EAP-Authentifizierung mit RADIUS-Server

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration eines Cisco IOS®-basierten Access Points für die EAP-Authentifizierung (Extensible Authentication Protocol) von Wireless-Benutzern für eine Datenbank, auf die von einem RADIUS-Server zugegriffen wird.

Aufgrund der passiven Rolle, die der Access Point im EAP übernimmt (überbrückt Wireless-Pakete vom Client in kabelgebundene Pakete, die für den Authentifizierungsserver bestimmt sind, und umgekehrt), wird diese Konfiguration mit praktisch allen EAP-Methoden verwendet. Zu diesen Methoden gehören (aber nicht beschränkt auf) LEAP, Protected EAP (PEAP)-MS-Challenge Handshake Authentication Protocol (CHAP) Version 2, PEAP-Generic Token Card (GTC), EAP-Flexible Authentication via Secure Tunneling (FAST), EAP-Transport Layer Security (TLS) und EAP-Tunneled TLS (TTLS). Sie müssen den Authentifizierungsserver für jede dieser EAP-Methoden entsprechend konfigurieren.

In diesem Dokument wird erläutert, wie der Access Point (AP) und der RADIUS-Server (Cisco Secure ACS) im Konfigurationsbeispiel dieses Dokuments konfiguriert werden.

Voraussetzungen

Anforderungen

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

- Sie kennen die Cisco IOS-GUI oder -CLI.
- Sie kennen die Konzepte der EAP-Authentifizierung.

Verwendete Komponenten

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

- Cisco Aironet AP-Produkte, die Cisco IOS ausführen.
- Es wird angenommen, dass im Netzwerk nur ein virtuelles LAN (VLAN) vorhanden ist.
- Ein RADIUS-Authentifizierungsserver-Produkt, das erfolgreich in eine Benutzerdatenbank integriert werden kann.Dies sind die unterstützten Authentifizierungsserver für Cisco LEAP und EAP-FAST:Cisco Secure Access Control Server (ACS)Cisco Access Registrar (CAR)Funk Steel Beled RADIUSLink-MergeDies sind die unterstützten Authentifizierungsserver für Microsoft PEAP-MS-CHAP Version 2 und PEAP-GTC:Microsoft Internet Authentication Service (IAS)Cisco Secure ACSFunk Steel Beled RADIUSLink-MergeJeder zusätzliche Authentifizierungsserver, den Microsoft autorisieren kann.**Hinweis:** GTC- oder Einmalkennwörter erfordern zusätzliche Dienste, die zusätzliche Software auf Client- und Serverseite sowie Hardware- oder Software-Token-Generatoren erfordern.Weitere Informationen darüber, welche Authentifizierungsserver mit ihren Produkten für EAP-TLS, EAP-TTLS und andere EAP-Methoden unterstützt werden, erhalten Sie vom Hersteller des Client-Supplicants.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, 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).

Konfigurieren

Diese Konfiguration beschreibt, wie die EAP-Authentifizierung auf einem IOS-basierten Access Point konfiguriert wird. Im Beispiel in diesem Dokument wird LEAP als Methode der EAP-Authentifizierung mit RADIUS-Server verwendet.

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

Wie bei den meisten kennwortbasierten Authentifizierungsalgorithmen ist Cisco LEAP anfällig für Wörterbuchangriffe. Dies ist kein neuer Angriff oder keine neue Schwachstelle von Cisco LEAP. Die Erstellung einer strikten Kennwortrichtlinie ist die effektivste Methode, um Wörterbuchangriffe zu verhindern. Dies umfasst die Verwendung sicherer Passwörter und den regelmäßigen Ablauf von Passwörtern. Unter Dictionary Attack auf Cisco LEAP finden Sie weitere Informationen zu Wörterbuchangriffen und deren Verhinderung.

In diesem Dokument wird diese Konfiguration sowohl für die GUI als auch für die CLI verwendet:

- Die IP-Adresse des Access Points lautet 10.0.0.106.
- Die IP-Adresse des RADIUS-Servers (ACS) lautet 10.0.0.3.

Netzwerk-EAP oder offene Authentifizierung mit EAP

Bei jeder EAP/802.1x-basierten Authentifizierungsmethode können Sie die Unterschiede zwischen Netzwerk-EAP und offener Authentifizierung mit EAP infrage stellen. Diese Elemente beziehen sich auf die Werte im Feld Authentifizierungsalgorithmus in den Headern der Management- und Zuordnungspakete. Die meisten Hersteller von Wireless-Clients setzen dieses Feld auf den Wert 0 (Open Authentication) und signalisieren dann den Wunsch, die EAP-Authentifizierung später im Zuordnungsprozess durchzuführen. Cisco legt den Wert anders fest, als bei Beginn der Verknüpfung mit dem Netzwerk-EAP-Flag.

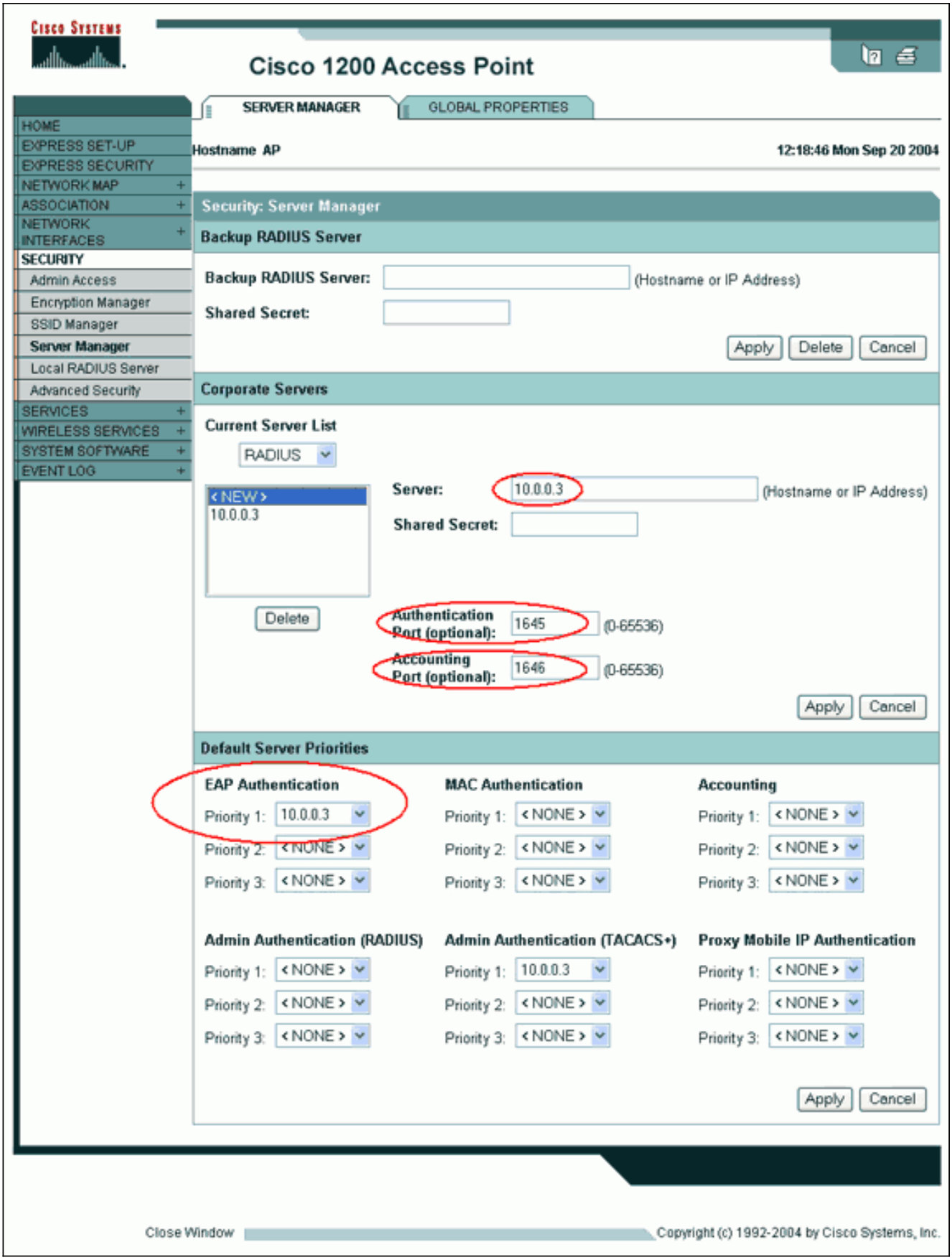
Wenn Ihr Netzwerk über Clients verfügt, die:

- Cisco Clients - Verwenden Sie Network-EAP.
- Drittanbieter-Clients (einschließlich CCX-kompatibler Produkte) - Verwenden Sie Open mit EAP.
- Kombination von Cisco und Drittanbieter-Clients - Wählen Sie Network-EAP und Open mit EAP.

Authentifizierungsserver definieren

Der erste Schritt in der EAP-Konfiguration besteht darin, den Authentifizierungsserver zu definieren und eine Beziehung mit ihm herzustellen.

1. Gehen Sie auf der Registerkarte "Access Point Server Manager" (unter der Menüoption **Security > Server Manager**) wie folgt vor:Geben Sie die IP-Adresse des Authentifizierungsservers im Feld Server ein.Geben Sie den Shared Secret und die Ports an.Klicken Sie auf **Apply**, um die Definition zu erstellen und die Dropdown-Listen zu füllen.Legen Sie unter "Default Server Priorities" (Standardserverprioritäten) das Feld "EAP Authentication Type Priority 1" (EAP-Authentifizierungstyp Priorität 1) auf die Server-IP-Adresse fest.Klicken Sie auf **Übernehmen**.

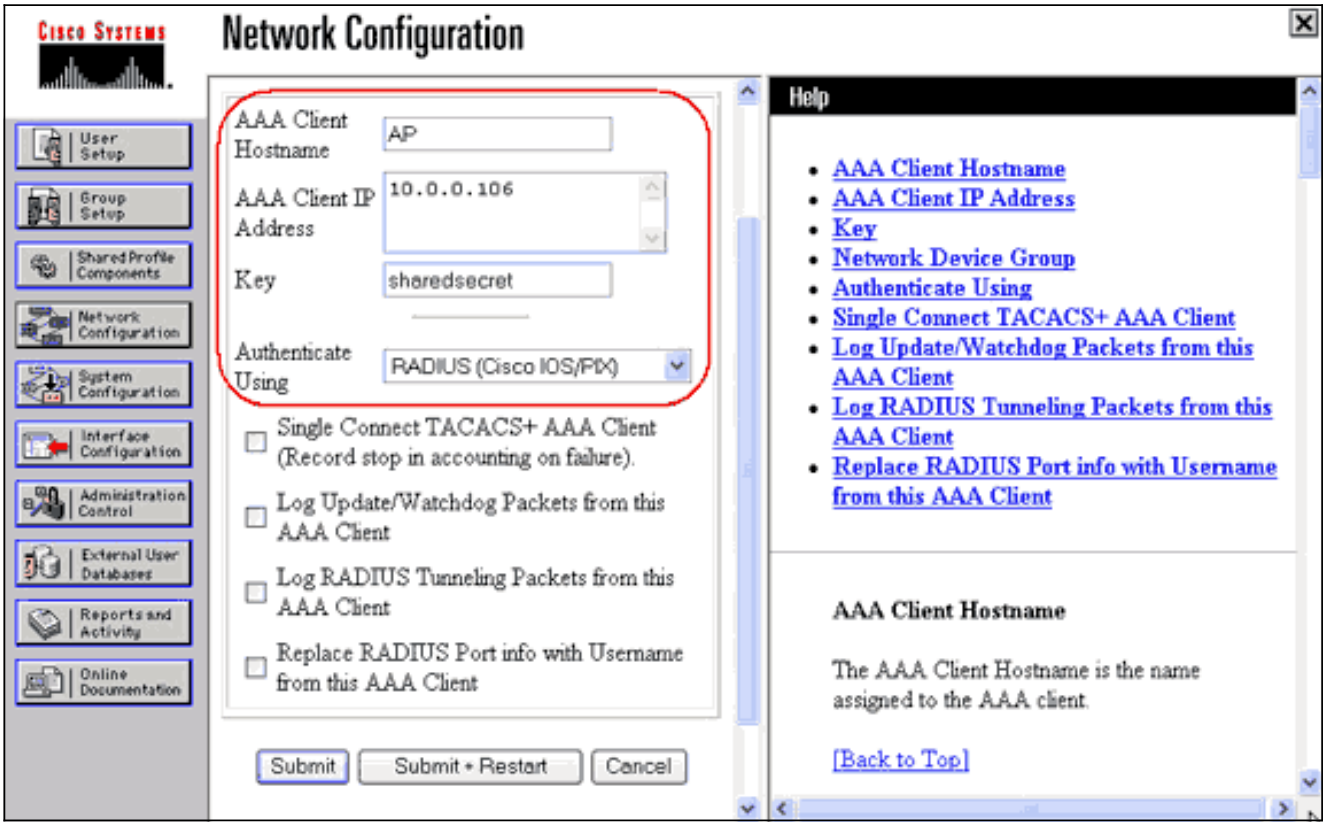


Sie können diese Befehle auch über die CLI ausführen:

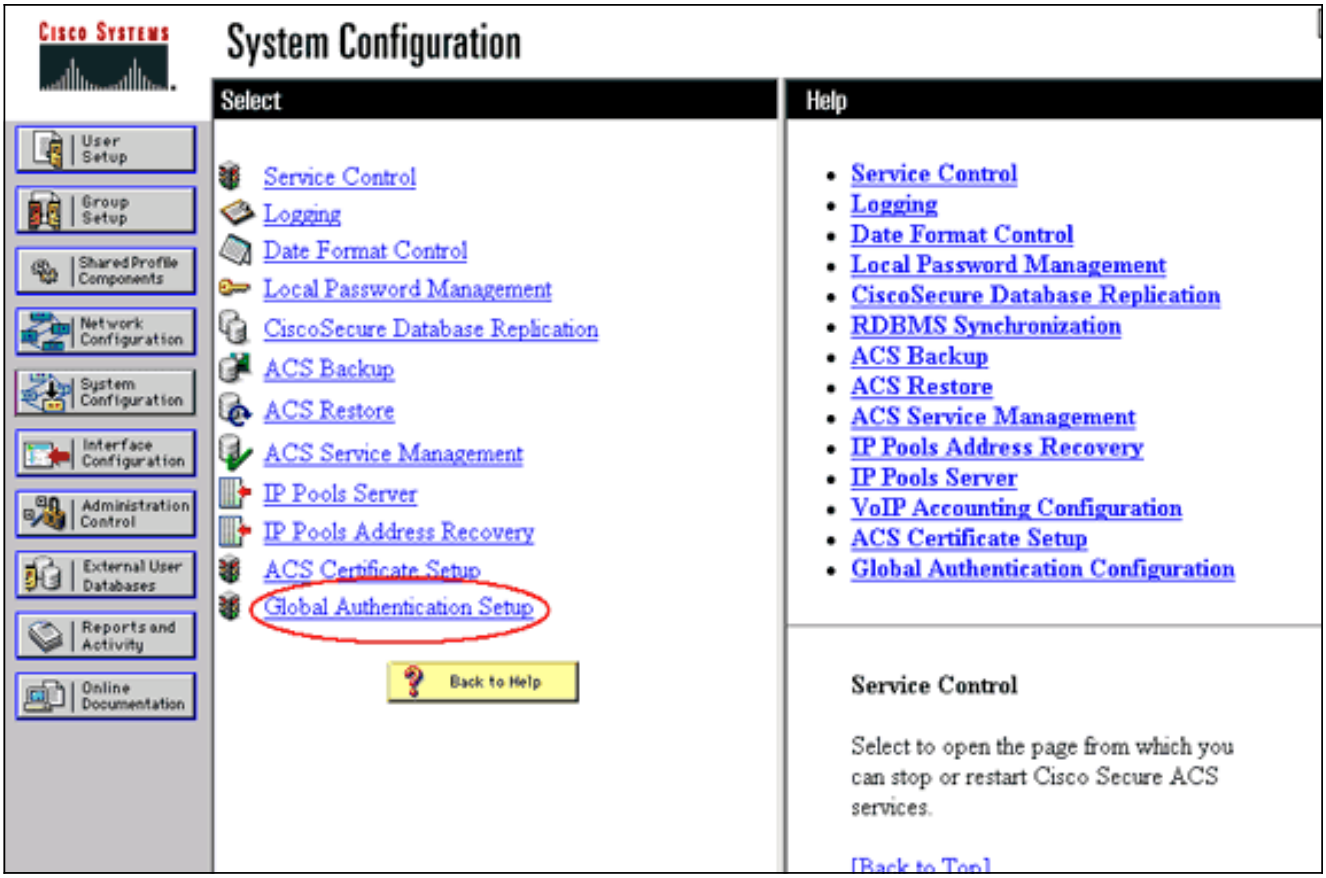
```
AP#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

AP(config)#aaa group server radius rad_eap

AP(config-sg-radius)#server 10.0.0.3 auth-port 1645 acct-port 1646
```

```
AP(config-sg-radius)#exit

AP(config)#aaa new-model

AP(config)#aaa authentication login eap_methods group rad_eap

AP(config)#radius-server host 10.0.0.3 auth-port 1645
acct-port 1646 key labap1200ip102

AP(config)#end

AP#write memory
```

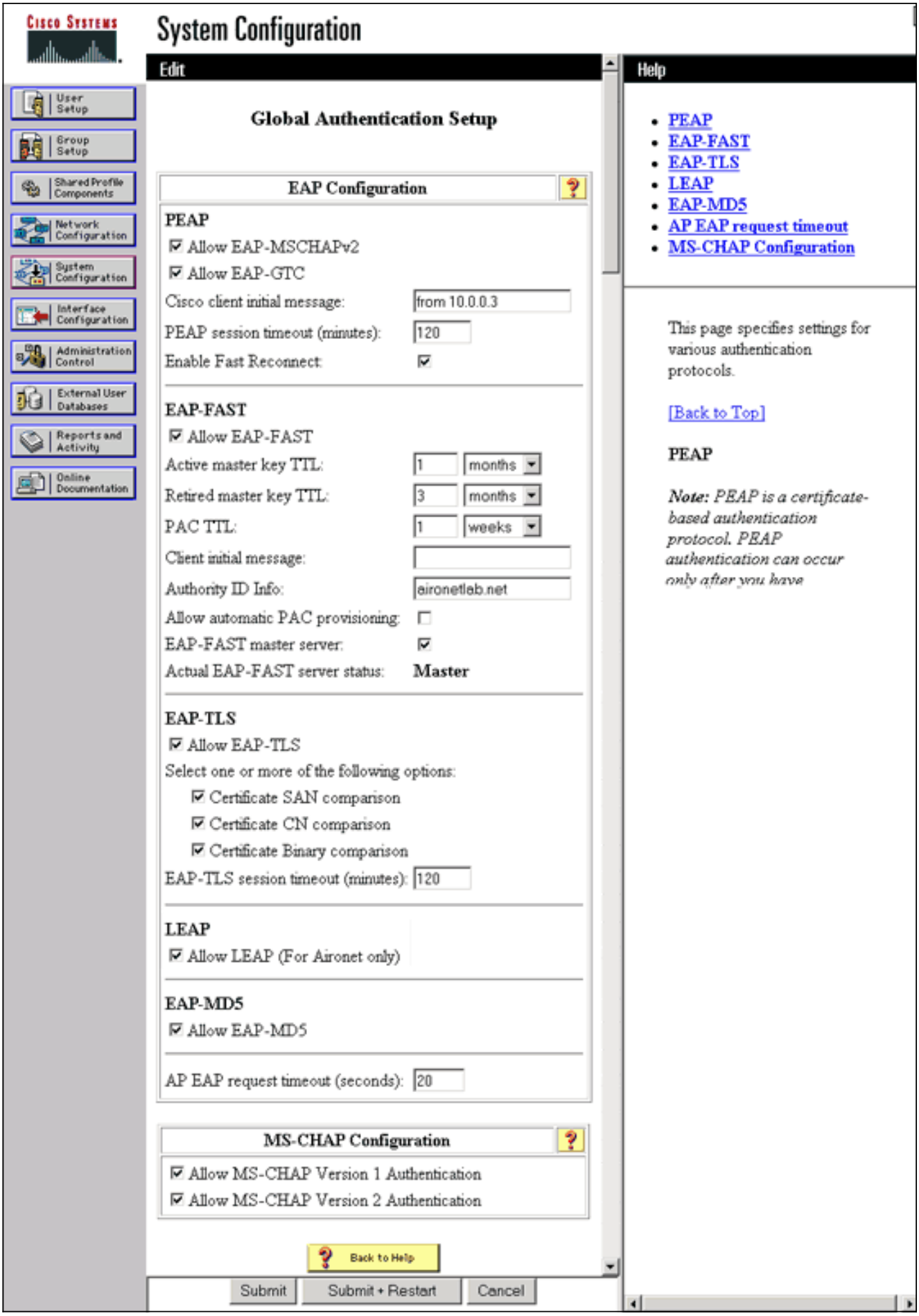
2. Der Access Point muss im Authentifizierungsserver als AAA-Client konfiguriert werden.In Cisco Secure ACS erfolgt dies beispielsweise auf der Seite Network Configuration (Netzwerkkonfiguration), auf der der Name des Access Points, die IP-Adresse, der gemeinsam genutzte geheime Schlüssel und die Authentifizierungsmethode (RADIUS Cisco Aironet oder RADIUS Cisco IOS/PIX) definiert sind. Informationen zu anderen Nicht-ACS-Authentifizierungsservern finden Sie in der Dokumentation des Herstellers.



Stellen Sie sicher, dass der Authentifizierungsserver so konfiguriert ist, dass er die gewünschte EAP-Authentifizierungsmethode ausführt. Bei einem Cisco Secure ACS, der LEAP ausführt, konfigurieren Sie beispielsweise die LEAP-Authentifizierung auf der Seite System Configuration - Global Authentication Setup (Systemkonfiguration - Globale Authentifizierung). Klicken Sie auf **Systemkonfiguration** und anschließend auf **Globales Authentifizierungs-Setup**. Weitere Nicht-ACS-Authentifizierungsserver oder andere EAP-Methoden finden Sie in der Dokumentation des Herstellers.



Dieses Bild zeigt Cisco Secure ACS, konfiguriert für PEAP, EAP-FAST, EAP-TLS, LEAP und EAP-
MD5.

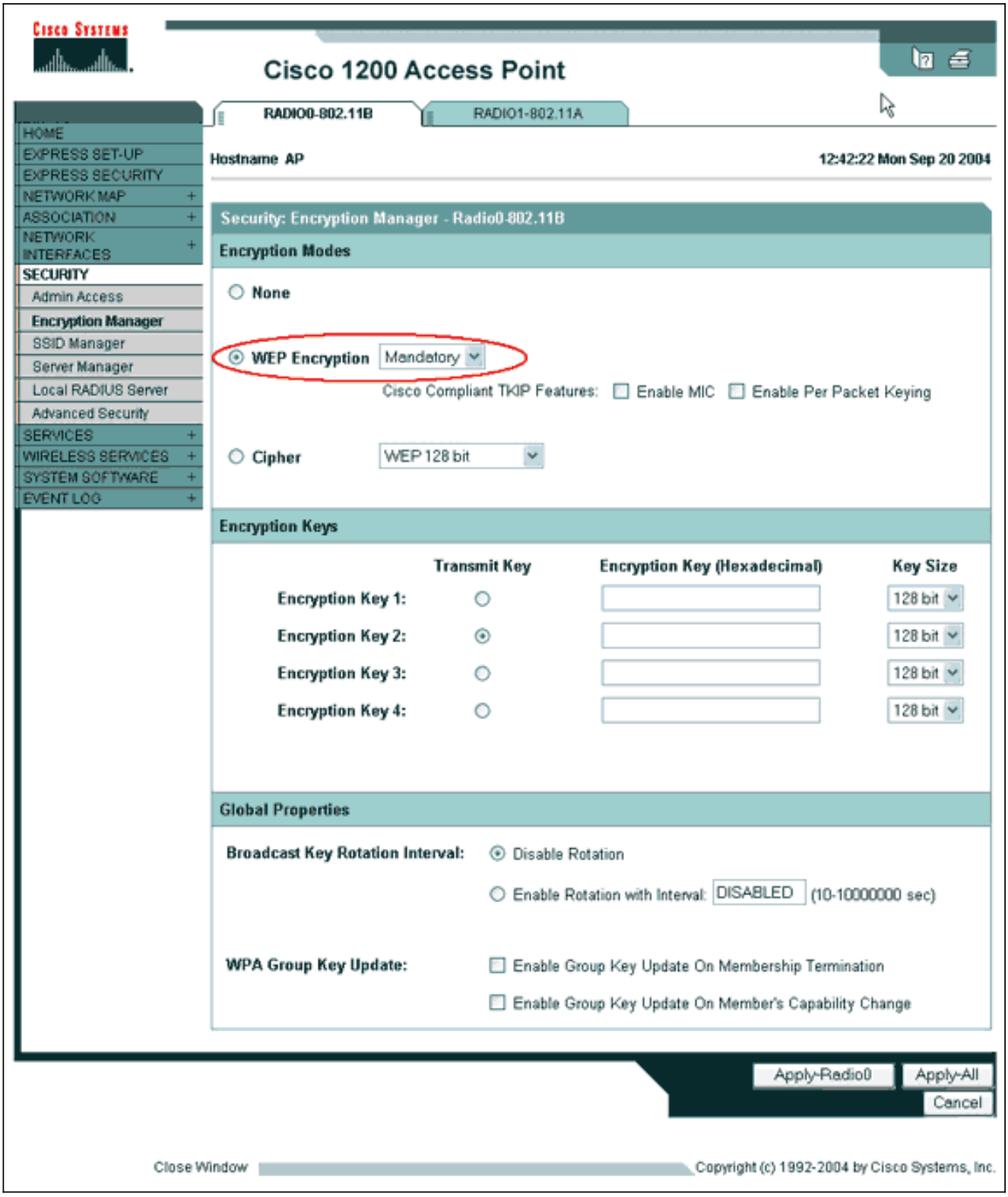


[Definieren von Client-Authentifizierungsmethoden]

Sobald der Access Point weiß, wohin er Client-Authentifizierungsanforderungen senden soll, konfigurieren Sie ihn so, dass er diese Methoden akzeptiert.

Hinweis: Diese Anweisungen gelten für eine WEP-basierte Installation. Informationen zu WPA (das statt WEP Chiffren verwendet) finden Sie unter Übersicht über die WPA-Konfiguration.

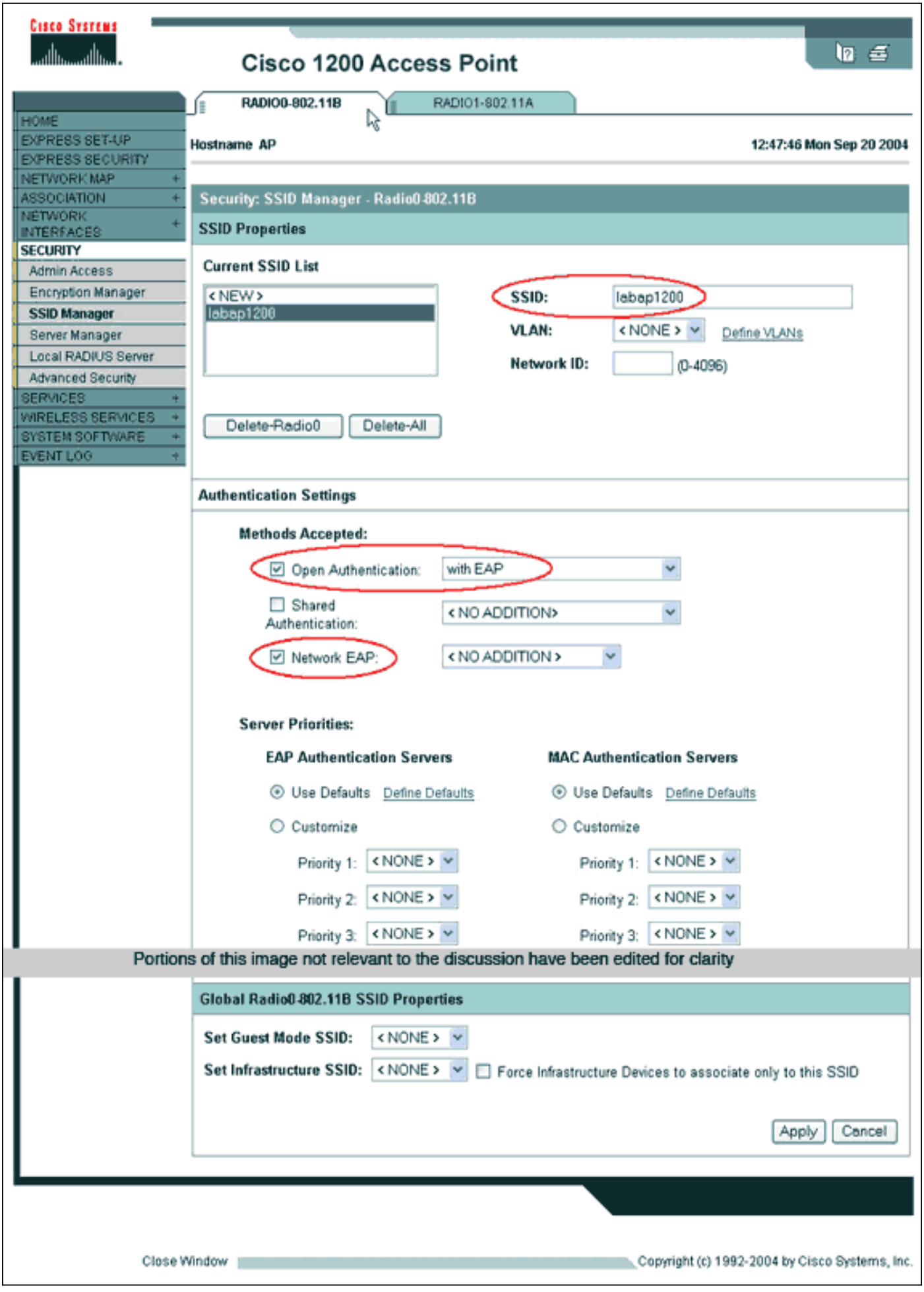
1. Gehen Sie auf der Registerkarte "Access Point Encryption Manager" (**Sicherheit > Verschlüsselungs-Manager**) wie folgt vor:Geben Sie an, dass Sie die **WEP-Verschlüsselung** verwenden möchten.Angeben, dass WEP **obligatorisch** ist.Stellen Sie sicher, dass die Schlüssellänge auf **128 Bit** eingestellt ist.Klicken Sie auf **Übernehmen**.



Sie können diese Befehle auch über die CLI ausführen:

```
AP#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

AP(config)#interface dot11radio 0

AP(config-if)#encryption mode wep mandatory

AP(config-if)#end

AP#write memory
```

2. Führen Sie die folgenden Schritte auf der Registerkarte "SSID Manager" des Access Points aus (unter dem Menüelement **Security > SSID Manager**):Wählen Sie die gewünschte SSID aus.Aktivieren Sie unter "Authentifizierungsmethoden akzeptiert" das Kontrollkästchen **Öffnen**, und wählen Sie in der Dropdown-Liste **With EAP aus**.Aktivieren Sie das Kontrollkästchen **Network-EAP**, wenn Sie über Cisco Client-Karten verfügen. Siehe Diskussion im Abschnitt Network EAP oder Open Authentication with EAP.Klicken Sie auf **Übernehmen**.



Sie können diese Befehle auch über die CLI ausführen:

```
AP#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

AP(config)#interface dot11radio 0

AP(config-if)#ssid labap1200

AP(config-if-ssid)#authentication open eap eap_methods

AP(config-if-ssid)#authentication network-eap eap_methods

AP(config-if-ssid)#end

AP#write memory
```

Wenn Sie die grundlegende Funktionalität mit einer grundlegenden EAP-Konfiguration bestätigen, können Sie zu einem späteren Zeitpunkt zusätzliche Funktionen und eine Schlüsselverwaltung hinzufügen. Vereinfachen Sie die Fehlerbehebung durch komplexere Funktionen auf funktionalen Fundamenten.

Überprüfen

Dieser Abschnitt enthält Informationen zur Bestätigung, dass Ihre Konfiguration ordnungsgemäß funktioniert.

Bestimmte **show**-Befehle werden vom Output Interpreter Tool unterstützt (nur registrierte Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

- **show radius server-group all**: Zeigt eine Liste aller konfigurierten RADIUS-Servergruppen im Access Point an.

Fehlerbehebung

Fehlerbehebungsverfahren

Führen Sie diese Schritte aus, um eine Fehlerbehebung für Ihre Konfiguration durchzuführen.

1. Erstellen Sie im clientseitigen Dienstprogramm oder in der clientseitigen Software ein neues Profil oder eine neue Verbindung mit denselben oder ähnlichen Parametern, um sicherzustellen, dass die Konfiguration des Clients nicht beschädigt wird.
2. Um Funkprobleme zu vermeiden, die eine erfolgreiche Authentifizierung verhindern, deaktivieren Sie vorübergehend die Authentifizierung, wie in den folgenden Schritten gezeigt:Verwenden Sie in der CLI die Befehle **no authentication open eap_methods**, **no authentication network-eap eap_methods** und **authentication open**.Deaktivieren Sie in der GUI auf der Seite SSID Manager die Option **Network-EAP**, aktivieren Sie **Open (Öffnen)**, und setzen Sie die Dropdown-Liste auf **No Addition (Kein Hinzufügen)** zurück.Wenn der Client erfolgreich eine Zuordnung vornimmt, trägt RF nicht zum Zuordnungsproblem bei.
3. Überprüfen Sie, ob die gemeinsamen geheimen Kennwörter zwischen dem Access Point und dem Authentifizierungsserver synchronisiert werden. Andernfalls können Sie die folgende

Fehlermeldung erhalten:
`Invalid message authenticator in EAP request`
Aktivieren Sie in der CLI den `RADIUS-Server-Host x.x.x auth-port x acct-port x-key <shared_secret>`.Geben Sie auf der Seite "Server Manager" in der GUI erneut den freigegebenen geheimen Schlüssel für den entsprechenden Server in das Feld "Shared Secret" (Gemeinsam genutzter geheimer Schlüssel) ein.Der gemeinsame geheime Eintrag für den Access Point auf dem RADIUS-Server muss das gleiche geheime Kennwort enthalten wie zuvor.

4. Entfernen Sie alle Benutzergruppen aus dem RADIUS-Server. Manchmal können Konflikte zwischen vom RADIUS-Server definierten Benutzergruppen und Benutzergruppen in der zugrunde liegenden Domäne auftreten. Überprüfen Sie die Protokolle des RADIUS-Servers auf fehlgeschlagene Versuche, und geben Sie an, warum diese Versuche fehlgeschlagen sind.

Fehlerbehebung bei Befehlen

Bestimmte **show**-Befehle werden vom Output Interpreter Tool unterstützt (nur registrierte Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

Debuggen-Authentifizierungen bieten eine Menge Details zum Erfassen und Interpretieren der Ausgabe von Debuggen in Bezug auf EAP.

Hinweis: Bevor Sie **Debugbefehle** ausgeben, lesen Sie die Informationen Wichtige Informationen über Debug-Befehle.

- **debug dot11 aaa authentifizierer state-machine**: Zeigt wichtige Abteilungen (oder Zustände) der Verhandlung zwischen dem Client und dem Authentifizierungsserver an. Im Folgenden finden Sie eine Ausgabe einer **erfolgreichen** Authentifizierung:

```
*Mar 1 02:37:46.846: dot11_auth_dot1x_send_id_req_to_client: Sending
identity request to 0040.96ac.dd05
*Mar 1 02:37:46.846: dot11_auth_dot1x_send_id_req_to_client:
0040.96ac.dd05 timer started for 30 seconds
*Mar 1 02:37:46.930: dot11_auth_dot1x_run_rfsm: Executing
Action(CLIENT_WAIT,EAP_START) for 0040.96ac.dd05
*Mar 1 02:37:46.931: dot11_auth_dot1x_send_id_req_to_client:
Sending identity request to 0040.96ac.dd05 (client)
*Mar 1 02:37:46.931: dot11_auth_dot1x_send_id_req_to_client: Client
0040.96ac.dd05 timer started for 30 seconds
*Mar 1 02:37:46.938: dot11_auth_dot1x_run_rfsm: Executing
Action(CLIENT_WAIT,CLIENT_REPLY) for 0040.96ac.dd05
*Mar 1 02:37:46.938: dot11_auth_dot1x_send_response_to_server:
Sending client 0040.96ac.dd05 data (User Name) to server
*Mar 1 02:37:46.938: dot11_auth_dot1x_send_response_to_server:
Started timer server_timeout 60 seconds
*Mar 1 02:37:47.017: dot11_auth_dot1x_run_rfsm: Executing
Action(SERVER_WAIT,SERVER_REPLY) for 0040.96ac.dd05
*Mar 1 02:37:47.017: dot11_auth_dot1x_send_response_to_client:
Forwarding server message(Challenge) to client 0040.96ac.dd05
*Mar 1 02:37:47.018: dot11_auth_dot1x_send_response_to_client:
Started timer client_timeout 20 seconds
*Mar 1 02:37:47.025: dot11_auth_dot1x_run_rfsm: Executing
Action(CLIENT_WAIT,CL IENT_REPLY) for 0040.96ac.dd05
*Mar 1 02:37:47.025: dot11_auth_dot1x_send_response_to_server:
Sending client 0040.96ac.dd05 data(User Credentials) to server
------------------Lines Omitted for simplicity------------------
*Mar 1 02:37:47.030: dot11_auth_dot1x_send_response_to_client:
```

```
Started timer client_timeout 20 seconds
*Mar 1 02:37:47.041: dot11_auth_dot1x_run_rfsm: Executing Action
(SERVER_WAIT,SE RVER_PASS) for 0040.96ac.dd05
*Mar 1 02:37:47.041: dot11_auth_dot1x_send_response_to_client:
Forwarding server message(Pass Message) to client
0040.96ac.dd05
*Mar 1 02:37:47.042: dot11_auth_dot1x_send_response_to_client:
Started timer client_timeout 30 seconds
*Mar 1 02:37:47.043: %DOT11-6-ASSOC: Interface Dot11Radio0,
Station TACWEB 0040 .96ac.dd05 Associated KEY_MGMT[NONE] (Client stays
associated to the access point)
```

Hinweis: In Cisco IOS Software-Versionen, die älter als 12.2(15)JA sind, lautet die Syntax dieses Debug-Befehls debug dot1a dot1x state-machine.

- debug dot11 aaa authentifizierer process: Zeigt die einzelnen Dialogeinträge der Verhandlung zwischen dem Client und dem Authentifizierungsserver an.Hinweis: In Cisco IOS Software-Versionen, die älter als 12.2(15)JA sind, lautet die Syntax dieses Befehls debug dot11 aaa dot1x process.
- debug radius authentication: Zeigt die RADIUS-Verhandlungen zwischen Server und Client an, die beide vom Access Point überbrückt werden. Dies ist eine Ausgabe für fehlgeschlagene Authentifizierung:

```
*Mar 1 02:34:55.086: RADIUS/ENCODE(00000031):Orig. component type = DOT11
*Mar 1 02:34:55.086: RADIUS: AAA Unsupported Attr: ssid [264] 5
*Mar 1 02:34:55.086: RADIUS: 73 73 69 [ssi]
*Mar 1 02:34:55.086: RADIUS: AAA Unsupported Attr: interface [157] 3
*Mar 1 02:34:55.087: RADIUS: 32 [2]
*Mar 1 02:34:55.087: RADIUS(00000031): Config NAS IP: 10.0.0.106
*Mar 1 02:34:55.087: RADIUS/ENCODE(00000031): acct_session_id: 47
*Mar 1 02:34:55.087: RADIUS(00000031): Config NAS IP: 10.0.0.106
*Mar 1 02:34:55.087: RADIUS(00000031): sending
*Mar 1 02:34:55.087: RADIUS(00000031): Send Access-Request
to 10.0.0.3 :164 5 id 1645/61, len 130
*Mar 1 02:34:55.088: RADIUS: authenticator 0F 6D B9 57 4B A3 F2 0E -
56 77 A4 7E D3 C2 26 EB
*Mar 1 02:34:55.088: RADIUS: User-Name [1] 8 "wirels"
*Mar 1 02:34:55.088: RADIUS: Framed-MTU [12] 6 1400
*Mar 1 02:34:55.088: RADIUS: Called-Station-Id [30] 16 "0019.a956.55c0"
*Mar 1 02:34:55.088: RADIUS: Calling-Station-Id [31] 16 "0040.96ac.dd05"
*Mar 1 02:34:55.088: RADIUS: Service-Type [6] 6 Login [1]
*Mar 1 02:34:55.088: RADIUS: Message-Authenticato[80] 18
*Mar 1 02:34:55.089: RADIUS: 73 8C 59 C4 98 51 53 9F 58 4D 1D EB A5
4A AB 88 [s?Y??QS?XM???J??]
*Mar 1 02:34:55.089: RADIUS: EAP-Message [79] 13
*Mar 1 02:34:55.089: RADIUS: NAS-Port-Id [87] 5 "299"
*Mar 1 02:34:55.090: RADIUS: NAS-IP-Address [4] 6 10.0.0.106
*Mar 1 02:34:55.090: RADIUS: Nas-Identifier [32] 4 "ap"
*Mar 1 02:34:55.093: RADIUS: Received from id 1645/61
10.0.0.3 :1645, Access-Challenge, len 79
*Mar 1 02:34:55.093: RADIUS: authenticator 72 FD C6 9F A1 53 8F D2 -
84 87 49 9B B4 77 B8 973
--------------------------Lines Omitted----------------------------------
*Mar 1 02:34:55.117: RADIUS(00000031): Config NAS IP: 10.0.0.106
*Mar 1 02:34:55.118: RADIUS/ENCODE(00000031): acct_session_id: 47
*Mar 1 02:34:55.118: RADIUS(00000031): Config NAS IP: 10.0.0.106
*Mar 1 02:34:55.118: RADIUS(00000031): sending
*Mar 1 02:34:55.118: RADIUS(00000031): Send Access-Request to
10.0.0.3 :164 5 id 1645/62, len 168
*Mar 1 02:34:55.118: RADIUS: authenticator 49 AE 42 83 C0 E9 9A A7 -
07 0F 4E 7C F4 C7 1F 24
*Mar 1 02:34:55.118: RADIUS: User-Name [1] 8 "wirels"
```

```
*Mar 1 02:34:55.119: RADIUS: Framed-MTU [12] 6 1400
---------------------------------Lines Omitted----------------------
*Mar 1 02:34:55.124: RADIUS: Received from id 1645/62
10.0.0.3 :1645, Access-Reject, len 56
*Mar 1 02:34:55.124: RADIUS: authenticator A6 13 99 32 2A 9D A6 25 -
AD 01 26 11 9A F6 01 37
*Mar 1 02:34:55.125: RADIUS: EAP-Message [79] 6
*Mar 1 02:34:55.125: RADIUS: 04 15 00 04 [????]
*Mar 1 02:34:55.125: RADIUS: Reply-Message [18] 12
*Mar 1 02:34:55.125: RADIUS: 52 65 6A 65 63 74 65 64 0A 0D
[Rejected??]
*Mar 1 02:34:55.125: RADIUS: Message-Authenticato[80] 18
*Mar 1 02:34:55.126: RADIUS(00000031): Received from id 1645/62
*Mar 1 02:34:55.126: RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes
*Mar 1 02:34:55.126: RADIUS/DECODE: Reply-Message fragments, 10, total 10 bytes
*Mar 1 02:34:55.127: %DOT11-7-AUTH_FAILED: Station
0040.96ac.dd05 Authentication failed
```

- **debug aaa authentication**: Zeigt die AAA-Verhandlungen für die Authentifizierung zwischen dem Clientgerät und dem Authentifizierungsserver an.

Zugehörige Informationen

- Debugauthentifizierungen
- Konfigurieren von Authentifizierungstypen
- LEAP-Authentifizierung auf einem lokalen RADIUS-Server
- Konfigurieren von RADIUS- und TACACS+-Servern
- Konfigurieren von Cisco Secure ACS für Windows 3.2 mit PEAP-MS-CHAPv2-Computerauthentifizierung
- Cisco Secure ACS für Windows 3.2 mit EAP-TLS-Computerauthentifizierung
- Konfigurieren von PEAP/EAP auf Microsoft IAS
- Fehlerbehebung bei Microsoft IAS als RADIUS-Server
- Microsoft 802.1X-Authentifizierungs-Client
- Technischer Support und Dokumentation - Cisco Systems