Configurazione dell'autenticazione Web esterna con Converged Access (5760/3650/3850)

Sommario

Introduzione

In questo documento viene descritto come configurare l'autenticazione Web esterna con i controller di accesso convergente. In questo esempio, la pagina del portale guest e l'autenticazione delle credenziali sono entrambe disponibili su Identity Services Engine (ISE).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

1. Cisco converged access controller.

2. Autenticazione Web

3. Cisco ISE

Componenti usati

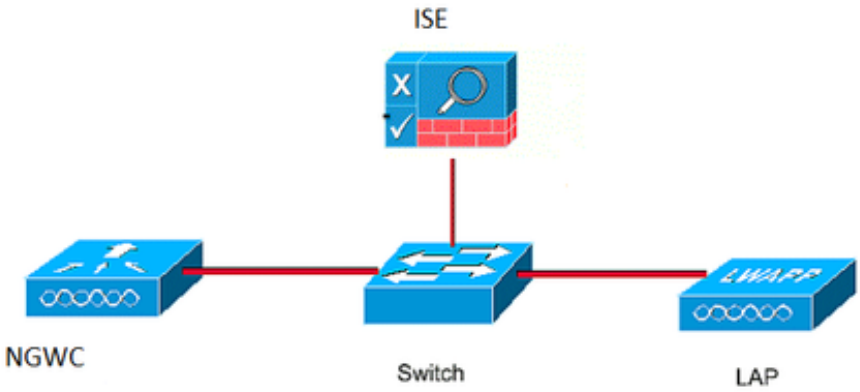
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

1. Controller Cisco 5760 (NGWC nel diagramma seguente), 03.06.05E

2. ISE 2.2

Configurazione

Esempio di rete



Configurazione CLI

Configurazione Radius sul controller

passaggio 1: Definisci server RADIUS esterno

```
radius server ISE.161
address ipv4 10.48.39.161 auth-port 1812 acct-port 1813
timeout 10
retransmit 5
key Cisco123
```

passaggio 2:. Definire il gruppo di raggi AAA e specificare il server radius da utilizzare

```
aaa group server radius ISE-Group
server name ISE.161
deadtime 10
```

passaggio 3. Definire l'elenco dei metodi che punta al gruppo del raggio e mapparlo sotto la WLAN.

```
aaa authentication login webauth group ISE-Group
```

Configurazione mappa parametri

passaggio 4. Configurare la mappa dei parametri globali con l'indirizzo ip virtuale richiesto per webauth esterno e interno. Il pulsante Disconnetti utilizza IP virtuale. È sempre buona norma configurare un IP virtuale non instradabile.

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 1.1.1.1
```

passaggio 5: Consente di configurare una mappa di parametri denominata. Funzionerà come un tipo di metodo webauth. Questa condizione viene chiamata nella configurazione WLAN.

```
parameter-map type webauth web
type webauth
redirect for-login https://10.48.39.161:8443/portal/PortalSetup.action?portal=0c712cd0-6d90-
11e5-978e-005056bf2f0a
redirect portal ipv4 10.48.39.161
```

ACL di preautenticazione. Questa condizione viene chiamata anche nella WLAN.

passaggio 6: Configurare Preauth_ACL che consente l'accesso ad ISE, DHCP e DNS prima del termine dell'autenticazione

```
ip access-list extended Preauth_ACL
permit ip any host 10.48.39.161
permit ip host 10.48.39.161 any
permit udp any eq bootps any
permit udp any any eq bootpc
permit udp any eq bootpc any
permit udp any eq domain any
permit udp any any eq domain
```

Configurazione WLAN

passaggio 7: configurazione della WLAN

```
wlan ext-webauth 7 ext-webauth
client vlan vlan232
ip access-group web Preauth_ACL
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list webauth
security web-auth parameter-map web
session-timeout 1800
no shutdown
```

passaggio 8: Attivare il server HTTP.

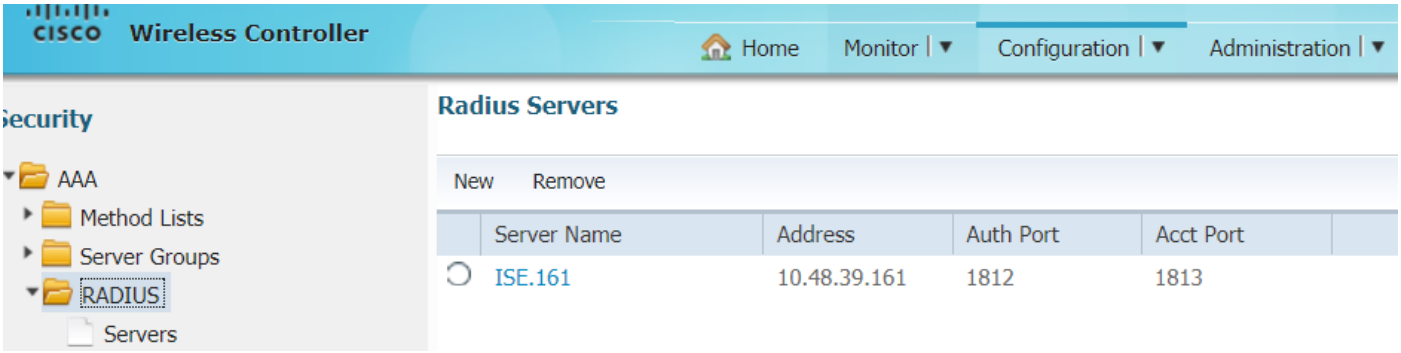
```
ip http server

ip http secure-server (for secure web-auth, use 'no' to disable secure web)
```

Configurazione GUI

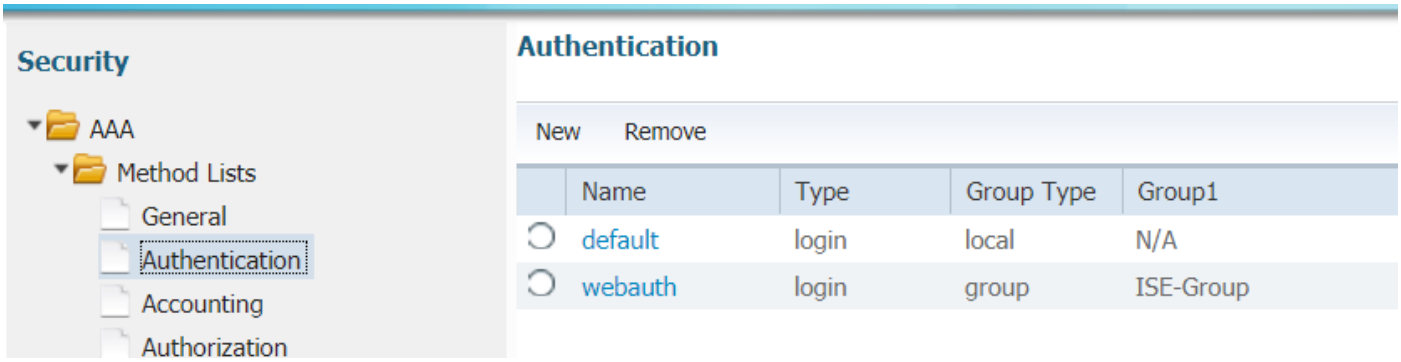
Stiamo seguendo la stessa procedura descritta sopra. Gli screenshot sono forniti solo come riferimento incrociato.

passaggio 1: Definire un server RADIUS esterno



passaggio 2:. Definire il gruppo di raggi AAA e specificare il server radius da utilizzare

passaggio 3. Definire l'elenco dei metodi che punta al gruppo del raggio e mapparlo sotto la WLAN.



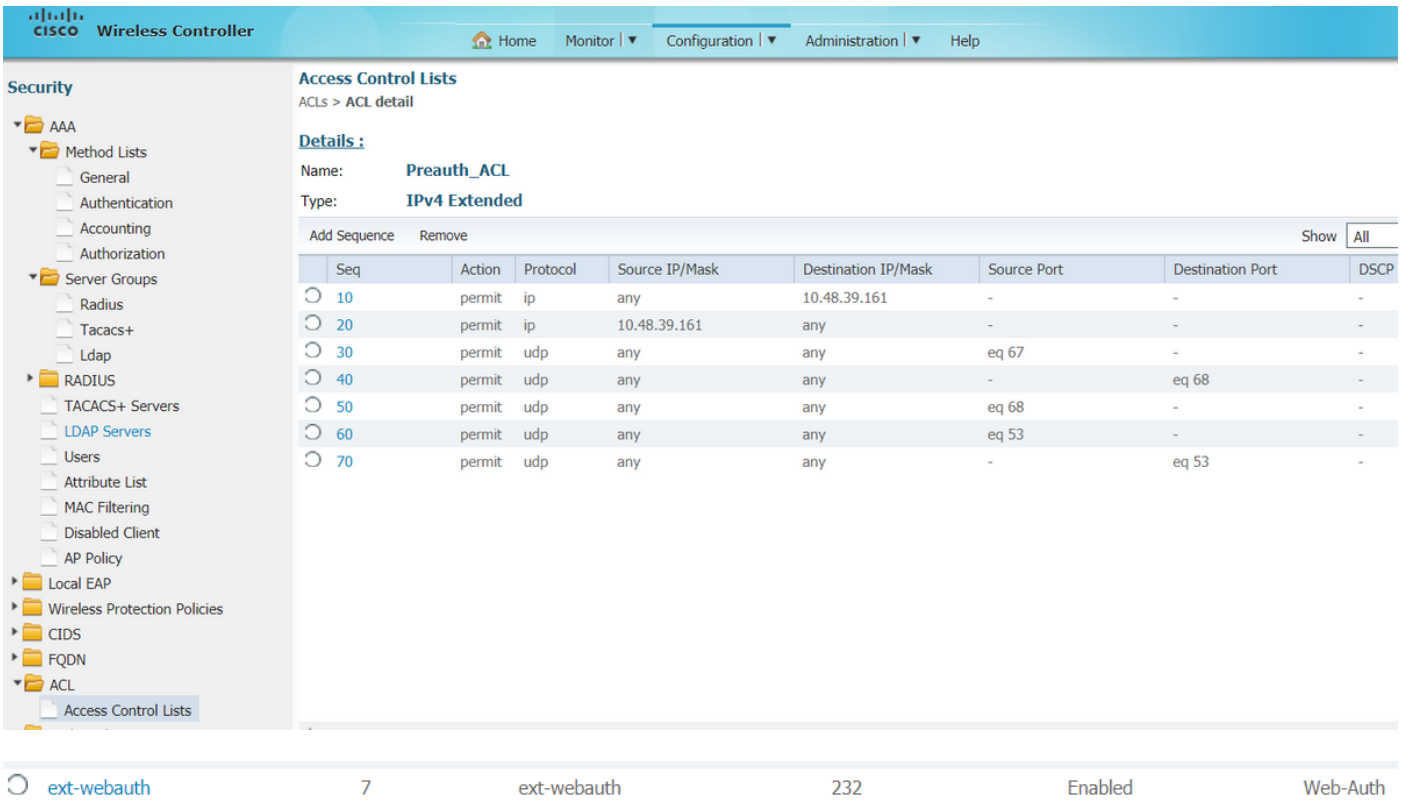
Configurazione mappa parametri

passaggio 4. Configurare la mappa dei parametri globali con l'indirizzo ip virtuale richiesto per webauth esterno e interno. Il pulsante Disconnetti utilizza IP virtuale. È sempre buona norma configurare un IP virtuale non instradabile.

passaggio 5: Consente di configurare una mappa di parametri denominata. Funzionerà come un tipo di metodo webauth. Questa condizione viene chiamata nella configurazione WLAN.

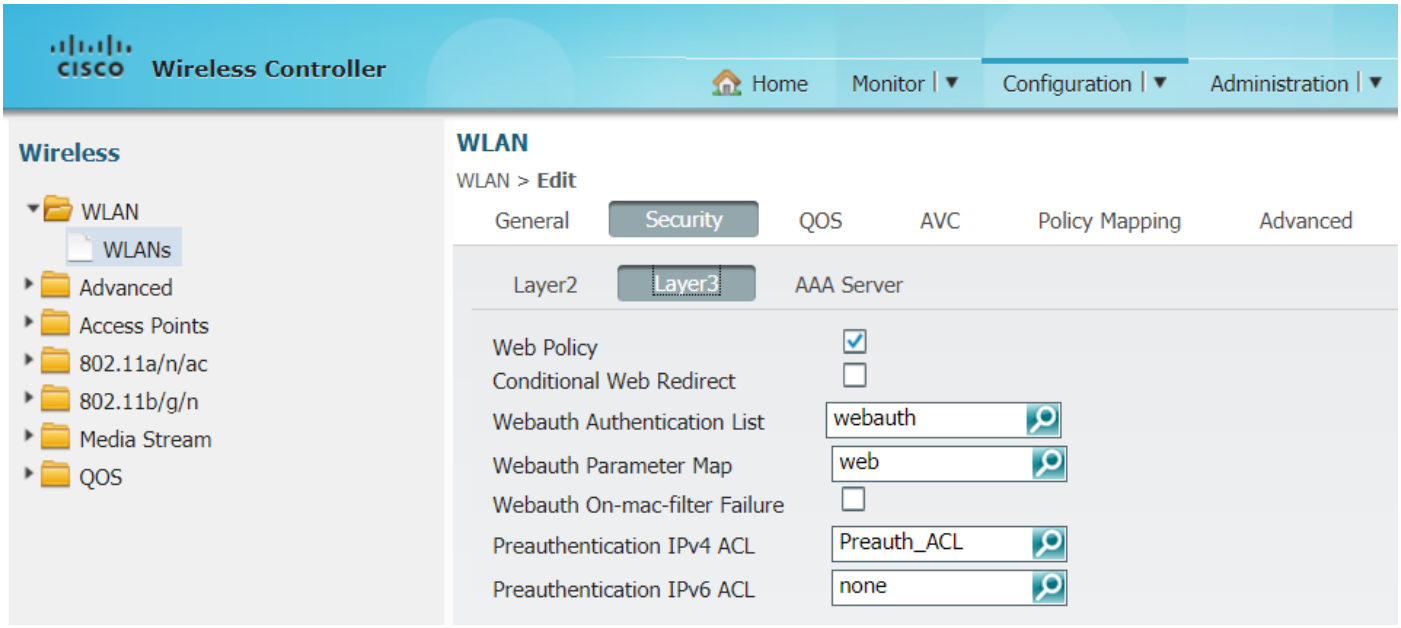
ACL di preautenticazione. Questa condizione viene chiamata anche nella WLAN.

passaggio 6: Configurare Preauth_ACL che consente l'accesso ad ISE, DHCP e DNS prima del termine dell'autenticazione



Configurazione WLAN

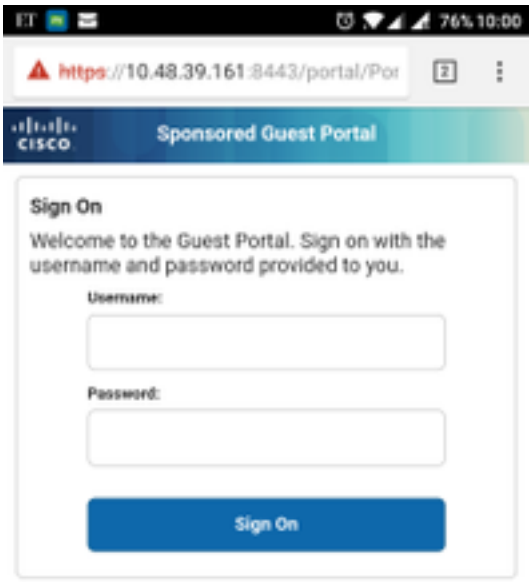
passaggio 7: configurazione della WLAN



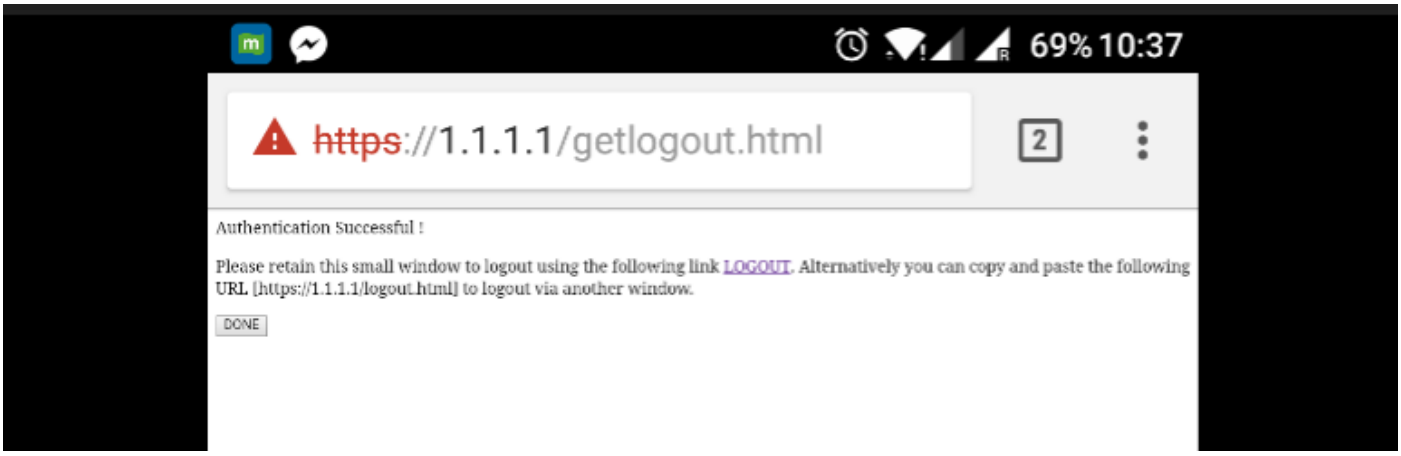
Verifica

Connettere un client e assicurarsi che, se si apre un browser, il client venga reindirizzato alla pagina del portale di accesso. Nello screenshot seguente viene illustrata la pagina del portale per

gli ospiti ISE.



Dopo l'invio delle credenziali corrette, verrà visualizzata la pagina della riuscita:



Il server ISE effettuerà due autenticazioni: una sulla pagina guest stessa (la riga inferiore con solo il nome utente) e una seconda autenticazione quando il WLC fornisce lo stesso nome utente/password tramite l'autenticazione radius (solo questa autenticazione farà passare il client alla fase di riuscita). Se non si verifica l'autenticazione radius (con indirizzo MAC e dettagli WLC come NAS), è necessario verificare la configurazione radius.