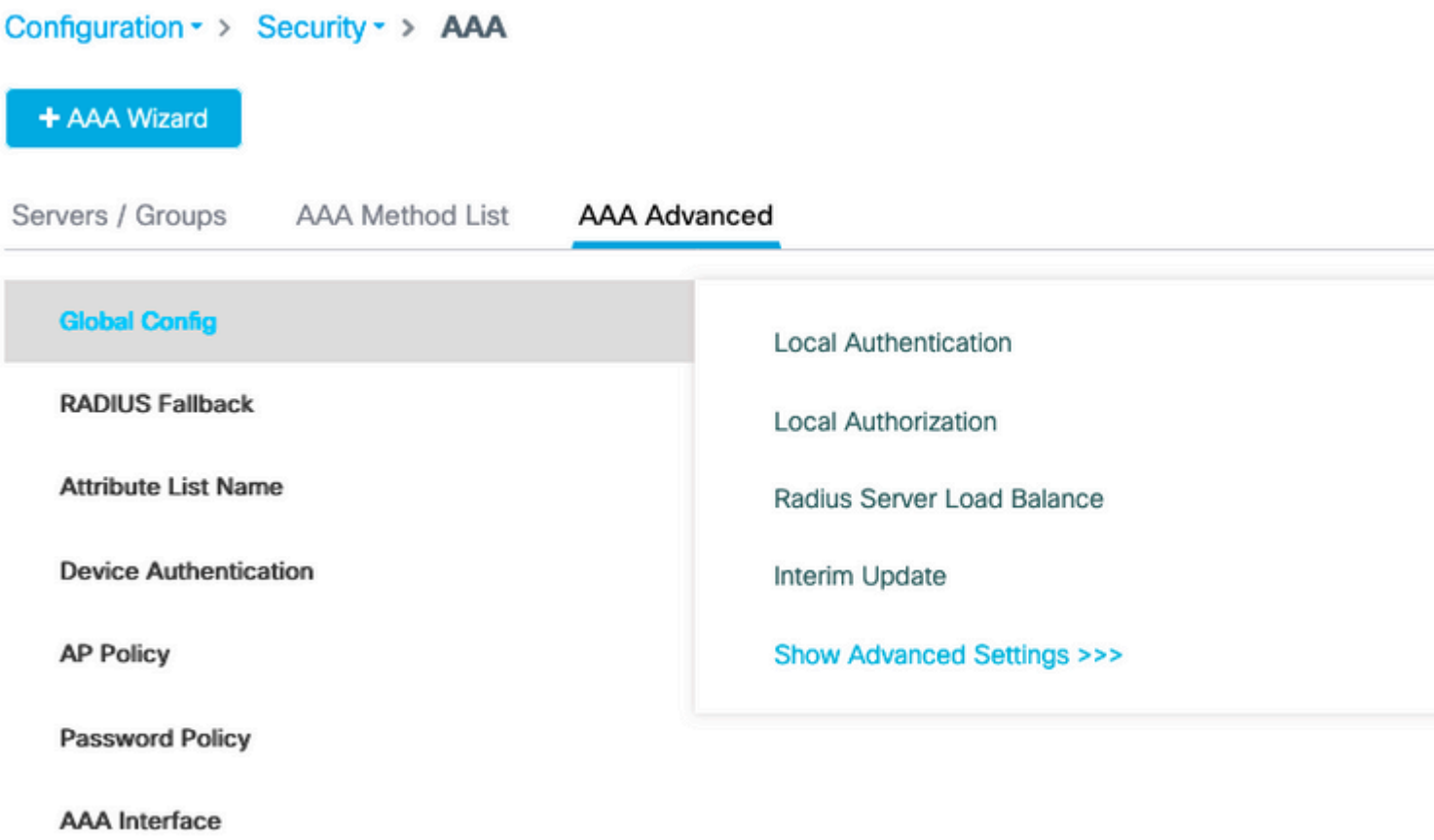
```
(config)#aaa new-model
(config)#aaa authentication dot1x default local
(config)#aaa authorization credential-download default local
(config)#aaa local authentication default authorization default
(config)#aaa authorization network default local
```

Passaggio 4. Configura metodi avanzati locali

Selezionare la scheda **Advanced AAA**.

Definire il metodo di autenticazione e autorizzazione locale. Poiché in questo esempio sono stati utilizzati il metodo "default" per il download delle credenziali e il metodo "Default" dot1x, è necessario impostare il valore predefinito sia per l'autenticazione locale che per le caselle di riepilogo a discesa delle autorizzazioni.

Se sono stati definiti metodi denominati, selezionare "elenco dei metodi" nell'elenco a discesa e un altro campo consente di immettere il nome del metodo.



CLI:

```
aaa local authentication default authorization default
```

Passaggio 5. Configurazione di una WLAN

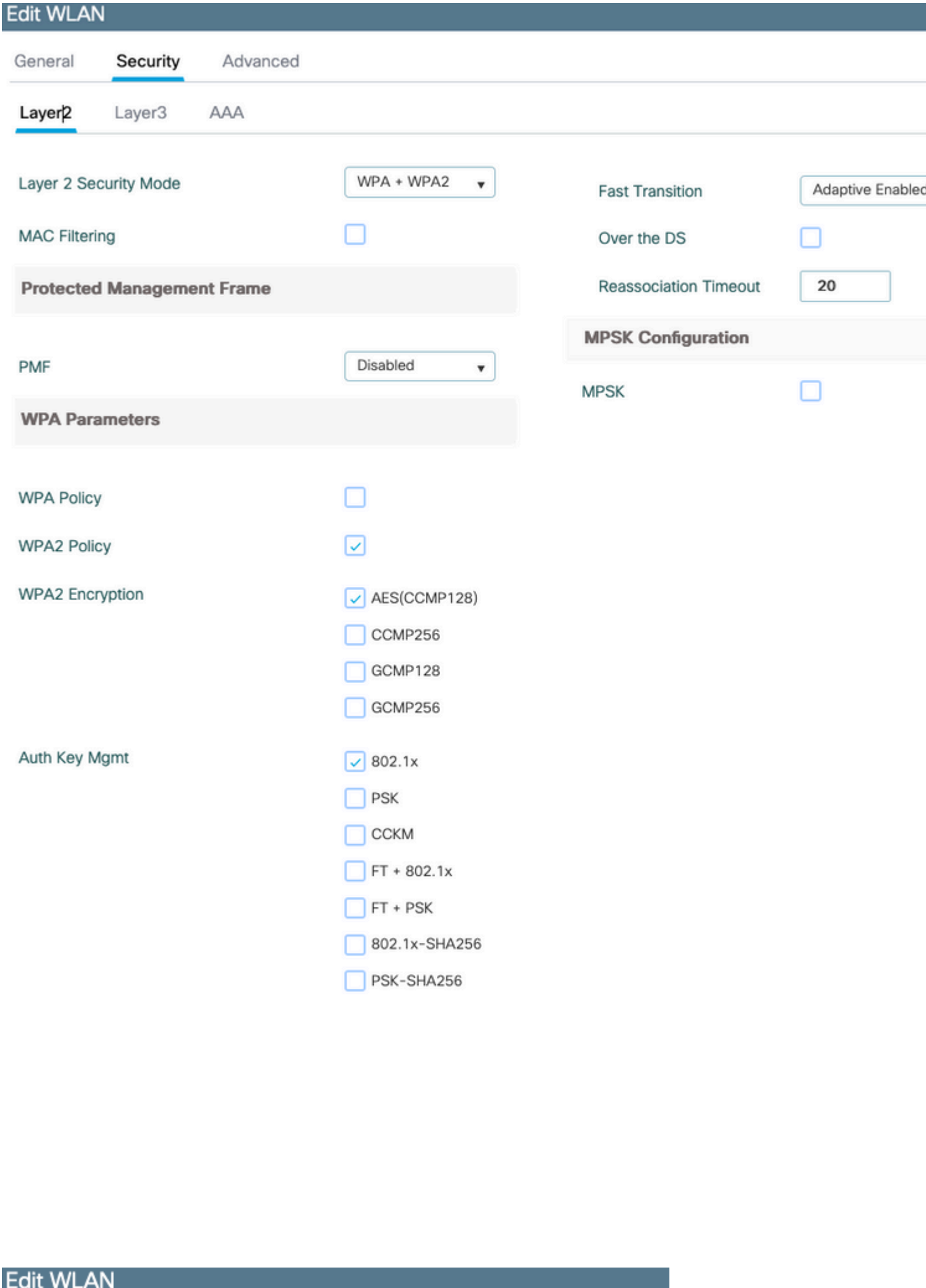
È quindi possibile configurare la WLAN per la sicurezza 802.1x in base al profilo EAP locale e al metodo di autenticazione AAA definiti nel passaggio precedente.

Andare a Configurazione > Tag e profili > WLAN > + Aggiungi >

Specificare SSID e nome profilo.

La protezione Dot1x è selezionata per impostazione predefinita in Layer 2.

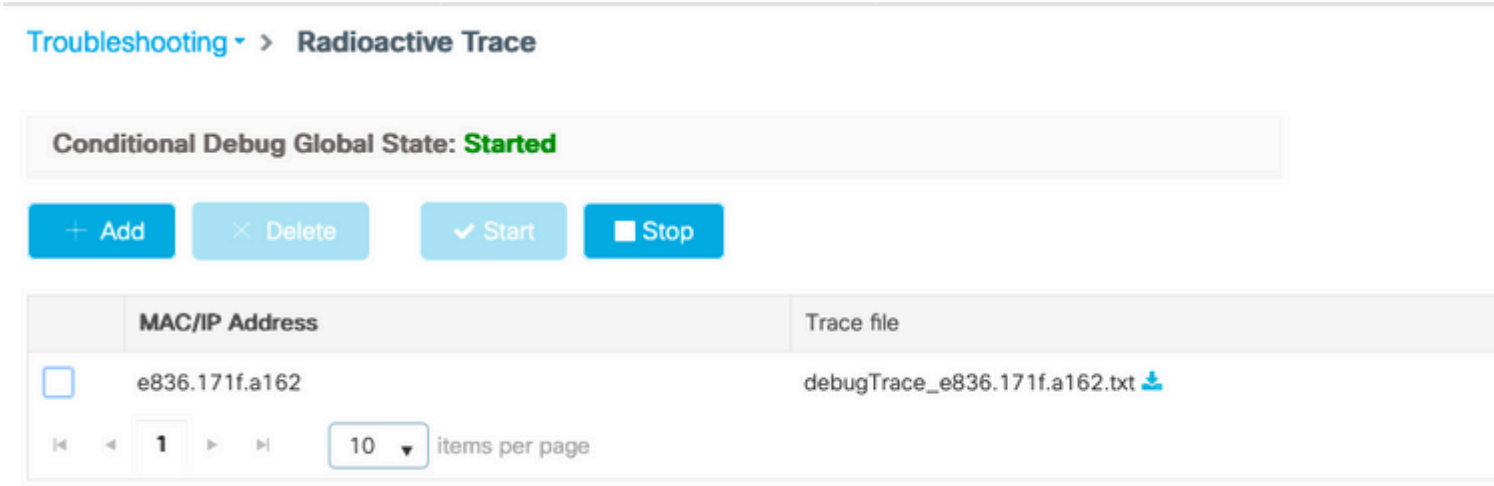
In AAA, selezionare Autenticazione EAP locale e scegliere Profilo EAP locale e elenco Autenticazione AAA dall'elenco a discesa.


Edit WLAN
General
Security
Advanced
Layer2
Layer3
AAA
Layer 2 Security Mode
WPA + WPA2
MAC Filtering
Protected Management Frame
PMF
Disabled
WPA Parameters
WPA Policy
WPA2 Policy
WPA2 Encryption
AES(CCMP128)
CCMP256
GCMP128
GCMP256
Auth Key Mgmt
802.1x
PSK
CCKM
FT + 802.1x
FT + PSK
802.1x-SHA256
PSK-SHA256
Fast Transition
Adaptive Enabled
Over the DS
Reassociation Timeout
20
MPSK Configuration
MPSK
Edit WLAN

16.12 e versioni precedenti supportano solo TLS 1.0 per l'autenticazione EAP locale che potrebbe causare problemi se il client supporta solo TLS 1.2 come è sempre più la norma. Cisco IOS® XE 17.1 e versioni successive supportano TLS 1.2 e TLS 1.0.

Per risolvere i problemi relativi alla connessione di uno specifico client, utilizzare RadioActive Tracing. Selezionare **Risoluzione dei problemi > RadioActive Trace** e aggiungere l'indirizzo MAC del client.

Selezionare **Start** per abilitare la traccia per il client.



Una volta riprodotto il problema, è possibile selezionare il pulsante **Genera** per generare un file che contenga l'output di debug.

Esempio di un client che non riesce a connettersi a causa di una password errata

```
2019/10/30 14:54:00.781 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sent
2019/10/30 14:54:00.781 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.784 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rece
2019/10/30 14:54:00.784 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.785 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: m
2019/10/30 14:54:00.788 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sent
2019/10/30 14:54:00.788 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.791 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rece
2019/10/30 14:54:00.791 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.791 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: m
2019/10/30 14:54:00.792 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sent
2019/10/30 14:54:00.792 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.795 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rece
2019/10/30 14:54:00.795 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.795 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: m
2019/10/30 14:54:00.796 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sent
2019/10/30 14:54:00.796 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.804 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rece
2019/10/30 14:54:00.804 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.804 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: m
2019/10/30 14:54:00.805 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sent
2019/10/30 14:54:00.805 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rece
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: m
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [eap] [23294]: (info): FAST:EAP_FAIL from inner method MSCHAPV
```

```
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sent
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.811 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rece
2019/10/30 14:54:00.811 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.811 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: m
2019/10/30 14:54:00.812 {wncd_x_R0-0}{2}: [eap-auth] [23294]: (info): FAIL for EAP method name: EAP-FAST
2019/10/30 14:54:00.812 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rais
2019/10/30 14:54:00.813 {wncd_x_R0-0}{2}: [errmsg] [23294]: (note): %DOT1X-5-FAIL: Authentication failed
2019/10/30 14:54:00.813 {wncd_x_R0-0}{2}: [auth-mgr] [23294]: (info): [e836.171f.a162:capwap_90000004] A
```

Traccia in caso di errore

È possibile controllare l'elenco degli eventi di errore per un determinato indirizzo MAC con il comando trace-on-failure, anche quando non sono abilitati debug.

Nell'esempio successivo, il metodo AAA era inizialmente assente (evento server AAA inattivo), quindi il client ha utilizzato credenziali errate qualche minuto dopo.

Il comando è **show logging trace-on-failure summary** nella versione 16.12 e precedenti e **show logging profile wireless (filter mac <mac>) trace-on-failure** in Cisco IOS® XE 17.1 e versioni successive. Non ci sono differenze tecniche, a parte che la versione 17.1 e successive consente di filtrare l'indirizzo MAC del client.

```
Nico9800#show logging profile wireless filter mac e836.171f.a162 trace-on-failure
Displaying logs from the last 0 days, 0 hours, 10 minutes, 0 seconds
executing cmd on chassis 2 ...
sending cmd to chassis 1 ...
Collecting files on current[1] chassis.
# of files collected = 30
Collecting files on current[2] chassis.
# of files collected = 30
Collecting files from chassis 1.
Time                          UUID                 Log

--------------------------------------------------------------------------------------------------


2019/10/30 14:51:04.438     0x0      SANET_AUTHC_FAILURE - AAA Server Down username , audit session id 0
2019/10/30 14:58:04.424     0x0      e836.171f.a162 CLIENT_STAGE_TIMEOUT State = AUTHENTICATING, WLAN pr
```

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).