Configurazione di Servizi di dominio wireless

Sommario

Introduzione

In questo documento viene introdotto il concetto di Servizi di dominio wireless (WDS). Nel documento viene descritto anche come configurare un access point (AP) o il Wireless LAN Services Module (WLSM) come WDS e almeno un altro come punto di accesso all'infrastruttura. La procedura illustrata in questo documento consente di configurare un servizio di distribuzione Windows funzionante e di associarlo al punto di accesso di Servizi di distribuzione Windows o a un punto di accesso dell'infrastruttura. Questo documento intende stabilire le basi da cui è possibile configurare Fast Secure Roaming o introdurre un Wireless LAN Solutions Engine (WLSE) nella rete, in modo da poter utilizzare le funzionalità.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Conoscere a fondo le reti LAN wireless e i problemi di sicurezza wireless.
- Conoscere i metodi di protezione EAP (Extensible Authentication Protocol) correnti.

Componenti usati

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

- AP con software Cisco IOS®
- Software Cisco IOS release 12.3(2)JA2 o successive
- Catalyst serie 6500 Wireless LAN Services Module

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 e l'indirizzo IP è impostato sull'interfaccia BVI1, in modo che l'unità sia accessibile dalla GUI del software Cisco IOS o dall'interfaccia della riga di comando (CLI). Se si lavora su una rete live, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Servizi di dominio wireless

WDS è una nuova funzionalità per gli access point nel software Cisco IOS e la base del WLSM Catalyst serie 6500. WDS è una funzione di base che abilita altre funzionalità come le seguenti:

- Roaming sicuro e rapido
- Interazione WLSE
- Gestione della radio

Ènecessario stabilire relazioni tra i punti di accesso che partecipano a Servizi di distribuzione Windows e il modulo WLSM prima che funzionino altre funzionalità basate su Servizi di distribuzione Windows. Uno degli scopi di Servizi di distribuzione Windows è eliminare la necessità che il server di autenticazione convalidi le credenziali utente e ridurre il tempo necessario per le autenticazioni client.

Per utilizzare Servizi di distribuzione Windows, è necessario designare un punto di accesso o il modulo WLSM come Servizi di distribuzione Windows. Un punto di accesso Servizi di distribuzione Windows deve utilizzare un nome utente e una password di Servizi di distribuzione Windows per stabilire una relazione con un server di autenticazione. Il server di autenticazione può essere un server RADIUS esterno o la funzionalità Server RADIUS locale nel punto di accesso di Servizi di distribuzione Windows. Il modulo WLSM deve avere una relazione con il server di autenticazione, anche se non è necessario eseguire l'autenticazione nel server.

Altri access point, detti access point di infrastruttura, comunicano con il servizio WDS. Prima della registrazione, i punti di accesso dell'infrastruttura devono autenticarsi nel servizio WDS. Un gruppo di server di infrastruttura in Servizi di distribuzione Windows definisce questa autenticazione dell'infrastruttura.

Uno o più gruppi di server client in Servizi di distribuzione Windows definiscono l'autenticazione client.

Quando un client tenta di associarsi a un punto di accesso dell'infrastruttura, quest'ultimo passa le credenziali dell'utente al servizio di distribuzione Windows per la convalida. Se WDS vede le credenziali per la prima volta, passa al server di autenticazione per convalidarle. WDS memorizza quindi le credenziali nella cache per evitare di dover tornare al server di autenticazione quando lo stesso utente tenta di eseguire nuovamente l'autenticazione. Di seguito sono riportati alcuni esempi di riautenticazione:

- Ridefinizione chiavi
- Roaming
- All'avvio del dispositivo client

Èpossibile eseguire il tunneling di qualsiasi protocollo di autenticazione EAP basato su RADIUS tramite Servizi di distribuzione Windows, ad esempio:

- LEAP (Lightweight EAP)
- PEAP (Protected EAP)
- EAP-Transport Layer Security (EAP-TLS)
- Autenticazione flessibile EAP tramite tunneling protetto (EAP-FAST)

L'autenticazione dell'indirizzo MAC può inoltre eseguire il tunnel a un server di autenticazione esterno o a un elenco locale a un punto di accesso Servizi di distribuzione Windows. WLSM non supporta l'autenticazione dell'indirizzo MAC.

WDS e i punti di accesso dell'infrastruttura comunicano tramite un protocollo multicast denominato WLAN Context Control Protocol (WLCCP). Questi messaggi multicast non possono essere instradati, quindi un servizio WDS e i punti di accesso dell'infrastruttura associati devono trovarsi nella stessa subnet IP e sullo stesso segmento LAN. Tra WDS e WLSE, WLCCP utilizza TCP e UDP (User Datagram Protocol) sulla porta 2887. Quando WDS e WLSE si trovano su subnet diverse, un protocollo come NAT (Network Address Translation) non è in grado di tradurre i pacchetti.

Un access point configurato come dispositivo WDS supporta fino a 60 access point partecipanti. Un ISR (Integrated Services Router) configurato come dispositivo WDS supporta fino a 100 access point partecipanti. Inoltre, uno switch dotato di WLSM supporta fino a 600 punti di accesso partecipanti e fino a 240 gruppi di mobilità. Un singolo access point supporta fino a 16 gruppi di mobilità.

Nota: Cisco consiglia che i punti di accesso all'infrastruttura eseguano la stessa versione di IOS del dispositivo WDS. Se si utilizza una versione precedente di IOS, è possibile che gli access point non riescano ad autenticarsi nel dispositivo WDS. Cisco consiglia inoltre di utilizzare la versione più recente del sistema operativo IOS. L'ultima versione di IOS è disponibile nella pagina Download wireless.

Ruolo del dispositivo WDS

Il dispositivo WDS esegue diverse attività sulla LAN wireless:

- Pubblicizza le funzionalità WDS e partecipa alla scelta del dispositivo WDS più adatto per la rete LAN wireless. Quando si configura la LAN wireless per Servizi di distribuzione Windows, si imposta un dispositivo come candidato principale per Servizi di distribuzione Windows e uno o più dispositivi aggiuntivi come candidati per Servizi di distribuzione Windows di backup. Se il dispositivo WDS principale non è in linea, viene sostituito da uno dei dispositivi WDS di

backup.
- Autentica tutti gli access point nella subnet e stabilisce un canale di comunicazione sicuro con ciascuno di essi.
- Raccoglie i dati radio dai punti di accesso della subnet, li aggrega e li inoltra al dispositivo WLSE della rete.
- Funge da pass-through per tutti i dispositivi client autenticati 802.1x associati agli access point partecipanti.
- Registra tutti i dispositivi client nella subnet che utilizzano chiavi dinamiche, stabilisce le chiavi di sessione per tali dispositivi e memorizza nella cache le relative credenziali di protezione. Quando un client esegue il roaming in un altro punto di accesso, il dispositivo WDS inoltra le credenziali di sicurezza del client al nuovo punto di accesso.

Ruolo dei punti di accesso tramite il dispositivo WDS

Gli access point sulla LAN wireless interagiscono con il dispositivo WDS nelle seguenti attività:

- Rilevare e tenere traccia del dispositivo WDS corrente e inoltrare gli annunci WDS alla LAN wireless.
- Eseguire l'autenticazione con il dispositivo Servizi di distribuzione Windows e stabilire un canale di comunicazione sicuro con il dispositivo Servizi di distribuzione Windows.
- Registrare i dispositivi client associati con il dispositivo WDS.
- Segnalare i dati radio al dispositivo WDS.

Configurazione

WDS presenta la configurazione in modo ordinato e modulare. Ogni concetto si basa su quello che lo precede. WDS omette altri elementi di configurazione quali password, accesso remoto e impostazioni radio per garantire chiarezza e attenzione al soggetto principale.

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

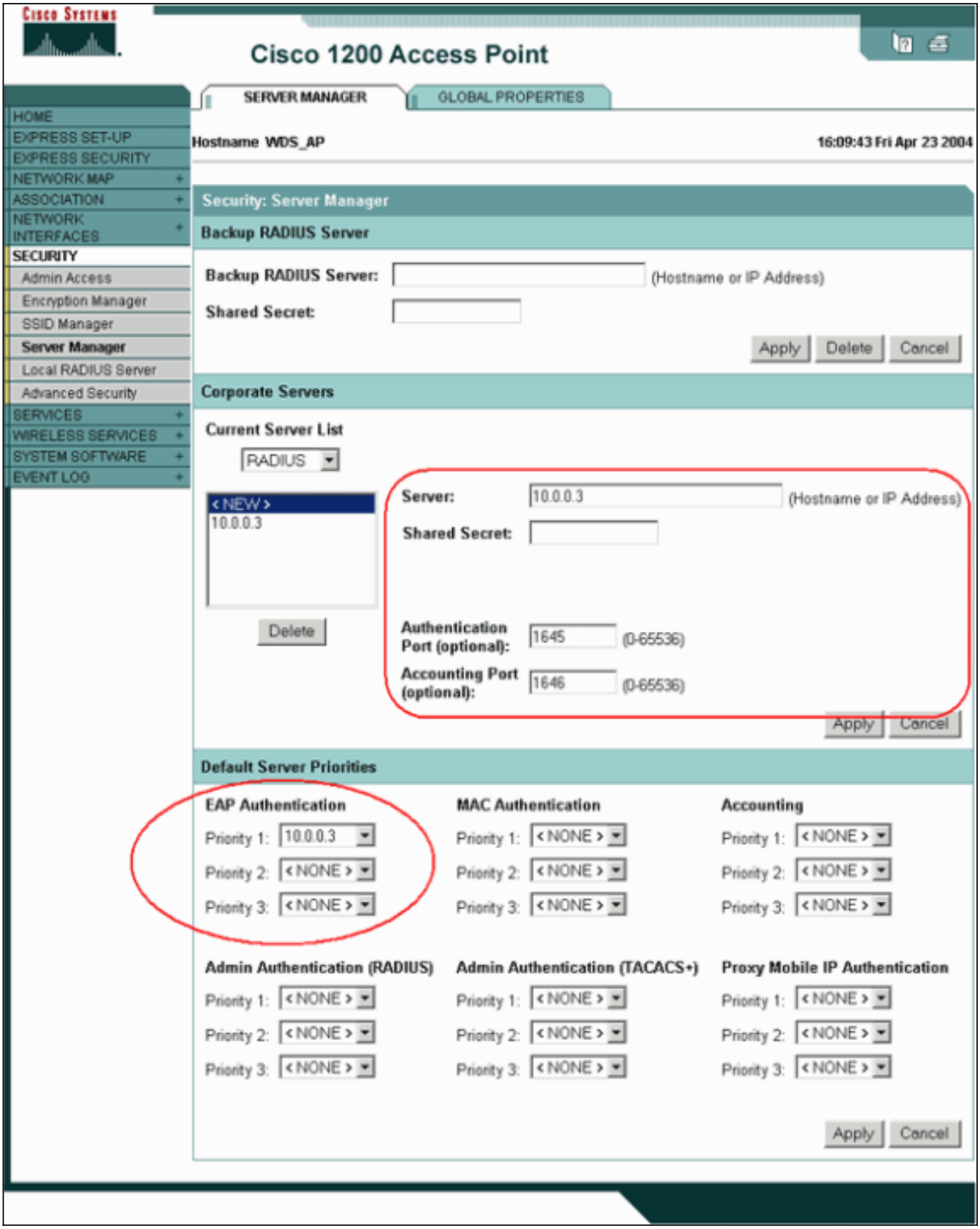
Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Designare un punto di accesso come WDS

Il primo passo consiste nel designare un punto di accesso come WDS. WDS AP è l'unico punto di accesso che comunica con il server di autenticazione.

Completare questi passaggi per designare un access point come WDS:

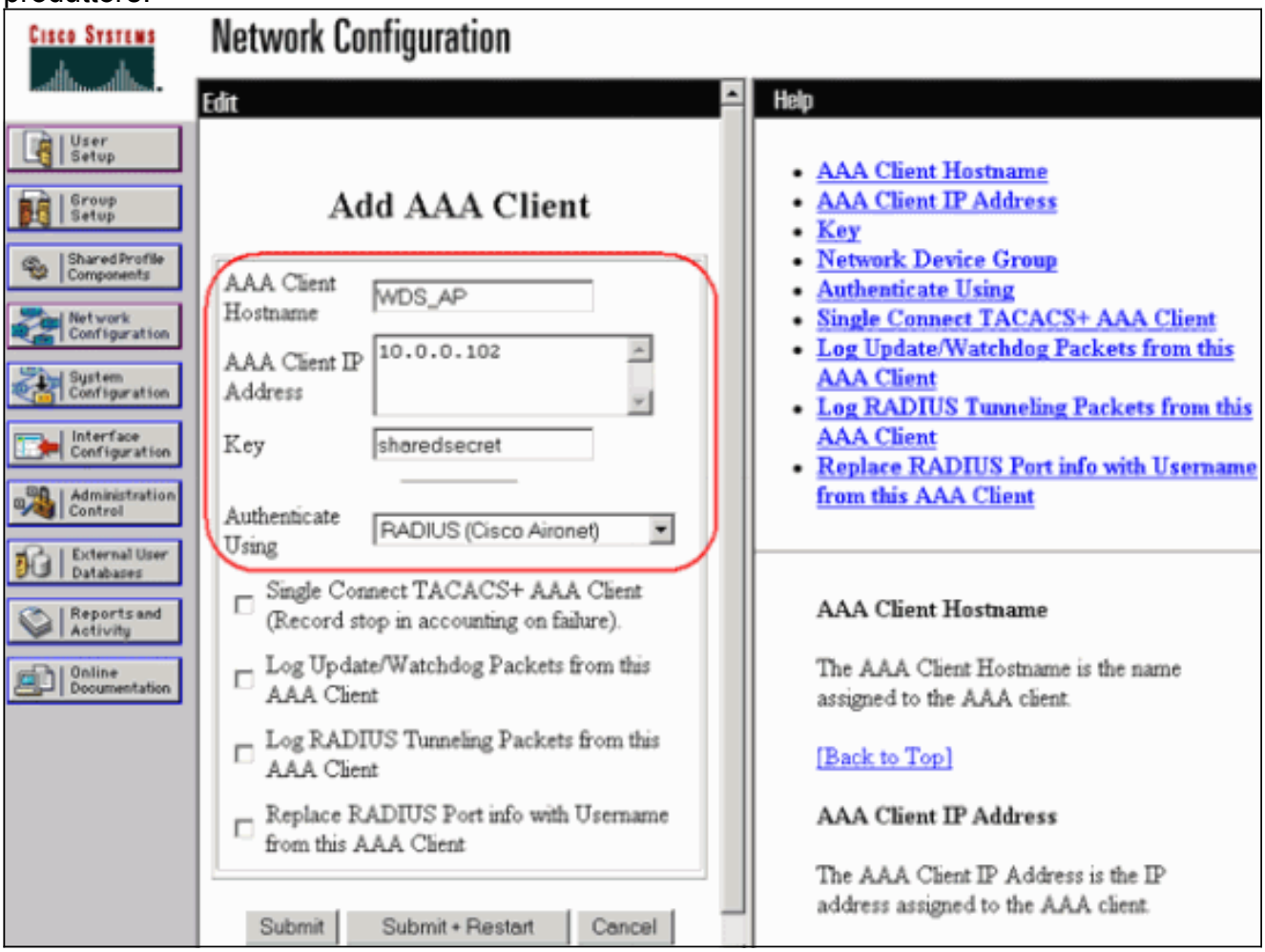
1. Per configurare il server di autenticazione in WDS AP, scegliere **Sicurezza > Server Manager** per andare alla scheda Server Manager:In Server aziendali digitare l'indirizzo IP del server di autenticazione nel campo Server.Specificare il segreto condiviso e le porte.In Priorità predefinite server impostare il campo Priorità 1 sull'indirizzo IP del server nel tipo di autenticazione
appropriato.



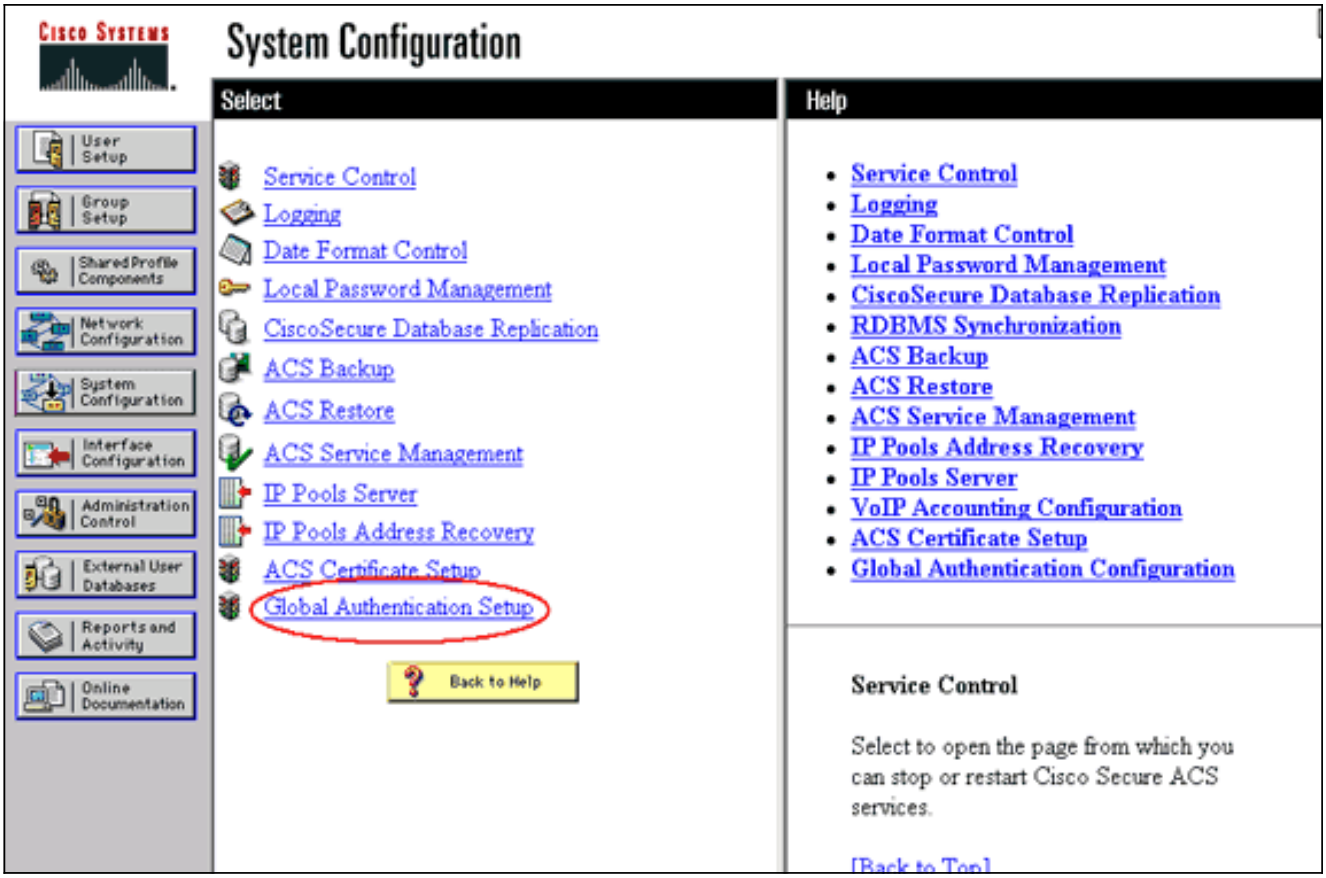
In alternativa, usare questi comandi dalla CLI:

2. Il passaggio successivo consiste nel configurare il punto di accesso Servizi di distribuzione Windows nel server di autenticazione come client di autenticazione, autorizzazione e accounting (AAA). Per questo motivo, è necessario aggiungere il WDS AP come client AAA. Attenersi alla seguente procedura:**Nota:** in questo documento viene usato il server Cisco Secure ACS come server di autenticazione.In Cisco Secure Access Control Server (ACS), questo si verifica nella pagina Configurazione di rete in cui è possibile definire i seguenti attributi per il punto di accesso di Servizi di distribuzione Windows:NomeIndirizzo IPSegreto condivisoMetodo di autenticazioneRADIUS Cisco AironetTask force ingegneria Internet

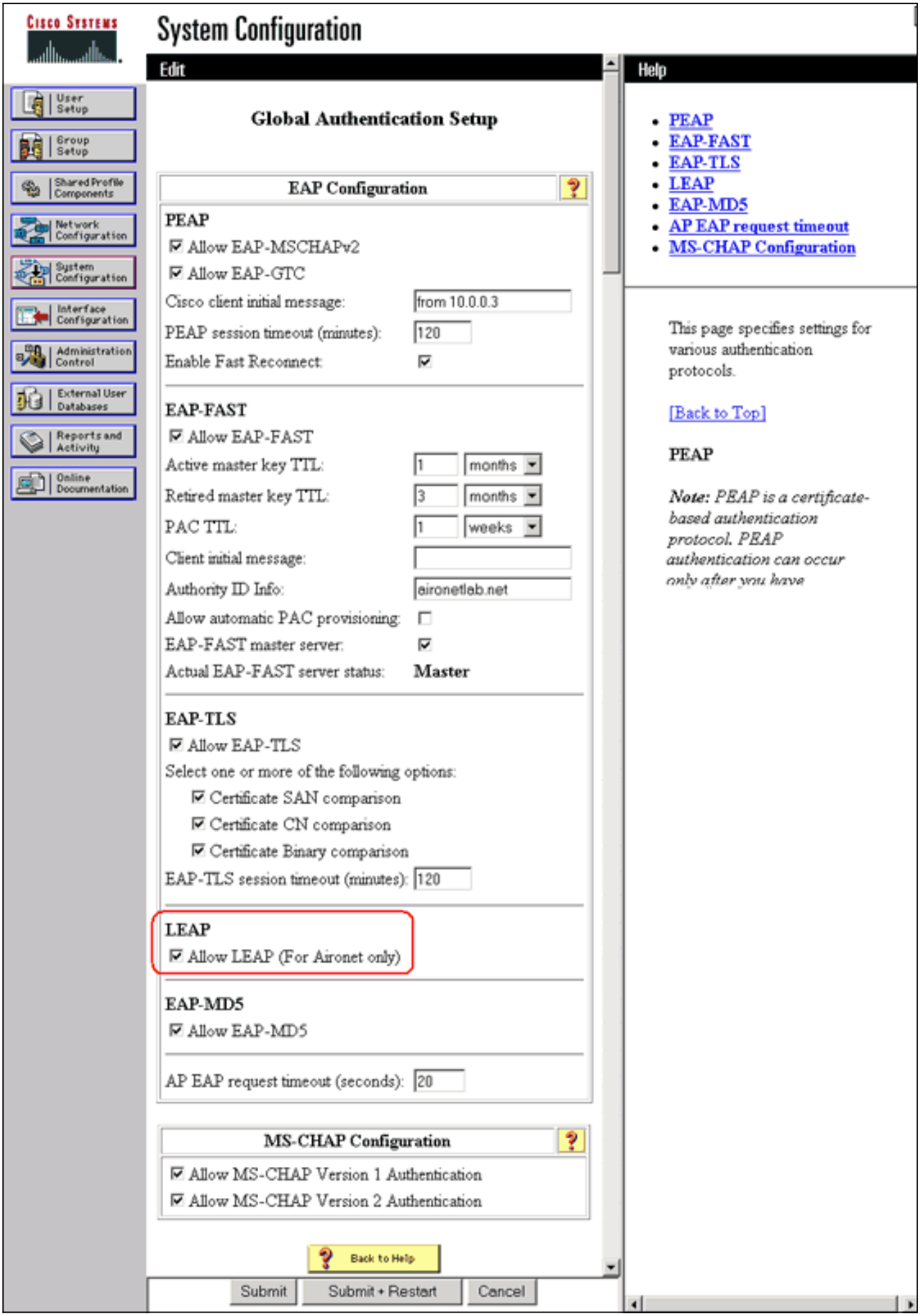
RADIUS [IETF]Fare clic su **Submit (Invia)**.Per altri server di autenticazione non ACS, consultare la documentazione del produttore.



Inoltre, in Cisco Secure ACS, accertarsi di configurare ACS in modo da eseguire l'autenticazione LEAP nella pagina Configurazione di sistema - Impostazione autenticazione globale. Fare clic su **Configurazione di sistema**, quindi su **Configurazione autenticazione globale**.

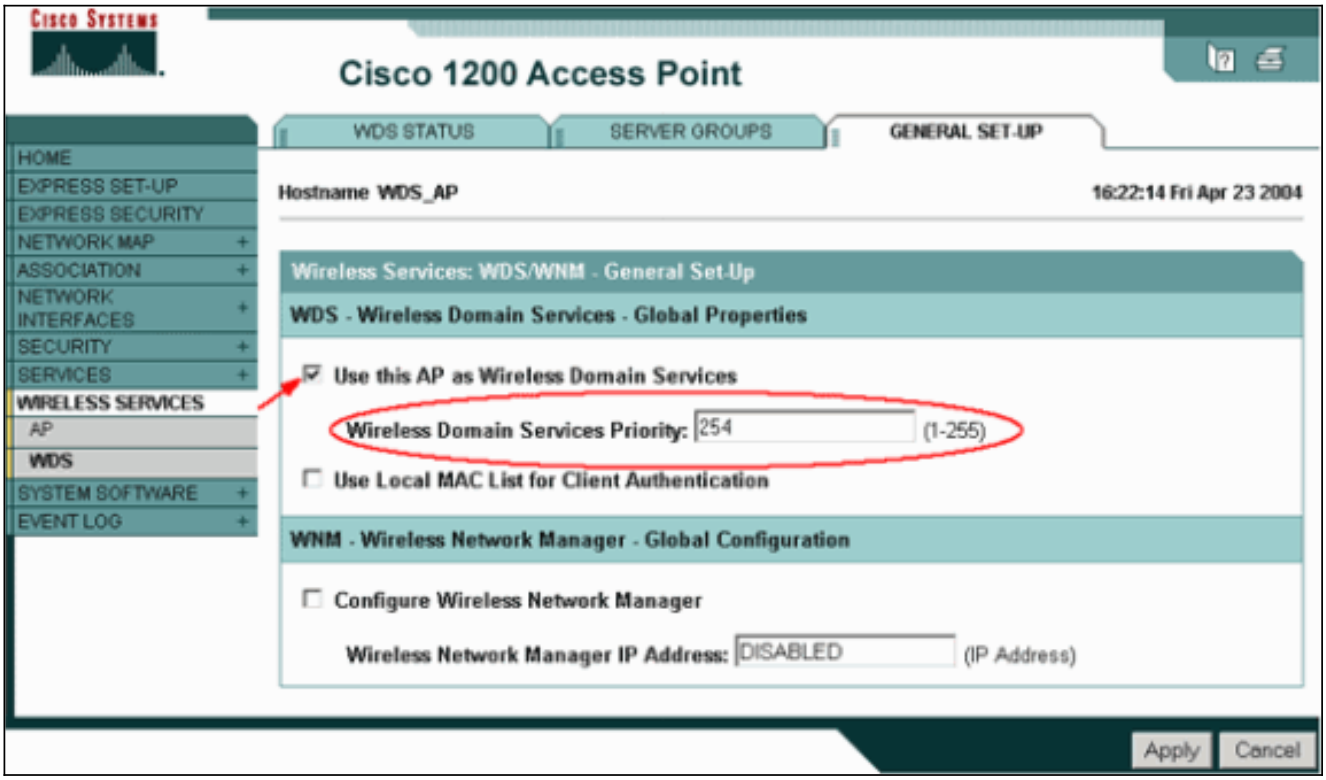


Scorrere la pagina fino a visualizzare l'impostazione LEAP. Quando si seleziona la casella, ACS autentica
LEAP.



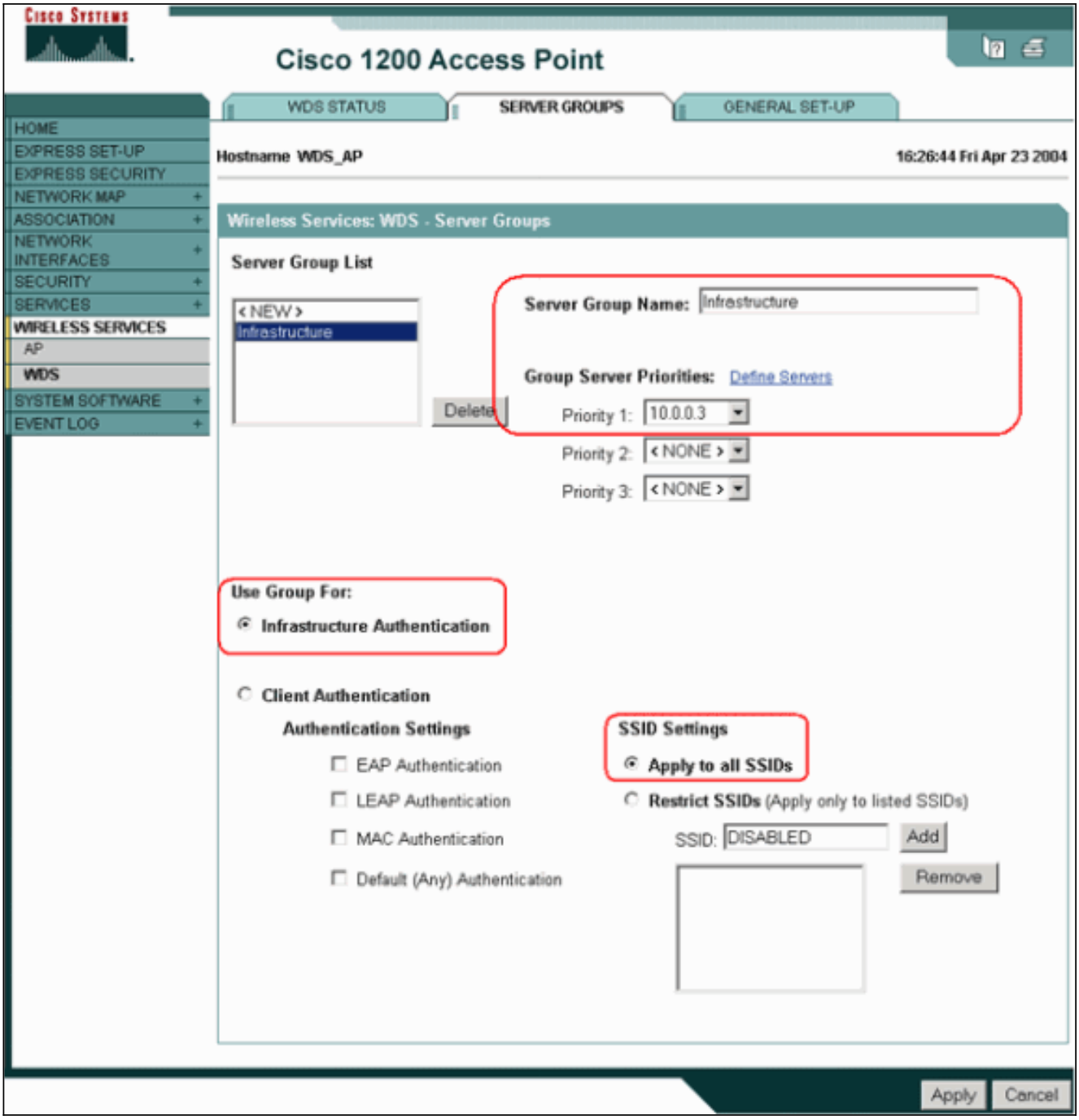
3. Per configurare le impostazioni di Servizi di distribuzione Windows nell'access point Servizi di distribuzione Windows, scegliere **Servizi wireless > Servizi di distribuzione Windows** nell'access point Servizi di distribuzione Windows e fare clic sulla scheda **Configurazione**

generale. Attenersi alla procedura seguente:In Servizi di dominio wireless WDS - Proprietà globali selezionare **Utilizza questo punto di accesso come servizi di dominio wireless**.Impostare il valore del campo Priorità servizi di dominio wireless su circa **254**, perché è il primo. È possibile configurare uno o più access point o switch come candidati per la fornitura di Servizi di distribuzione Windows. Il dispositivo con la priorità più alta fornisce WDS.



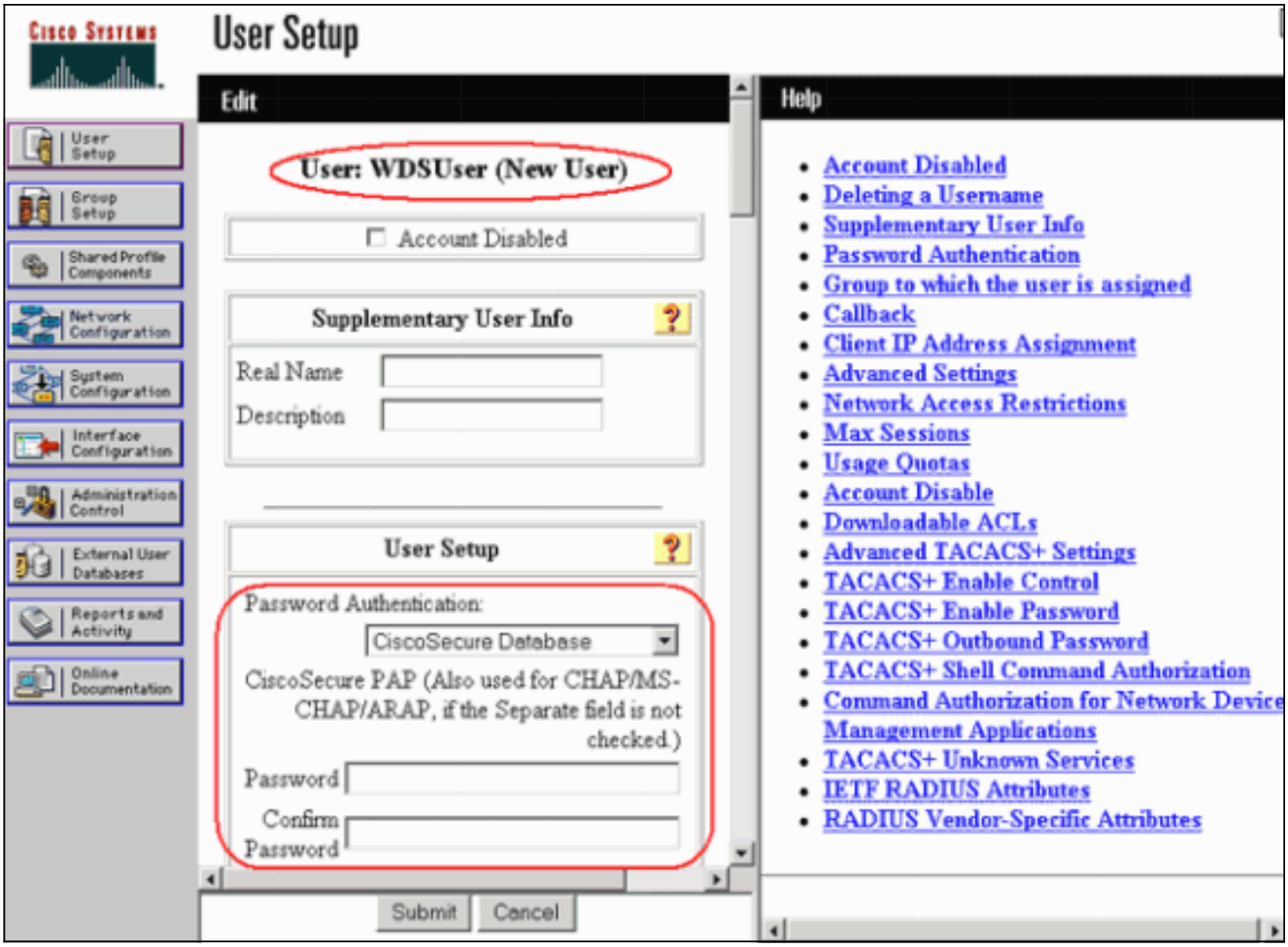
In alternativa, usare questi comandi dalla CLI:

4. Scegliere **Servizi wireless > Servizi di distribuzione Windows** e passare alla scheda **Gruppi di server**:Definire un nome per il gruppo di server che autentichi gli altri access point, ossia un gruppo Infrastructure.Impostare Priorità 1 sul server di autenticazione configurato in precedenza.Fare clic su **Usa gruppo per:** Pulsante di opzione **Autenticazione infrastruttura**.Applicare le impostazioni agli identificatori dei set di servizi (SSID) rilevanti.



In alternativa, usare questi comandi dalla CLI:

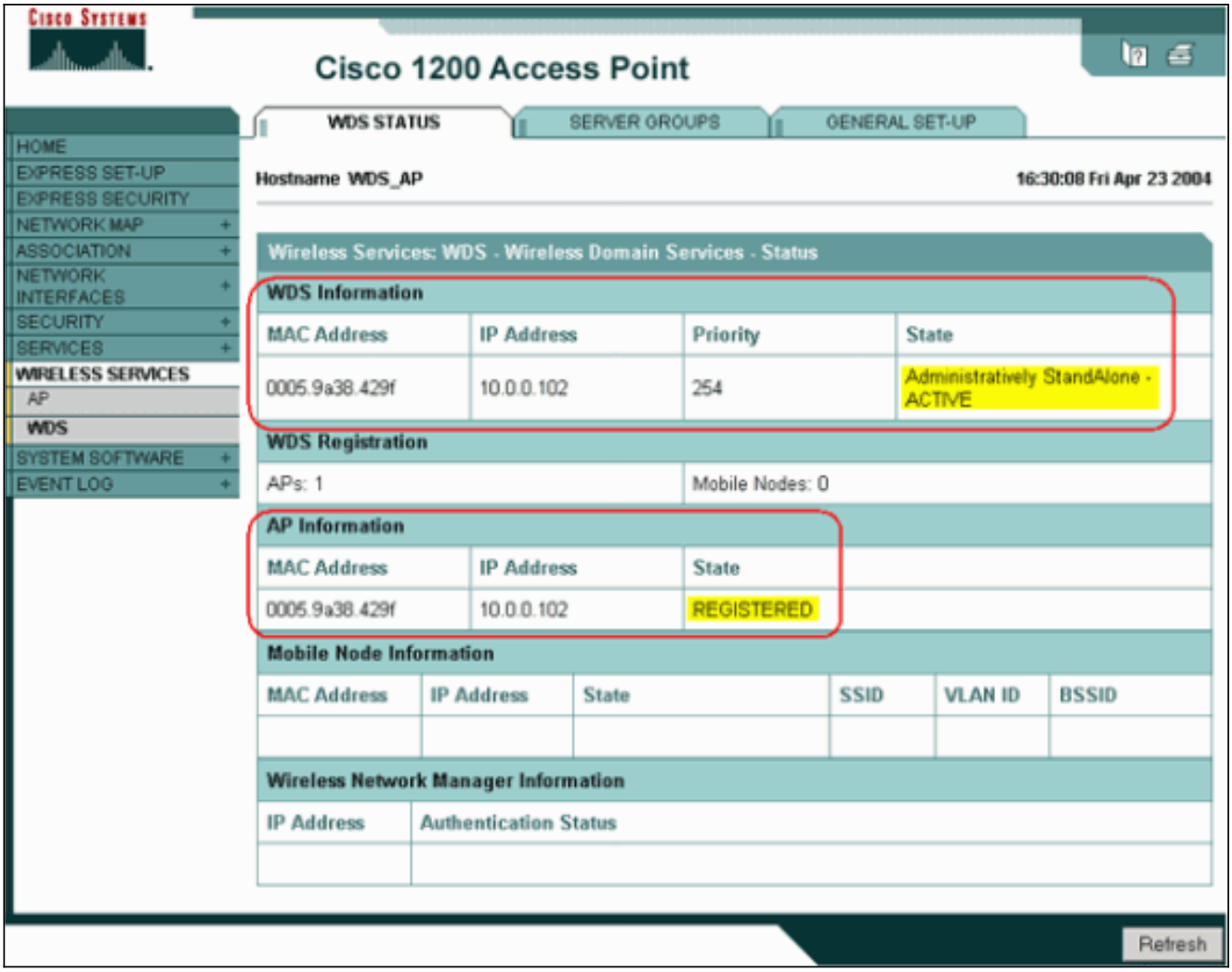
5. Configurare il nome utente e la password di Servizi di distribuzione Windows come utente nel server di autenticazione.In Cisco Secure ACS, questo si verifica nella pagina Configurazione utente, in cui è possibile definire il nome utente e la password di Servizi di distribuzione Windows. Per altri server di autenticazione non ACS, consultare la documentazione del produttore.**Nota:** non inserire l'utente di Servizi di distribuzione Windows in un gruppo a cui sono assegnati molti diritti e privilegi. Per Servizi di distribuzione Windows è necessaria solo l'autenticazione
limitata.



6. Scegliere **Servizi wireless > AP**, quindi fare clic su **Attiva** per l'opzione Partecipa all'infrastruttura SWAN. Digitare quindi il nome utente e la password di Servizi di distribuzione Windows.Ènecessario definire un nome utente e una password di Servizi di distribuzione Windows nel server di autenticazione per tutti i dispositivi designati come membri di Servizi di distribuzione
Windows.

In alternativa, usare questi comandi dalla CLI:

7. Scegliere **Servizi wireless > Servizi di distribuzione Windows**. Nella scheda Stato WDS AP di WDS verificare se l'access point di WDS viene visualizzato nell'area Informazioni di WDS, in Stato ATTIVO. L'access point deve essere visualizzato anche nell'area Informazioni access point con lo stato REGISTERED.Se l'access point non viene visualizzato come REGISTRATO o ATTIVO, controllare se nel server di autenticazione sono presenti errori o tentativi di autenticazione non riusciti.Quando il punto di accesso si registra in modo appropriato, aggiungere un punto di accesso all'infrastruttura per utilizzare i servizi del WDS.



In alternativa, usare questi comandi dalla CLI:**Nota:** non è possibile testare le associazioni client perché per l'autenticazione client non sono ancora disponibili i provisioning.

Designare un WLSM come WDS

In questa sezione viene illustrato come configurare un WLSM come WDS. WDS è l'unico dispositivo che comunica con il server di autenticazione.

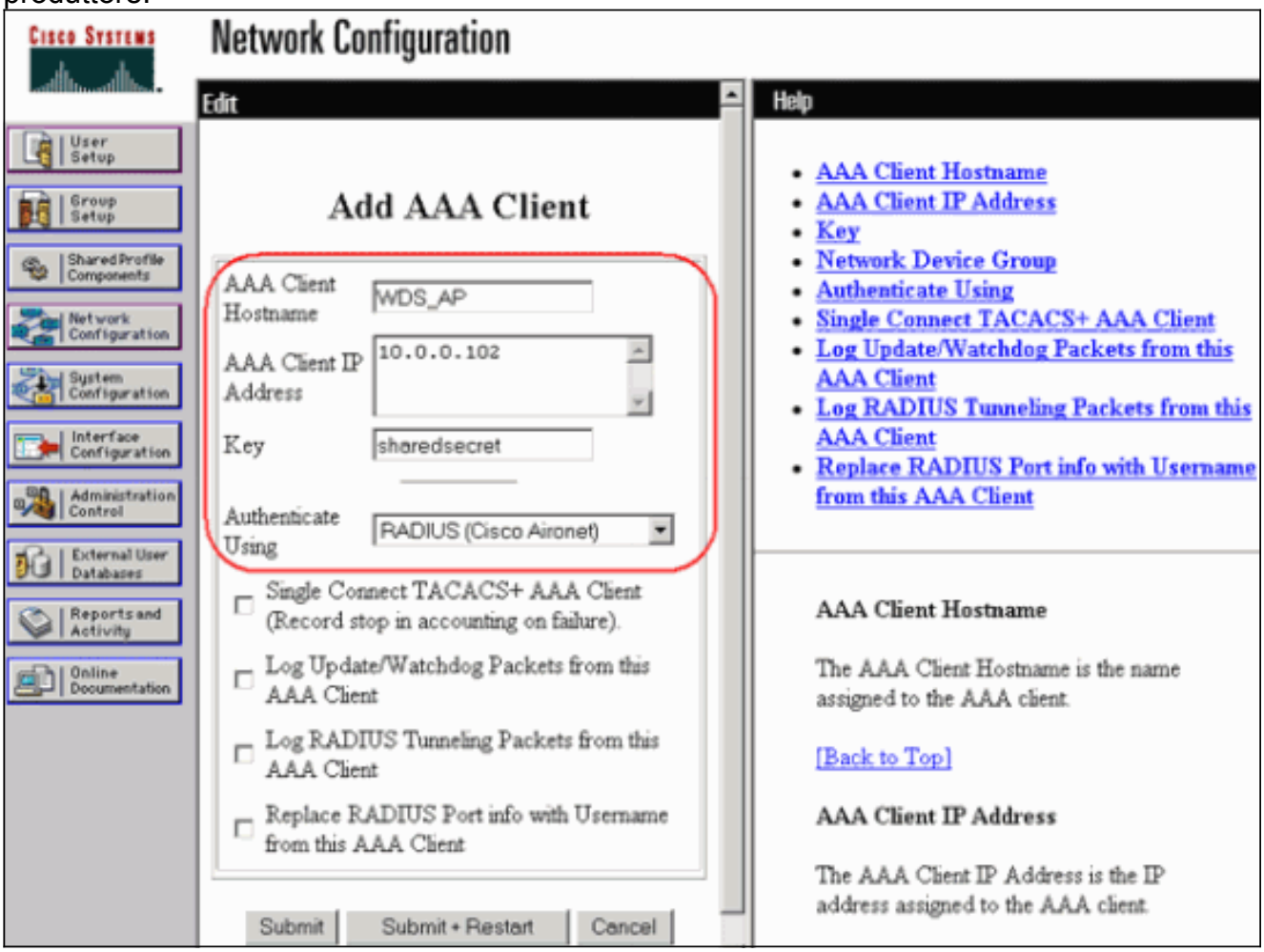
Nota: eseguire questi comandi al prompt dei comandi `enable` del WLSM, non del Supervisor Engine 720. Per accedere al prompt dei comandi del WLSM, eseguire questi comandi al prompt dei comandi `enable` del Supervisor Engine 720:

```
c6506#session slot x proc 1
!--- In this command, x is the slot number where the
WLSM resides. The default escape character is Ctrl-^,
then x. You can also type 'exit' at the remote prompt to
end the session Trying 127.0.0.51 ... Open User Access
Verification Username: <username> Password: <password>
wlan>enable
Password: <enable password>
wlan#
```

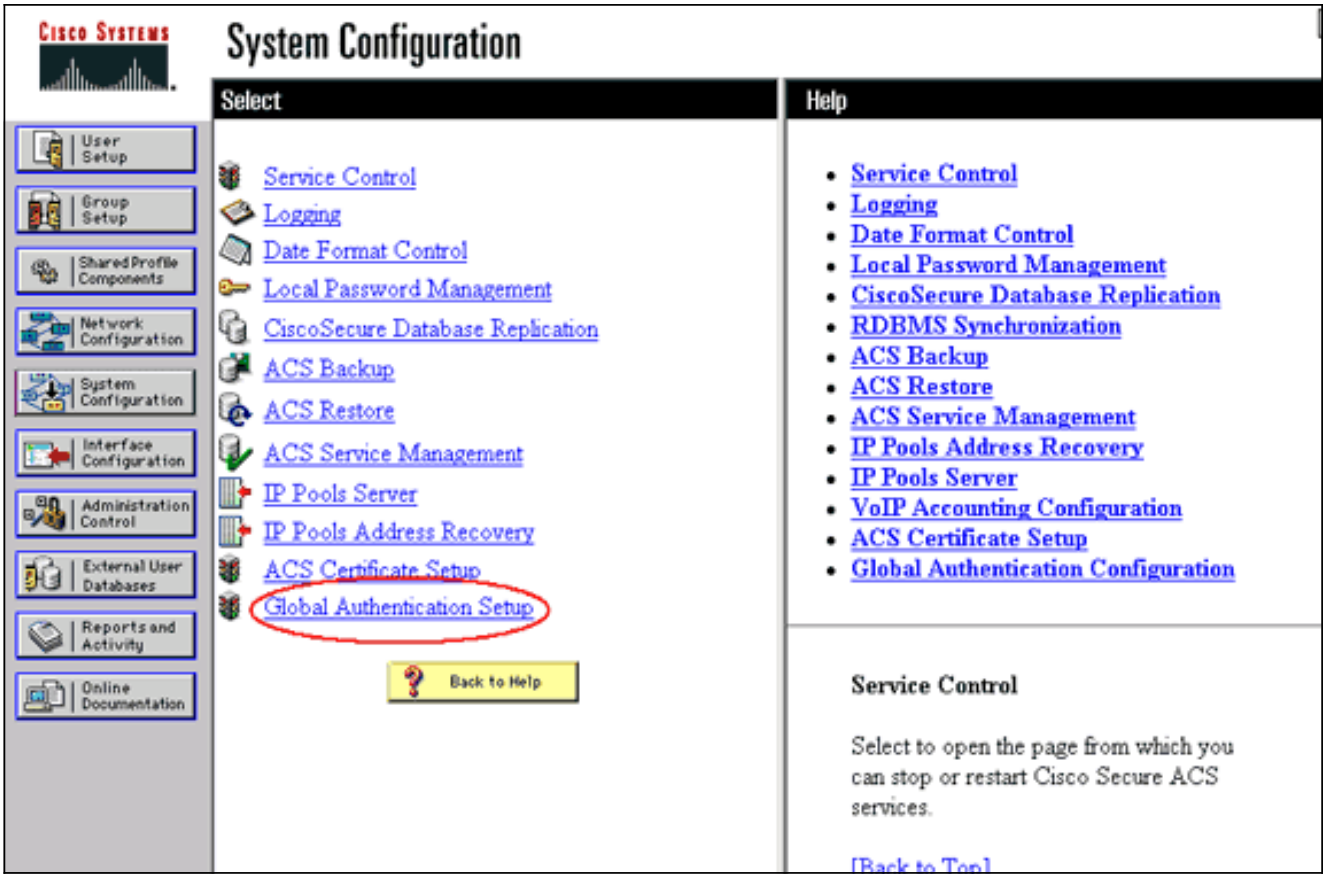
Nota: per semplificare la risoluzione dei problemi e la manutenzione del modulo WLSM, configurare l'accesso remoto Telnet al modulo WLSM. Fare riferimento alla sezione Configurazione dell'accesso remoto Telnet.

Per designare un WLSM come WDS:

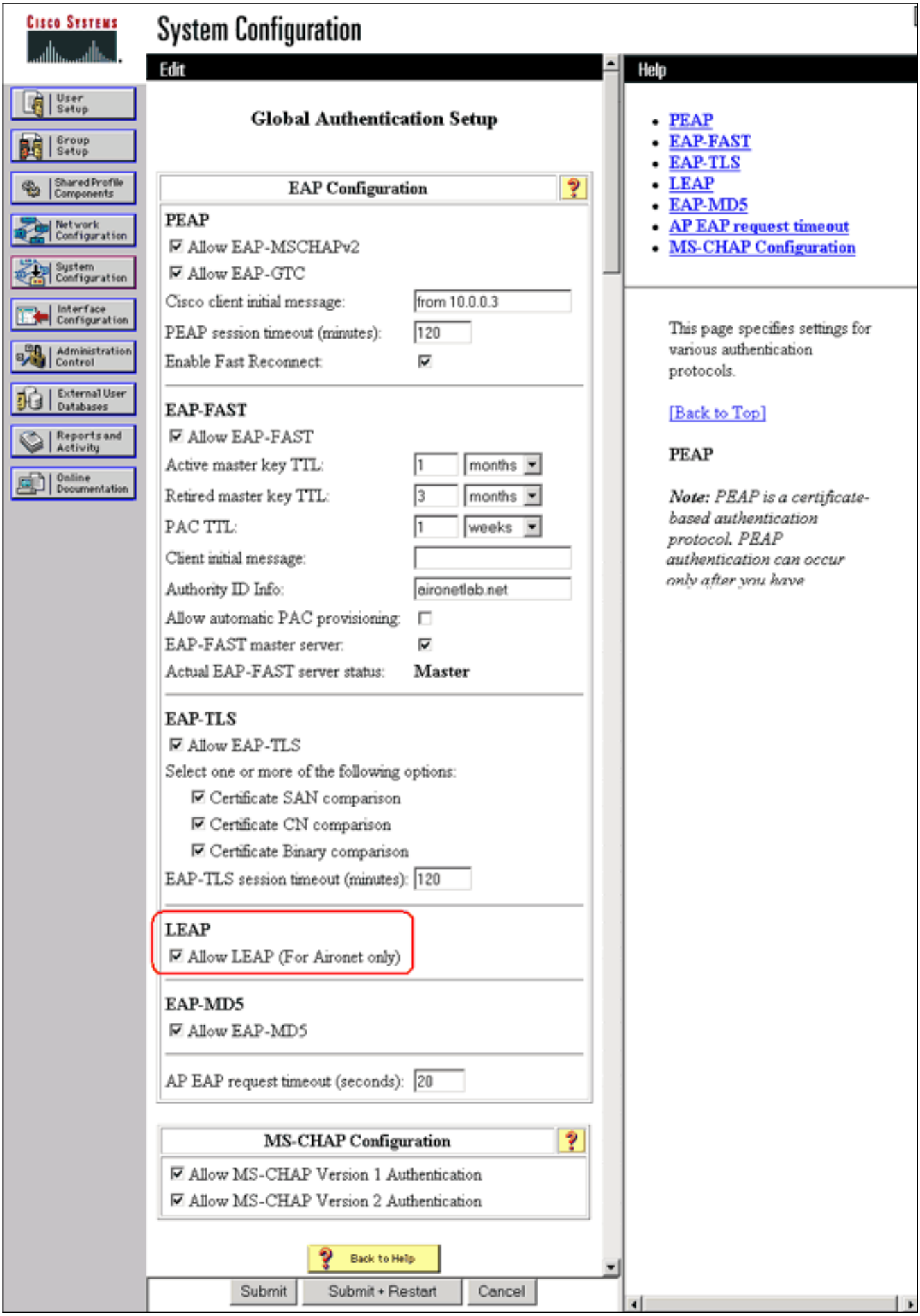
1. Dalla CLI del WLSM, eseguire questi comandi e stabilire una relazione con il server di autenticazione:**Nota:** il modulo WLSM non prevede alcun controllo della priorità. Se la rete contiene più moduli WLSM, WLSM utilizza la configurazione di ridondanza per determinare il modulo principale.
2. Configurare il modulo WLSM nel server di autenticazione come client AAA.In Cisco Secure ACS, questo si verifica nella pagina Configurazione di rete in cui è possibile definire i seguenti attributi per il WLSM:NomeIndirizzo IPSegreto condivisoMetodo di autenticazioneRADIUS Cisco AironetRADIUS IETFPer altri server di autenticazione non ACS, consultare la documentazione del produttore.



Inoltre, in Cisco Secure ACS, configurare ACS in modo da eseguire l'autenticazione LEAP nella pagina Configurazione di sistema - Configurazione dell'autenticazione globale. Fare clic su **Configurazione di sistema**, quindi su **Configurazione autenticazione globale**.



Scorrere la pagina fino a visualizzare l'impostazione LEAP. Quando si seleziona la casella, ACS autentica
LEAP.



3. Nel modulo WLSM definire un metodo che autentichi gli altri access point (un gruppo di server di infrastruttura).
4. Sul modulo WLSM, definire un metodo che autentichi i dispositivi client (un gruppo di server

client) e i tipi EAP utilizzati da tali client.**Nota:** questo passaggio elimina la necessità di definire il processo Metodo di autenticazione client.
5. Definire una VLAN univoca tra il Supervisor Engine 720 e il WLSM in modo da consentire al WLSM di comunicare con entità esterne come i punti di accesso e i server di autenticazione. La VLAN è inutilizzata per altri scopi o per qualsiasi altro scopo sulla rete. Creare prima la VLAN sul Supervisor Engine 720, quindi usare questi comandi:Sul Supervisor Engine 720:Sul modulo WLSM:
6. Verificare il funzionamento del WLSM con questi comandi:Sul modulo WLSM:Sul Supervisor Engine 720:

Designare un punto di accesso come dispositivo di infrastruttura

Èquindi necessario designare almeno un punto di accesso all'infrastruttura e associarlo al servizio WDS. I client vengono associati ai punti di accesso dell'infrastruttura. I punti di accesso dell'infrastruttura richiedono al punto di accesso Servizi di distribuzione Windows o al modulo WLSM di eseguire l'autenticazione per tali punti di accesso.

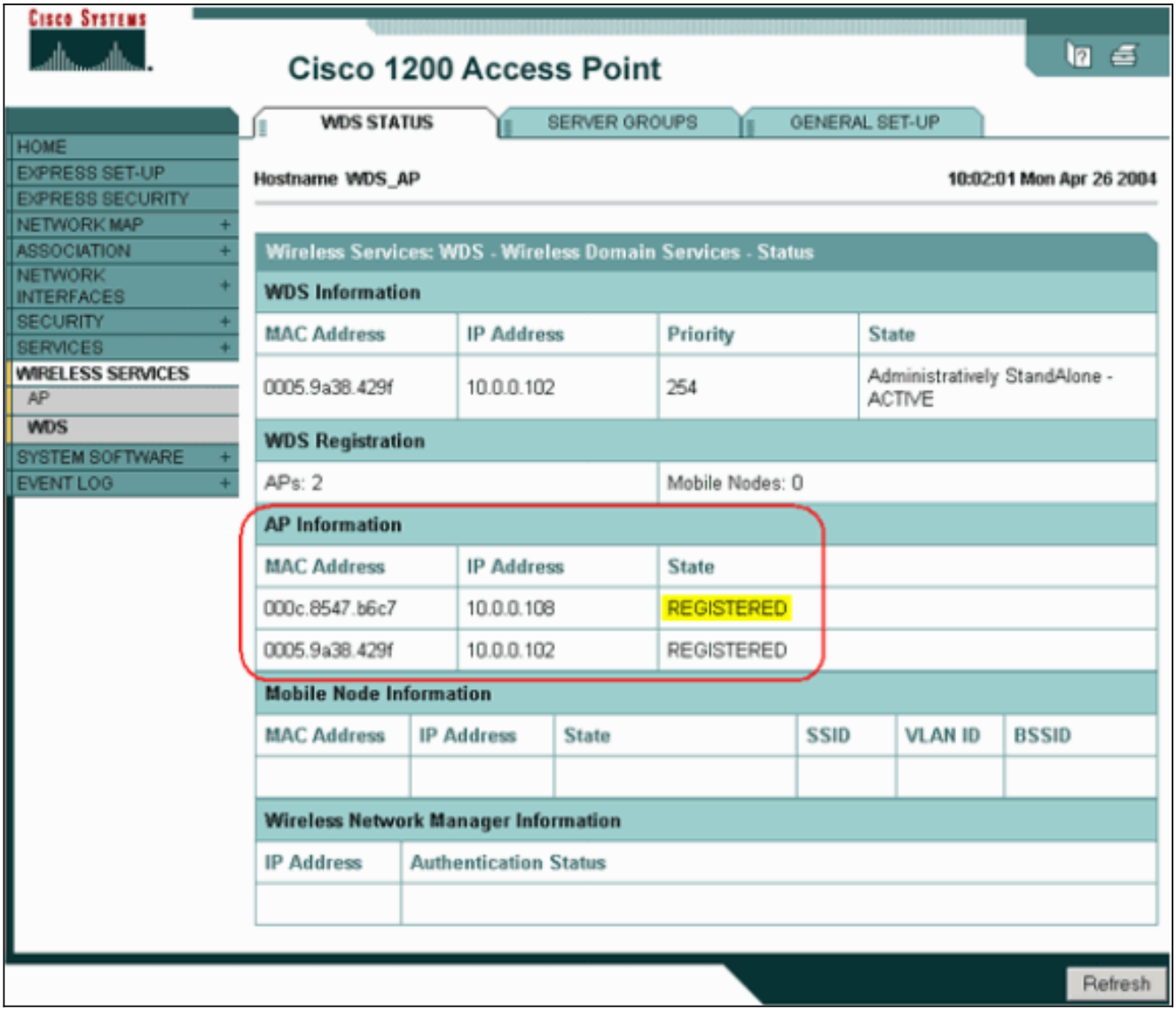
Completare questi passaggi per aggiungere un punto di accesso all'infrastruttura che utilizzi i servizi di Servizi di distribuzione Windows:

Nota: questa configurazione si applica solo ai punti di accesso all'infrastruttura e non al punto di accesso di Servizi di distribuzione Windows.

1. Scegliere **Servizi wireless > AP**. Nel punto di accesso dell'infrastruttura, selezionare **Attiva** per l'opzione Servizi wireless. Digitare quindi il nome utente e la password di Servizi di distribuzione Windows.Ènecessario definire un nome utente e una password di Servizi di distribuzione Windows nel server di autenticazione per tutti i dispositivi che devono essere membri di Servizi di distribuzione
Windows.

In alternativa, usare questi comandi dalla CLI:

2. Scegliere **Servizi wireless > Servizi di distribuzione Windows**. Nella scheda Stato WDS AP WDS il nuovo punto di accesso all'infrastruttura viene visualizzato nell'area Informazioni WDS, con lo stato Attivo, e nell'area Informazioni punto di accesso, con lo stato REGISTRATO.Se l'access point non viene visualizzato come ATTIVO e/o REGISTRATO, controllare se nel server di autenticazione sono presenti errori o tentativi di autenticazione non riusciti.Dopo aver visualizzato l'access point ATTIVO e/o REGISTRATO, aggiungere un metodo di autenticazione client a Servizi di distribuzione Windows.



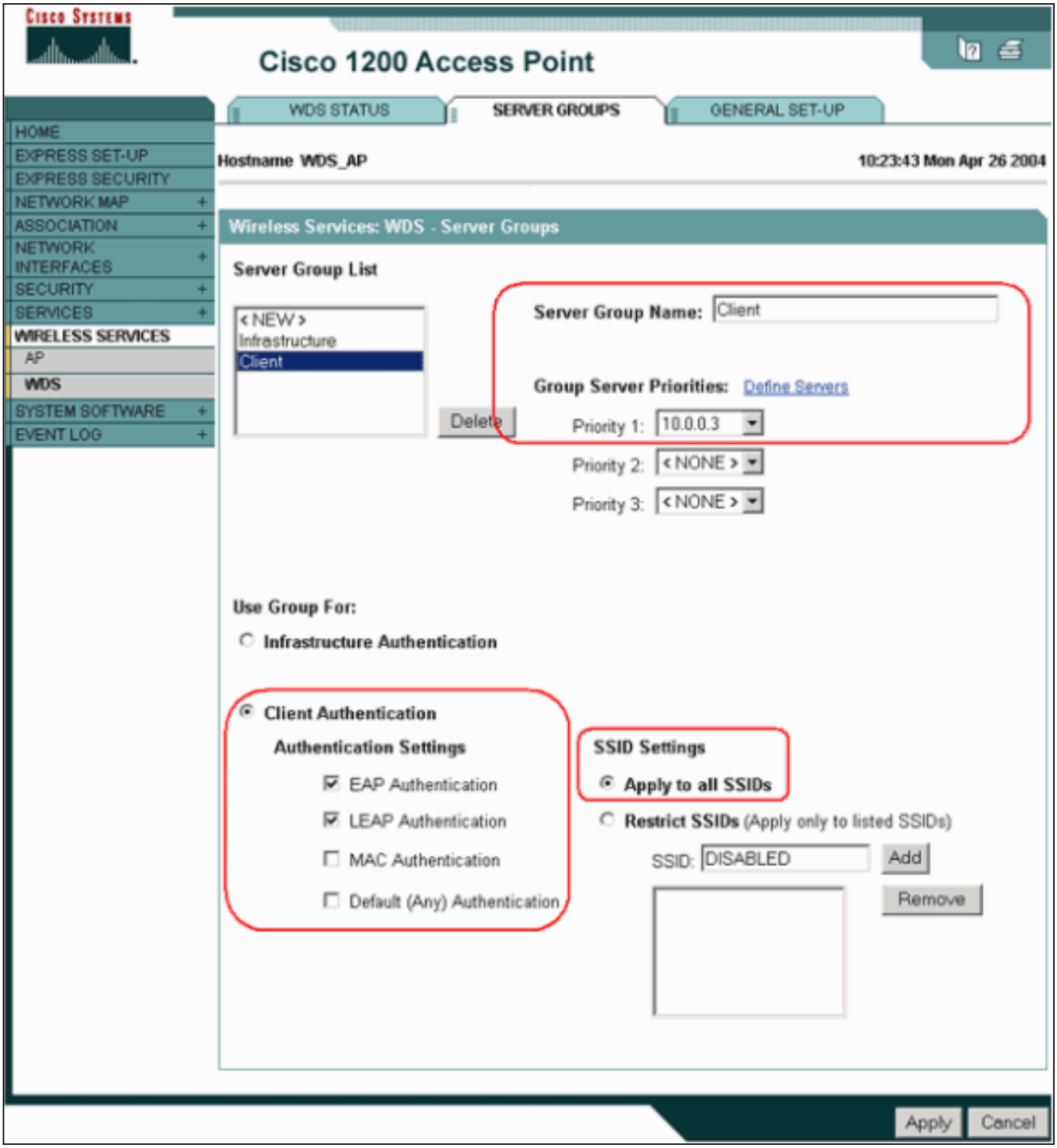
In alternativa, usare questo comando dalla CLI:In alternativa, usare questo comando dal modulo WLSM:Quindi, usare questo comando sul punto di accesso dell'infrastruttura:**Nota:** non è possibile testare le associazioni client perché per l'autenticazione client non sono ancora disponibili i provisioning.

Definisci metodo di autenticazione client

Definire infine un metodo di autenticazione client.

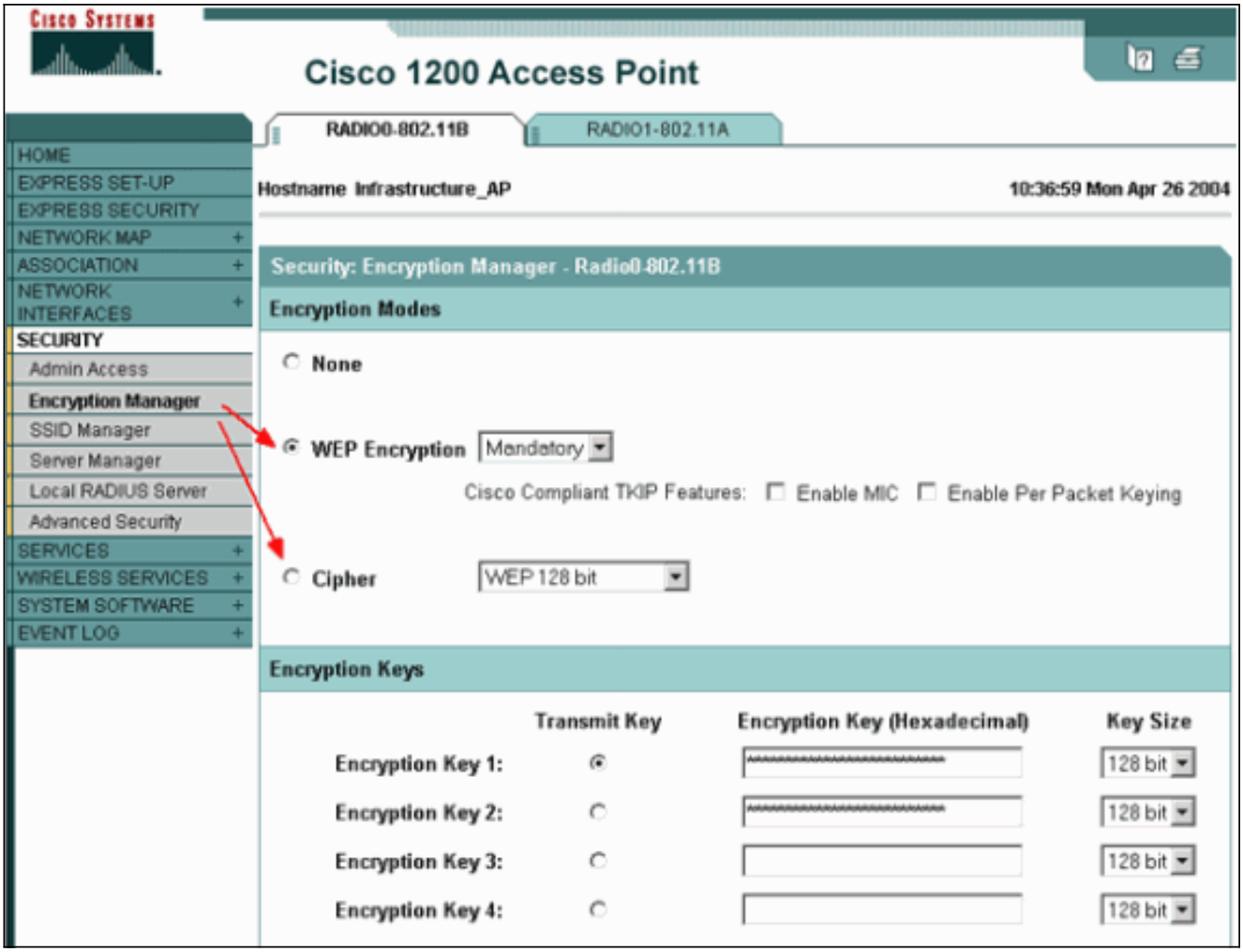
Per aggiungere un metodo di autenticazione client, completare i seguenti passaggi:

1. Scegliere **Servizi wireless > Servizi di distribuzione Windows**. Eseguire la procedura seguente nella scheda Gruppi di server AP Servizi di distribuzione Windows:Definire un gruppo di server che autentica i client (un gruppo di client).Impostare Priorità 1 sul server di autenticazione configurato in precedenza.Impostare il tipo di autenticazione applicabile (LEAP, EAP, MAC e così via).Applicare le impostazioni agli SSID pertinenti.

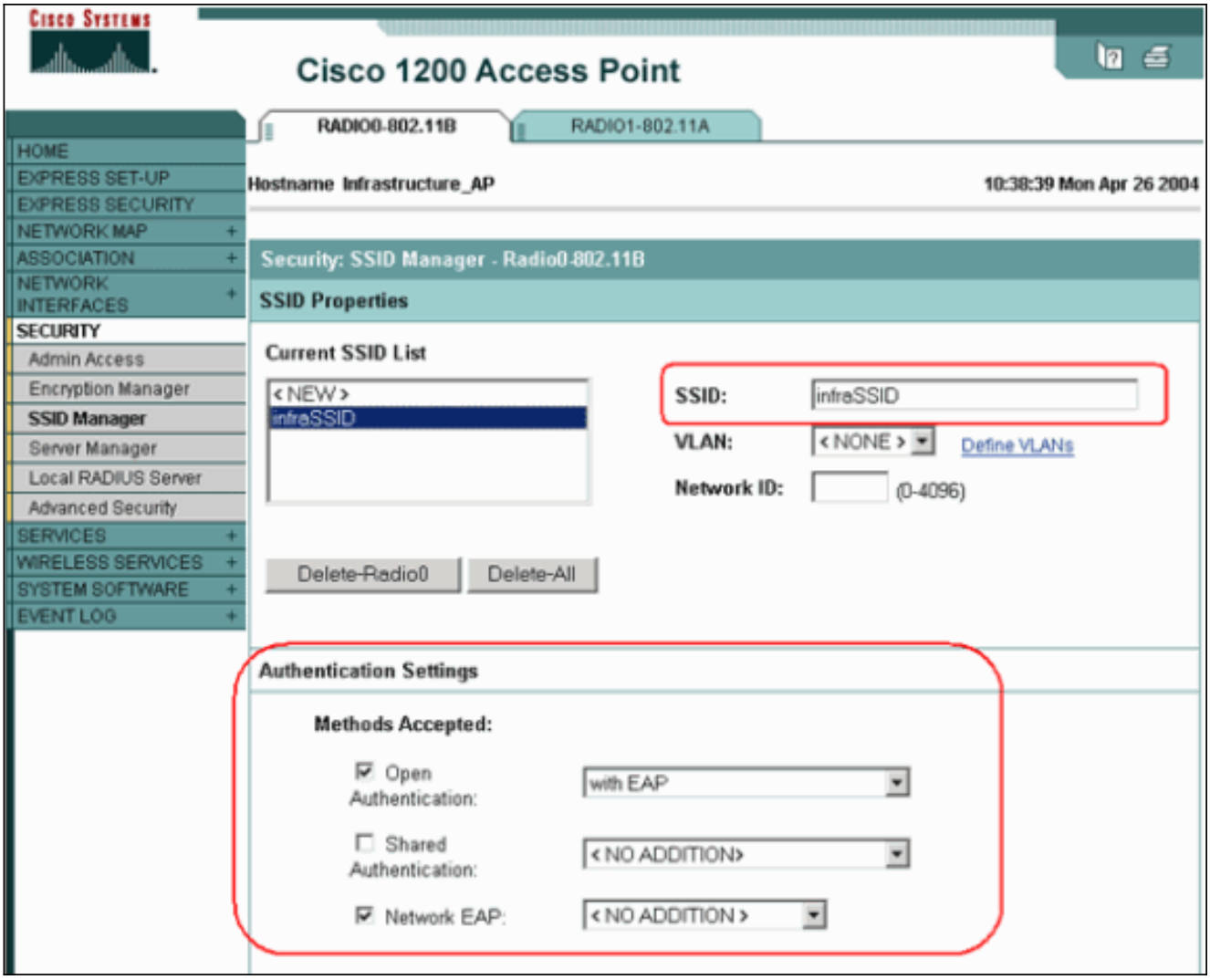


In alternativa, usare questi comandi dalla CLI:**Nota:** l'access point WDS di esempio è dedicato e non accetta associazioni client.**Nota:** non configurare nei punti di accesso dell'infrastruttura per i gruppi di server perché i punti di accesso dell'infrastruttura inoltrano eventuali richieste al servizio di distribuzione Windows da elaborare.

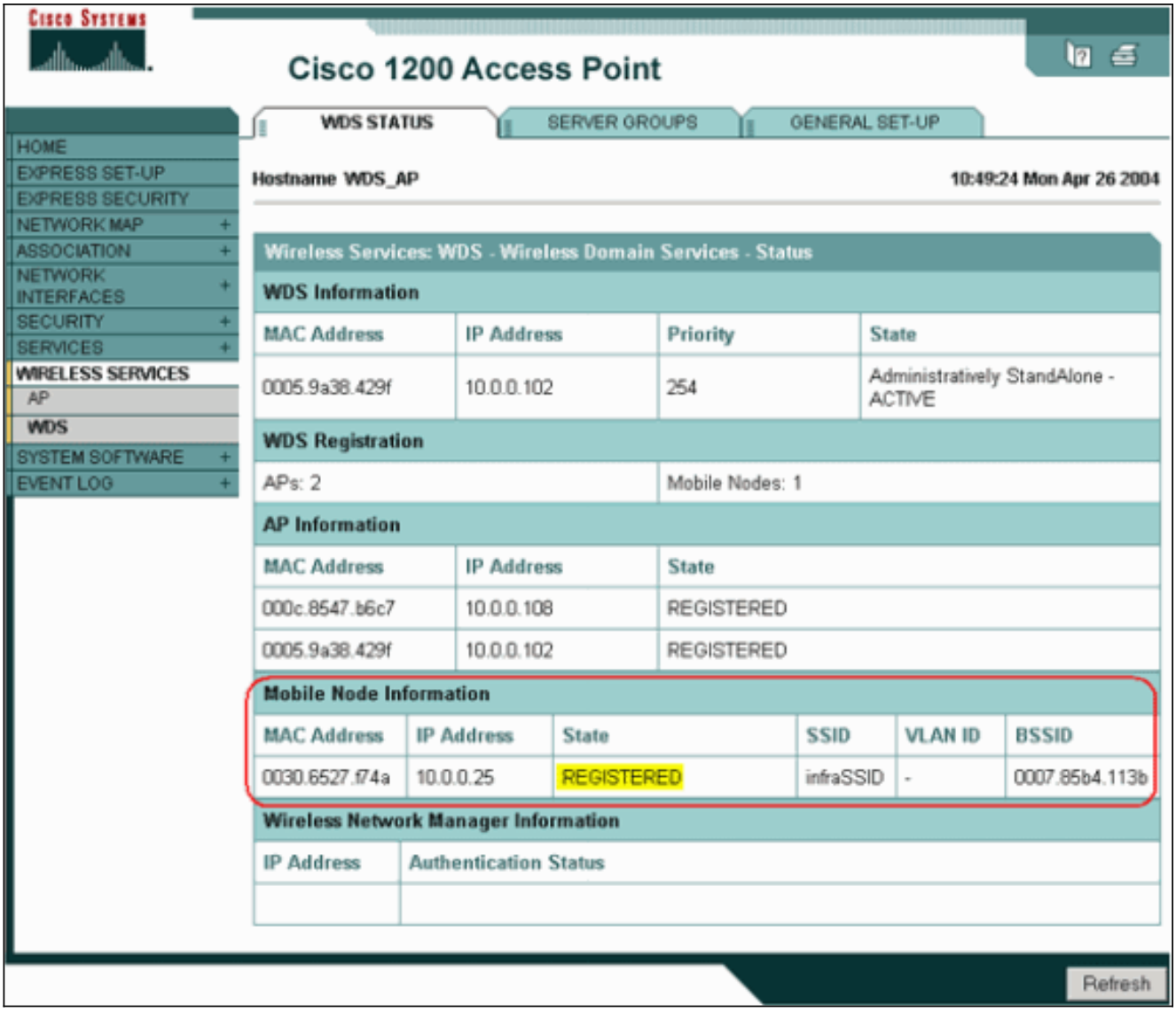
2. Sui punti di accesso dell'infrastruttura:Nella voce di menu **Security > Encryption Manager**, fare clic su **WEP Encryption** o **Cipher**, come richiesto dal protocollo di autenticazione utilizzato.



Nella voce di menu **Protezione >** Gestione **SSID** selezionare i metodi di autenticazione richiesti dal protocollo di autenticazione
utilizzato.



3. Èora possibile verificare se i client eseguono l'autenticazione ai punti di accesso dell'infrastruttura. L'access point di Servizi di distribuzione Windows nella scheda Stato Servizi di distribuzione Windows (sotto la voce di menu **Servizi wireless >** Servizi di distribuzione Windows) indica che il client viene visualizzato nell'area Informazioni nodo mobile e ha uno stato REGISTRATO.Se il client non viene visualizzato, controllare il server di autenticazione per individuare eventuali errori o tentativi di autenticazione non riusciti da parte dei
client.



In alternativa, usare questi comandi dalla CLI:**Nota:** se è necessario eseguire il debug dell'autenticazione, eseguire il debug nell'access point Servizi di distribuzione Windows, in quanto è il dispositivo che comunica con il server di autenticazione.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione. Nell'elenco vengono visualizzate alcune delle domande comuni relative al comando WDS per chiarire ulteriormente l'utilità di tali comandi:

- **Domanda: In WDS AP, quali sono le impostazioni consigliate per questi elementi?timeout radius-serverdeadtime server radiusTempo di attesa errore MIC (Message Integrity Check) TKIP (Temporal Key Integrity Protocol)Tempo di attesa clientIntervallo di riautenticazione EAP o MACTimeout client EAP (facoltativo)Risposta.** Si consiglia di mantenere la configurazione con le impostazioni predefinite relative a queste impostazioni speciali e di utilizzarle solo in caso di problemi relativi alla temporizzazione.Di seguito sono riportate le impostazioni

consigliate per WDS AP:Disabilita **timeout server radius**. Numero di secondi di attesa di una risposta a una richiesta RADIUS da parte di un punto di accesso prima di inviare nuovamente la richiesta. L'impostazione predefinita è 5 secondi.Disabilitare il **deadtime del server radius**. RADIUS viene ignorato da ulteriori richieste per la durata di minuti, a meno che tutti i server non siano contrassegnati come inattivi.L'opzione Tempo di arresto errori MIC TKIP è attivata per impostazione predefinita su 60 secondi. Se si abilita il tempo di sospensione, è possibile immettere l'intervallo in secondi. Se l'access point rileva due errori MIC entro 60 secondi, blocca tutti i client TKIP su quell'interfaccia per il periodo di tempo di attesa specificato qui.Per impostazione predefinita, l'opzione Tempo di attesa client deve essere disattivata. Se si abilita la sospensione, immettere il numero di secondi di attesa dell'access point dopo un errore di autenticazione prima che venga elaborata una richiesta di autenticazione successiva.L'intervallo di riautenticazione EAP o MAC è disabilitato per impostazione predefinita. Se si abilita la riautenticazione, è possibile specificare l'intervallo o accettare quello fornito dal server di autenticazione. Se si sceglie di specificare l'intervallo, immettere l'intervallo in secondi di attesa dell'access point prima che un client autenticato debba eseguire nuovamente l'autenticazione.Il timeout del client EAP (facoltativo) è di 120 secondi per impostazione predefinita. Immettere il tempo di attesa dei client wireless per rispondere alle richieste di autenticazione EAP.

- **Domanda: Per quanto riguarda il tempo di sospensione TKIP, ho letto che dovrebbe essere impostato su 100 ms e non 60 secondi. Suppongo che sia impostato su un secondo dal browser perché è il numero più basso che si può selezionare?Risposta.** Non è consigliabile impostarlo su 100 ms a meno che non venga segnalato un errore in cui l'unica soluzione consiste nell'aumentare questo tempo. Un secondo è l'impostazione più bassa.
- **Domanda: Questi due comandi aiutano in qualche modo l'autenticazione del client e sono necessari su WDS o su Infrastructure AP?attributo radius-server 6 on-for-login-authradius-server attribute 6 support-multipleRisposta.** Questi comandi non facilitano il processo di autenticazione e non sono necessari in Servizi di distribuzione Windows o nell'access point.
- **Domanda: Nel punto di accesso dell'infrastruttura, si presume che nessuna delle impostazioni di Server Manager e delle proprietà globali sia necessaria perché il punto di accesso riceve informazioni da WDS. Sono necessari questi comandi specifici per il punto di accesso dell'infrastruttura?attributo radius-server 6 on-for-login-authradius-server attribute 6 support-multipletimeout radius-serverdeadtime server radiusRisposta.** Non è necessario disporre di Server Manager e delle proprietà globali per i punti di accesso dell'infrastruttura. WDS si occupa di tale compito e non è necessario disporre delle impostazioni seguenti:**attributo radius-server 6 on-for-login-authradius-server attribute 6 support-multipletimeout radius-serverdeadtime server radius**L'impostazione **%h dell'attributo radius-server 32 include-in-access-req format** rimane per impostazione predefinita ed è obbligatoria.

Un access point è un dispositivo di livello 2. Pertanto, l'access point non supporta la mobilità di layer 3 quando è configurato per funzionare come dispositivo WDS. È possibile ottenere la mobilità di layer 3 solo quando si configura il WLSM come dispositivo WDS. Fare riferimento alla sezione *Layer 3 Mobility Architecture* di Cisco Catalyst serie 6500 Wireless LAN Services Module: White paper per ulteriori informazioni.

Pertanto, quando si configura un access point come dispositivo WDS, non utilizzare il comando **mobility network-id**. Questo comando si applica alla mobilità di livello 3 ed è necessario disporre di un WLSM come dispositivo WDS per configurare correttamente la mobilità di livello 3. Se si utilizza il comando **mobility network-id** in modo non corretto, è possibile che si verifichino alcuni dei seguenti sintomi:

- I client wireless non possono associarsi al punto di accesso.
- I client wireless possono essere associati al punto di accesso, ma non ricevono un indirizzo IP dal server DHCP.
- Un telefono wireless non viene autenticato quando si dispone di una distribuzione Voice over WLAN.
- L'autenticazione EAP non viene eseguita. Con l'**id della rete per la mobilità** configurato, l'access point cerca di creare un tunnel GRE (Generic Routing Encapsulation) per inoltrare i pacchetti EAP. Se non viene stabilito alcun tunnel, i pacchetti non vanno da nessuna parte.
- Un punto di accesso configurato come dispositivo Servizi di distribuzione Windows non funziona come previsto e la configurazione di Servizi di distribuzione Windows non funziona.**Nota:** non è possibile configurare Cisco Aironet 1300 AP/Bridge come dispositivo master WDS. 1300 AP/Bridge non supporta questa funzionalità. Il 1300 AP/Bridge può partecipare a una rete WDS come dispositivo di infrastruttura in cui un altro AP o WLSM è configurato come dispositivo master WDS.

Comandi per la risoluzione dei problemi

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

- **debug dot11 aaa authenticator all**: visualizza le varie negoziazioni che un client deve eseguire mentre il client si associa ed esegue l'autenticazione tramite il processo 802.1x o EAP. Questo debug è stato introdotto nel software Cisco IOS versione 12.2(15)JA. Questo comando rende obsoleto **debug dot11 aaa dot1x** in quella e nelle versioni successive.
- **debug aaa authentication**: visualizza il processo di autenticazione da una prospettiva AAA generica.
- **debug wlcp ap**: visualizza le negoziazioni WLCCP interessate quando un access point si unisce a un servizio di distribuzione Windows.
- **debug wlcp packet**: visualizza le informazioni dettagliate sulle negoziazioni WLCCP.
- **debug wlcp leap-client**: visualizza i dettagli quando un dispositivo di infrastruttura si unisce a un servizio WDS.

Informazioni correlate

- Configurazione di WDS, Fast Secure Roaming e gestione della radio
- Nota sulla configurazione del Catalyst serie 6500 Wireless LAN Services Module
- Configurazione di suite di cifratura e WEP
- Configurazione dei tipi di autenticazione
- Pagine di supporto LAN wireless
- Documentazione e supporto tecnico – Cisco Systems