

Configurazione di FlexConnect EWA su Catalyst 9800 WLC e ISE

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Verifica](#)

[Traccia AR Esempio di tentativo riuscito](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive come configurare FlexConnect EWA su Catalyst 9800 WLC e ISE.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza della configurazione dei Wireless LAN Controller (WLC) 9800.

Componenti usati

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

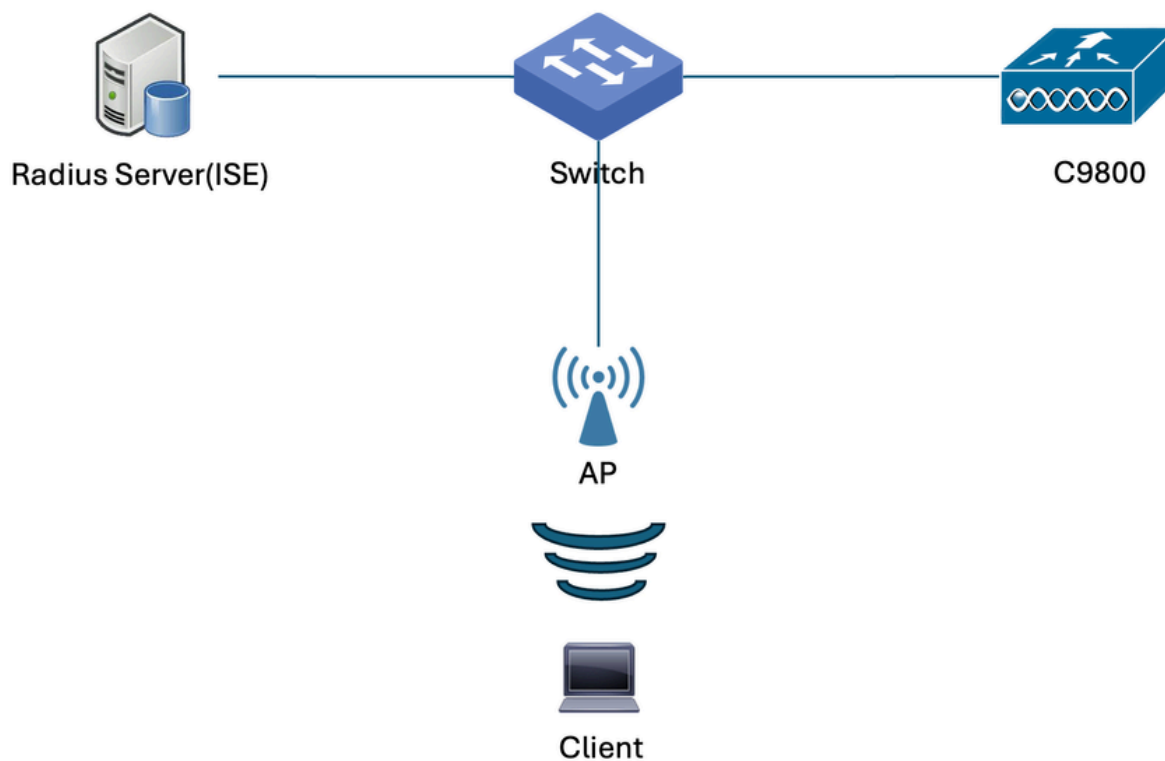
- Cisco Catalyst 9800 WLC Cisco IOS® XE versione 17.15.3
- Identity Service Engine (ISE) v3.4.0.608

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.

Configurazione

Esempio di rete

Supponiamo di avere questa topologia:

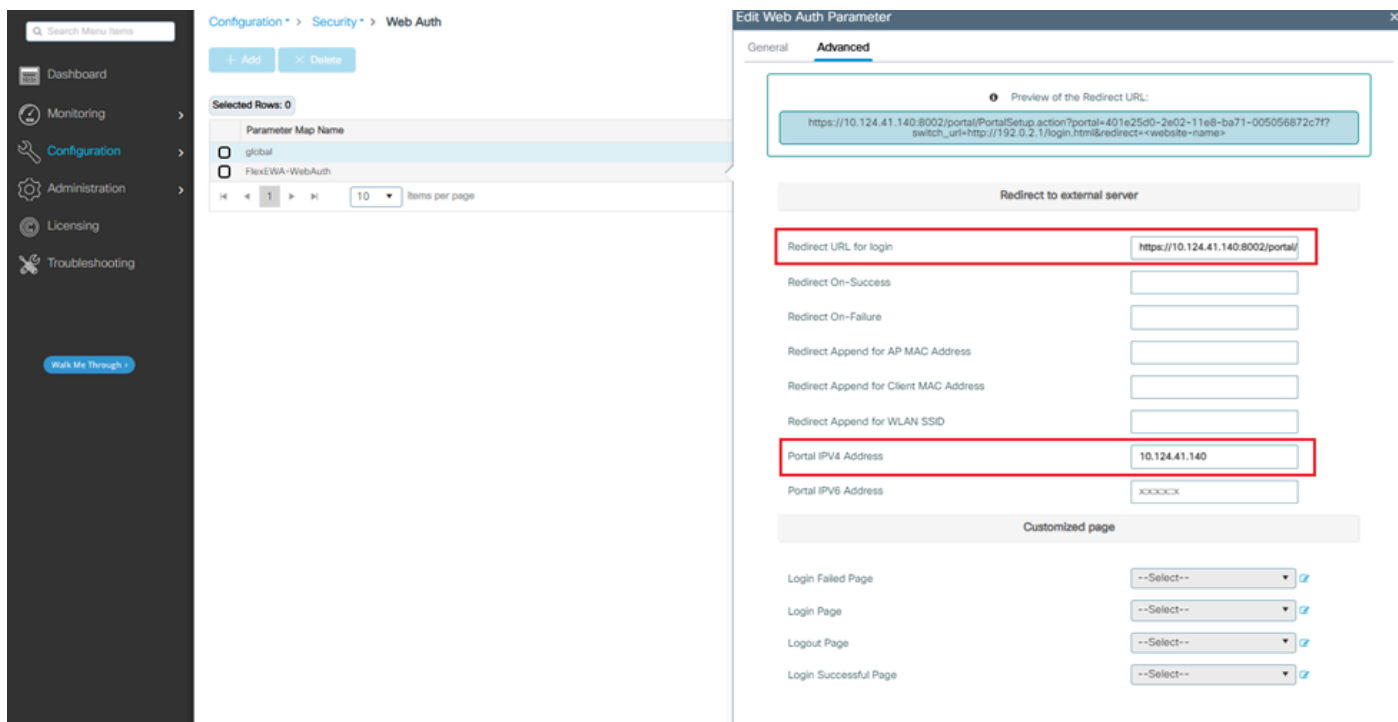


Configurazioni

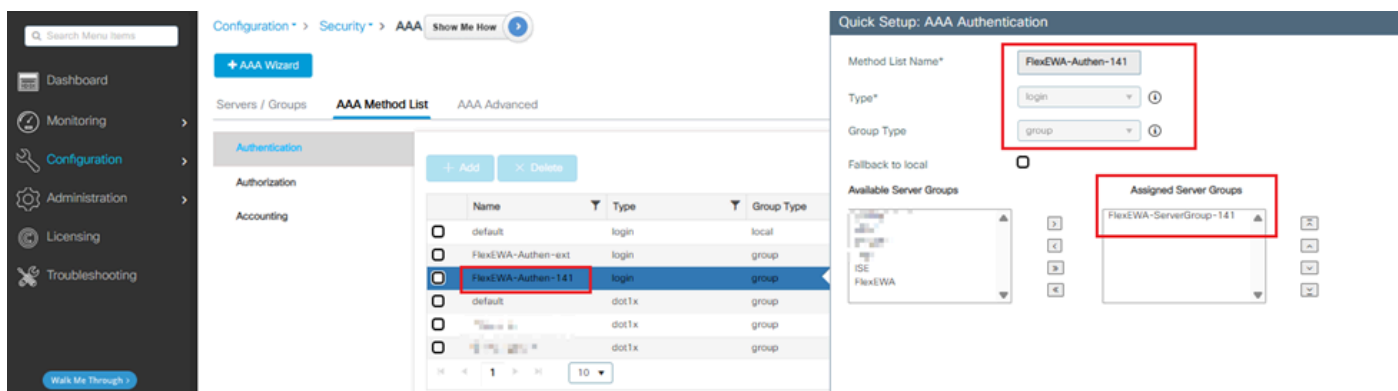
Passaggio 1. Passare a Configurazione > Sicurezza > Autenticazione Web > +Aggiungi mappa parametri autenticazione Web.

The screenshot shows the Cisco ISE configuration interface. On the left is a navigation menu with options like Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main area displays the 'Configuration > Security > Web Auth' path. A table lists 'Parameter Map Name' entries: 'global', 'FlexEWA-WebAuth', and 'FlexEWA-WebAuth-141'. The 'FlexEWA-WebAuth' entry is selected. On the right, the 'Edit Web Auth Parameter' window is open, showing the 'General' tab. Key fields are highlighted with red boxes: 'Parameter-map Name' is set to 'FlexEWA-WebAuth-1', 'Type' is set to 'webauth', and 'Banner Configuration' is set to 'None'. Other fields include 'Maximum HTTP connections' (100), 'Init-State Timeout(secs)' (120), and 'Sleeping Client Timeout (minutes)' (720).

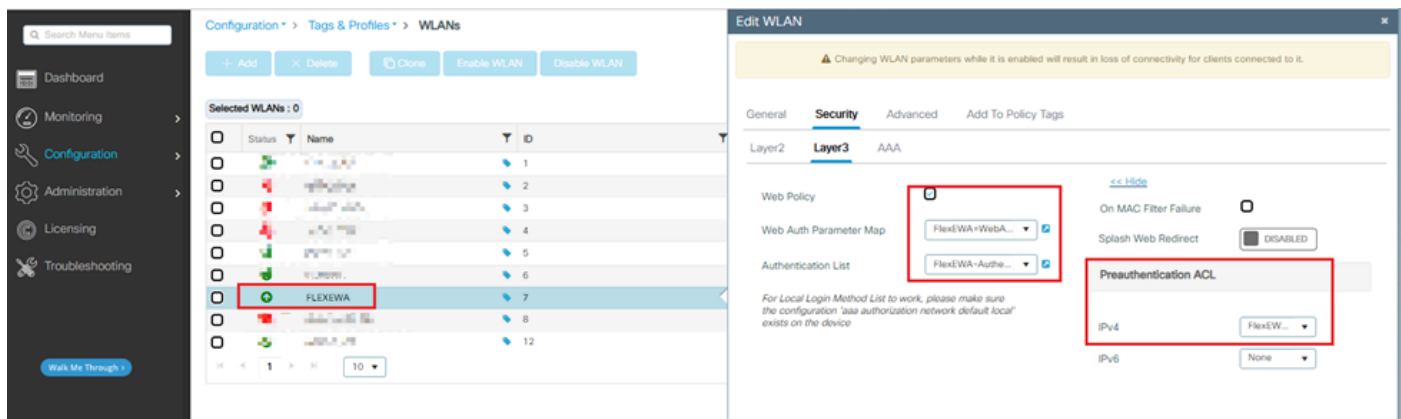
L'URL del portale viene generato da ISE (passaggio 7).



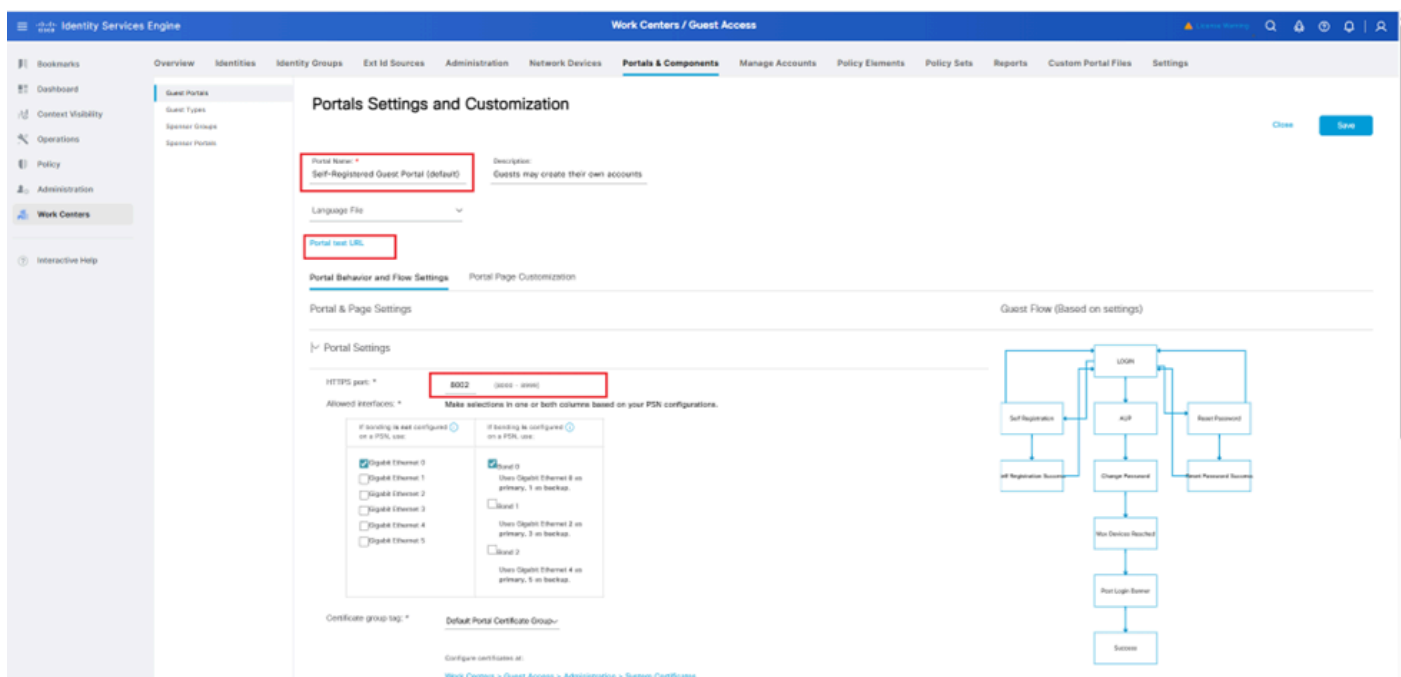
Passaggio 2. Passare a Configurazione > Sicurezza > AAA > Elenco metodi AAA > Autenticazione > + Aggiungi elenco autenticazione.



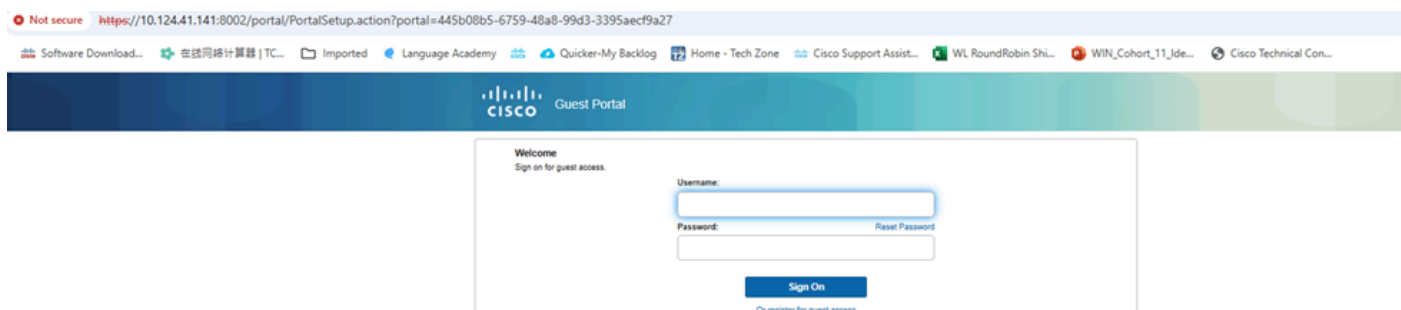
Passaggio 3. Si supponga che la porta HTTPS sia 8002, fare riferimento all'ACL WA-sec-10.124.41.140 generato automaticamente per aggiungere un nuovo ACL di preautenticazione.



Passaggio 7. Passare a Centri di lavoro > Portali e componenti > Portali guest > Impostazioni e personalizzazione portali > Nome portale > Portale guest con registrazione automatica (predefinito) per generare l'URL del portale da ISE.

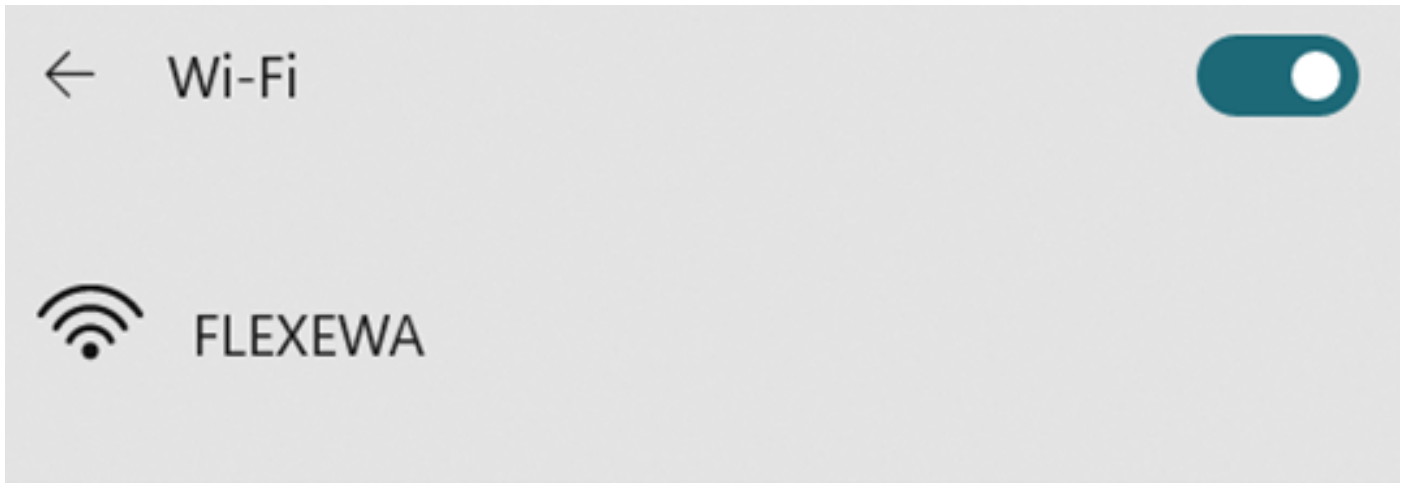


Il portale Web elencato viene visualizzato dopo aver fatto clic su URL test portale.

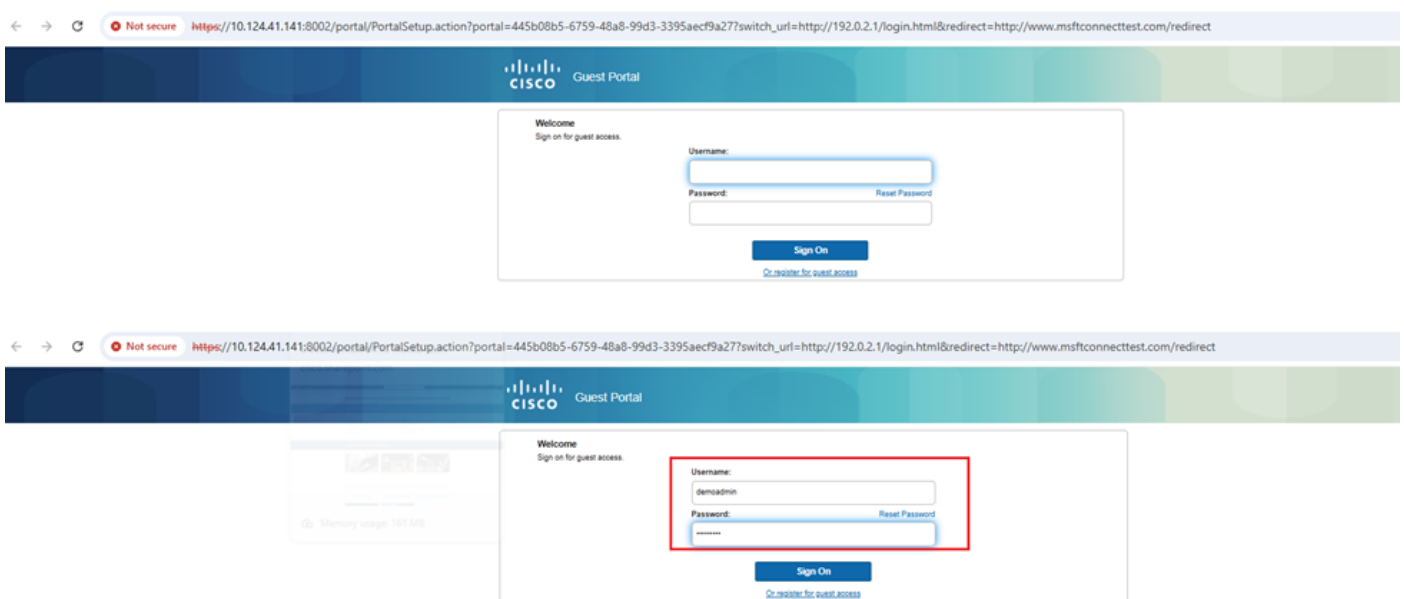


Verifica

Passaggio 1. Connessione di FLEXEWA SSID.



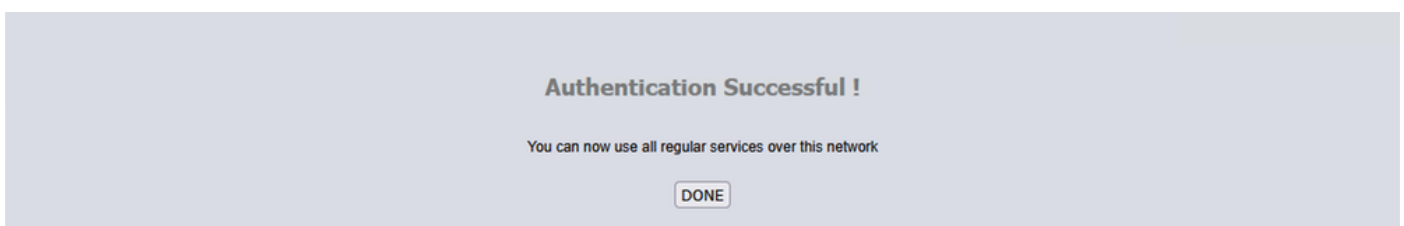
Passaggio 2. Reindirizzare al portale e immettere nome utente e password.



Passaggio 3. Viene visualizzato il portale per gli ospiti:



Passaggio 4. Dopo aver fatto clic su Continua, l'autenticazione ha esito positivo:



Traccia AR Esempio di tentativo riuscito

Questo è l'output di un tentativo di connessione riuscito dalla prospettiva di traccia Radio Active. Utilizzare questo come riferimento per identificare le fasi della sessione client per i client che si connettono a un SSID di autenticazione Web di layer 3.

Associazione client completata:

2025/09/09 15:21:48.617769958 {wncd_x_R0-0}{1}: [client-orch-sm] [17842]: Nota: MAC: f0b6.1e39.9ce8 Associazione ricevuta. BSSID c418.fc82.bb0b, WLAN FLEXEWA, Slot 1 AP c418.fc82.bb00, 9178_1, tag sito HK, tag criteri default-policy-tag, profilo criteri default-policy-profilo, Switching Central, ritardo socket 0ms, AP BSSID MAC c418.fc82.bb0b

2025/09/09 15:21:48.617813534 {wncd_x_R0-0}{1}: [client-orch-sm] [17842]: (debug) MAC: f0b6.1e39.9ce8 Ricevuta richiesta di associazione Dot11. Elaborazione avviata, SSID: FLEXEWA, Profilo criterio: default-policy-profile, Nome punto di accesso: 9178_1, Indirizzo Mac Ap: c418.fc82.bb00BSSID MAC000.0000.0000WLAN ID: 7RSSI: -30, SNR: 67

2025/09/09 15:21:48.618002570 {wncd_x_R0-0}{1}: [client-orch-state] [17842]: Nota: MAC: f0b6.1e39.9ce8 Transizione stato client: S_CO_INIT -> S_CO_ASSOCIATING

2025/09/09 15:21:48.618017149 {wncd_x_R0-0}{1}: [client-orch-sm] [17842]: ERR: MAC: f0b6.1e39.9ce8 Impossibile ottenere il record dot11

2025/09/09 15:21:48.618301251 {wncd_x_R0-0}{1}: [convalida11] [17842]: (info): MAC: f0b6.1e39.9ce8 Dot11 ie convalida le velocità di uscita/alimentazione. Convalida superata per tariffe supportate radio_type 2

2025/09/09 15:21:48.618320304 {wncd_x_R0-0}{1}: [convalida11] [17842]: (debug) MAC: f0b6.1e39.9ce8 Dot11 ie convalida rsnx, client che non utilizza sae, ignora controllo

2025/09/09 15:21:48.618339230 {wncd_x_R0-0}{1}: [convalida11] [17842]: (info): MAC: f0b6.1e39.9ce8 WiFi diretto: Dot11 convalida IP2P IE. IP2P IE non presente.

2025/09/09 15:21:48.618598747 {wncd_x_R0-0}{1}: [dot11] [17842]: (debug) MAC: f0b6.1e39.9ce8 dot11 invia risposta associazione. Risposta associazione di frame con resp_status_code: 0

2025/09/09 15:21:48.618604733 {wncd_x_R0-0}{1}: [dot11] [17842]: (debug) MAC: f0b6.1e39.9ce8 Dot11 Informazioni sulla capacità byte1 1, byte2: 11

2025/09/09 15:21:48.618696034 {wncd_x_R0-0}{1}: [dot11-frame] [17842]: (info): MAC: f0b6.1e39.9ce8 WiFi diretto: ignorare la compilazione di Assoc Resp con P2P IE: Criteri diretti Wi-Fi disabilitati

2025/09/09 15:21:48.618785409 {wncd_x_R0-0}{1}: [dot11] [17842]: (info): MAC: f0b6.1e39.9ce8 dot11 invia risposta associazione. Invio risposta assoc di lunghezza: 177 con resp_status_code: 0, DOT11_STATUS: DOT11_STATUS_SUCCESS

2025/09/09 15:21:48.618791096 {wncd_x_R0-0}{1}: [dot11] [17842]: Nota: MAC: f0b6.1e39.9ce8 Associazione riuscita. AID 33, roaming = False, WGB = False, 11r = False, 11w = False, roaming veloce = False

2025/09/09 15:21:48.618806595 {wncd_x_R0-0}{1}: [dot11] [17842]: (info): MAC: f0b6.1e39.9ce8 DOT11 transizione di stato: S_DOT11_INIT -> S_DOT11_ASSOCIATED

2025/09/09 15:21:48.618855282 {wncd_x_R0-0}{1}: [client-orch-sm] [17842]: (debug) MAC: f0b6.1e39.9ce8 L'associazione Station Dot11 ha esito positivo.

Autenticazione di livello 2 ignorata:

2025/09/09 15:21:48.618992721 {wncd_x_R0-0}{1}: [client-orch-sm] [17842]: (debug) MAC:

f0b6.1e39.9ce8 Avvio dell'autenticazione L2. Bssid nella macchina a stati:c418.fc82.bb0b Bssid nella richiesta è:c418.fc82.bb0b
2025/09/09 15:21:48.619006036 {wncd_x_R0-0}{1}: [client-orch-state] [17842]: Nota: MAC: f0b6.1e39.9ce8 Transizione stato client: S_CO_ASSOCIATING -> S_CO_L2_AUTH_IN_PROGRESS
2025/09/09 15:21:48.619093387 {wncd_x_R0-0}{1}: [client-auth] [17842]: Nota: MAC: Autenticazione f0b6.1e39.9ce8 L2 avviata. metodo WEBAUTH, VLAN criterio 0, override AAA = 0 [...]
2025/09/09 15:21:48.623839337 {wncd_x_R0-0}{1}: [client-auth] [17842]: (info): MAC: f0b6.1e39.9ce8 Transizione stato interfaccia di autenticazione client: S_AUTHIF_L2_WEBAUTH_PENDING -> S_AUTHIF_L2_WEBAUTH_DONE
2025/09/09 15:21:48.623863687 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (info): [f0b6.1e39.9ce8:capwap_90000008] Il tipo di dispositivo per la sessione viene rilevato come Intel-Device e il vecchio nome di dispositivo e dispositivo Intel-Device per la sessione viene rilevato come INTEL CORPORATE e il vecchio Intel CORPORATE & Old Protocol Map 1 e il nuovo è 1
2025/09/09 15:21:48.623873529 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (info): [f0b6.1e39.9ce8:capwap_90000008] ricezione della notifica di aggiunta/modifica attr di auth mgr per attr dc-profile-name(1130)
2025/09/09 15:21:48.623911035 {wncd_x_R0-0}{1}: [client-orch-sm] [17842]: (debug) MAC: f0b6.1e39.9ce8 L2 Autenticazione della stazione riuscita., Autenticazione L3: 1

Piombo ACL:

2025/09/09 15:21:48.620896754 {wncd_x_R0-0}{1}: [webauth-sm] [17842]: (info): [0.0.0.0]Avvio di Webauth, mac [f0:b6:1e:39:9c:e8],IIF 0 , audit-ID D1257C0A00000CA2D54F867
2025/09/09 15:21:48.620927053 {wncd_x_R0-0}{1}: [webauth-state] [17842]: (info): [f0b6.1e39.9ce8][0.0.0.0]Mappa parametri utilizzata: globale
2025/09/09 15:21:48.620935005 {wncd_x_R0-0}{1}: [webauth-state] [17842]: (info): [f0b6.1e39.9ce8][0.0.0.0]Stato non valido -> INIT
2025/09/09 15:21:48.620942683 {wncd_x_R0-0}{1}: [webauth-sess] [17842]: (info): capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Crea sessione, Aggiungi indirizzo 0.0.0.0
2025/09/09 15:21:48.620946808 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [17842]: (info): [0000.0000.0000:sconosciuto] ID zona recuperata 0x0 per bssid 12364632846638254486
2025/09/09 15:21:48.620958619 {wncd_x_R0-0}{1}: [webauth-state] [17842]: (info): capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Mappa-param utilizzata: FlexEWA=WebAuth-141
2025/09/09 15:21:48.620962048 {wncd_x_R0-0}{1}: [webauth-state] [17842]: (info): capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]State INIT -> INIT
2025/09/09 15:21:48.620978097 {wncd_x_R0-0}{1}: [webauth-sm] [17842]: (info): capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Avvio della sessione, inoltro dello stato a 0 IF 0x90000008 mac [f0b6.1e39.9ce8]
2025/09/09 15:21:48.620981018 {wncd_x_R0-0}{1}: [webauth-sm] [17842]: (info): capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Avvio sessione, sessioni di inizializzazione SM 5
2025/09/09 15:21:48.620988217 {wncd_x_R0-0}{1}: [webauth-state] [17842]: (info): capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Mappa-param utilizzata: FlexEWA=WebAuth-141
2025/09/09 15:21:48.620991618 {wncd_x_R0-0}{1}: [webauth-state] [17842]: (info): capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]State INIT -> INIT

2025/09/09 15:21:48.621023019 {wncd_x_R0-0}{1}: [webauth-acl] [17842]: (info):
capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Applicazione dell'ACL di intercettazione IPv4 tramite
SVM, nome: WA-v4-int-10.124.41.141-7, priorità: 50, IIF-ID: 0

2025/09/09 15:21:48.621032776 {wncd_x_R0-0}{1}: [svm] [17842]: (info): INFO_SVM:
Applicazione del modello Svc WA-v4-int-10.124.41.141-7 (ML:NONE)

2025/09/09 15:21:48.621786262 {wncd_x_R0-0}{1}: [epm] [17842]: (info):
[f0b6.1e39.9ce8:capwap_90000008] Funzionalità (PLUG-IN URL EPM) avviata (stato riuscito)

2025/09/09 15:21:48.621804034 {wncd_x_R0-0}{1}: [epm-acl] [17842]: (info):
[f0b6.1e39.9ce8:capwap_90000008] ID filtro: FlexEWA141-sec-ACL ricevuti

2025/09/09 15:21:48.622151544 {wncd_x_R0-0}{1}: [epm] [17842]: (info):
[f0b6.1e39.9ce8:capwap_90000008] Funzionalità (PLUG-IN ACL EPM) avviata (stato riuscito)

2025/09/09 15:21:48.622187815 {wncd_x_R0-0}{1}: [svm] [17842]: (info): INFO_SVM: La risposta
di epm è SYNC con codice restituito Success

2025/09/09 15:21:48.62226011 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (info):
[f0b6.1e39.9ce8:capwap_90000008] Generazione del modello di evento successivo attivata (9) in
questa sessione, client (sconosciuto) (0)

2025/09/09 15:21:48.62265240 {wncd_x_R0-0}{1}: [webauth-acl] [17842]: (info):
capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Applicazione dell'ACL di intercettazione IPv6 tramite
SVM, nome: IP-Adm-V6-Int-ACL-global-7, priorità: 52, IIF-ID: 0

2025/09/09 15:21:48.62270327 {wncd_x_R0-0}{1}: [svm] [17842]: (info): INFO_SVM: Applicazione
del modello Svc IP-Adm-V6-Int-ACL-global-7 (ML:NONE)

2025/09/09 15:21:48.622898831 {wncd_x_R0-0}{1}: [epm] [17842]: (info):
[f0b6.1e39.9ce8:capwap_90000008] Funzionalità (PLUG-IN URL EPM) avviata (stato riuscito)

2025/09/09 15:21:48.622932973 {wncd_x_R0-0}{1}: [svm] [17842]: (info): INFO_SVM: La risposta
di epm è SYNC con codice restituito Success

2025/09/09 15:21:48.622957784 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (info):
[f0b6.1e39.9ce8:capwap_90000008] Generazione del modello di evento successivo attivata (9) in
questa sessione, client (sconosciuto) (0)

2025/09/09 15:21:48.623119047 {wncd_x_R0-0}{1}: [dot11] [17842]: (debug) MAC:
f0b6.1e39.9ce8 Dot11 SAE trova l'avanzamento ipsk come 0, non in stato in sospeso

2025/09/09 15:21:48.623126095 {wncd_x_R0-0}{1}: [llbridge-main] [17842]: (debug) MAC:
f0b6.1e39.9ce8 Bridging locale del collegamento non abilitato per questo client. Verifica della
validità della VLAN non eseguita.

2025/09/09 15:21:48.623205421 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (info):
[f0b6.1e39.9ce8:capwap_90000008] Modifica dello stato del contesto da 'Inattivo' a 'In esecuzione'

2025/09/09 15:21:48.623209350 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (info):
[f0b6.1e39.9ce8:capwap_90000008] Modifica dello stato di webauth del metodo da 'Non in
esecuzione' a 'In esecuzione'

2025/09/09 15:21:48.623572855 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (info):
[f0b6.1e39.9ce8:capwap_90000008] SM non può inviare il modello di evento attivato a PRE per
0x8D0000C0

2025/09/09 15:21:48.623680228 {wncd_x_R0-0}{1}: [client-auth] [17842]: (info): MAC:
f0b6.1e39.9ce8 Transizione stato interfaccia di autenticazione client:
S_AUTHIF_AWAIT_L2_WEBAUTH_START_RESP -> S_AUTHIF_L2_WEBAUTH_PENDING

Processo di apprendimento IP:

2025/09/09 15:21:51.628124695 {wncd_x_R0-0}{1}: [client-orch-state] [17842]: Nota: MAC: f0b6.1e39.9ce8 Transizione stato client: S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS

2025/09/09 15:21:51.628463813 {wncd_x_R0-0}{1}: [client-iplearn] [17842]: (info): MAC: f0b6.1e39.9ce8 Transizione dello stato di apprendimento IP: S_IPLEARN_INIT -> S_IPLEARN_IN_PROGRESS

2025/09/09 15:21:51.632284534 {wncd_x_R0-0}{1}: [client-auth] [17842]: (info): MAC: f0b6.1e39.9ce8 Transizione stato interfaccia di autenticazione client: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_L2_WEBAUTH_DONE

2025/09/09 15:21:51.676501288 {wncd_x_R0-0}{1}: [17842]: (info): RX: IPv6 DHCP da intf capwap_9000008 su vlan 174 Src MAC: f0b6.1e39.9ce8 Dst MAC: 333.0001.0002 Ipv6 SRC: fe80:3f83:2848:d30:7aea, Ipv6 DST: ff02:1:2, tipo: tipo messaggio: DHCPV6_MSG_SOLICIT xid: 14443573

2025/09/09 15:21:51.676541447 {wncd_x_R0-0}{1}: [17842]: (info): TX: IPv6 DHCP da intf capwap_9000008 su vlan 174 Src MAC: f0b6.1e39.9ce8 Dst MAC: 333.0001.0002 Ipv6 SRC: fe80:3f83:2848:d30:7aea, Ipv6 DST: ff02:1:2, tipo: tipo messaggio: DHCPV6_MSG_SOLICIT xid: 14443573

2025/09/09 15:21:51.706187097 {wncd_x_R0-0}{1}: [17842]: (info): RX: ARP dall'interfaccia capwap_9000008 sulla vlan 174. MAC di origine: f0b6.1e39.9ce8 Dest MAC: ffff.ffff.ffff RICHIESTA ARP, MAC mittente ARP: f0b6.1e39.9ce8 ARP target MAC: 0000.0000.0000 ARP mittente IP: 169.254.137.222, ARP target IP: 169.254.137.222, [...]

2025/09/09 15:21:52.686190945 {wncd_x_R0-0}{1}: [client-iplearn] [17842]: Nota: MAC: f0b6.1e39.9ce8 Client IP imparare riuscito. Metodo: IP DHCP: 10.124.37.251

2025/09/09 15:21:52.686244192 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (info): [f0b6.1e39.9ce8:capwap_90000008] ricezione notifica di aggiunta/modifica attr di auth mgr per attr addr(8)

2025/09/09 15:21:52.686285422 {wncd_x_R0-0}{1}: [webauth-sess] [17842]: (info): capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Notif CB modificato, aggiungere l'indirizzo 10.124.37.251 [f0b6.1e39.9ce8]

2025/09/09 15:21:52.686289265 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [17842]: (info): [0000.0000.0000:sconosciuto] ID zona recuperata 0x0 per bssid 12364632846638254486

2025/09/09 15:21:52.686291647 {wncd_x_R0-0}{1}: [webauth-sess] [17842]: (info): aggiunta della sessione webauth alla tabella hash ipv4 per l'id vrf 0, id tabella vrf ipv4 0

2025/09/09 15:21:52.686430038 {wncd_x_R0-0}{1}: [auth-mgr-feat_acct] [17842]: (info): [f0b6.1e39.9ce8:capwap_90000008] SM Notified, attributo Add/Update addr 10.124.37.251

2025/09/09 15:21:52.686456653 {wncd_x_R0-0}{1}: [epm] [17842]: (info): [0000.0000.0000:sconosciuto] HDL = 0x0 vlan 174 fail count 0 dirty_counter 0 is_dirty 0

2025/09/09 15:21:52.686710209 {wncd_x_R0-0}{1}: [client-iplearn] [17842]: (info): MAC: f0b6.1e39.9ce8 Transizione dello stato di apprendimento IP: S_IPLEARN_IN_PROGRESS -> S_IPLEARN_COMPLETE

Processo di autenticazione e reindirizzamento di livello 3:

2025/09/09 15:21:52.687395906 {wncd_x_R0-0}{1}: [client-auth] [17842]: Nota: MAC: Autenticazione f0b6.1e39.9ce8 L3 avviata. LWA

2025/09/09 15:21:52.687472722 {wncd_x_R0-0}{1}: [client-auth] [17842]: (info): MAC: f0b6.1e39.9ce8 Transizione stato interfaccia di autenticazione client:
S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_WEBAUTH_PENDING

2025/09/09 15:21:52.687723489 {wncd_x_R0-0}{1}: [17842]: (info): RX: DHCPv4 dall'interfaccia Po1 sull'indirizzo MAC Src vlan 174: 4006.d589.4e78 Dst MAC: ffff.ffff.ffff src_ip: 10.124.37.242, dst_ip: 255.255.255.255, BOOTPREPLY, SIFS_DHCPACK, giaddr: 0.0.0.0, yiaddr: 10.124.37.251, CMAC: f0b6.1e39.9ce8

2025/09/09 15:21:52.687992316 {wncd_x_R0-0}{1}: [17842]: (info): TX: DHCPv4 dall'interfaccia Po1 sull'indirizzo MAC Src vlan 174: 4006.d589.4e78 Dst MAC: f0b6.1e39.9ce8 src_ip: 10.124.37.242, dst_ip: 255.255.255.255, BOOTPREPLY, SIFS_DHCPACK, giaddr: 0.0.0.0, yiaddr: 10.124.37.251, CMAC: f0b6.1e39.9ce8

2025/09/09 15:21:52.68020475 {wncd_x_R0-0}{1}: [well-infra-evq] [17842]: (dettagliata): Tipo:EWLC_CAPWAP_HDR_AP, Id:23277

[...]

2025/09/09 15:21:55.663715832 {wncd_x_R0-0}{1}: [webauth-io] [17842]: (info): capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]54129/197 IO stato NEW -> READING

2025/09/09 15:21:55.664060604 {wncd_x_R0-0}{1}: [webauth-io] [17842]: (info): capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]54129/197 Evento Read, Message ready

2025/09/09 15:21:55.64071121 {wncd_x_R0-0}{1}: [webauth-httpd] [17842]: (info): capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]GET ricevuto quando in stato INIT

2025/09/09 15:21:55.64077798 {wncd_x_R0-0}{1}: [webauth-httpd] [17842]: (info): capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]Richiesta HTTP GET

2025/09/09 15:21:55.664094019 {wncd_x_R0-0}{1}: [webauth-httpd] [17842]: (info): capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]Parse GET, src [10.124.37.251] dst [23.5.165.82] url [<http://www.msftconnecttest.com/connecttest.txt>]

[...]

2025/09/09 15:22:16.420792303 {wncd_x_R0-0}{1}: [webauth-httpd] [17842]: (info): capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]POST ricevuto quando in stato LOGIN

2025/09/09 15:22:32.375197748 {wncd_x_R0-0}{1}: [webauth-acl] [17842]: (info): capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]Scollegare l'ACL IPv4 tramite SVM, nome "WA-v4-int-10.124.41.141-7", pri 50, IIF 0

2025/09/09 15:22:32.376230716 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (info): [f0b6.1e39.9ce8:capwap_90000008] Generazione del modello di eventi successivo disattivata (11) in questa sessione, client (sconosciuto) (0)

2025/09/09 15:22:32.376262689 {wncd_x_R0-0}{1}: [webauth-acl] [17842]: (info): capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]Annulla applicazione dell'ACL IPv6 tramite SVM, nome "IP-Adm-V6-Int-ACL-global", pri 52, IIF 0

2025/09/09 15:22:32.376734374 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (info): [f0b6.1e39.9ce8:capwap_90000008] Generazione del modello di eventi successivo disattivata (11) in questa sessione, client (sconosciuto) (0)

2025/09/09 15:22:32.376865998 {wncd_x_R0-0}{1}: [dot11] [17842]: (debug) MAC: f0b6.1e39.9ce8 Dot11 SAE trova l'avanzamento ipsk come 0, non in stato in sospeso

2025/09/09 15:22:32.376870611 {wncd_x_R0-0}{1}: [llbridge-main] [17842]: (debug) MAC: f0b6.1e39.9ce8 Bridging locale del collegamento non abilitato per questo client. Verifica della

validità della VLAN non eseguita.

2025/09/09 15:22:32.376949875 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (info):

[f0b6.1e39.9ce8:capwap_90000008] Autenticazione riuscita da WebAuth, evento Auth riuscito

Transizione allo stato RUN:

2025/09/09 15:22:32.379351256 {wncd_x_R0-0}{1}: [client-auth] [17842]: Nota: MAC:

f0b6.1e39.9ce8 ADD MOBILE inviato. Flag di stato client: 0x38 BSSID: MAC: c418.fc82.bb0b

capwap IFID: 0x90000008, Aggiungi dispositivi mobili inviati: 1

2025/09/09 15:22:32.379583842 {wncd_x_R0-0}{1}: [errmsg] [17842]: (info):

%CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE: R0/0: wncd: Voce del nome utente (demoadmin) unita a ssid (FLEXEWA) per il dispositivo con MAC: f0b6.1e39.9ce8 su canale (100)

2025/09/09 15:22:32.379671775 {wncd_x_R0-0}{1}: [aaa-attr-inf] [17842]: (info): [Attributo applicato: bsn-vlan-interface-name 0 "wlc-management"]

2025/09/09 15:22:32.379673695 {wncd_x_R0-0}{1}: [aaa-attr-inf] [17842]: (info): [Attributo applicato: timeout 0 2800 (0x7080)]

2025/09/09 15:22:32.379683417 {wncd_x_R0-0}{1}: [aaa-attr-inf] [17842]: (info): [Attributo applicato: url-redirect-acl 0 "IP-Adm-V4-LOGOUT-ACL"]

2025/09/09 15:22:32.379727993 {wncd_x_R0-0}{1}: [ewlc-qos-client] [17842]: (info): MAC: Gestore stato di esecuzione QoS client f0b6.1e39.9ce8

2025/09/09 15:22:32.379756610 {wncd_x_R0-0}{1}: [rog-proxy-capwap] [17842]: (debug) Notifica stato di ESECUZIONE client gestito: f0b6.1e39.9ce8

2025/09/09 15:22:32.379810670 {wncd_x_R0-0}{1}: [client-orch-state] [17842]: Nota: MAC: f0b6.1e39.9ce8 Transizione stato client: S_CO_L3_AUTH_IN_PROGRESS -> ESEGUI_CO

Informazioni correlate

- [Configurazione e risoluzione dei problemi di autenticazione Web esterna su 9800 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).