

Configurazione di CWA con FlexConnect AP su un WLC con ISE

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazione WLC](#)

[Configurazione di ISE](#)

[Creazione del profilo di autorizzazione](#)

[Creare una regola di autenticazione](#)

[Creare una regola di autorizzazione](#)

[Abilita rinnovo IP \(facoltativo\)](#)

[Flusso del traffico](#)

[Verifica](#)

Introduzione

In questo documento viene descritto come configurare l'autenticazione Web centrale con i FlexConnect Access Point (AP) su un controller WLC (Wireless LAN Controller) con Identity Services Engine (ISE) nella modalità di commutazione locale.

Nota importante: al momento, l'autenticazione locale sui FlexAP non è supportata per questo scenario.

Altri documenti di questa serie

- [Esempio di autenticazione Web centrale con uno switch e configurazione di Identity Services Engine](#)
- [Esempio di autenticazione Web centralizzata su WLC e ISE](#)

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

- Cisco Identity Services Engine (ISE), versione 1.2.1
- Software Wireless LAN Controller, versione 7.4.100.0

Configurazione

Sono disponibili diversi metodi per configurare l'autenticazione Web centrale sul controller WLC. Il primo metodo è l'autenticazione Web locale, in cui il WLC reindirizza il traffico HTTP a un server interno o esterno in cui viene richiesta l'autenticazione dell'utente. Il WLC recupera quindi le credenziali (restituite tramite una richiesta HTTP GET nel caso di un server esterno) ed esegue un'autenticazione RADIUS. Nel caso di un utente guest, è necessario un server esterno, ad esempio Identity Service Engine (ISE) o NAC Guest Server (NGS), in quanto il portale offre funzionalità quali la registrazione dei dispositivi e l'autoprovisioning. Questo processo include i seguenti passaggi:

1. L'utente viene associato al SSID di autenticazione Web.
2. L'utente apre il browser.
3. Il WLC reindirizza al portale guest (ad esempio ISE o NGS) non appena viene immesso un URL.
4. L'utente esegue l'autenticazione nel portale.
5. Il portale guest reindirizza nuovamente al WLC con le credenziali immesse.
6. Il WLC autentica l'utente guest tramite RADIUS.
7. Il WLC reindirizza all'URL originale.

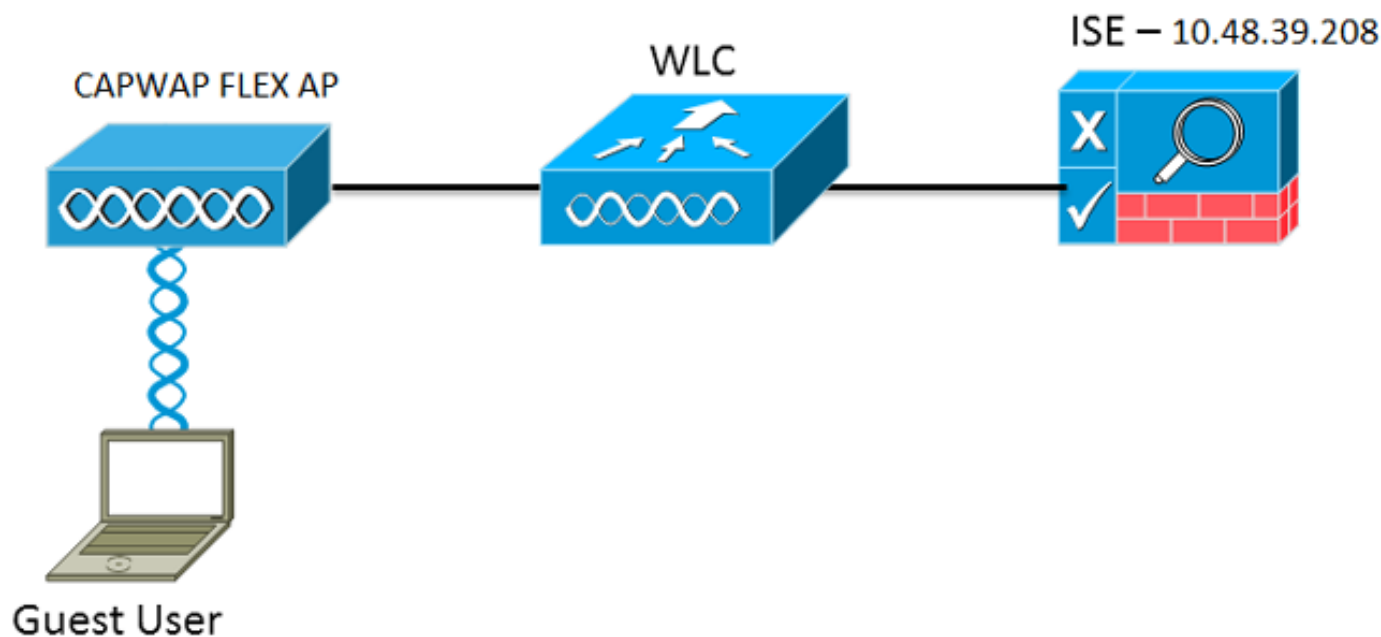
Questo processo include molti reindirizzamenti. Il nuovo approccio prevede l'utilizzo dell'autenticazione Web centrale, che funziona con ISE (versioni successive alla 1.1) e WLC (versioni successive alla 7.2). Questo processo include i seguenti passaggi:

1. L'utente viene associato al SSID di autenticazione Web.
2. L'utente apre il browser.
3. Il WLC reindirizza al portale guest.
4. L'utente esegue l'autenticazione nel portale.
5. L'ISE invia una richiesta di modifica dell'autorizzazione RADIUS (CoA - UDP Port 1700) per indicare al controller che l'utente è valido ed eventualmente preme gli attributi RADIUS come l'Access Control List (ACL).
6. All'utente viene richiesto di riprovare l'URL originale.

In questa sezione vengono descritti i passaggi necessari per configurare l'autenticazione Web centrale su WLC e ISE.

Esempio di rete

Questa configurazione utilizza la seguente configurazione di rete:



Configurazione WLC

La configurazione del WLC è abbastanza semplice. Per ottenere l'URL di autenticazione dinamica da ISE, viene usato un "trucco?" (come sugli switch). (Poiché usa la CoA, è necessario creare una sessione perché l'ID sessione fa parte dell'URL.) Il SSID è configurato per l'uso del filtro MAC e l'ISE è configurato per restituire un messaggio di accesso accettato anche se l'indirizzo MAC non viene trovato in modo da inviare l'URL di reindirizzamento per tutti gli utenti.

Inoltre, è necessario abilitare RADIUS Network Admission Control (NAC) e l'override AAA. Il RADIUS NAC consente all'ISE di inviare una richiesta CoA che indica che l'utente è ora autenticato e può accedere alla rete. Viene anche utilizzato per la valutazione della postura in cui l'ISE cambia il profilo utente in base al risultato della postura.

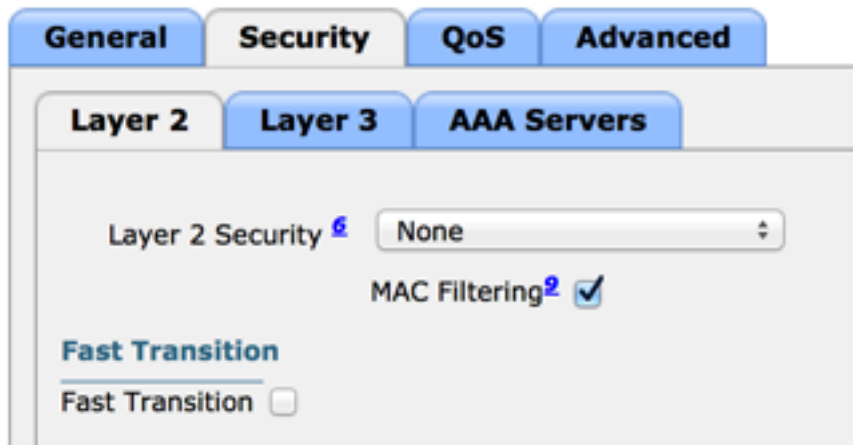
1. Verificare che per il server RADIUS sia abilitata la specifica RFC3576 (CoA), che è l'impostazione predefinita.

The screenshot shows the Cisco configuration interface for RADIUS Authentication Servers. The left sidebar contains a navigation menu with categories like AAA, Local EAP, Priority Order, Certificate, Access Control Lists, Wireless Protection Policies, Web Auth, TrustSec SXP, and Advanced. The main content area is titled 'RADIUS Authentication Servers > Edit' and displays various configuration parameters for a server with index 1. The parameters include Server Address (10.48.39.208), Shared Secret Format (ASCII), Shared Secret (masked with ***), Confirm Shared Secret (masked with ***), Key Wrap (disabled), Port Number (1812), Server Status (Enabled), Support for RFC 3576 (Enabled), Server Timeout (2 seconds), Network User (Enabled), Management (Enabled), and IPsec (disabled). The 'Support for RFC 3576' option is highlighted with a red box.

2. Creare una nuova WLAN. In questo esempio viene creata una nuova WLAN chiamata *CWAFlex* che viene assegnata alla *vlan33*. Si noti che l'operazione non avrà molti effetti in quanto il punto di accesso è in modalità di commutazione locale.

The screenshot shows the Cisco configuration interface for the WLAN configuration page. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The main content area is titled 'WLANs > Edit 'CWAFlex'' and has four tabs: General, Security, QoS, and Advanced. The 'Security' tab is selected, showing the following configuration: Profile Name (CWAFlex), Type (WLAN), SSID (CWAFlex), Status (Enabled), Security Policies (MAC Filtering), Radio Policy (All), Interface/Interface Group(G) (vlan33), Multicast Vlan Feature (Disabled), Broadcast SSID (Enabled), and NAS-ID (WLC). A note indicates that modifications done under the security tab will appear after applying the changes.

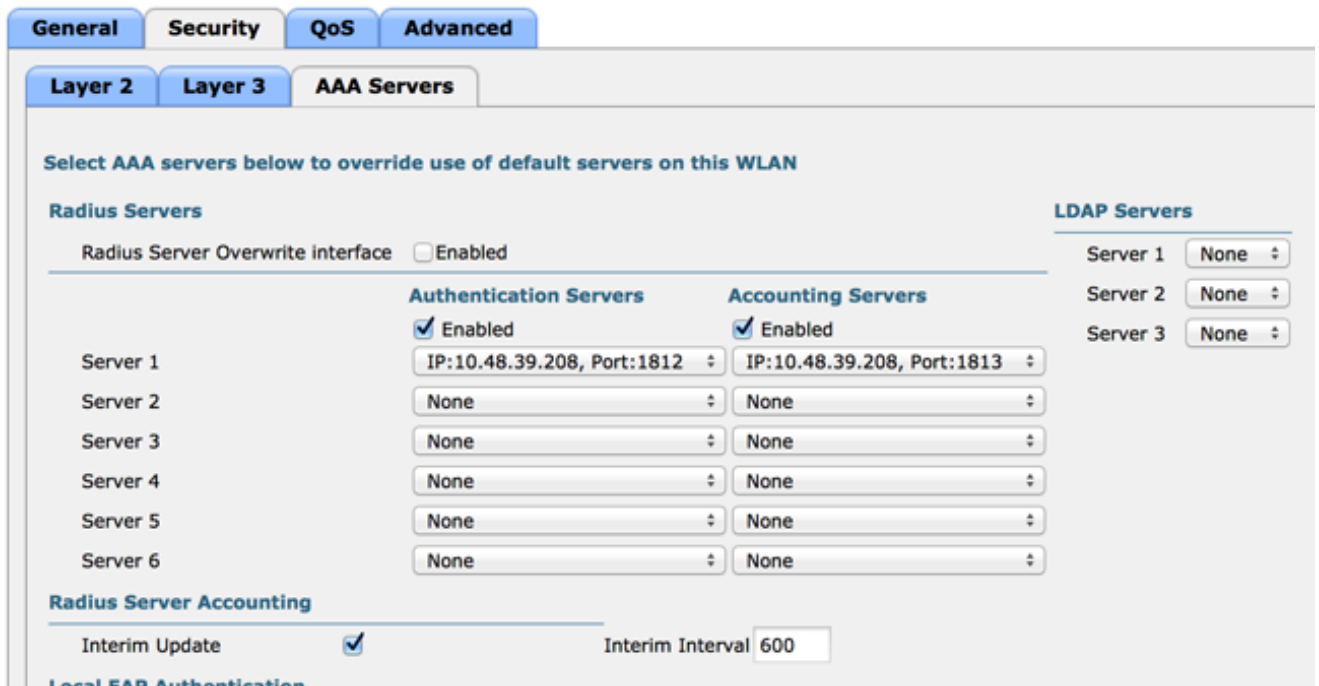
3. Nella scheda Protezione, abilitare il filtro MAC come protezione di livello 2.



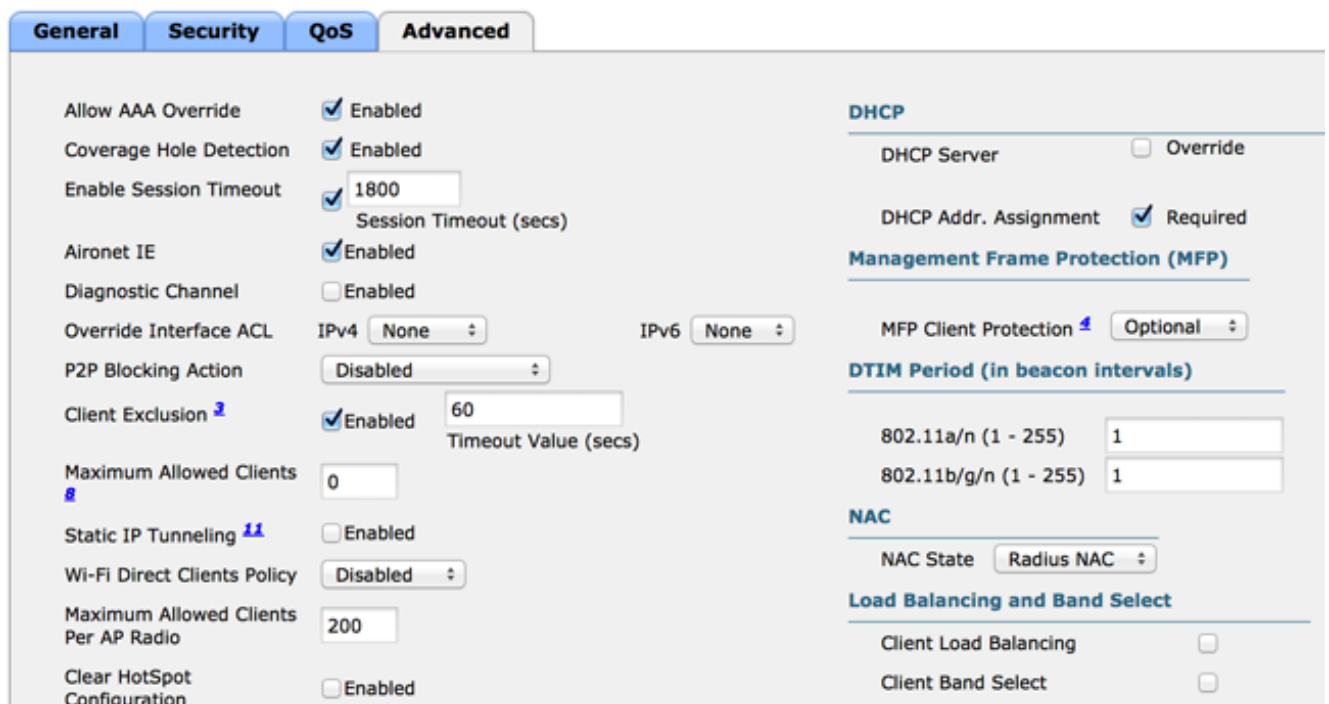
4. Nella scheda Layer 3 verificare che la protezione sia disattivata. Se l'autenticazione Web è attivata sul layer 3, l'autenticazione Web locale è attivata, non l'autenticazione Web centrale.



5. Nella scheda Server AAA, selezionare il server ISE come server radius per la WLAN. Facoltativamente, è possibile selezionarlo per l'accounting in modo da ottenere informazioni più dettagliate su ISE.



6. Nella scheda Advanced (Avanzate), verificare che Allow AAA Override (Consenti sostituzione AAA) sia selezionato e Radius NAC (Stato NAC) sia selezionato.



7. Creare un ACL di reindirizzamento.

Nel messaggio Access-Accept dell'ISE viene fatto riferimento a questo ACL e vengono definiti il traffico che deve essere reindirizzato (rifiutato dall'ACL) e il traffico che non deve essere reindirizzato (autorizzato dall'ACL). Fondamentalmente, è necessario autorizzare il DNS e il traffico da e verso l'ISE. **Nota:** un problema con gli access point FlexConnect è che è necessario creare un ACL FlexConnect separato dal normale ACL. Questo problema è documentato nel bug Cisco CSCue68065 ed è risolto nella release 7.5. Nella versione WLC 7.5 e successive, è richiesto solo un FlexACL e non è necessario alcun ACL standard. Il WLC si aspetta che l'ACL di reindirizzamento restituito da ISE sia un ACL normale. Tuttavia,

per assicurarne il corretto funzionamento, è necessario applicare lo stesso ACL dell'ACL FlexConnect.

Nell'esempio viene mostrato come creare un ACL FlexConnect con nome *flexred*:

The screenshot shows the Cisco Wireless configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', and 'SECURITY'. The left sidebar is titled 'Wireless' and contains a tree view with 'Access Points' (All APs, Radios: 802.11a/n, 802.11b/g/n, Dual-Band Radios, Global Configuration), 'Advanced', 'Mesh', 'RF Profiles', 'FlexConnect Groups', and 'FlexConnect ACLs'. The main content area is titled 'FlexConnect Access Control Lists' and shows a dropdown menu for 'Acl Name' with 'flexred' selected.

Crea regole per autorizzare il traffico DNS e il traffico verso ISE e nega il resto.

The screenshot shows the 'Access Control Lists > Edit' configuration page for the 'flexred' ACL. The 'General' section shows the 'Access List Name' as 'flexred'. Below is a table of rules:

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP
1	Permit	0.0.0.0 / 0.0.0.0	10.48.39.208 / 255.255.255.255	Any	Any	Any	Any <input checked="" type="checkbox"/>
2	Permit	10.48.39.208 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any <input checked="" type="checkbox"/>
3	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any <input checked="" type="checkbox"/>
4	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any <input checked="" type="checkbox"/>
5	Deny	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any <input checked="" type="checkbox"/>

Se si desidera la massima sicurezza, è possibile consentire solo la porta 8443 verso ISE. (In caso di postura, è necessario aggiungere le porte di postura tipiche, ad esempio 8905,8906,8909,8910.)

(Solo sul codice precedente alla versione 7.5 a causa di [CSCue68065](#)) Scegliere **Sicurezza** > **Access Control Lists** per creare un ACL identico con lo stesso nome.

The screenshot shows the Cisco Security configuration interface. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS, and SECURITY. The left sidebar shows the Security menu with 'Access Control Lists' selected. The main content area is titled 'Access Control Lists' and features an 'Enable Counters' checkbox. Below this is a table with columns for Name and Type. One entry is visible: 'flexred' with Type 'IPv4'.

Name	Type
flexred	IPv4

Preparare il punto di accesso FlexConnect specifico. Si noti che per un'implementazione più ampia, in genere si utilizzano i gruppi FlexConnect e non si eseguono questi elementi per punto di accesso per motivi di scalabilità.

Fare clic su **Wireless** e selezionare il punto di accesso specifico. Fare clic sulla scheda **FlexConnect** e selezionare **ACL di autenticazione Web esterna**. Nelle versioni precedenti alla 7.4, questa opzione era denominata *criteri Web*.

The screenshot shows the Cisco Wireless configuration interface for 'FlexAP1'. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar shows the Wireless menu with 'FlexConnect Groups' selected. The main content area is titled 'All APs > Details for FlexAP1' and features several tabs: General, Credentials, Interfaces, High Availability, Inventory, FlexConnect, and Advanced. The 'FlexConnect' tab is active. Under the 'PreAuthentication Access Control Lists' section, 'External_WebAuthentication.ACLs' is selected and highlighted with a red box.

Aggiungere l'ACL (denominato *flexred* in questo esempio) all'area dei criteri Web. In questo

modo, l'ACL viene pre-indirizzato al punto di accesso. Non è ancora stato applicato, ma il contenuto dell'ACL viene assegnato all'access point in modo che possa essere applicato quando necessario.

The screenshot shows the Cisco Wireless LAN Controller (WLC) configuration interface. The top navigation bar includes: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, and COMMANDS. The left sidebar shows the configuration tree with 'Wireless' expanded to 'Access Points' > 'FlexAP1' > 'ACL Mappings'. The main content area displays the configuration for FlexAP1, including the AP Name (FlexAP1) and Base Radio MAC (00:1c:f9:c2:42:30). Under 'WLAN ACL Mapping', there is a form with 'WLAN Id' set to 0 and 'WebAuth ACL' set to 'flexred', with an 'Add' button. Below this is a table with columns 'WLAN Id', 'WLAN Profile Name', and 'WebAuth ACL'. Under 'WebPolicies', there is a form with 'WebPolicy ACL' set to 'flexred' and an 'Add' button. At the bottom, under 'WebPolicy Access Control Lists', the 'flexred' policy is listed with a dropdown arrow.

Configurazione WLC completata.

Configurazione di ISE

Creazione del profilo di autorizzazione

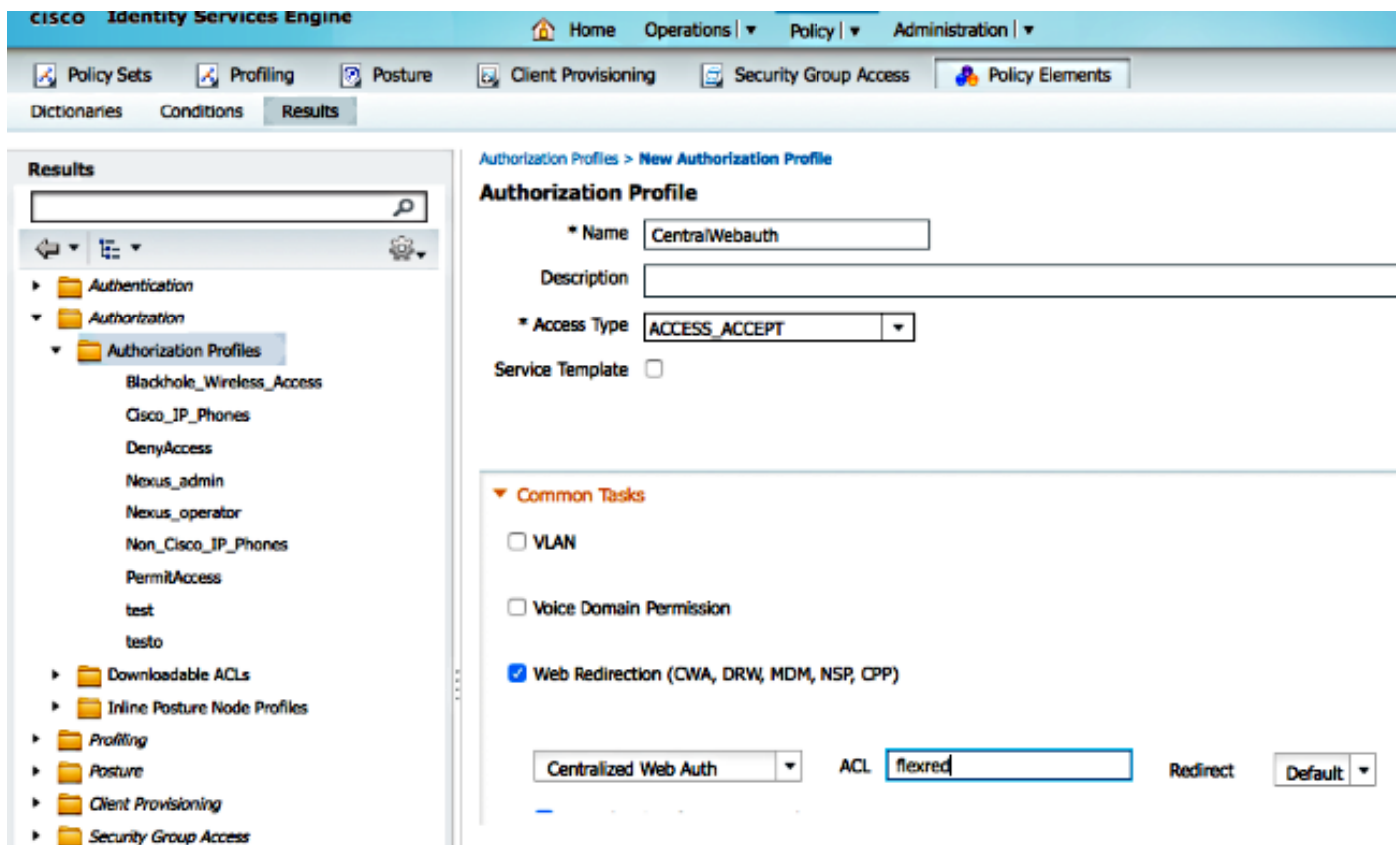
Per creare il profilo di autorizzazione, completare i seguenti passaggi:

1. Fare clic su **Criterio** e quindi su **Elementi criterio**.
2. Fare clic su **Risultati**.
3. Espandere **Autorizzazione** e quindi fare clic su **Profilo di autorizzazione**.
4. Per creare un nuovo profilo di autorizzazione per webauth centrale, fare clic sul pulsante **Add** (Aggiungi).
5. Nel campo **Nome**, immettere un nome per il profilo. In questo esempio viene utilizzato *CentralWebauth*.
6. Selezionare **ACCESS_ACCEPT** dall'elenco a discesa Access Type.
7. Selezionare la casella di controllo **Autenticazione Web** e scegliere **Autenticazione Web centralizzata** dall'elenco a discesa.
8. Nel campo ACL, immettere il nome dell'ACL sul WLC che definisce il traffico che verrà

reindirizzato. In questo esempio viene utilizzato *flexred*.

9. Selezionare **Predefinito** dall'elenco a discesa Reindirizza.

L'attributo Redirect definisce se l'ISE deve vedere il portale Web predefinito o un portale Web personalizzato creato dall'amministratore ISE. Ad esempio, l'ACL *flessibile* di questo esempio attiva un reindirizzamento sul traffico HTTP dal client a qualsiasi destinazione.



Creare una regola di autenticazione

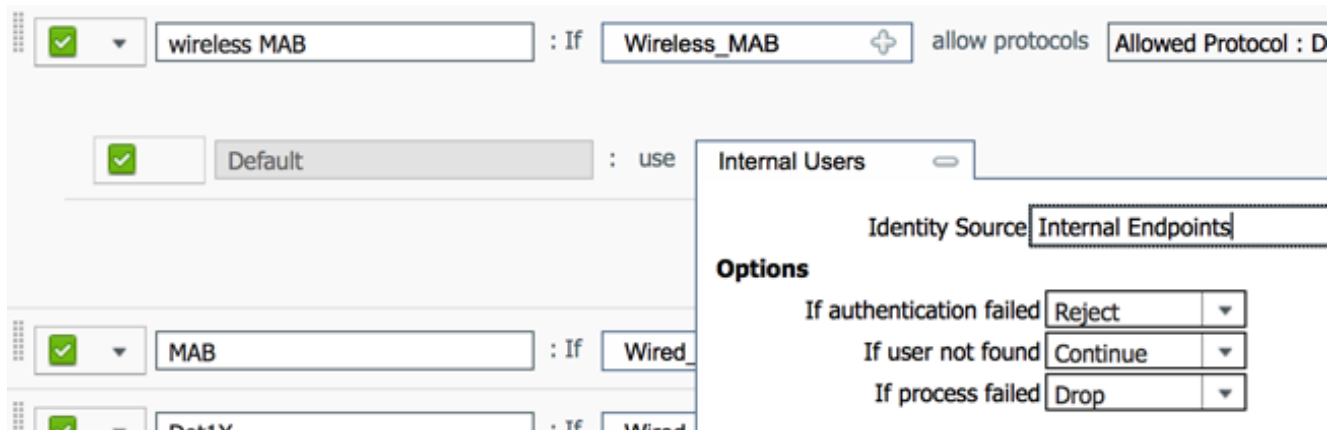
Per utilizzare il profilo di autenticazione per creare la regola di autenticazione, completare la procedura seguente:

1. Scegliere **Autenticazione** dal menu Criteri. In questa immagine viene illustrato un esempio di come configurare la regola dei criteri di autenticazione. In questo esempio, viene configurata una regola che verrà attivata quando viene rilevato il filtro MAC.



2. Immettere un nome per la regola di autenticazione. In questo esempio viene utilizzato *Wireless mab*.
3. Selezionare l'icona più (+) nel campo Condizione If.
4. Selezionate **Condizione composta (Compound condition)**, quindi **Wireless_MAB**.
5. Scegliere "Accesso di rete predefinito" come protocollo consentito.

6. Fare clic sulla freccia accanto a **e ...** per espandere ulteriormente la regola.
7. Fare clic sull'icona **+** nel campo Origine identità e scegliere **Endpoint interni**.
8. Scegliere **Continua** dall'elenco a discesa Se l'utente non è stato trovato.



Questa opzione consente di autenticare un dispositivo (tramite webauth) anche se il relativo indirizzo MAC non è noto. I client Dot1x possono ancora eseguire l'autenticazione con le credenziali e non devono essere interessati da questa configurazione.

Creare una regola di autorizzazione

Sono ora disponibili diverse regole da configurare nei criteri di autorizzazione. Quando il PC è associato, viene filtrato tramite mac; si presume che l'indirizzo MAC non sia noto, quindi vengono restituiti webauth e ACL. Questa regola *MAC sconosciuto* è mostrata nell'immagine seguente ed è configurata in questa sezione.

<input checked="" type="checkbox"/>	2nd AUTH	if Guest AND Network Access:UseCase EQUALS Guest Flow	then vlan24
<input checked="" type="checkbox"/>	MAC not known	if Network Access:AuthenticationStatus EQUALS UnknownUser	then CentralWebauth

Per creare la regola di autorizzazione, completare i seguenti passaggi:

1. Creare una nuova regola e immettere un nome. In questo esempio viene utilizzato un *indirizzo MAC sconosciuto*.
2. Fare clic sull'icona più (**+**) nel campo condizione e scegliere di creare una nuova condizione.
3. Espandere l'elenco a discesa **espressione**.
4. Scegliere **Accesso alla rete** ed espanderlo.
5. Fare clic su **AuthenticationStatus**, quindi scegliere l'operatore **Equals**.
6. Scegliere **UnknownUser** (Utente sconosciuto) nel campo di destra.
7. Nella pagina Autorizzazione generale, scegliere **CentralWebauth** ([Profilo di autorizzazione](#)) nel campo a destra della parola **quindi**. Questo passaggio consente all'ISE di continuare anche se l'utente (o l'MAC) non è noto. Agli utenti sconosciuti viene ora visualizzata la pagina Accesso. Tuttavia, una volta immesse le credenziali, vengono nuovamente presentate con una richiesta di autenticazione sull'ISE; pertanto, un'altra regola deve essere configurata con una condizione che viene soddisfatta se l'utente è un utente guest. In questo esempio, se

UseridentityGroup è uguale a *Guest* viene utilizzato e si presuppone che tutti gli utenti guest appartengano a questo gruppo.

8. Fare clic sul pulsante delle azioni situato alla fine della regola *MAC sconosciuto* e scegliere di inserire una nuova regola. **Nota:** è molto importante che questa nuova regola venga prima della regola *MAC sconosciuta*.
9. Immettere **2a AUTH** nel campo del nome.
10. Selezionare un gruppo di identità come condizione. In questo esempio viene scelto **Guest**.
11. Nel campo condizione, fare clic sul più (+) icona e scegliere di creare una nuova condizione.
12. Scegliere **Accesso alla rete**, quindi fare clic su **UseCase**.
13. Selezionate **Uguale a (Equals)** come operatore.
14. Scegliere **GuestFlow** come operando destro. Ciò significa che gli utenti che hanno appena eseguito l'accesso alla pagina Web verranno individuati e torneranno dopo una modifica di autorizzazione (la parte della regola relativa al flusso guest) e solo se appartengono al gruppo di identità guest.
15. Nella pagina di autorizzazione, fare clic sul pulsante più (+) accanto a *quindi* per scegliere un risultato per la regola.

nell'esempio, viene assegnato un profilo preconfigurato (vlan34); questa configurazione non viene mostrata in questo documento.

È possibile scegliere l'opzione **Permit Access** (Autorizza accesso) o creare un profilo personalizzato in modo che restituisca la VLAN o gli attributi desiderati.

Nota importante: in ISE versione 1.3, a seconda del tipo di autenticazione Web, è possibile che lo scenario "Guest Flow" non sia più disponibile. La regola di autorizzazione dovrà quindi contenere il gruppo di utenti guest come unica condizione possibile.

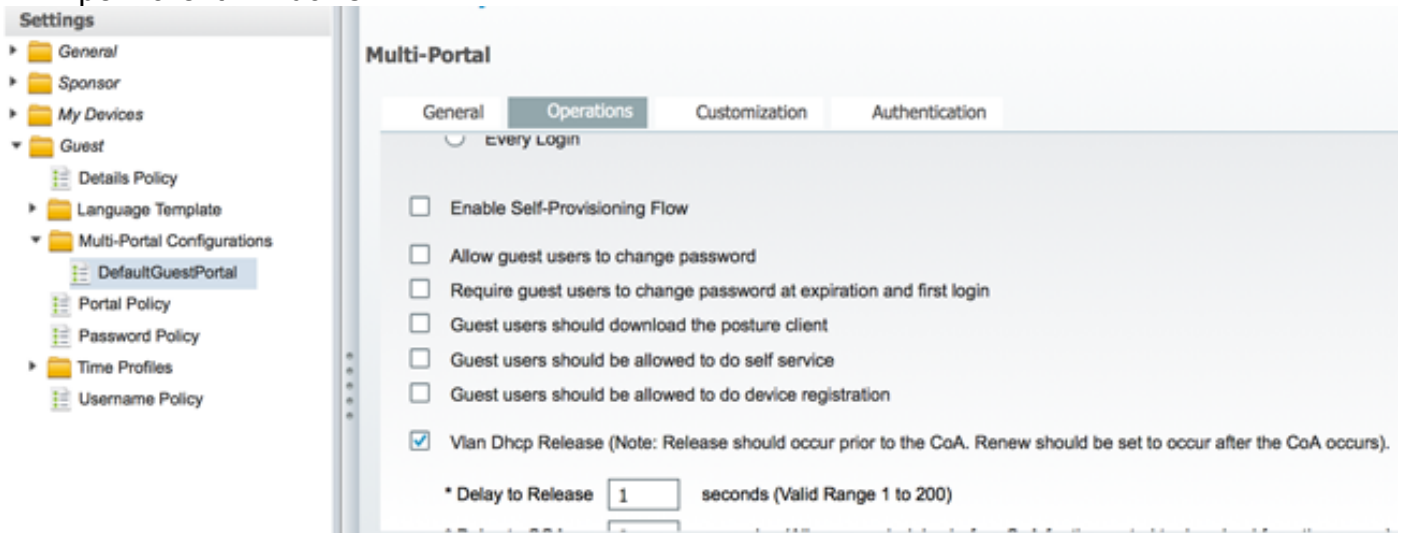
Abilita rinnovo IP (facoltativo)

Se si assegna una VLAN, il passaggio finale è che il PC client rinnovi il proprio indirizzo IP. Questo passaggio viene eseguito dal portale guest per i client Windows. Se in precedenza non è stata impostata una VLAN per la *seconda* regola di *AUTENTICAZIONE*, è possibile ignorare questo passaggio.

Notare che sugli access point FlexConnect, la VLAN deve preesistere sull'access point stesso. Pertanto, in caso contrario, è possibile creare un mapping VLAN-ACL sull'access point stesso o sul gruppo flessibile, in cui non viene applicato alcun ACL alla nuova VLAN che si desidera creare. In realtà, viene creata una VLAN (senza ACL).

Se è stata assegnata una VLAN, completare questi passaggi per abilitare il rinnovo dell'IP:

1. Fare clic su **Amministrazione** e quindi su **Gestione guest**.
2. Fare clic su **Impostazioni**.
3. Espandere **Guest**, quindi **Configurazione portale multiplo**.
4. Fare clic su **DefaultGuestPortal** o sul nome di un portale personalizzato eventualmente creato.
5. Selezionare la casella di controllo **Vlan DHCP Release**. **Nota:** questa opzione funziona solo per i client Windows.



Flusso del traffico

In questo scenario, può sembrare difficile capire dove viene inviato il traffico. Ecco una breve recensione:

- Il client invia una richiesta di associazione via etere per l'SSID.
- Il WLC gestisce l'autenticazione del filtro MAC con ISE (dove riceve gli attributi di reindirizzamento).
- Il client riceve una risposta assoc solo dopo il completamento del filtro MAC.
- Il client invia una richiesta DHCP, ovvero **LOCALMENTE** commutato dal punto di accesso per ottenere un indirizzo IP del sito remoto.
- Nello stato Central_webauth, il traffico contrassegnato per la negazione sull'ACL di reindirizzamento (in genere HTTP) è **CENTRALMENTE** commutato. Quindi non è l'AP a fare il reindirizzamento ma il WLC; ad esempio, quando il client chiede un sito web, l'AP lo invia al WLC incapsulato in CAPWAP e il WLC falsifica l'indirizzo IP del sito web e lo reindirizza verso ISE.
- Il client viene reindirizzato all'URL di reindirizzamento ISE. Questa è **LOCALMENTE** è stato riattivato (perché è stato attivato il comando allow sull'ACL di reindirizzamento flessibile).
- Una volta attivato lo stato RUN, il traffico viene commutato localmente.

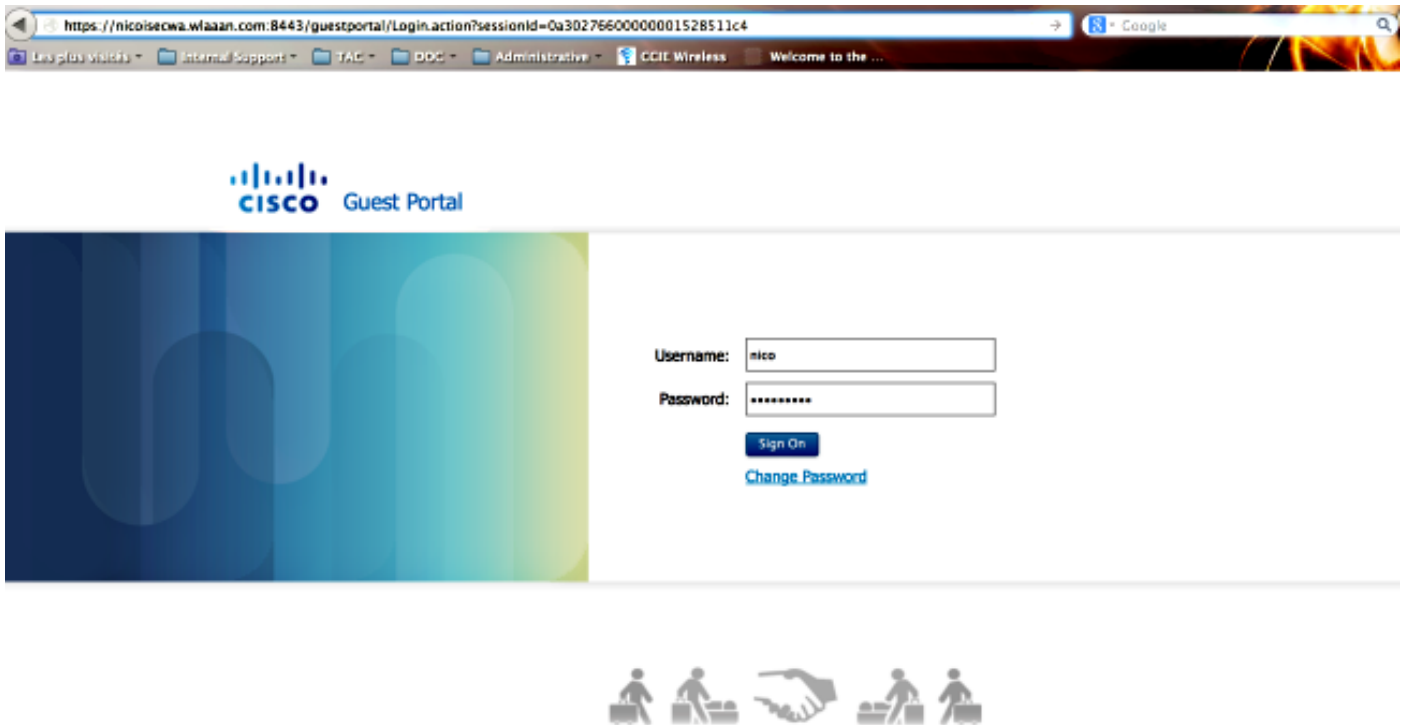
Verifica

Una volta che l'utente è associato al SSID, l'autorizzazione viene visualizzata nella pagina ISE.

Apr 09,13 11:49:27.179 AM	✓		Nico	00:13:10:21:70:13	nicowlc	vlan34	Guest	NotApplicable
Apr 09,13 11:49:27.174 AM	✓				nicowlc			Dynamic Author...
Apr 09,13 11:48:58.372 AM	✓		Nico	00:13:10:21:70:13			Guest	Guest Authentic..
Apr 09,13 11:47:19.475 AM	✓			00:13:10:21:70:13	00:13:10:21:70:13	nicowlc	CentralWebauth	Pending Authentication ...

Dal basso verso l'alto, è possibile vedere l'autenticazione di filtro degli indirizzi MAC che restituisce gli attributi CWA. Di seguito è riportato il login al portale con il nome utente. L'ISE invia un CoA al WLC e l'ultima autenticazione è un'autenticazione del filtro MAC di layer 2 sul lato WLC, ma ISE ricorda il client e il nome utente e applica la VLAN necessaria configurata in questo esempio.

Quando si apre un indirizzo sul client, il browser viene reindirizzato all'ISE. Verificare che il DNS (Domain Name System) sia configurato correttamente.



L'accesso alla rete viene concesso dopo che l'utente ha accettato i criteri.



Signed on successfully
You can now type in the original URL in the browser's address bar.

You can now type in the original URL in the browser's address bar.



Sul controller, lo stato di Policy Manager e lo stato di RADIUS NAC cambiano da *POSTURE_REQD* a *RUN*.

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).