RADIUS サーバとの EAP 認証

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[表記法](#)
[設定](#)
[ネットワーク EAP または EAP を使用したオープン認証](#)
[認証サーバの定義](#)
[クライアントの認証方式の定義](#)
[確認](#)
[トラブルシュート](#)
[トラブルシューティングの手順](#)
[トラブルシューティングのためのコマンド](#)
[関連情報](#)

概要

このドキュメントでは、Extensible Authentication Protocol（EAP）を使用して、RADIUS サーバからアクセスされるデータベースに対して無線ユーザを認証できるように Cisco IOS® ベースのアクセス ポイントを設定する例を紹介しています。

EAP においてアクセス ポイントは、クライアントから送出された無線パケットを認証サーバ宛ての有線パケットにブリッジするか、その逆の処理を行うというパッシブ ロールを担っているため、この設定は事実上あらゆる EAP 方式で使用されます。このような方式には、LEAP、Protected EAP（PEAP）-MS-Challenge Handshake Authentication Protocol（CHAP）バージョン 2、PEAP-Generic Token Card（GTC）、EAP-Flexible Authentication via Secure Tunneling（FAST）、EAP-Transport Layer Security（TLS）、EAP-Tunneled TLS（TTLS）などがあります（これらだけに限られません）。 このような EAP 方式ごとに認証サーバを適切に設定する必要があります。

このドキュメントでは、Access Point（AP; アクセス ポイント）および RADIUS サーバ（このドキュメントの設定例では Cisco Secure ACS）の設定方法について説明しています。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- Cisco IOS GUI または CLI に精通していること。
- EAP 認証の背景にあるコンセプトに精通していること。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco IOS が稼働する Cisco Aironet AP 製品。
- ネットワーク内に Virtual LAN（VLAN; 仮想 LAN）は 1 つしか存在しないものとします。
- ユーザ データベースに正常に統合される RADIUS 認証サーバ製品。Cisco LEAP および EAP-FAST でサポートされる認証サーバを次に示します。Cisco Secure Access Control Server（ACS）Cisco Access Registrar（CAR）Funk Software Steel-Belted RADIUSInterlink MeritMicrosoft PEAP-MS-CHAP バージョン 2 および PEAP-GTC でサポートされる認証サーバを次に示します。Microsoft Internet Authentication Service（IAS）Cisco Secure ACSFunk Software Steel-Belted RADIUSInterlink MeritMicrosoft が認可できる追加の認証サーバ。**注**：GTCまたはワンタイムパスワードには、クライアント側とサーバ側の両方に追加のソフトウェアが必要な追加サービスと、ハードウェアまたはソフトウェアのトークンジェネレータが必要です。EAP-TLS や EAP-TTLS などの EAP 方式の製品でサポートされている認証サーバについての詳細は、クライアント サプリカントの製造業者にお問い合わせください。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

この設定は、IOS ベースの AP 上で EAP 認証を設定する方法を記述しています。このドキュメントの例では、RADIUS サーバによる EAP 認証の方式として LEAP を使用しています。

注：このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

ほとんどのパスワード ベースの認証アルゴリズムと同様、Cisco LEAP は辞書攻撃に対して脆弱です。辞書攻撃は新しい攻撃でもなければ、Cisco LEAP の新しい脆弱性でもありません。強力なパスワード ポリシーを作成することが、辞書攻撃を緩和する最も有効な方法です。具体的には、強力なパスワードを使用することや、パスワードを定期的に期限切れにすることなどがあります。辞書攻撃と辞書攻撃の防止方法の詳細は、『Cisco LEAP に対する辞書攻撃』を参照してください。

このドキュメントでは、GUI と CLI の両方で次の設定を使用しています。

- AP の IP アドレスは 10.0.0.106 です。
- RADIUS サーバ（ACS）の IP アドレスは 10.0.0.3 です。

ネットワーク EAP または EAP を使用したオープン認証

EAP/802.1x ベースの認証方式では、ネットワーク EAP と EAP を使用したオープン認証の違いについて疑問に思われるかもしれません。これらの項目は、管理パケットおよびアソシエーション パケットのヘッダー内にある Authentication Algorithm フィールドの値を指しています。無線クライアントのほとんどの製造業者は、このフィールドの値を 0（オープン認証）に設定しており、後のアソシエーション プロセスで EAP 認証を行いたいという要望を通知します。シスコは、アソシエーションの始めから、ネットワーク EAP フラグを使ってこの値を別の方法で設定します。

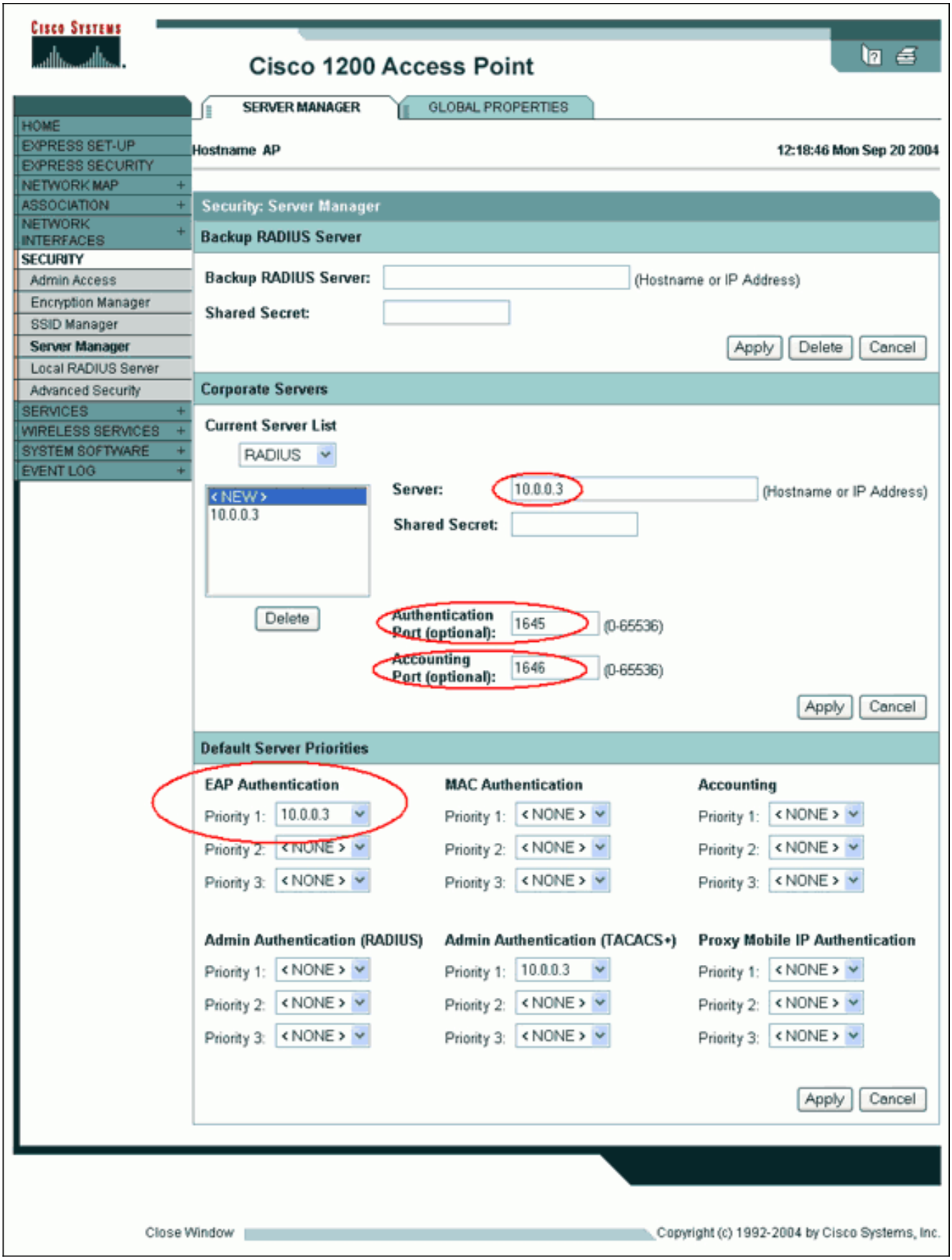
ネットワーク内のクライアントの種類によって、次のように設定します。

- Cisco のクライアント：ネットワーク EAP を使用する。
- サードパーティ製のクライアント（CCX 準拠製品を含む）：EAP によるオープン認証を使用する。
- Cisco クライアントとサードパーティ製クライアントの組み合わせ：ネットワーク EAP と EAP によるオープン認証の両方を選択する。

認証サーバの定義

EAP 設定の最初の手順では、認証サーバを定義し、そのサーバとの関係を確立します。

1. アクセス ポイントの Server Manager タブ（**[Security] > [Server Manager]** の順で開いたメニュー項目内）で、次の手順を実行します。[Server] フィールドに認証サーバの IP アドレスを入力します。共有秘密とポートを指定します。定義を作成し、ドロップダウン リストにデータを入力するには、[Apply] をクリックします。[Default Server Priorities] の下にある [EAP Authentication] タイプの [Priority 1] フィールドにサーバ IP アドレスを設定します。[Apply] をクリックします。

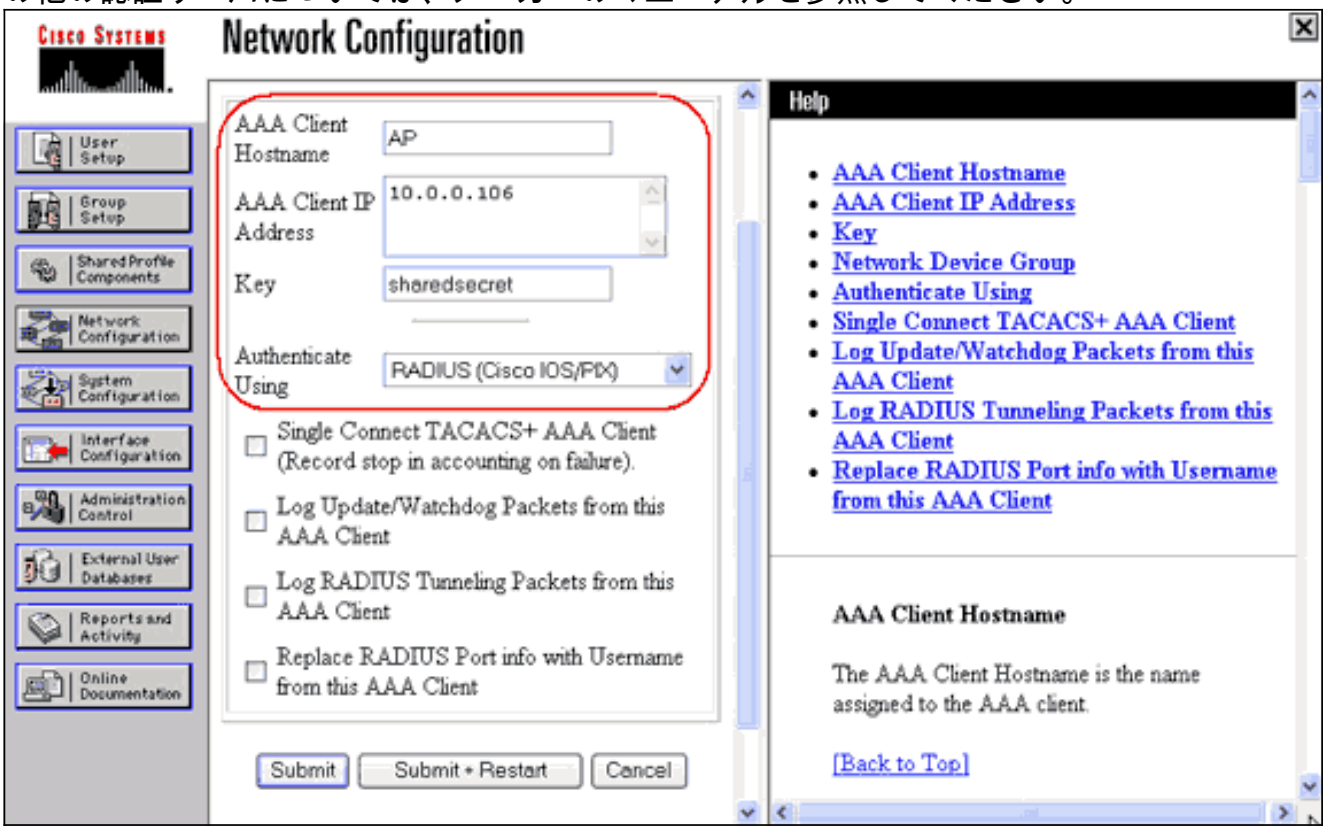


CLI から次のコマンドを発行することもできます。

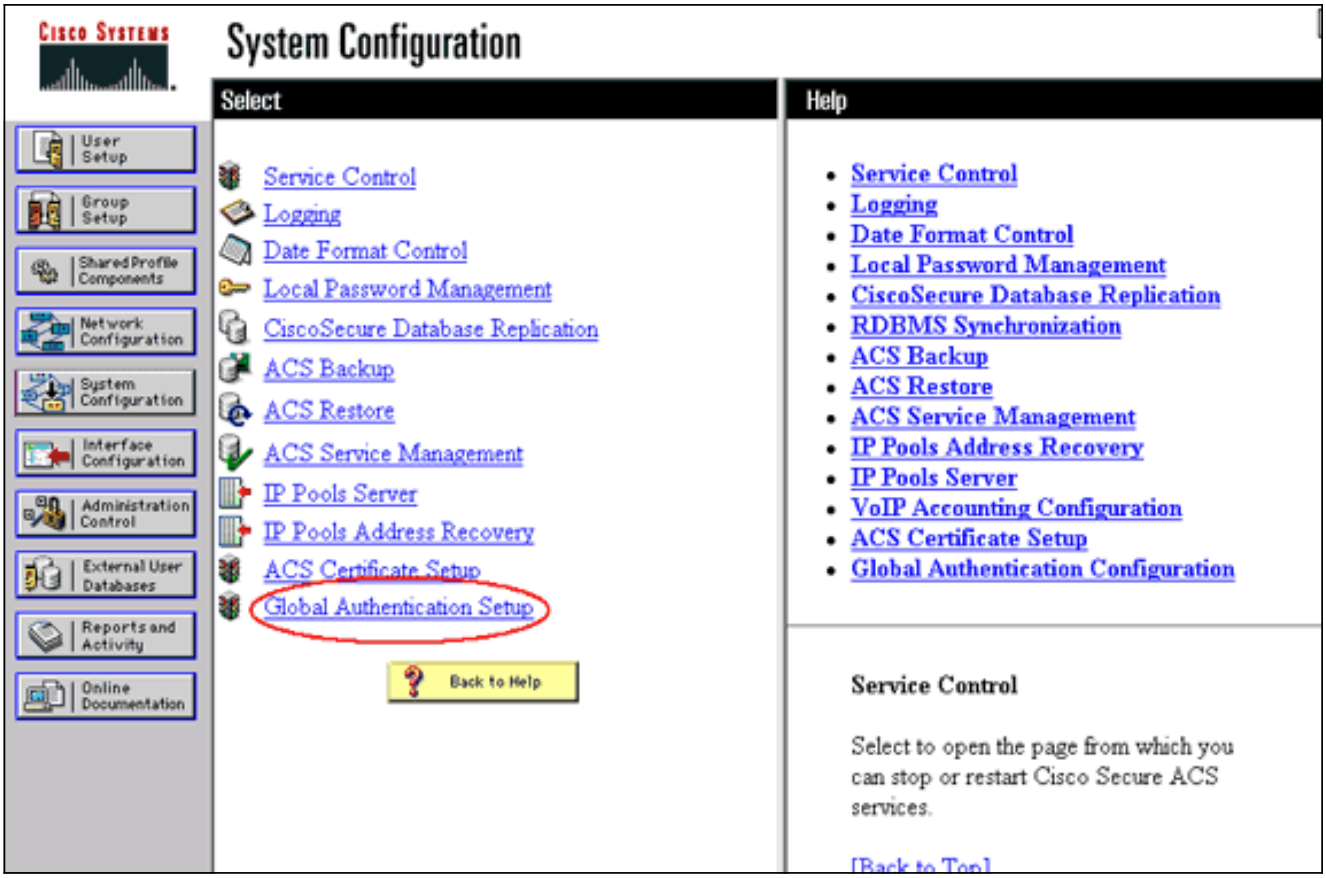
```
AP#configure terminal

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
```

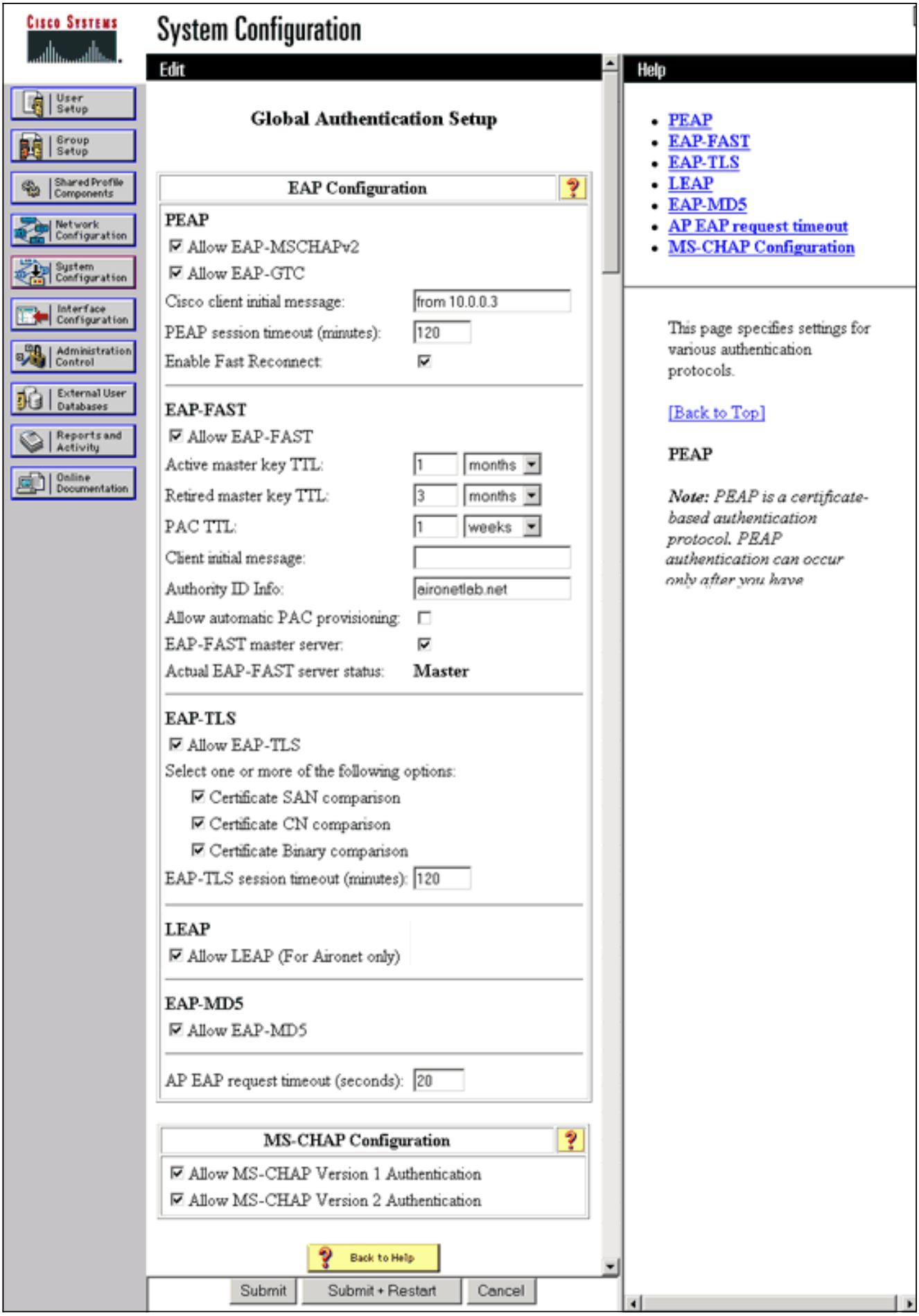
2. アクセス ポイントは、認証サーバに AAA クライアントとして設定する必要があります。たとえば、Cisco Secure ACS では、この設定は [Network Configuration] ページで行います。このページでは、アクセス ポイントの名前、IP アドレス、共有秘密キー、および認証方式（RADIUS Cisco Aironet または RADIUS Cisco IOS/PIX）が定義されています。ACS 以外の他の認証サーバについては、メーカーのマニュアルを参照してください。



目的の EAP 認証方式を実行するように認証サーバが設定されていることを確認します。たとえば、LEAP を行う Cisco Secure ACS の場合、System Configuration - Global Authentication Setup ページで LEAP 認証を設定します。[**System Configuration**] をクリックし、次に [**Global Authentication Setup**] をクリックします。ACS 以外の他の認証サーバまたは他の EAP 方式については、各製造業者のマニュアルを参照してください。



次の図は、Cisco Secure ACS を PEAP、EAP-FAST、EAP-TLS、LEAP、および EAP-MD5 用の設定例を示します。

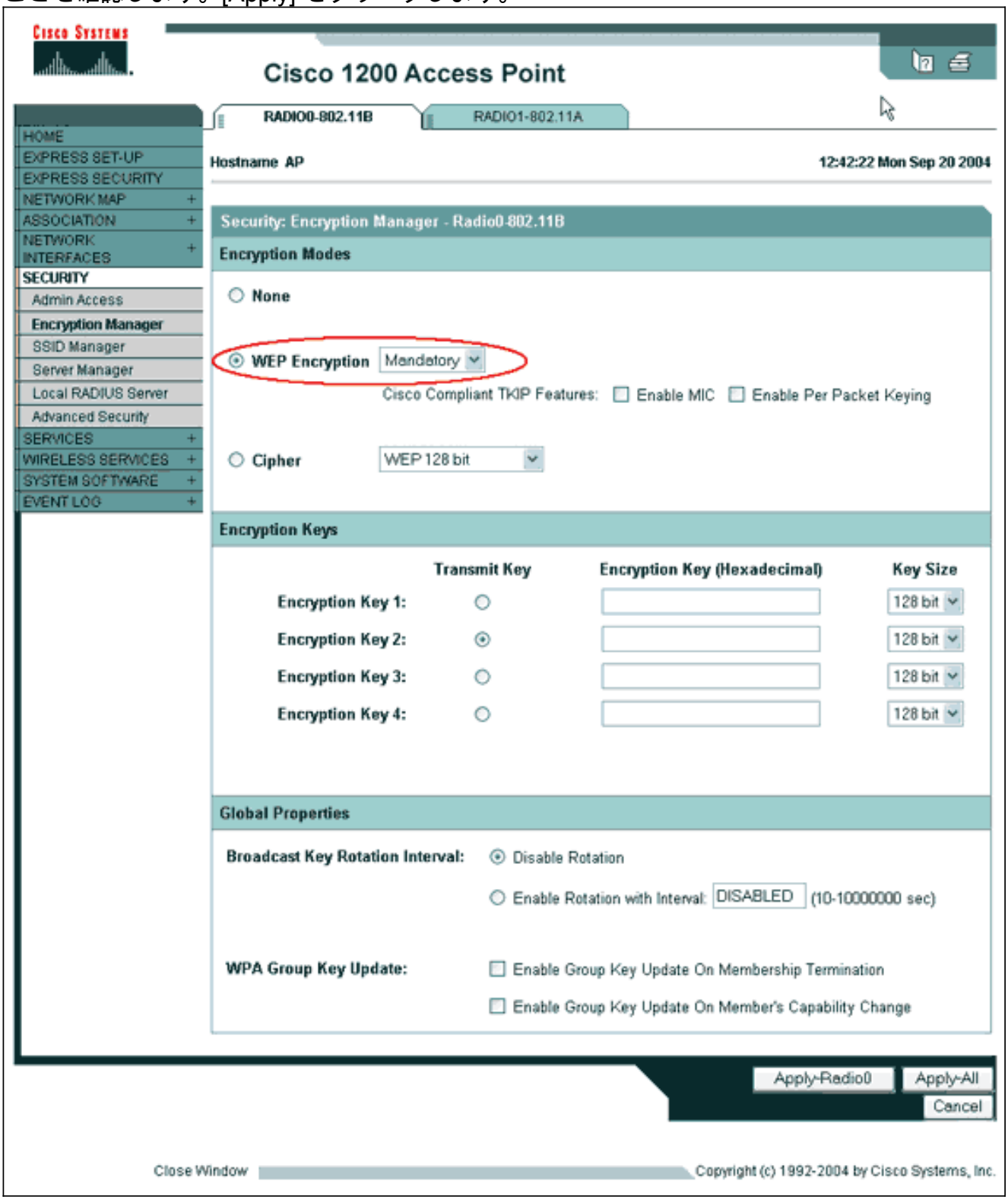


[クライアントの認証方式の定義]

アクセス ポイントがクライアント認証要求の送信先を認識するようになったら、その認証方式に対応するようにアクセス ポイントを設定します。

注：これらの手順は、WEPベースのインストール用です。WPA（WEP とは異なる暗号化を使用）については、『WPA 設定の概要』を参照してください。

1. アクセス ポイントの [Encryption Manager] タブ（[Security] > [Encryption Manager] の順で開いたメニュー項目内）で、次の手順を実行します。**WEP encryption** を使用することを指定します。WEP を [Mandatory] に指定します。キー サイズが [128-bits] に設定されていることを確認します。[Apply] をクリックします。

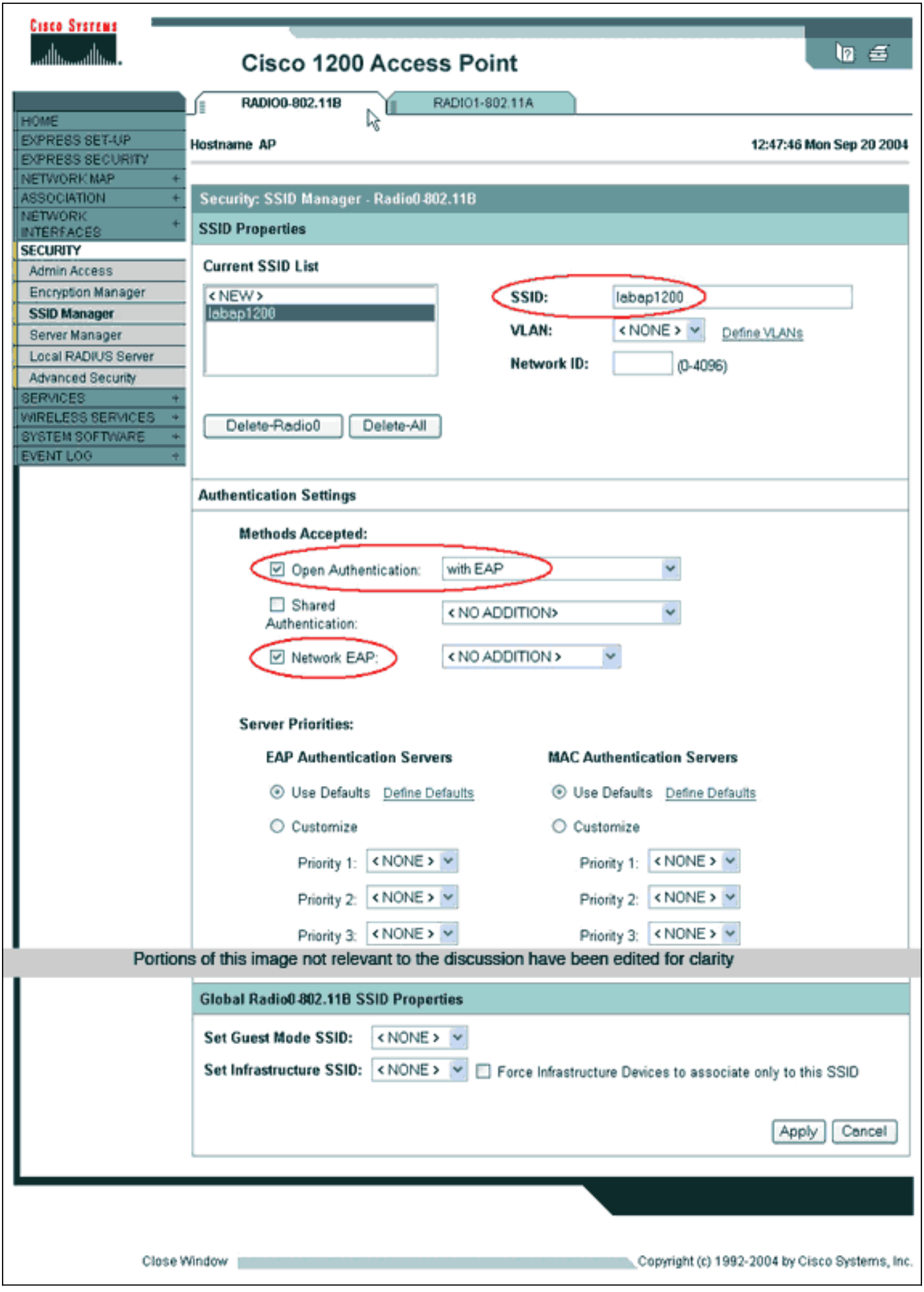


CLI から次のコマンドを発行することもできます。

```
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. アクセス ポイントの [SSID Manager] タブ（**[Security] > [SSID Manager]** の順で開いたメニュー項目内）で、次の手順を実行します。目的の SSID を選択します。[Methods Accepted:] で、**[Open]** のチェックボックスにチェック マークを付け、ドロップダウン リストから **[With EAP]** を選択します。Cisco クライアント カードを使用している場合には、**Network-EAP** チェックボックスをオンにします。「ネットワーク EAP または EAP を使用したオープン認証」セクションの説明を参照してください。[Apply] をクリックします。



CLI から次のコマンドを発行することもできます。

```
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
```

基本の EAP 設定での基本的な機能を確定したら、後で他の機能およびキー管理を追加できます。簡単にトラブルシューティングできるようにするには、基本の機能の上により複雑な機能を重ねて設定していきます。

確認

この項では、設定が正常に動作しているかどうかを確認する際に役立つ情報を紹介しています。

一部の show コマンドはアウトプット インタープリタ ツールによってサポートされています（登録ユーザ専用）。このツールを使用することによって、show コマンド出力の分析結果を表示できます。

- **show radius server-group all**：AP 上の設定済み RADIUS サーバ グループをすべて一覧表示します。

トラブルシュート

トラブルシューティングの手順

次の手順に従って、設定のトラブルシューティングを行います。

1. クライアントの設定で破損した部分がないことを確認するために、クライアント側のユーティリティまたはソフトウェアで、同じパラメータまたは類似のパラメータを使用して新規にプロファイルまたは接続を作成します。
2. 正常な認証を妨げる RF の問題が生じないようにするため、次の手順を使用して認証を一時的に無効にします。CLI からは、**no authentication open eap eap_methods**、**no authentication network-eap eap_methods**、**authentication open** の各コマンドを使用します。GUI からは、SSID Manager ページで、[Network-EAP] チェックボックスをオフにし、[Open] のチェックボックスにチェック マークを付け、ドロップダウン リストを [No Addition] に戻します。クライアントが関連付けに成功する場合には、RF はアソシエーションの問題に関係しません。
3. アクセス ポイントと認証サーバ間で共有秘密鍵パスワードが同期していることを確認します。同期していない場合は、次のエラー メッセージが返されます。
   ```
   Invalid message authenticator in EAP request
   ```

CLI からは、radius-server host x.x.x.x auth-port x acct-port x key <shared_secret> の行を確認します。GUI からは、[Server Manager] ページで、[Shared Secret] のボックスに対象となるサーバの共有秘密鍵を再入力します。RADIUS サーバ上のアクセス ポイントに対する共有秘密鍵エントリには、上記と同じ共有秘密鍵パスワードが記載されている必要があります。

4. RADIUS サーバからすべてのユーザ グループを削除します。場合によっては、RADIUS サーバが定義したユーザ グループと、基本ドメインのユーザ グループ間で、競合が発生することがあります。RADIUS サーバのログで、失敗した試行がないかどうかを確認し、ある場合にはその理由も確認します。

トラブルシューティングのためのコマンド

一部の show コマンドはアウトプット インタープリタ ツールによってサポートされています（登録ユーザ専用）。このツールを使用することによって、show コマンド出力の分析結果を表示できます。

EAP に関するデバッグの出力を収集し、その意味を把握する方法については、『認証のデバッグ』で詳しく説明されています。

注：debugコマンドを発行する前に、『debugコマンドの重要な情報』を参照してください。

- **debug dot11 aaa authenticator state-machine**：クライアントと認証サーバ間のネゴシエーションの主な分類（または状態）を表示します。**正常に終了した**認証の出力を次に示します。

```
*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)
```

注：12.2(15)JAより前のCisco IOSソフトウェアリリースでは、この**debugコマンドの構文は debug dot11 aaa dot1x state-machineです。**

- **debug dot11 aaa authenticator process**：クライアントと認証サーバ間のネゴシエーションの個々のダイアログ エントリを表示します。**注：**12.2(15)JAより前のCisco IOSソフトウェアリリースでは、このdebugコマンドの構文は**debug dot11 aaa dot1x processです。**
- **debug radius authentication**：サーバとクライアント間の RADIUS ネゴシエーションを表示します。サーバもクライアントも、AP でブリッジされています。**失敗した**認証の出力を次に示します。

```
*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**：クライアント デバイスと認証サーバ間の認証の AAA ネゴシエーションを表示します。

関連情報

- 認証のデバッグ
- 認証タイプの設定
- ローカル RADIUS サーバでの LEAP 認証
- RADIUS サーバと TACACS+ サーバの設定
- PEAP-MS-CHAPv2 マシン認証が設定された Cisco Secure ACS for Windows v3.2
- EAP-TLS マシン認証が設定された Cisco Secure ACS for Windows v3.2
- Configuring PEAP/EAP on Microsoft IAS
- Troubleshooting Microsoft IAS as a RADIUS server
- Microsoft 802.1X認証クライアント
- テクニカル サポートとドキュメント – Cisco Systems