Konfiguration von Wireless-Domänenservices

Inhalt

Einführung

In diesem Dokument wird das Konzept der Wireless Domain Services (WDS) vorgestellt. Außerdem wird beschrieben, wie ein Access Point (AP) oder das Wireless LAN Services Module (WLSM) als WDS und mindestens ein anderer als Infrastruktur-AP konfiguriert werden. Das Verfahren in diesem Dokument führt Sie zu einem funktionierenden WDS, dem es Clients ermöglicht, entweder dem WDS AP oder einem Infrastruktur-AP zuzuordnen. In diesem Dokument soll eine Grundlage für die Konfiguration von Fast Secure Roaming oder die Einführung einer Wireless LAN Solutions Engine (WLSE) im Netzwerk festgelegt werden, damit Sie die Funktionen nutzen können.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Verfügen Sie über umfassende Kenntnisse der Wireless LAN-Netzwerke und der Wireless-Sicherheit.

- Kenntnis der aktuellen EAP-Sicherheitsmethoden (Extensible Authentication Protocol)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- APs mit Cisco IOS® Software
- Cisco IOS Software Release 12.3(2)JA2 oder höher
- Catalyst Wireless LAN Services Module der Serie 6500

Die in diesem Dokument enthaltenen Informationen wurden aus Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte begannen mit einer gelöschten (Standard-)Konfiguration und einer IP-Adresse auf der Schnittstelle BVI1, sodass der Zugriff auf die Einheit über die Benutzeroberfläche der Cisco IOS-Software oder die Befehlszeilenschnittstelle (CLI) möglich ist. Wenn Sie in einem Live-Netzwerk arbeiten, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Wireless-Domänendienste

WDS ist eine neue Funktion für APs in der Cisco IOS-Software und die Grundlage des WLSM der Catalyst Serie 6500. WDS ist eine Kernfunktion, die andere Funktionen wie diese ermöglicht:

- Schnelles und sicheres Roaming
- WLSE-Interaktion
- Funkverwaltung

Bevor andere WDS-basierte Funktionen funktionieren, müssen Sie Beziehungen zwischen den APs, die am WDS teilnehmen, und dem WLSM herstellen. WDS dient u. a. dazu, die Überprüfung von Benutzeranmeldeinformationen durch den Authentifizierungsserver zu überflüssig zu machen und die für die Client-Authentifizierung erforderliche Zeit zu verkürzen.

Um WDS verwenden zu können, müssen Sie einen Access Point oder WLSM als WDS festlegen. Ein WDS-WAP muss einen WDS-Benutzernamen und ein WDS-Kennwort verwenden, um eine Beziehung zu einem Authentifizierungsserver herzustellen. Beim Authentifizierungsserver kann es sich entweder um einen externen RADIUS-Server oder um die Funktion eines lokalen RADIUS-Servers im WDS AP handeln. Das WLSM muss über eine Beziehung zum Authentifizierungsserver verfügen, obwohl WLSM keine Authentifizierung für den Server benötigt.

Andere APs, so genannte Infrastruktur-APs, kommunizieren mit dem WDS. Vor der Registrierung müssen sich die Infrastruktur-APs beim WDS authentifizieren. Eine Infrastrukturservergruppe im WDS definiert diese Infrastrukturauthentifizierung.

Eine oder mehrere Clientservergruppen im WDS definieren die Client-Authentifizierung.

Wenn ein Client versucht, eine Verbindung zu einem Infrastruktur-AP herzustellen, übergibt der Infrastruktur-AP die Anmeldeinformationen des Benutzers zur Validierung an das WDS. Wenn das

WDS die Anmeldeinformationen zum ersten Mal erkennt, wechselt WDS zum Authentifizierungsserver, um die Anmeldeinformationen zu validieren. Das WDS speichert die Anmeldeinformationen im Cache, um zu verhindern, dass beim erneuten Authentifizierungsversuch desselben Benutzers zum Authentifizierungsserver zurückkehrt wird. Beispiele für die erneute Authentifizierung:

- Erneute Keying
- Roaming
- Wenn der Benutzer das Client-Gerät startet

Jedes RADIUS-basierte EAP-Authentifizierungsprotokoll kann über WDS getunnelt werden, z. B.:

- Lightweight EAP (LEAP)
- Protected EAP (PEAP)
- EAP-Transport Layer Security (EAP-TLS)
- EAP-Flexible Authentifizierung durch sicheres Tunneling (EAP-FAST)

Die MAC-Adressenauthentifizierung kann auch zu einem externen Authentifizierungsserver oder zu einer lokalen Liste eines WDS-AP weitergeleitet werden. Das WLSM unterstützt keine MAC-Adressauthentifizierung.

Der WDS und die Infrastruktur-APs kommunizieren über ein Multicast-Protokoll, das als WLAN Context Control Protocol (WLCCP) bezeichnet wird. Diese Multicast-Nachrichten können nicht geroutet werden. Daher müssen sich ein WDS und die zugehörigen Infrastruktur-APs im gleichen IP-Subnetz und im gleichen LAN-Segment befinden. Zwischen WDS und WLSE verwendet WLCCP TCP und UDP an Port 2887. Wenn sich WDS und WLSE in unterschiedlichen Subnetzen befinden, können Pakete nicht durch ein Protokoll wie Network Address Translation (NAT) übersetzt werden.

Ein als WDS-Gerät konfigurierter Access Point unterstützt bis zu 60 teilnehmende Access Points. Ein als WDS-Geräte konfigurierter Integrated Services Router (ISR) unterstützt bis zu 100 teilnehmende APs. Ein mit WLSM ausgestatteter Switch unterstützt bis zu 600 teilnehmende APs und bis zu 240 Mobilitätsgruppen. Ein einzelner AP unterstützt bis zu 16 Mobilitätsgruppen.

Hinweis: Cisco empfiehlt, dass auf den Infrastruktur-APs dieselbe IOS-Version wie auf dem WDS-Gerät ausgeführt wird. Wenn Sie eine ältere IOS-Version verwenden, können sich die Access Points möglicherweise nicht beim WDS-Gerät authentifizieren. Darüber hinaus empfiehlt Cisco, die neueste IOS-Version zu verwenden. Die neueste Version von IOS finden Sie auf der Seite Wireless-Downloads.

Rolle des WDS-Geräts

Das WDS-Gerät führt mehrere Aufgaben im WLAN aus:

- Bewerbt seine WDS-Funktion und nimmt an der Auswahl des besten WDS-Geräts für Ihr WLAN teil. Wenn Sie Ihr WLAN für WDS konfigurieren, richten Sie ein Gerät als WDS-Hauptkandidat und ein oder mehrere zusätzliche Geräte als Backup-WDS-Kandidaten ein. Wenn das Haupt-WDS-Gerät offline geht, wird eines der Backup-WDS-Geräte ersetzt.
- Authentifiziert alle APs im Subnetz und stellt einen sicheren Kommunikationskanal mit jedem dieser APs her.
- Sammelt Funkdaten von APs im Subnetz, aggregiert die Daten und leitet sie an das WLSE-Gerät im Netzwerk weiter.

- Dient als Passthrough für alle 802.1x-authentifizierten Client-Geräte, die den teilnehmenden APs zugeordnet sind.
- Registriert alle Client-Geräte im Subnetz, die dynamische Keying-Funktion verwenden, erstellt Sitzungsschlüssel für sie und speichert ihre Sicherheitsanmeldeinformationen. Wenn ein Client zu einem anderen AP wechselt, leitet das WDS-Gerät die Sicherheitsanmeldeinformationen des Clients an den neuen Access Point weiter.

Rolle von Access Points mithilfe des WDS-Geräts

Die APs im WLAN interagieren bei folgenden Aktivitäten mit dem WDS-Gerät:

- Ermitteln und verfolgen Sie das aktuelle WDS-Gerät, und leiten Sie WDS-Meldungen an das Wireless LAN weiter.
- Authentifizierung mit dem WDS-Gerät und Einrichtung eines sicheren Kommunikationskanals zum WDS-Gerät.
- Registrieren Sie zugeordnete Client-Geräte beim WDS-Gerät.
- Senden Sie Funkdaten an das WDS-Gerät.

Konfiguration

WDS stellt die Konfiguration in einer geordneten, modularen Form dar. Jedes Konzept baut auf dem Konzept auf, das dem Konzept vorausgeht. Das WDS ignoriert andere Konfigurationselemente wie Kennwörter, Remote-Zugriff und Funkeinstellungen, um Klarheit zu schaffen und sich auf das Kernthema zu konzentrieren.

In diesem Abschnitt werden die Informationen beschrieben, die zum Konfigurieren der in diesem Dokument beschriebenen Funktionen erforderlich sind.

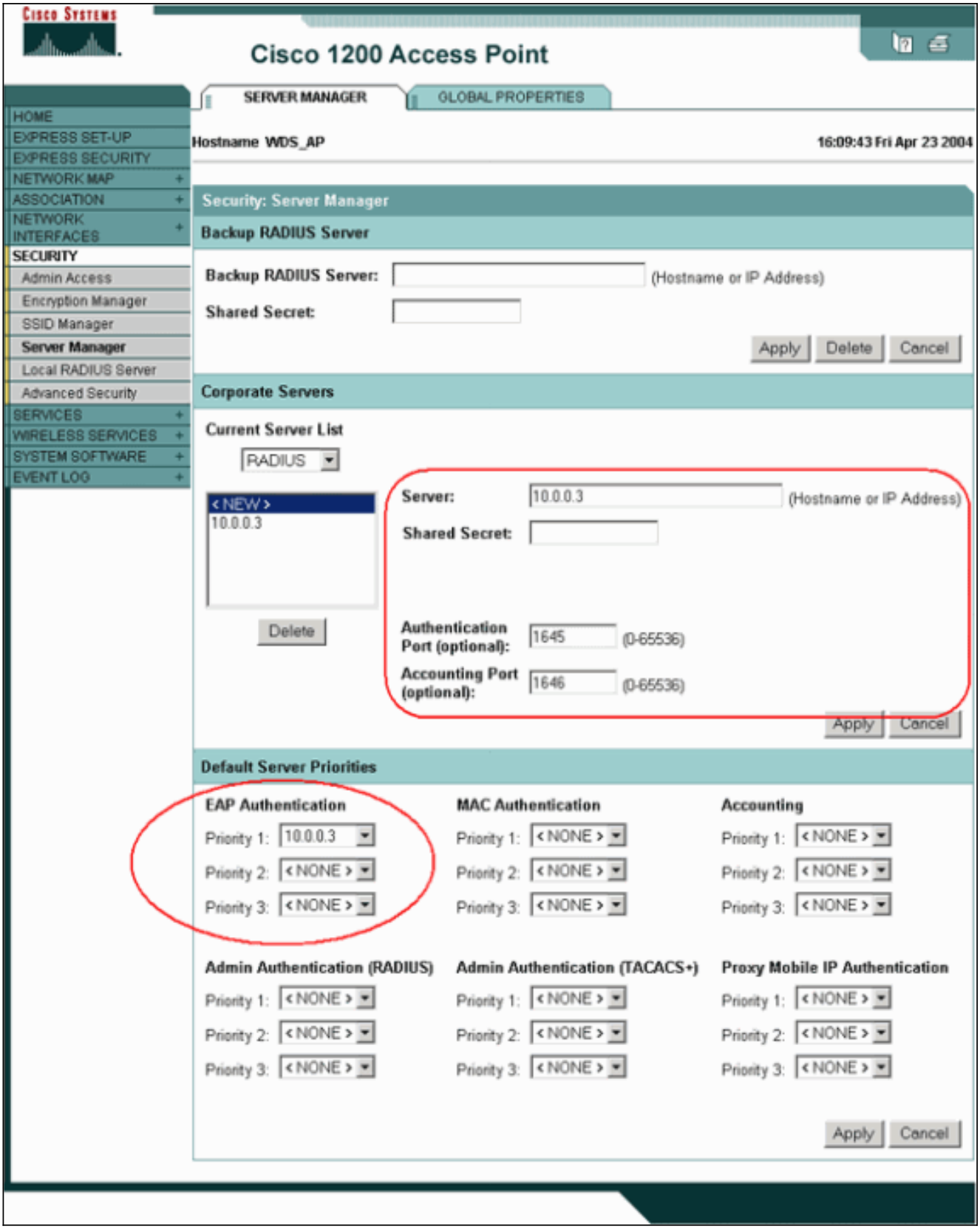
Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Zugangspunkt als WDS festlegen

Der erste Schritt besteht darin, einen Access Point als WDS festzulegen. Der WDS AP ist der einzige Access Point, der mit dem Authentifizierungsserver kommuniziert.

Gehen Sie wie folgt vor, um einen Access Point als WDS zu definieren:

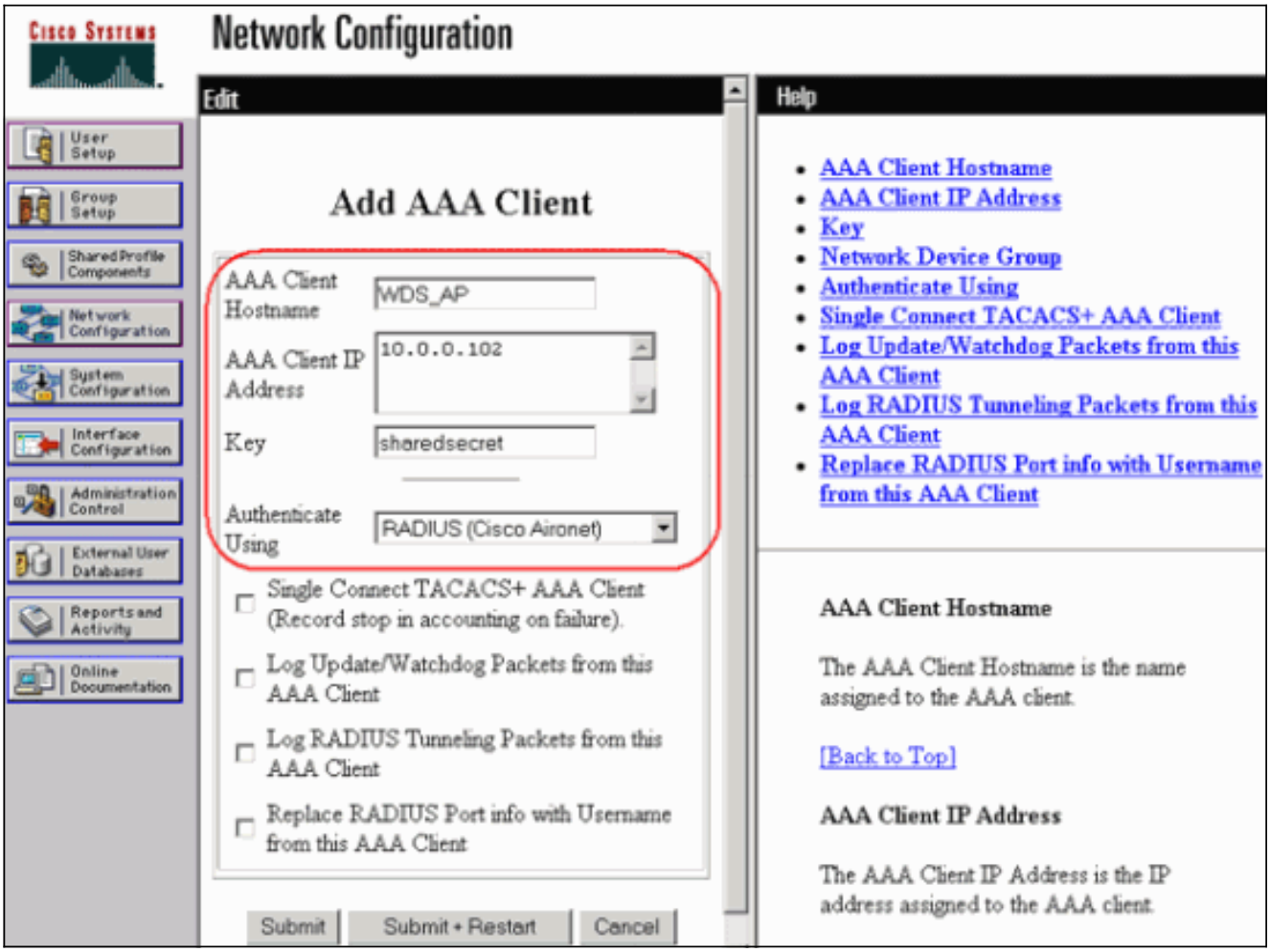
1. Um den Authentifizierungsserver im WDS AP zu konfigurieren, wählen Sie **Security > Server Manager aus**, um zur Registerkarte Server Manager zu wechseln:Geben Sie unter Corporate Servers (Unternehmensserver) die IP-Adresse des Authentifizierungsservers im Feld Server ein.Geben Sie den Shared Secret und die Ports an.Legen Sie unter Default Server Priorities (Standardserverprioritäten) das Feld Priority 1 (Priorität 1) unter dem entsprechenden Authentifizierungstyp auf diese Server-IP-Adresse
   fest.



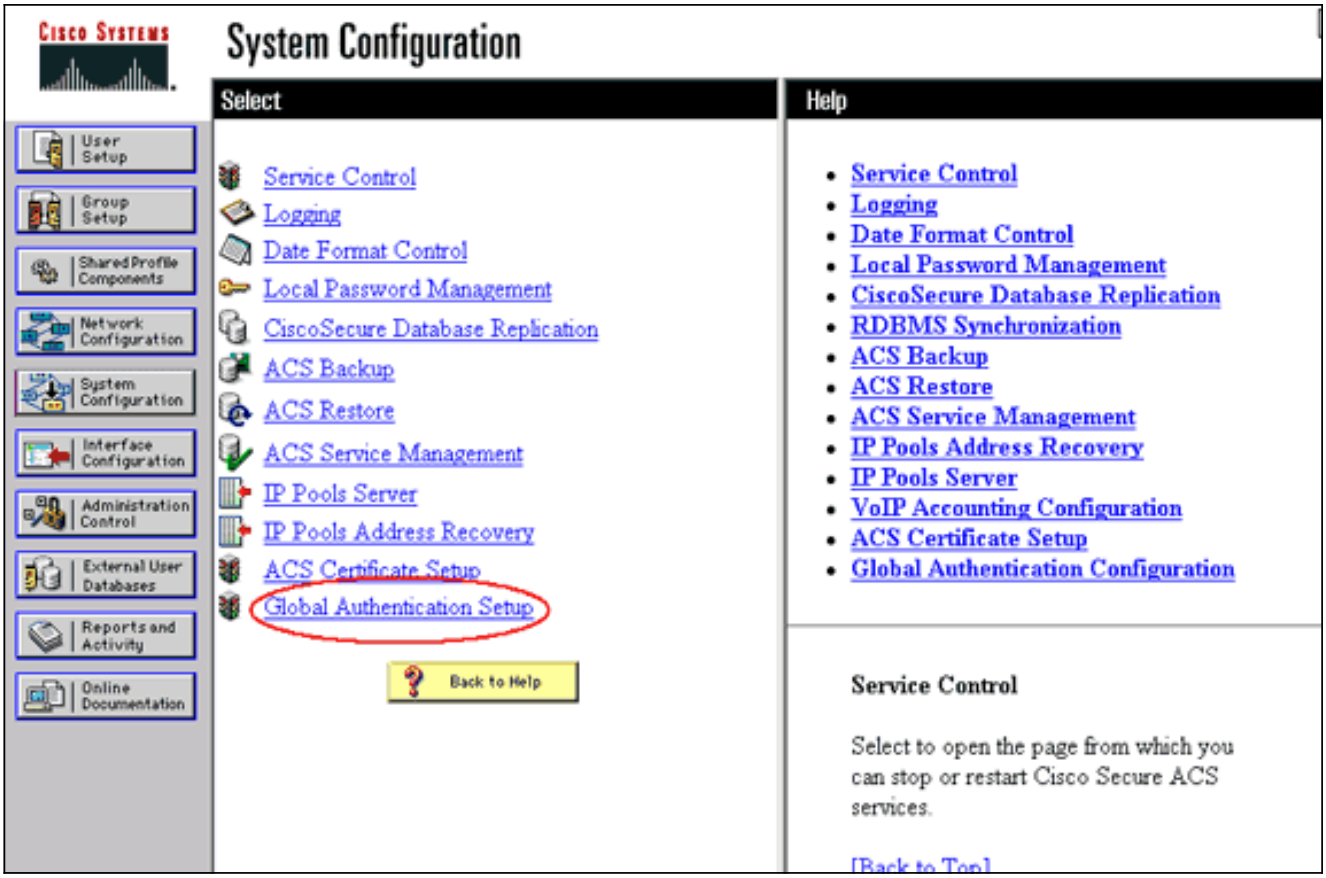
Alternativ können Sie die folgenden Befehle über die CLI ausführen:

2. Der nächste Schritt besteht in der Konfiguration des WDS-Access Points im Authentifizierungsserver als AAA-Client (Authentication, Authorization, Accounting). Dazu müssen Sie den WDS AP als AAA-Client hinzufügen. Gehen Sie wie folgt vor:**Hinweis:** In diesem Dokument wird der Cisco Secure ACS-Server als Authentifizierungsserver verwendet.Im Cisco Secure Access Control Server (ACS) wird dies auf der Seite "Network Configuration" (Netzwerkkonfiguration) beschrieben, auf der Sie diese Attribute für den WDS Access Point definieren:NameIP-AdresseGemeinsamer geheimer SchlüsselAuthentifizierungsmethodeRADIUS Cisco AironetRADIUS Internet Engineering

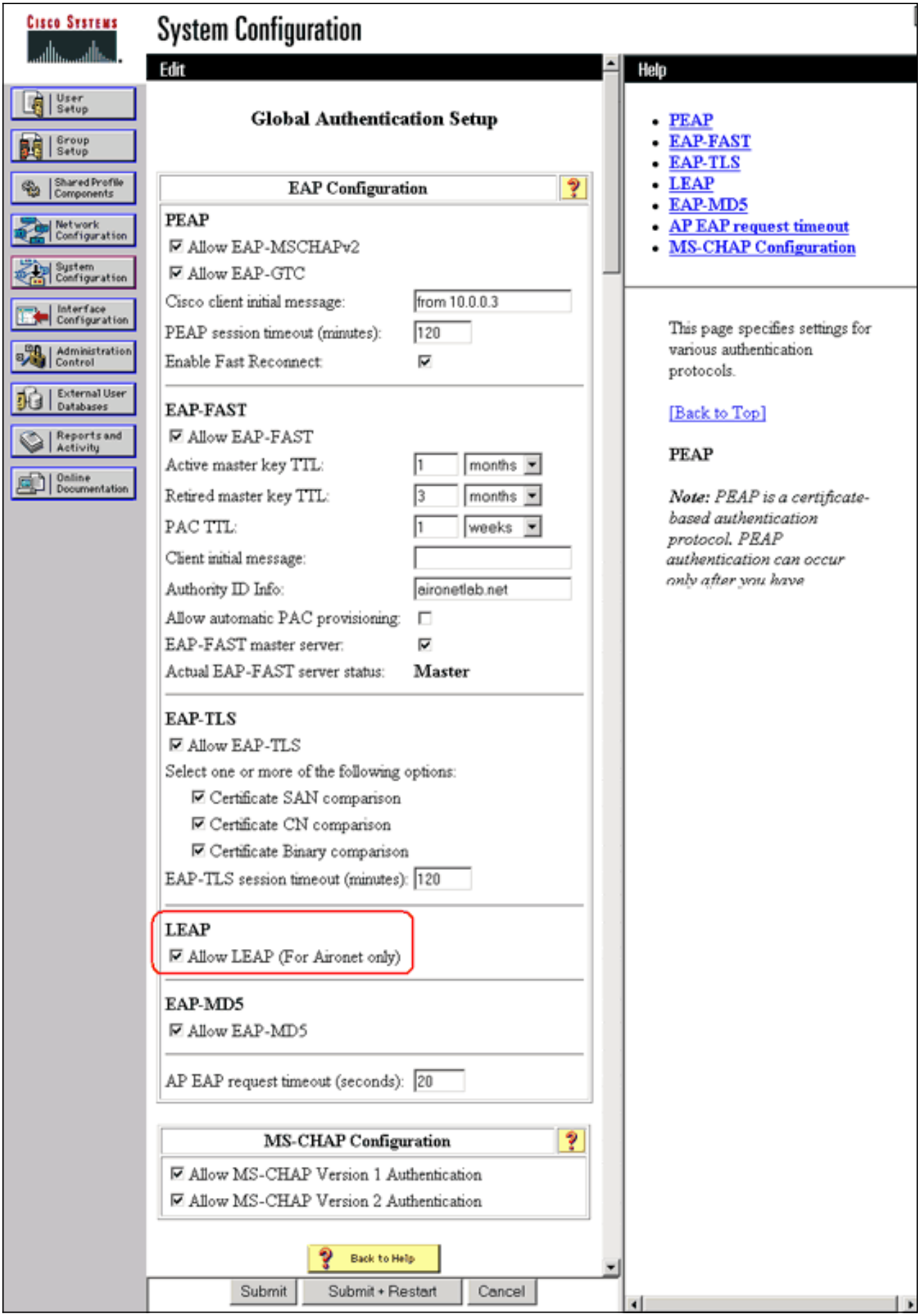
Task Force [IETF]Klicken Sie auf **Senden**.Informationen zu anderen Authentifizierungsservern ohne ACS finden Sie in der Dokumentation des Herstellers.



Stellen Sie darüber hinaus in Cisco Secure ACS sicher, dass Sie ACS so konfigurieren, dass auf der Seite System Configuration - Global Authentication Setup (Systemkonfiguration - Globale Authentifizierung - Einrichtung) LEAP-Authentifizierung ausgeführt wird. Klicken Sie zuerst auf **Systemkonfiguration** und dann auf **Globales Authentifizierungs-Setup**.

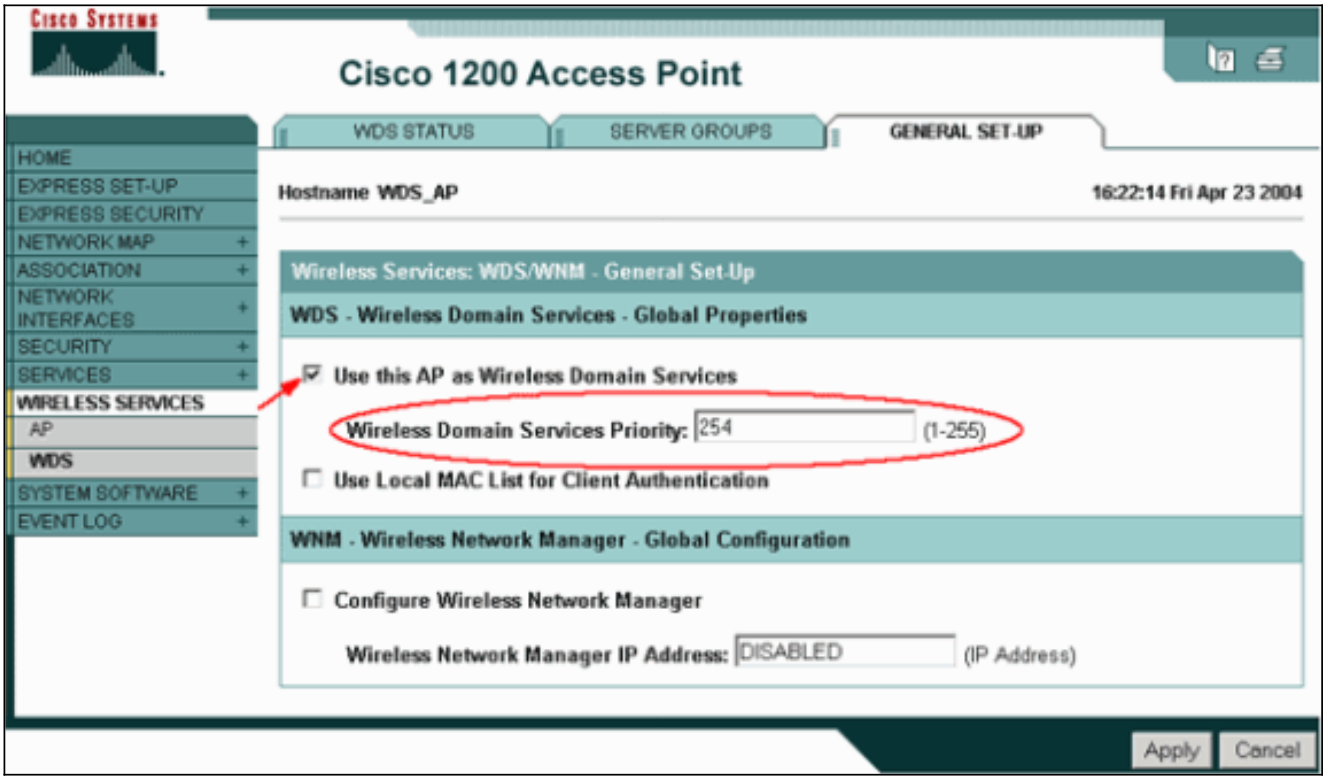


Blättern Sie auf der Seite nach unten zur LEAP-Einstellung. Wenn Sie das Kontrollkästchen aktivieren, authentifiziert ACS
LEAP.



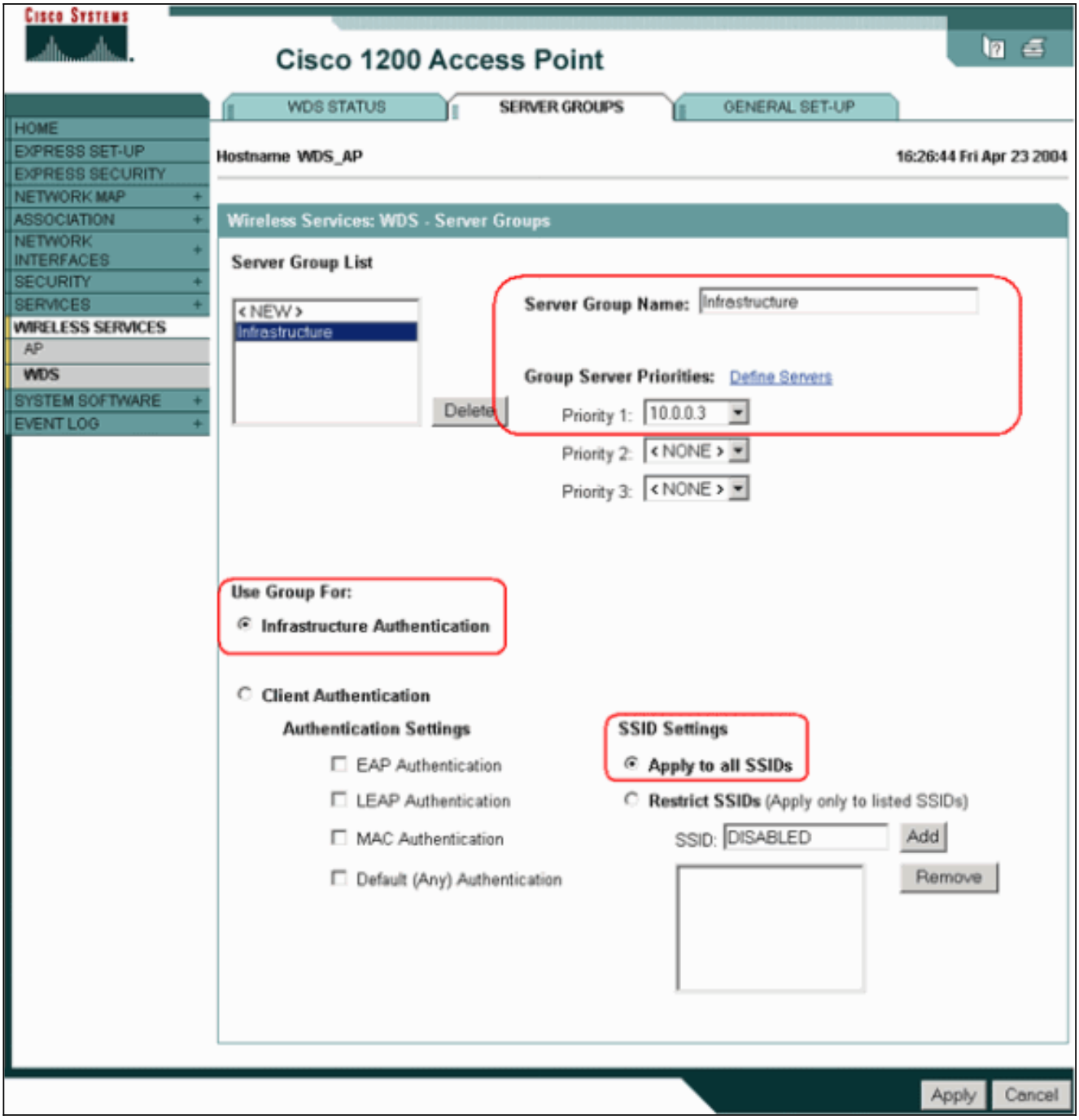
3. Um die WDS-Einstellungen auf dem WDS AP zu konfigurieren, wählen Sie **Wireless Services > WDS** im WDS AP aus, und klicken Sie auf die Registerkarte **General Set-Up (Allgemeine Einrichtung)**. Gehen Sie wie folgt vor:Aktivieren Sie unter WDS-Wireless Domain

Services (WDS-Wireless-Domänendienste) - Global Properties (Globale Eigenschaften) die Option **Use this AP as Wireless Domain Services (Diesen Access Point als Wireless-Domänendienste verwenden)**.Legen Sie den Wert für das Feld Wireless Domain Services Priority (Wireless-Domänendienstpriorität) auf ca. **254 fest**, da dies der erste Wert ist. Sie können einen oder mehrere APs oder Switches als Kandidaten für die Bereitstellung von WDS konfigurieren. Das Gerät mit der höchsten Priorität stellt WDS
bereit.



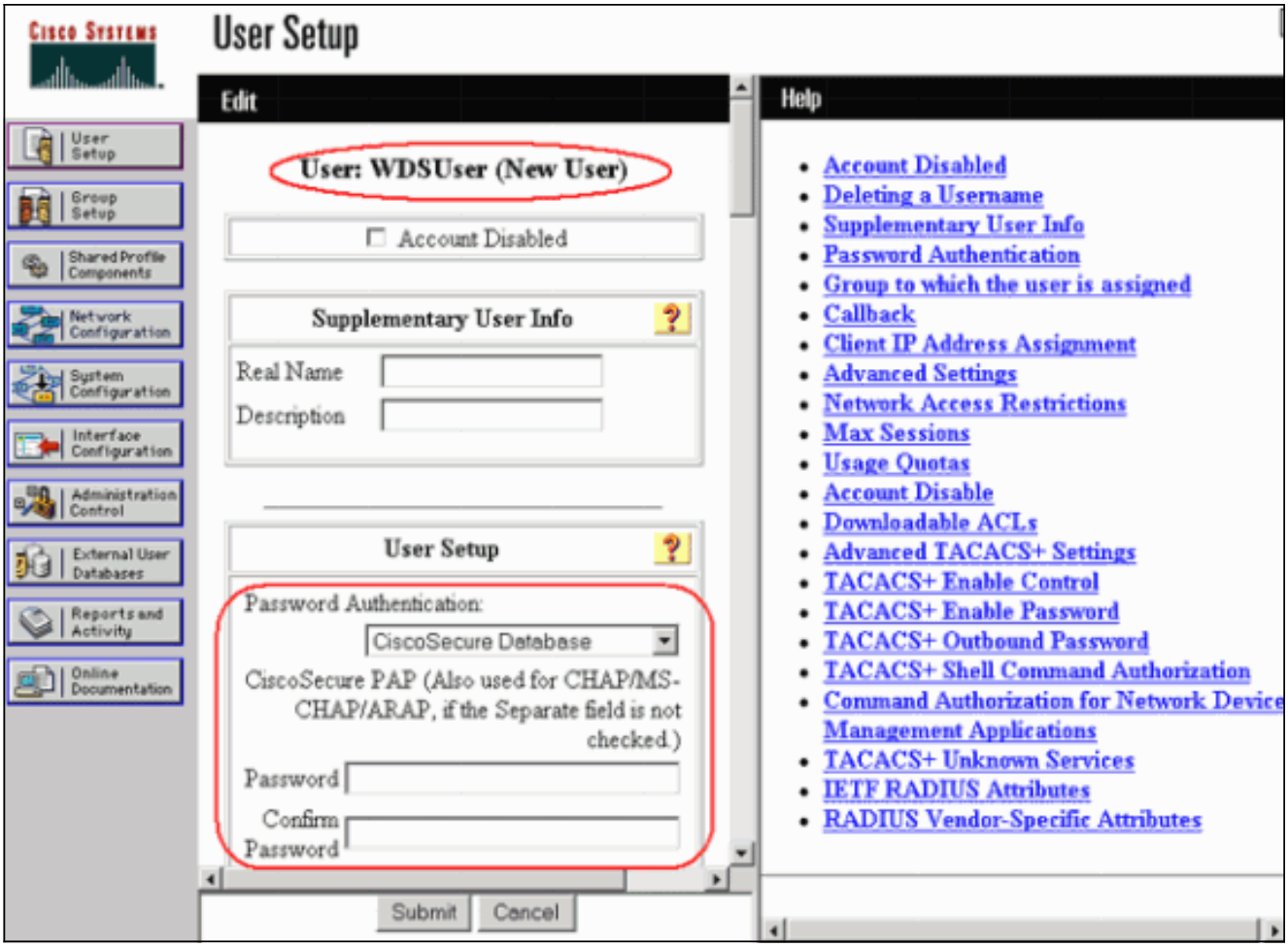
Alternativ können Sie die folgenden Befehle über die CLI ausführen:

4. Wählen Sie **Wireless Services > WDS aus**, und wechseln Sie zur Registerkarte **Servergruppen**:Definieren Sie einen Servergruppennamen, der die anderen APs authentifiziert, eine Infrastrukturgruppe.Legen Sie die Priorität 1 auf den zuvor konfigurierten Authentifizierungsserver fest.Klicken Sie auf die **Benutzergruppe für:** Optionsfeld **"Infrastrukturauthentifizierung"**.Wenden Sie die Einstellungen auf die entsprechenden Service Set Identifiers (SSIDs)
an.



Alternativ können Sie die folgenden Befehle über die CLI ausführen:

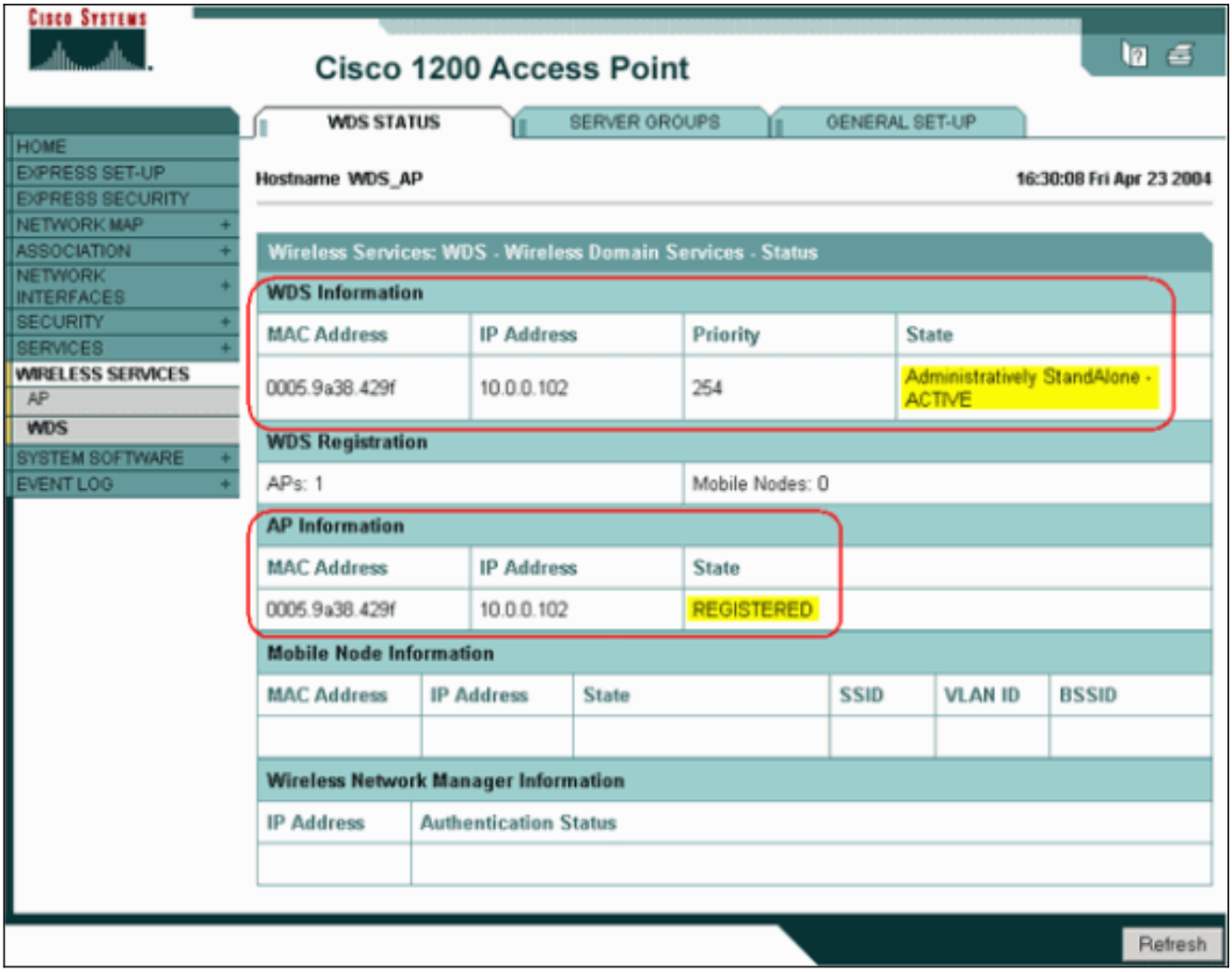
5. Konfigurieren Sie den WDS-Benutzernamen und das Kennwort als Benutzer im Authentifizierungsserver.In Cisco Secure ACS wird dies auf der Seite User Setup (Benutzereinrichtung) angezeigt, auf der Sie den WDS-Benutzernamen und das WDS-Kennwort definieren. Informationen zu anderen Authentifizierungsservern ohne ACS finden Sie in der Dokumentation des Herstellers.**Hinweis:** Setzen Sie den WDS-Benutzer nicht in eine Gruppe ein, der viele Rechte und Berechtigungen zugewiesen sind - WDS erfordert nur eine eingeschränkte
Authentifizierung.



6. Wählen Sie **Wireless Services > AP aus**, und klicken Sie auf **Aktivieren** für die Option An SWAN-Infrastruktur teilnehmen. Geben Sie dann den WDS-Benutzernamen und das Kennwort ein.Sie müssen auf dem Authentifizierungsserver einen WDS-Benutzernamen und ein WDS-Kennwort für alle Geräte definieren, die Sie als Mitglieder des WDS festlegen.

Alternativ können Sie die folgenden Befehle über die CLI ausführen:

7. Wählen Sie **Wireless Services > WDS aus**. Überprüfen Sie auf der Registerkarte WDS AP WDS Status (WDS AP-WDS-Status), ob der WDS AP im Bereich WDS Information (WDS-AP-Informationen) im Bereich ACTIVE State (AKTIVER Status) angezeigt wird. Der Access Point muss auch im Bereich "AP Information" (AP-Informationen) mit Status als REGISTRIERT angezeigt werden.Wenn der Access Point nicht REGISTRIERT oder AKTIV angezeigt wird, überprüfen Sie den Authentifizierungsserver auf Fehler oder fehlgeschlagene Authentifizierungsversuche.Wenn der Access Point ordnungsgemäß registriert ist, fügen Sie einen Infrastruktur-Access Point hinzu, um die Dienste des WDS zu nutzen.



Alternativ können Sie die folgenden Befehle über die CLI ausführen:**Hinweis:** Clientzuordnungen können nicht getestet werden, da die Clientauthentifizierung noch keine Bestimmungen enthält.

Festlegen eines WLSM als WDS

In diesem Abschnitt wird erläutert, wie ein WLSM als WDS konfiguriert wird. Das WDS ist das einzige Gerät, das mit dem Authentifizierungsserver kommuniziert.

Hinweis: Geben Sie diese Befehle an der `enable`-Eingabeaufforderung des WLSM und nicht der Supervisor Engine 720 aus. Um zur Eingabeaufforderung des WLSM zu gelangen, geben Sie diese Befehle an einer `aktivierten` Eingabeaufforderung in der Supervisor Engine 720 aus:

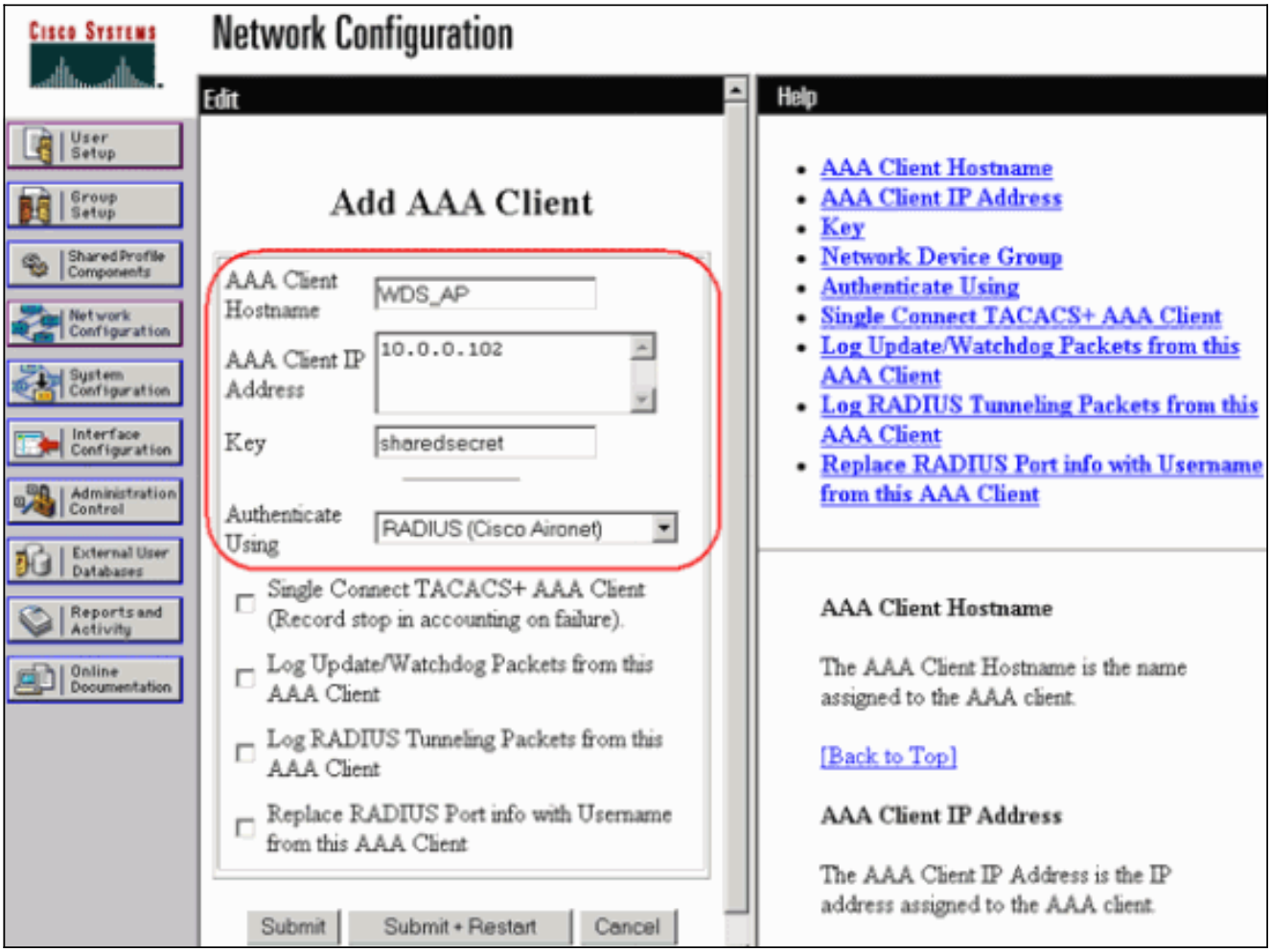
```
c6506#session slot x proc 1
!--- In this command, x is the slot number where the
WLSM resides. The default escape character is Ctrl-^,
then x. You can also type 'exit' at the remote prompt to
end the session Trying 127.0.0.51 ... Open User Access
Verification Username: <username> Password: <password>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

Hinweis: Um die Fehlerbehebung und Wartung des WLSM zu vereinfachen, konfigurieren Sie Telnet-Remote-Zugriff auf das WLSM. Weitere Informationen finden Sie unter Konfigurieren von

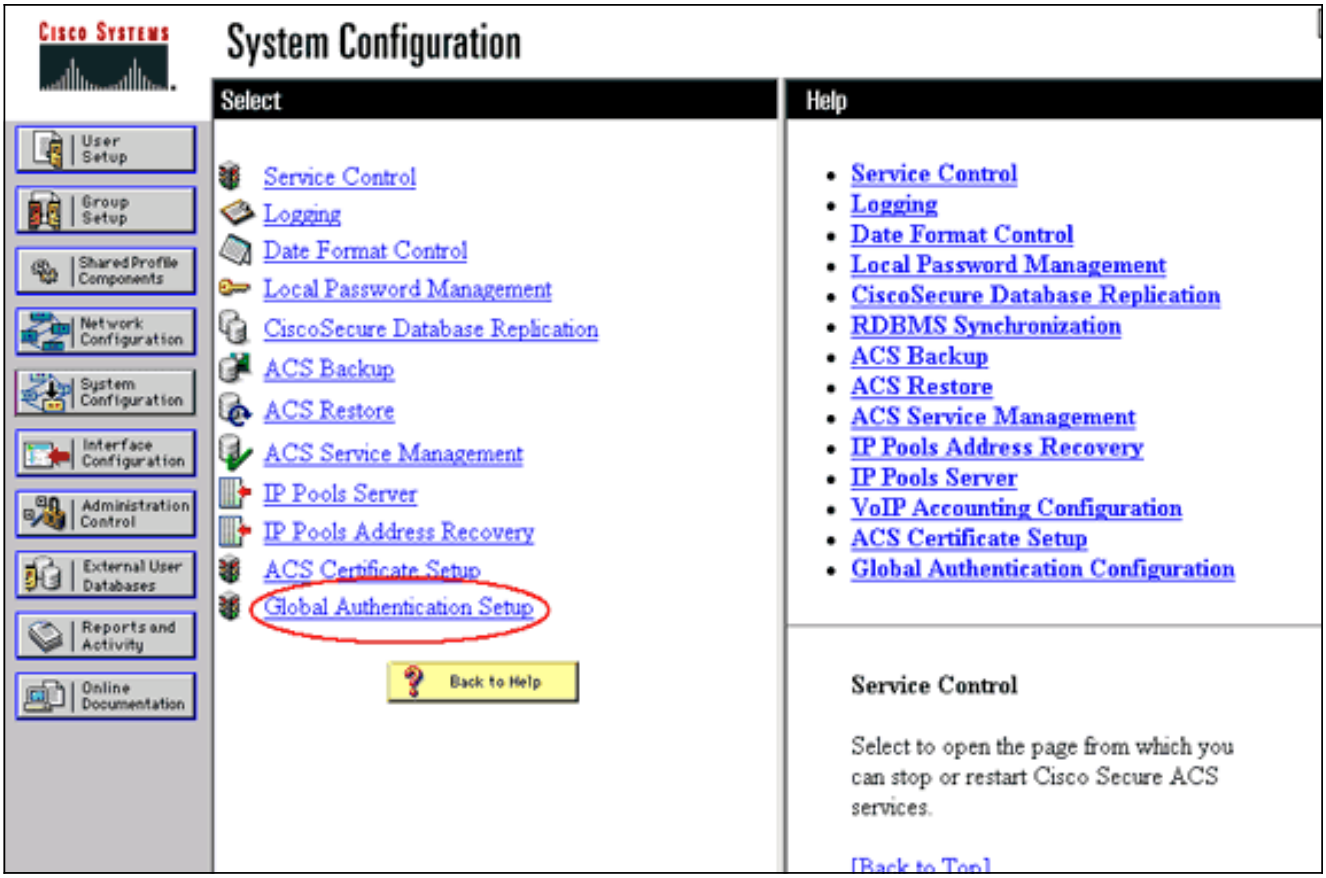
Telnet Remote Access.

So bestimmen Sie ein WLSM als WDS:

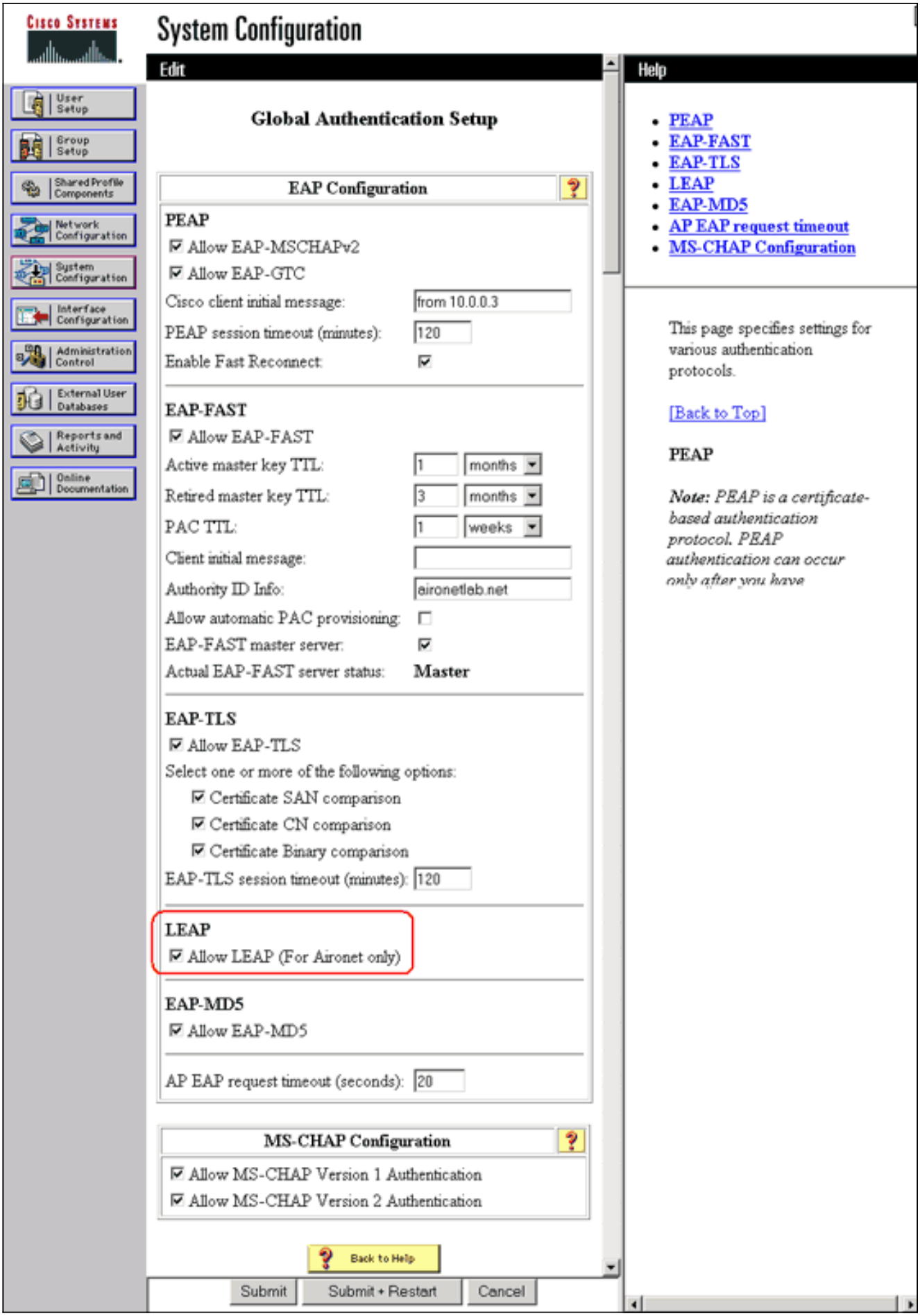
1. Führen Sie über die CLI des WLSM diese Befehle aus, und stellen Sie eine Beziehung zum Authentifizierungsserver her:**Hinweis:** Im WLSM gibt es keine Prioritätssteuerung. Wenn das Netzwerk mehrere WLSM-Module enthält, verwendet WLSM die Redundanzkonfiguration, um das primäre Modul zu bestimmen.
2. Konfigurieren Sie das WLSM im Authentifizierungsserver als AAA-Client.In Cisco Secure ACS wird dies auf der Seite "Network Configuration" (Netzwerkkonfiguration) beschrieben, auf der Sie diese Attribute für das WLSM definieren:NameIP-AdresseGemeinsamer geheimer SchlüsselAuthentifizierungsmethodeRADIUS Cisco AironetRADIUS-IETFInformationen zu anderen Authentifizierungsservern ohne ACS finden Sie in der Dokumentation des Herstellers.



Konfigurieren Sie außerdem in Cisco Secure ACS ACS für die LEAP-Authentifizierung auf der Seite "System Configuration - Global Authentication Setup" (Systemkonfiguration - Globale Authentifizierungs-Einrichtung). Klicken Sie zuerst auf **Systemkonfiguration** und dann auf **Globales Authentifizierungs-Setup**.



Blättern Sie auf der Seite nach unten zur LEAP-Einstellung. Wenn Sie das Kontrollkästchen aktivieren, authentifiziert ACS
LEAP.



3. Definieren Sie im WLSM eine Methode, die die anderen APs (eine Infrastrukturservergruppe) authentifiziert.
4. Definieren Sie auf dem WLSM eine Methode, die die Client-Geräte (eine Clientservergruppe)

authentifiziert und welche EAP-Typen diese Clients verwenden.**Hinweis:** Mit diesem Schritt ist der Prozess zur Definition der Client-Authentifizierungsmethode nicht mehr erforderlich.

5. Definieren Sie ein eindeutiges VLAN zwischen der Supervisor Engine 720 und dem WLSM, um dem WLSM die Kommunikation mit externen Einheiten wie APs und Authentifizierungsservern zu ermöglichen. Dieses VLAN wird nirgendwo anders oder für andere Zwecke im Netzwerk verwendet. Erstellen Sie zuerst das VLAN auf der Supervisor Engine 720, und geben Sie dann die folgenden Befehle aus:Auf der Supervisor Engine 720:Im WLSM:
6. Überprüfen Sie die Funktion des WLSM mithilfe der folgenden Befehle:Im WLSM:Auf der Supervisor Engine 720:

Festlegen eines Access Points als Infrastrukturgerät

Als Nächstes müssen Sie mindestens einen Infrastruktur-Access Point definieren und den Access Point mit dem WDS verknüpfen. Die Clients sind mit Infrastruktur-APs verknüpft. Die Infrastruktur-APs fordern den WDS-AP oder WLSM an, die Authentifizierung für sie durchzuführen.

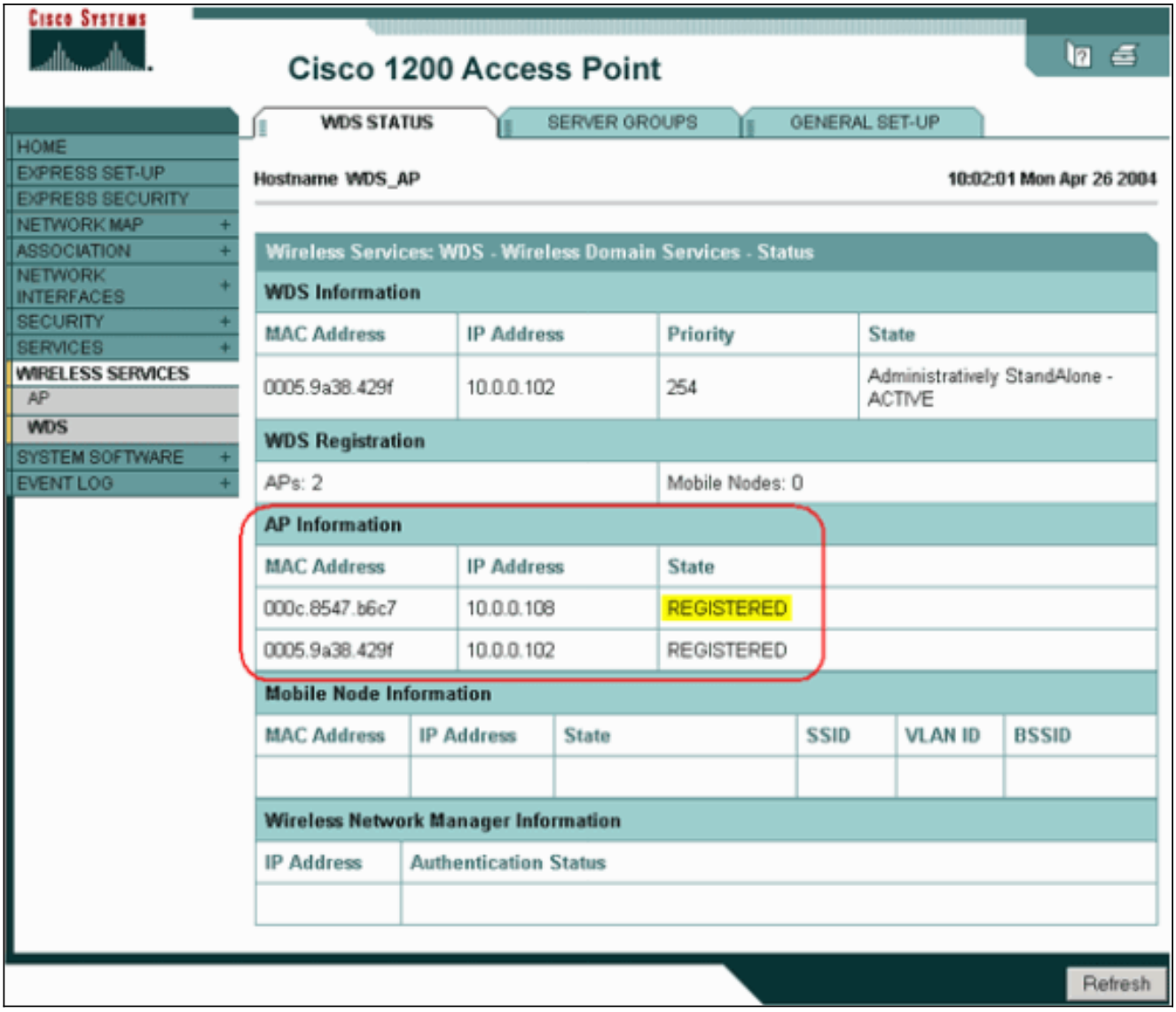
Gehen Sie wie folgt vor, um einen Infrastruktur-Access Point hinzuzufügen, der die Dienste des WDS verwendet:

Hinweis: Diese Konfiguration gilt nur für die Infrastruktur-APs und nicht für den WDS-AP.

1. Wählen Sie **Wireless Services > AP aus**. Wählen Sie im Infrastruktur-Access-Point die Option **Aktivieren** für die Wireless-Services aus. Geben Sie dann den WDS-Benutzernamen und das Kennwort ein.Sie müssen auf dem Authentifizierungsserver einen WDS-Benutzernamen und ein WDS-Kennwort für alle Geräte definieren, die Mitglieder des WDS sein
   sollen.

Alternativ können Sie die folgenden Befehle über die CLI ausführen:

2. Wählen Sie **Wireless Services > WDS aus**. Auf der Registerkarte "WDS AP WDS Status" (WDS-AP-WDS-Status) wird der neue Infrastruktur-AP im Bereich WDS Information (WDS-Informationen) mit Status als ACTIVE (Status als aktiv) und im Bereich AP Information (AP-Informationen) mit Status als REGISTRIERT angezeigt.Wenn der Access Point nicht als aktiv und/oder REGISTRIERT angezeigt wird, überprüfen Sie den Authentifizierungsserver auf Fehler oder fehlgeschlagene Authentifizierungsversuche.Wenn der Access Point aktiv und/oder REGISTRIERT angezeigt wird, fügen Sie dem WDS eine Client-Authentifizierungsmethode
hinzu.



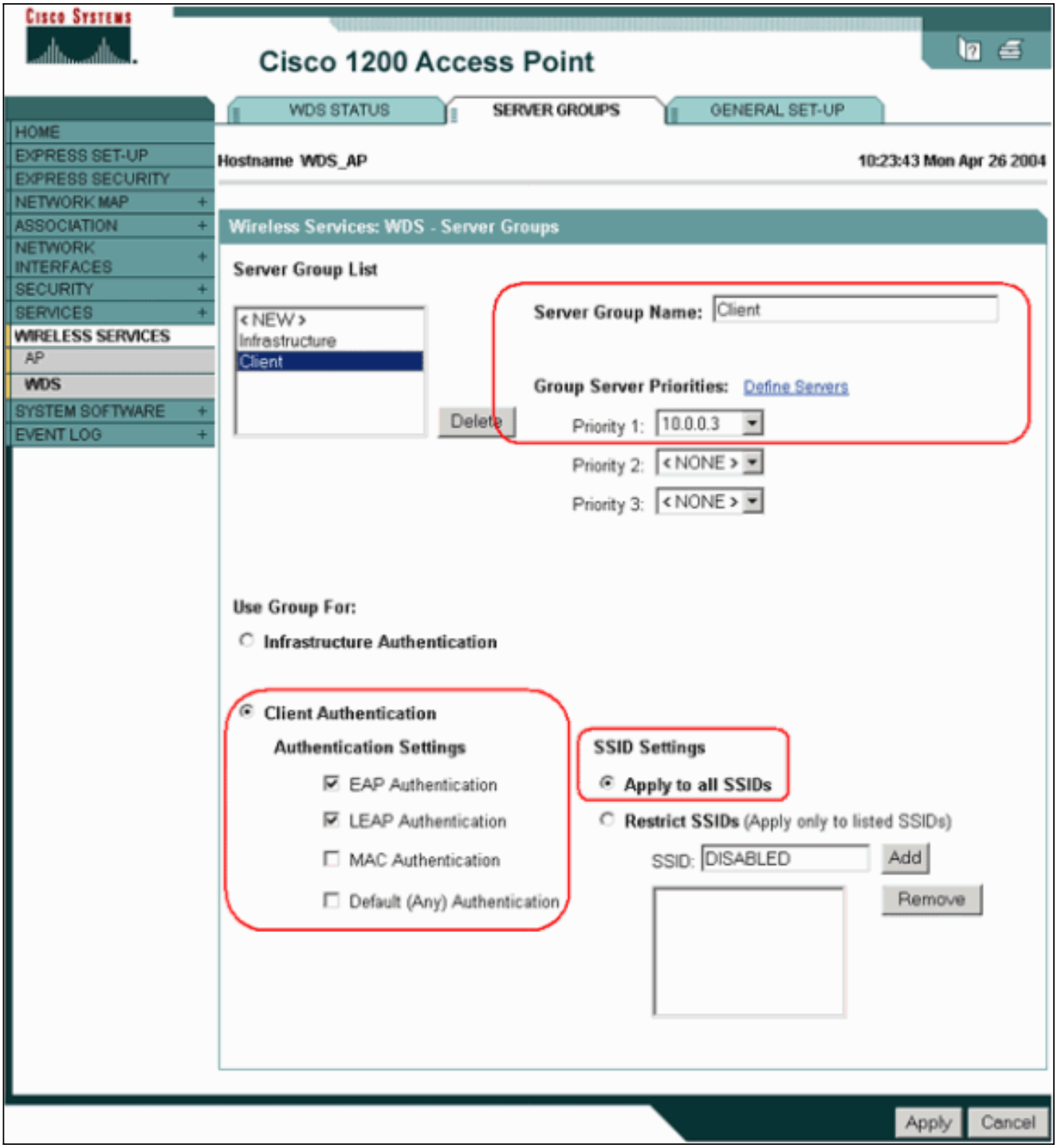
Alternativ können Sie diesen Befehl über die CLI ausführen:Alternativ können Sie diesen Befehl aus dem WLSM ausführen:Führen Sie dann den folgenden Befehl auf dem Infrastruktur-Access Point aus:**Hinweis:** Clientzuordnungen können nicht getestet werden, da die Clientauthentifizierung noch keine Bestimmungen enthält.

Clientauthentifizierungsmethode definieren

Definieren Sie abschließend eine Methode der Clientauthentifizierung.

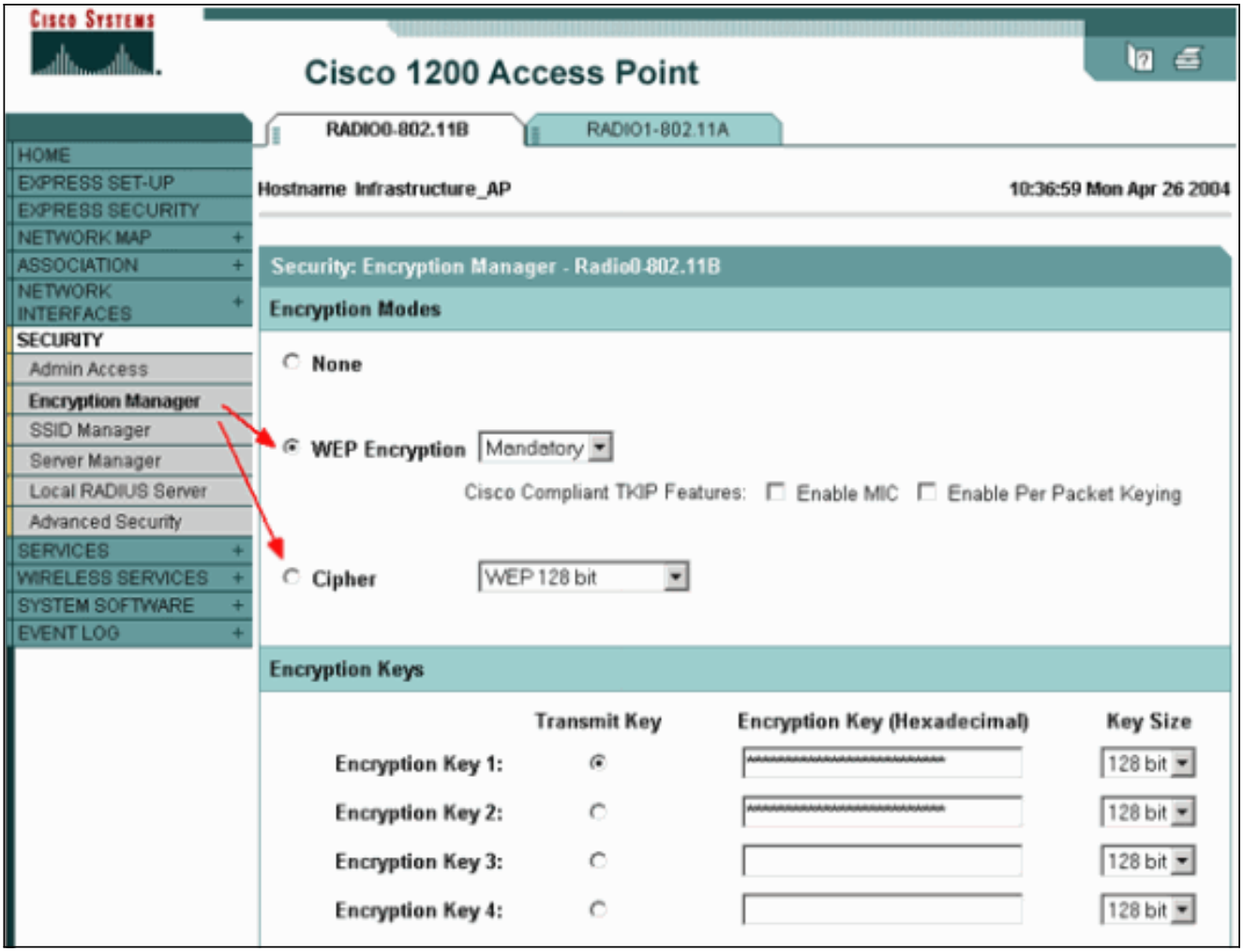
Gehen Sie wie folgt vor, um eine Client-Authentifizierungsmethode hinzuzufügen:

1. Wählen Sie **Wireless Services > WDS aus**. Führen Sie die folgenden Schritte auf der Registerkarte WDS AP-Servergruppen aus:Definieren Sie eine Servergruppe, die Clients authentifiziert (eine Clientgruppe).Legen Sie die Priorität 1 auf den zuvor konfigurierten Authentifizierungsserver fest.Legen Sie den entsprechenden Authentifizierungstyp fest (LEAP, EAP, MAC usw.).Wenden Sie die Einstellungen auf die relevanten SSIDs an.

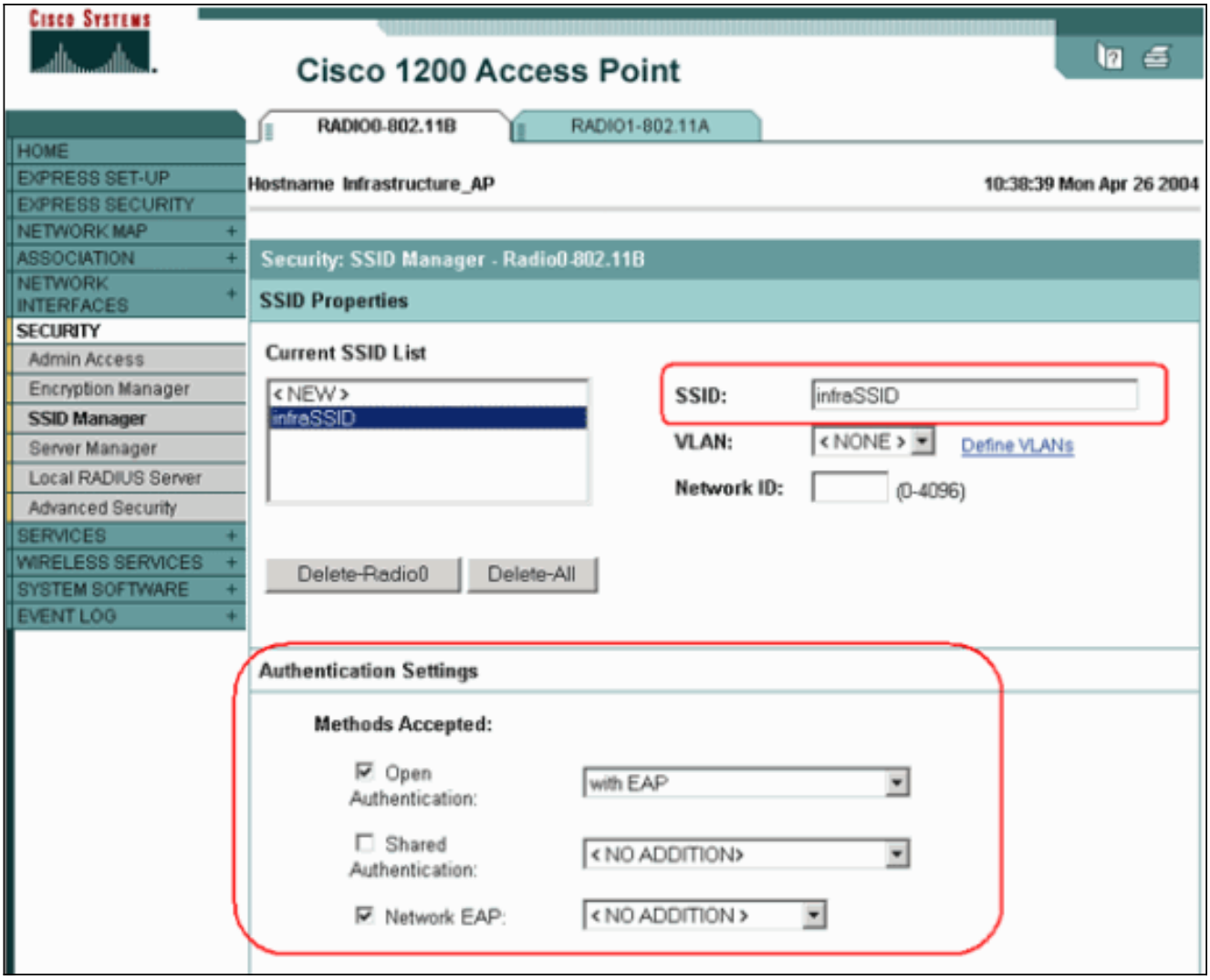


Alternativ können Sie die folgenden Befehle über die CLI ausführen:**Hinweis:** Der WDS-Zugangspunkt ist dediziert und akzeptiert keine Clientzuordnungen.**Hinweis:** Konfigurieren Sie auf den Infrastruktur-APs keine Servergruppen, da Infrastruktur-APs Anfragen an das zu verarbeitende WDS weiterleiten.

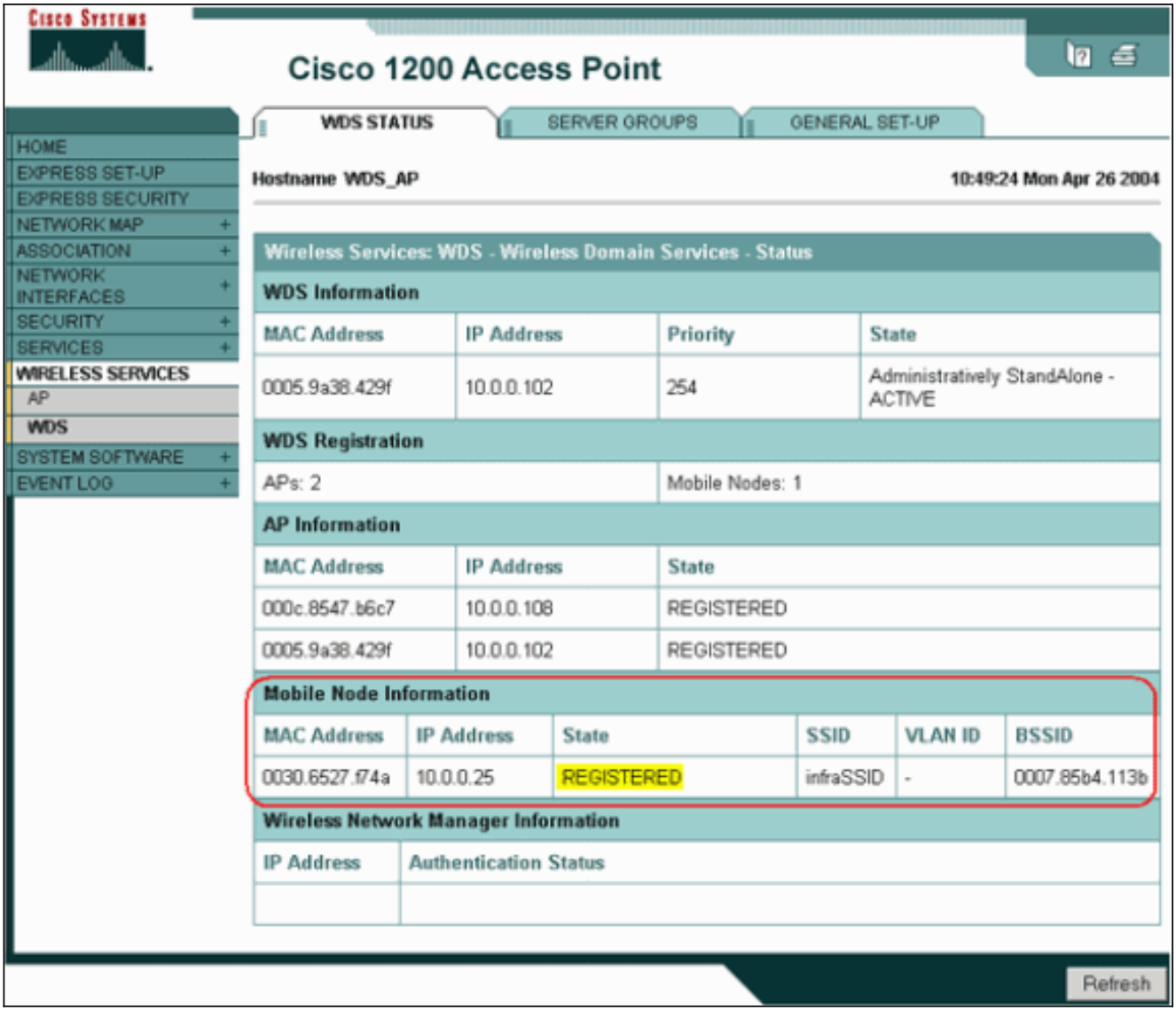
2. Auf den Infrastruktur-APs oder -APs:Klicken Sie unter dem Menüelement **Security > Encryption Manager** auf **WEP Encryption** oder **Cipher**, wie dies für das von Ihnen verwendete Authentifizierungsprotokoll erforderlich ist.



Wählen Sie unter dem Menüelement **Security > SSID Manager** die Authentifizierungsmethoden aus, die für das von Ihnen verwendete Authentifizierungsprotokoll erforderlich sind.



3. Sie können jetzt erfolgreich testen, ob Clients sich bei Infrastruktur-APs authentifizieren. Der WDS-Zugangspunkt auf der Registerkarte WDS Status (unter dem Menüelement **Wireless Services > WDS**) gibt an, dass der Client im Bereich Informationen für mobile Knoten angezeigt wird und über einen REGISTRIERTEN Status verfügt.Wenn der Client nicht angezeigt wird, überprüfen Sie den Authentifizierungsserver auf Fehler oder fehlgeschlagene Authentifizierungsversuche der
Clients.



Alternativ können Sie die folgenden Befehle über die CLI ausführen:**Hinweis:** Wenn Sie die Authentifizierung debuggen müssen, stellen Sie sicher, dass Sie das Debugging auf dem WDS AP durchführen, da der WDS AP das Gerät ist, das mit dem Authentifizierungsserver kommuniziert.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können. Diese Liste enthält einige der allgemeinen Fragen zum WDS-Befehl, um die Nützlichkeit dieser Befehle weiter zu klären:

- **Frage: Welche Einstellungen werden für diese Elemente auf dem WDS-Access Point empfohlen?Radius-Server-TimeoutRadius-Server-DeadtimeTemporal Key Integrity Protocol (TKIP) Message Integrity Check (MIC) Failure Holdoff TimeClient-WartezeitEAP- oder MAC-AuthentifizierungsintervallEAP-Client-Timeout (optional)Antwort:** Es wird empfohlen, die Konfiguration mit den Standardeinstellungen für diese Sondereinstellungen beizubehalten und

diese nur zu verwenden, wenn ein Timing-Problem auftritt.Dies sind die empfohlenen Einstellungen für den WDS Access Point:Deaktivieren Sie **Radius-Server-Timeout**. Dies ist die Anzahl der Sekunden, die ein Access Point auf eine Antwort auf eine RADIUS-Anfrage wartet, bevor er die Anforderung erneut sendet. Der Standardwert ist 5 Sekunden.Deaktivieren Sie **die Radius-Server-Deadtime**. Der RADIUS wird für einen Zeitraum von Minuten durch zusätzliche Anfragen übersprungen, es sei denn, alle Server sind als "Dead" (Deaktiviert) gekennzeichnet.Die Haltezeit für den Ausfall des TKIP-MIC ist standardmäßig auf 60 Sekunden festgelegt. Wenn Sie die Haltezeit aktivieren, können Sie das Intervall in Sekunden eingeben. Wenn der Access Point innerhalb von 60 Sekunden zwei MIC-Ausfälle erkennt, blockiert er alle TKIP-Clients auf dieser Schnittstelle für die hier angegebene Haltezeit.Client Holdoff Time sollte standardmäßig deaktiviert werden. Wenn Sie holdoff aktivieren, geben Sie die Anzahl der Sekunden ein, die der Access Point nach einem Authentifizierungsfehler warten soll, bevor eine nachfolgende Authentifizierungsanfrage verarbeitet wird.EAP oder MAC Reauthentication Interval ist standardmäßig deaktiviert. Wenn Sie die erneute Authentifizierung aktivieren, können Sie das Intervall angeben oder das vom Authentifizierungsserver angegebene Intervall akzeptieren. Wenn Sie das Intervall angeben möchten, geben Sie das Intervall in Sekunden ein, die der Access Point wartet, bevor er die erneute Authentifizierung eines authentifizierten Clients erzwingt.Das EAP-Client-Timeout (optional) beträgt standardmäßig 120 Sekunden. Geben Sie an, wie lange der Access Point auf die Reaktion von Wireless-Clients auf EAP-Authentifizierungsanforderungen warten soll.

- **Frage: Was die TKIP-Haltezeit angeht, so habe ich gelesen, dass diese auf 100 ms und nicht auf 60 Sekunden festgelegt werden sollte. Ich nehme an, es ist auf eine Sekunde im Browser eingestellt, weil dies die niedrigste Zahl ist, die Sie auswählen können.Antwort:** Es wird nicht empfohlen, die Geschwindigkeit auf 100 ms zu setzen, es sei denn, es wird ein Fehler gemeldet, bei dem die einzige Lösung darin besteht, diese Zeit zu erhöhen. Eine Sekunde ist die niedrigste Einstellung.
- **Frage: Unterstützen diese beiden Befehle die Client-Authentifizierung in irgendeiner Weise und werden sie auf dem WDS oder dem Infrastruktur-AP benötigt?radius-server-Attribut 6 on-for-login-authRADIUS-Server-Attribut 6 unterstützen mehrereAntwort:** Diese Befehle unterstützen den Authentifizierungsprozess nicht und werden auf dem WDS oder dem Access Point nicht benötigt.
- **Frage: Auf dem Infrastruktur-Access-Point nehme ich an, dass keine der Einstellungen für den Server Manager und die globalen Eigenschaften erforderlich sind, da der Access Point Informationen vom WDS empfängt. Sind diese spezifischen Befehle für den Infrastruktur-AP erforderlich?radius-server-Attribut 6 on-for-login-authRADIUS-Server-Attribut 6 unterstützen mehrereRadius-Server-TimeoutRadius-Server-DeadtimeAntwort:** Für die Infrastruktur-APs sind weder Server Manager noch globale Eigenschaften erforderlich. Das WDS übernimmt diese Aufgabe, und die folgenden Einstellungen sind nicht erforderlich:**radius-server-Attribut 6 on-for-login-authRADIUS-Server-Attribut 6 unterstützen mehrereRadius-Server-TimeoutRadius-Server-Deadtime**Die Einstellung **für das RADIUS-Serverattribut 32 include-in-access-req format %h** bleibt standardmäßig erhalten und ist erforderlich.

Ein Access Point ist ein Layer-2-Gerät. Daher unterstützt der Access Point keine Layer-3-Mobilität, wenn der Access Point als WDS-Gerät konfiguriert ist. Sie können Layer-3-Mobilität nur erreichen, wenn Sie das WLSM als WDS-Gerät konfigurieren. Weitere Informationen finden Sie im Abschnitt *Layer-3-Mobilitätsarchitektur* des Cisco Catalyst Wireless LAN Services Module der Serie 6500: Whitepaper für weitere Informationen.

Wenn Sie einen Access Point daher als WDS-Gerät konfigurieren, verwenden Sie nicht den

Befehl **mobility network-id**. Dieser Befehl gilt für die Layer-3-Mobilität. Sie benötigen ein WLSM als WDS-Gerät, um die Layer-3-Mobilität ordnungsgemäß konfigurieren zu können. Wenn Sie den Befehl **mobility network-id** falsch verwenden, sehen Sie einige dieser Symptome:

- Wireless-Clients können keine Verbindung zum AP herstellen.
- Wireless-Clients können eine Verbindung zum AP herstellen, erhalten jedoch keine IP-Adresse vom DHCP-Server.
- Ein Wireless-Telefon wird nicht authentifiziert, wenn Sie über eine Voice-over-WLAN-Bereitstellung verfügen.
- Die EAP-Authentifizierung erfolgt nicht. Bei konfigurierter **Mobility-Netzwerk-ID** versucht der Access Point, einen GRE-Tunnel (Generic Routing Encapsulation) zu erstellen, um EAP-Pakete weiterzuleiten. Wenn kein Tunnel eingerichtet ist, gehen die Pakete nirgendwo hin.
- Ein als WDS-Gerät konfigurierter Access Point funktioniert nicht wie erwartet, und die WDS-Konfiguration funktioniert nicht.**Hinweis:** Sie können den Cisco Aironet 1300 AP/Bridge nicht als WDS-Master konfigurieren. Diese Funktionalität wird von der 1300 AP/Bridge nicht unterstützt. Die 1300 AP/Bridge kann als Infrastrukturgerät in einem WDS-Netzwerk verwendet werden, in dem ein anderer AP oder WLSM als WDS-Master konfiguriert ist.

Befehle zur Fehlerbehebung

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

- **debug dot11 aaa authentiator all** - Zeigt die verschiedenen Verhandlungen, die ein Client durchführt, während der Client über den 802.1x- oder EAP-Prozess eine Verbindung herstellt und authentifiziert. Diese Fehlerbehebung wurde in Version 12.2(15)JA der Cisco IOS-Software eingeführt. Dieser Befehl löst **Debug dot11 aaa dot1x alle** in diesen und späteren Versionen aus.
- **debug aaa authentication**: Zeigt den Authentifizierungsprozess aus generischer AAA-Perspektive.
- **debug wlccp ap**: Zeigt die WLCCP-Verhandlungen an, die erforderlich sind, wenn ein Access Point einem WDS beitritt.
- **debug wlccp paket**: Zeigt detaillierte Informationen über WLCCP-Verhandlungen an.
- **debug wlccp leap client** - Zeigt die Details an, wenn ein Infrastrukturgerät einem WDS beitritt.

Zugehörige Informationen

- Konfigurieren von WDS, schnellem sicherem Roaming und Radio-Management
- Konfigurationshinweis für das Catalyst Wireless LAN Services Module der Serie 6500
- Konfigurieren von Cipher-Suiten und WEP
- Konfigurieren von Authentifizierungstypen
- Support-Seiten für Wireless LAN
- Technischer Support und Dokumentation - Cisco Systems