Autenticação de EAP com servidor RADIUS

Contents

Introduction

Este documento fornece uma configuração de exemplo de um ponto de acesso baseado no Cisco IOS® para autenticação EAP (Extensible Authentication Protocol) de usuários sem fio em relação a um banco de dados acessado por um servidor RADIUS.

Devido à função passiva que o access point desempenha no EAP (liga pacotes sem fio do cliente em pacotes com fio destinados ao servidor de autenticação e vice-versa), essa configuração é usada com praticamente todos os métodos EAP. Esses métodos incluem (mas não se limitam a) LEAP, Protected EAP (PEAP)-MS-Challenge Handshake Authentication Protocol (CHAP) versão 2, PEAP-Generic Token Card (GTC), EAP-Flexible Authentication via Secure Tunneling (FAST), EAP-Transport Layer Security (TLS) e EAP-Tunneled TLS (TTLS). Você deve configurar adequadamente o servidor de autenticação para cada um desses métodos EAP.

Este documento aborda como configurar o ponto de acesso (AP) e o servidor RADIUS, que é o Cisco Secure ACS no exemplo de configuração deste documento.

Prerequisites

Requirements

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Você está familiarizado com a GUI ou CLI do Cisco IOS.

- Você está familiarizado com os conceitos por trás da autenticação EAP.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Produtos Cisco Aironet AP que executam o Cisco IOS.
- Suposição de apenas uma LAN virtual (VLAN) na rede.
- Um produto de servidor de autenticação RADIUS que se integra com êxito em um banco de dados de usuários.Estes são os servidores de autenticação suportados para Cisco LEAP e EAP-FAST:Cisco Secure Access Control Server (ACS)Cisco Access Registrar (CAR)Funk Steel Belted RADIUSInterlink MeritEstes são os servidores de autenticação suportados para o Microsoft PEAP-MS-CHAP versão 2 e PEAP-GTC:Serviço de Autenticação da Internet (IAS - Microsoft Internet Authentication Service)Cisco Secure ACSFunk Steel Belted RADIUSInterlink MeritQualquer servidor de autenticação adicional que a Microsoft possa autorizar.**Observação:** as senhas GTC ou One-Time exigem serviços adicionais que exigem software adicional no lado do cliente e do servidor, bem como geradores de token de hardware ou software.Consulte o fabricante do requerente cliente para obter detalhes sobre quais servidores de autenticação são suportados com seus produtos para EAP-TLS, EAP-TTLS e outros métodos EAP.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar

Esta configuração descreve como configurar a autenticação EAP em um AP baseado em IOS. No exemplo deste documento, LEAP é usado como um método de autenticação EAP com servidor RADIUS.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Como a maioria dos algoritmos de autenticação baseados em senha, o LEAP Cisco é vulnerável a ataques de dicionários. Esse não é um novo ataque ou uma nova vulnerabilidade do Cisco LEAP. A criação de uma política de senhas forte é a forma mais eficaz de mitigar ataques de dicionários. Isso inclui o uso de senhas fortes e a expiração periódica de senhas. Consulte Ataque de Dicionário no Cisco LEAP para obter mais informações sobre ataques de dicionários e como evitá-los.

Este documento usa esta configuração para GUI e CLI:

- O endereço IP do AP é 10.0.0.106.
- O endereço IP do servidor RADIUS (ACS) é 10.0.0.3.

EAP de rede ou autenticação aberta com EAP

Em qualquer método de autenticação baseado em EAP/802.1x, você pode questionar quais são as diferenças entre o EAP de rede e a autenticação aberta com EAP. Esses itens se referem aos valores no campo Authentication Algorithm nos cabeçalhos dos pacotes de gerenciamento e associação. A maioria dos fabricantes de clientes sem fio define esse campo com o valor 0 (autenticação aberta) e sinaliza o desejo de fazer a autenticação EAP posteriormente no processo de associação. A Cisco define o valor de maneira diferente, desde o início da associação com o flag Network EAP.

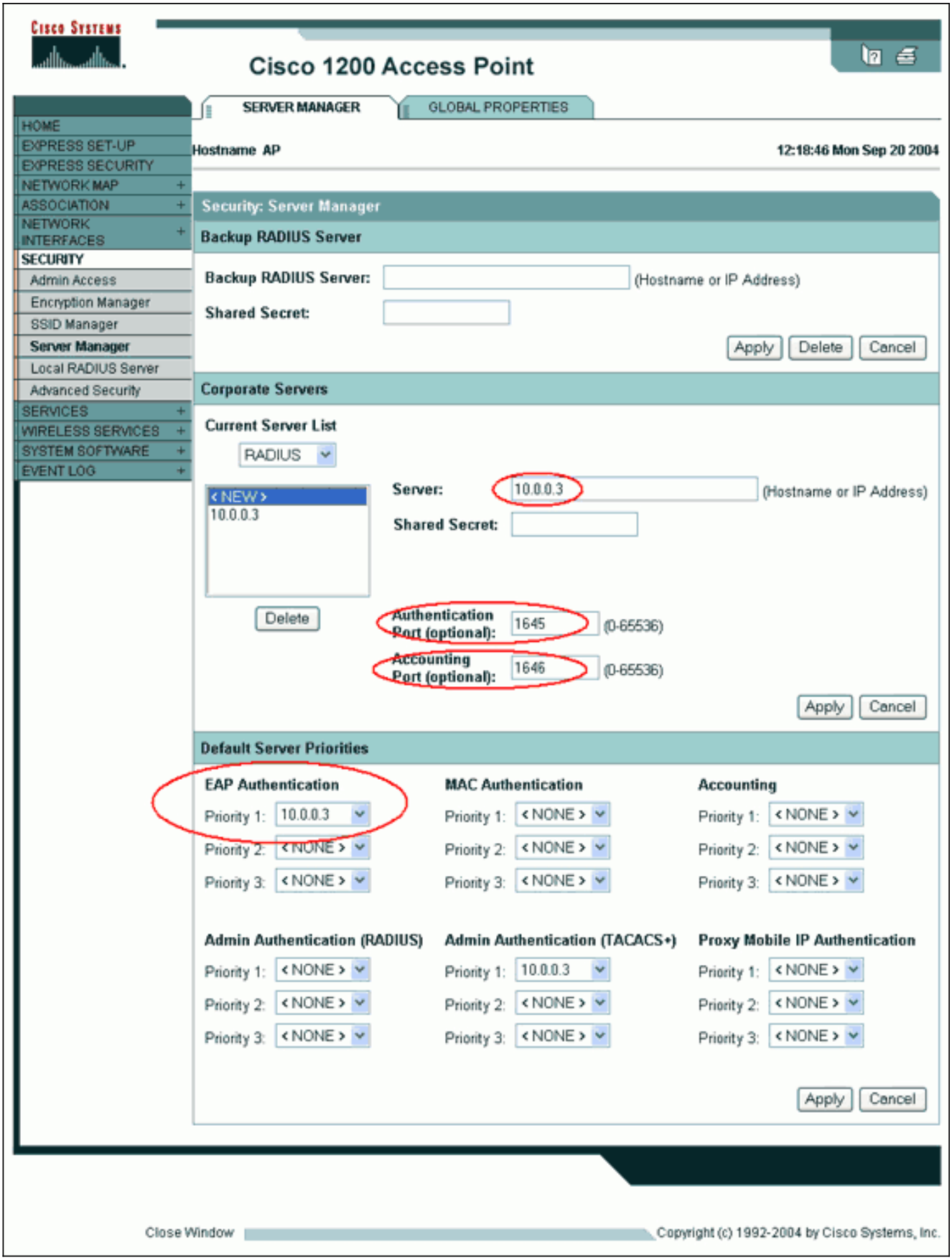
Se sua rede possui clientes que são:

- Clientes Cisco—Use Network-EAP.
- Clientes terceirizados (incluem produtos compatíveis com CCX) — Use Abrir com EAP.
- Uma combinação de clientes da Cisco e de terceiros: escolha Network-EAP e Open com EAP.

Definir Servidor de Autenticação

A primeira etapa na configuração do EAP é definir o servidor de autenticação e estabelecer uma relação com ele.

1. Na guia Server Manager do ponto de acesso (no item de menu **Security > Server Manager**), faça o seguinte:Insira o endereço IP do servidor de autenticação no campo Servidor.Especifique o segredo compartilhado e as portas.Clique em **Apply** para criar a definição e preencher as listas suspensas.Defina o campo Prioridade 1 do tipo de autenticação EAP para o endereço IP do servidor em Prioridades de servidor padrão.Clique em
   Apply.

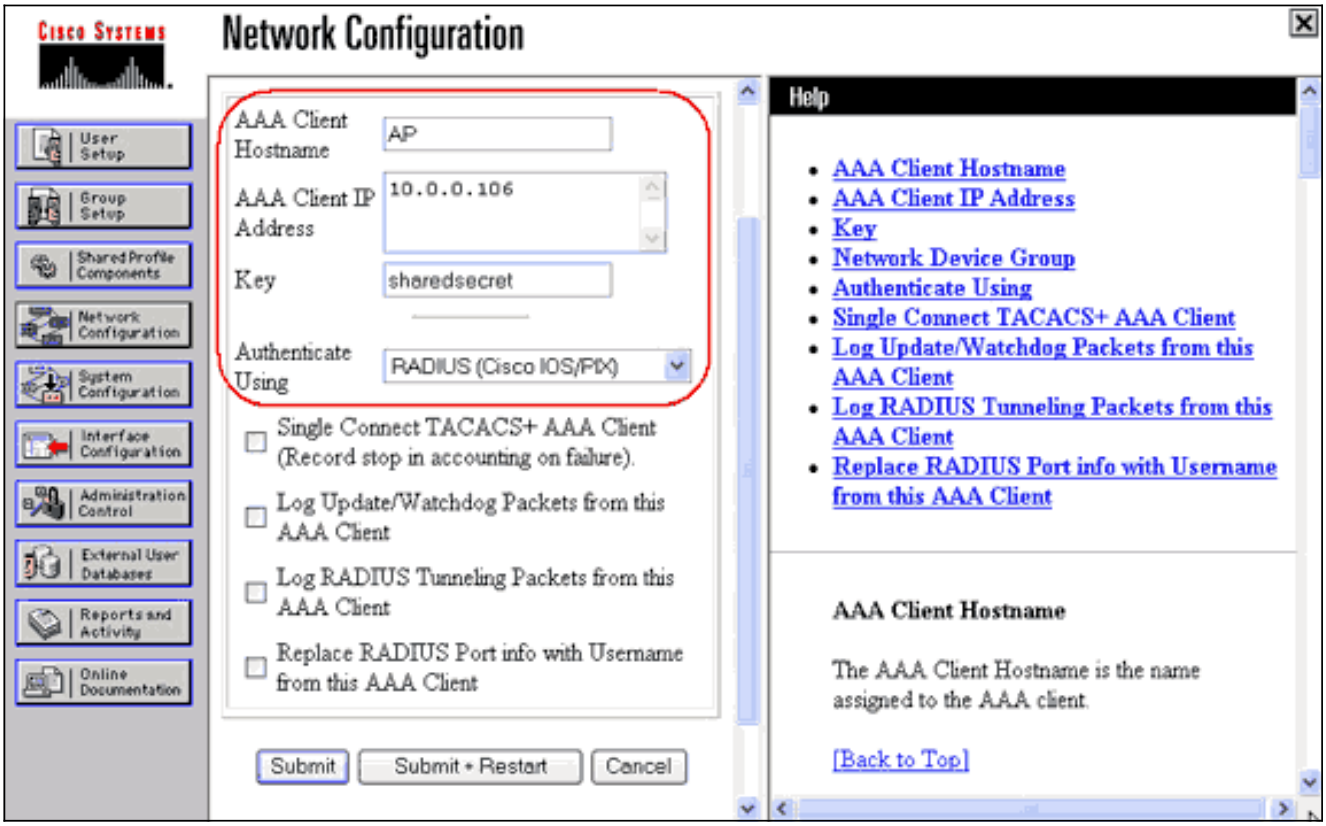


Você também pode emitir estes comandos a partir da CLI:

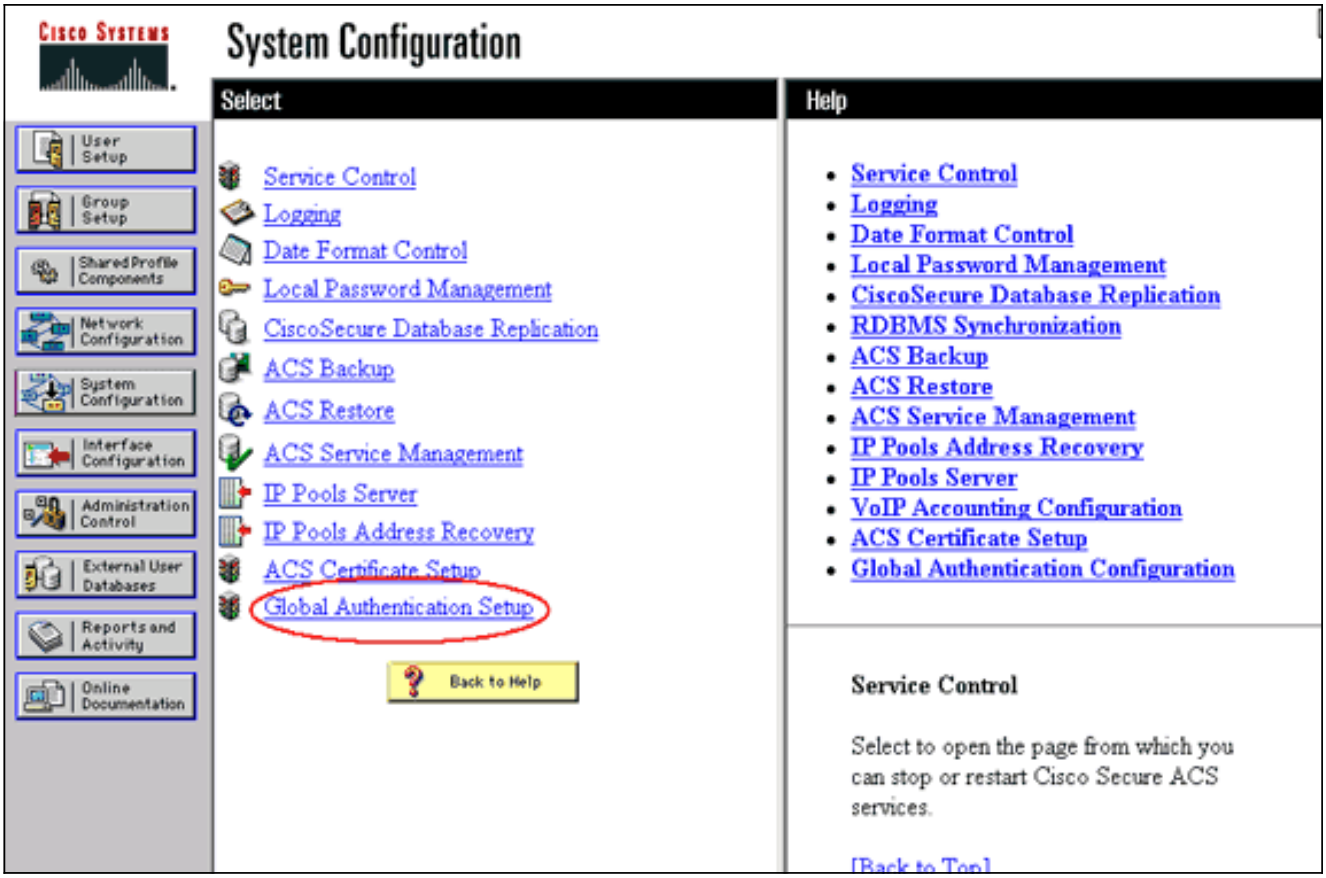
```
AP#configure terminal

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
```

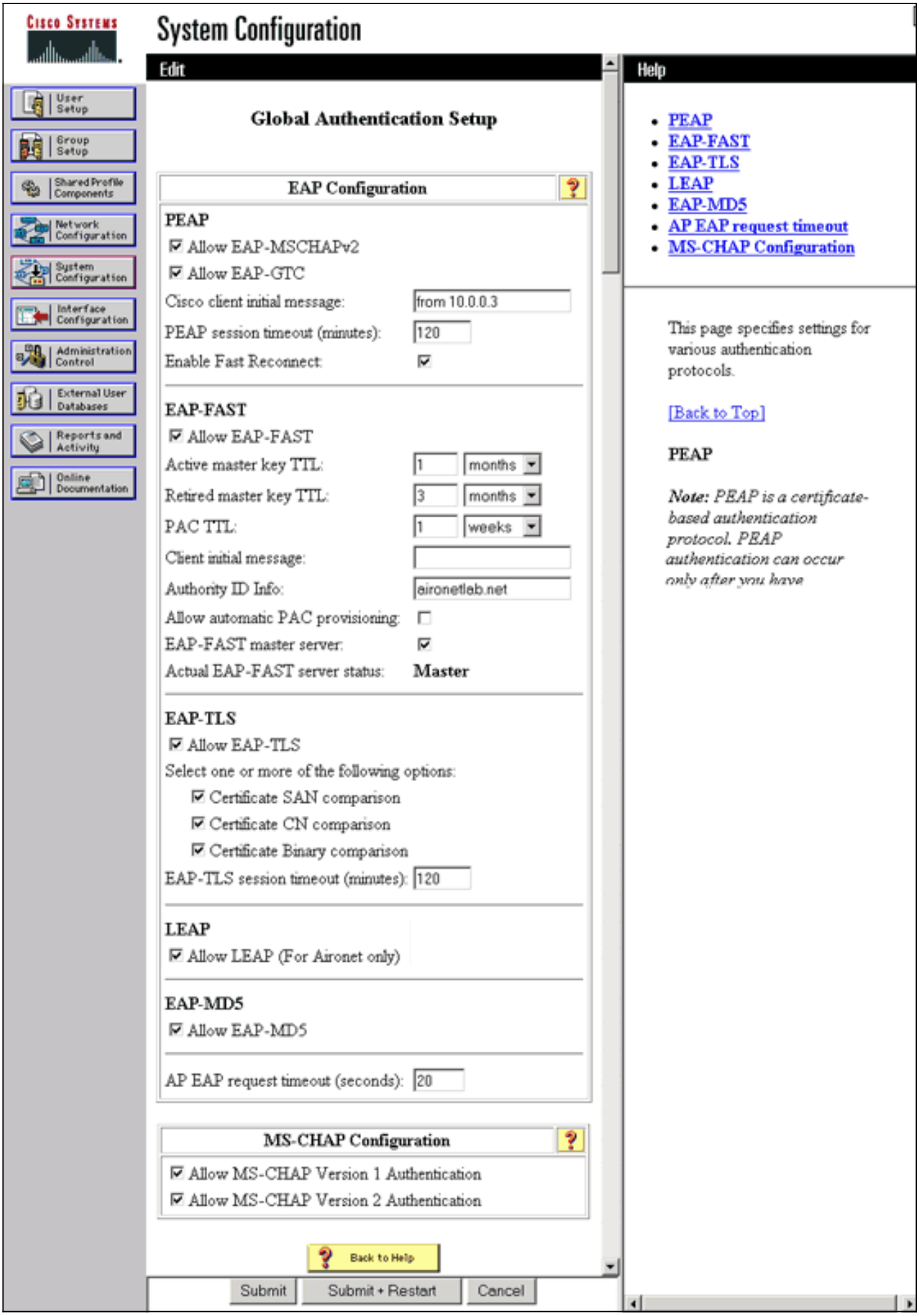
2. O ponto de acesso deve ser configurado no servidor de autenticação como um cliente AAA.Por exemplo, no Cisco Secure ACS, isso acontece na página Configuração de Rede onde o nome do ponto de acesso, endereço IP, segredo compartilhado e método de autenticação (RADIUS Cisco Aironet ou RADIUS Cisco IOS/PIX) são definidos. Consulte a documentação do fabricante para outros servidores de autenticação não-ACS.



Verifique se o servidor de autenticação está configurado para executar o método de autenticação EAP desejado. Por exemplo, para um Cisco Secure ACS que faz LEAP, configure a autenticação LEAP na página Configuração do sistema - Configuração da autenticação global. Clique em **Configuração do sistema** e, em seguida, clique em **Configuração de autenticação global**. Consulte a documentação do fabricante para obter outros servidores de autenticação não ACS ou outros métodos EAP.



Esta imagem mostra o Cisco Secure ACS configurado para PEAP, EAP-FAST, EAP-TLS, LEAP e EAP-
MD5.

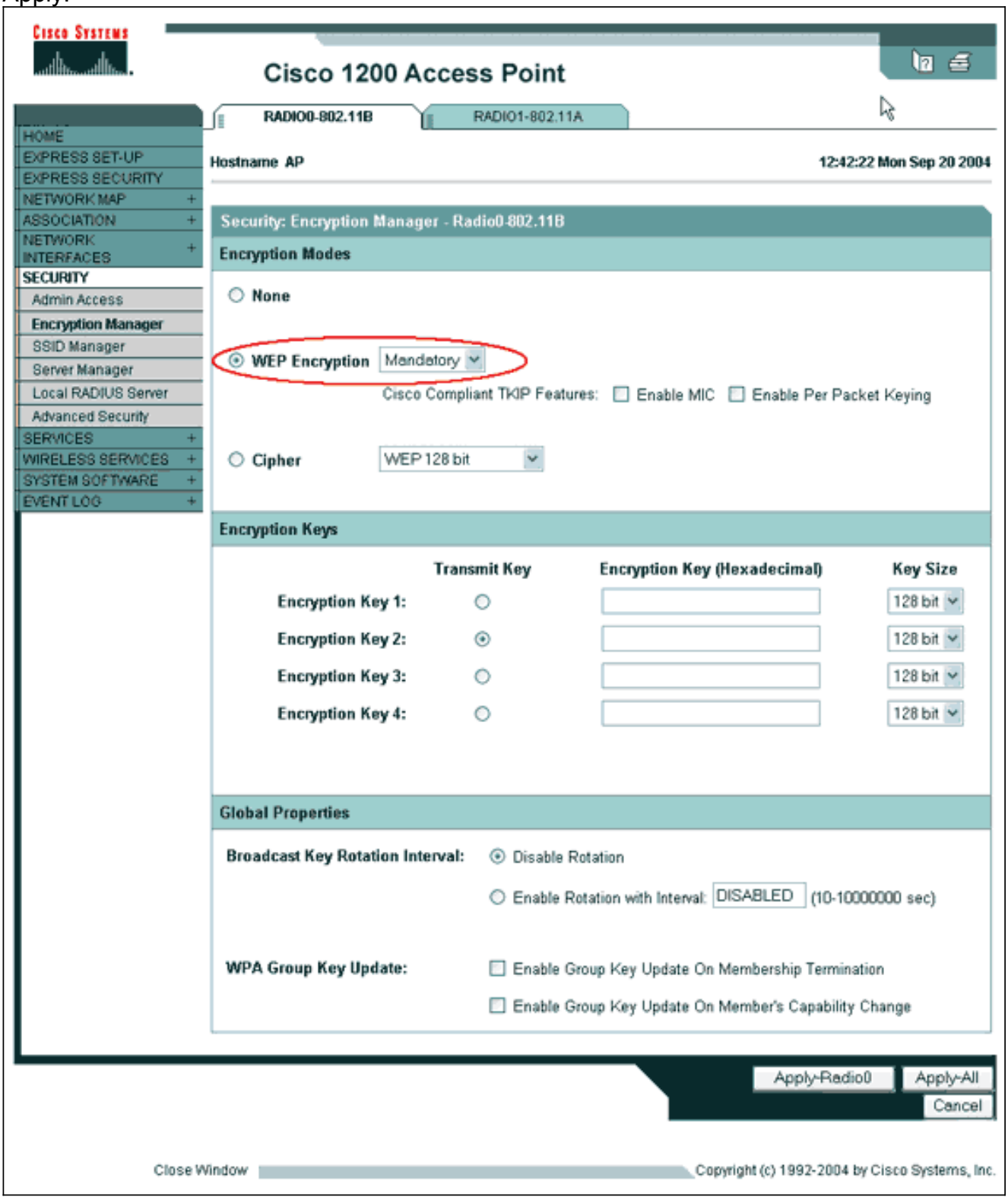


[Definir Métodos de Autenticação do Cliente]

Quando o ponto de acesso souber para onde enviar solicitações de autenticação de cliente, configure-o para aceitar esses métodos.

Observação: essas instruções são para uma instalação baseada em WEP. Para WPA (que usa cifras em vez de WEP), consulte Visão geral da configuração de WPA.

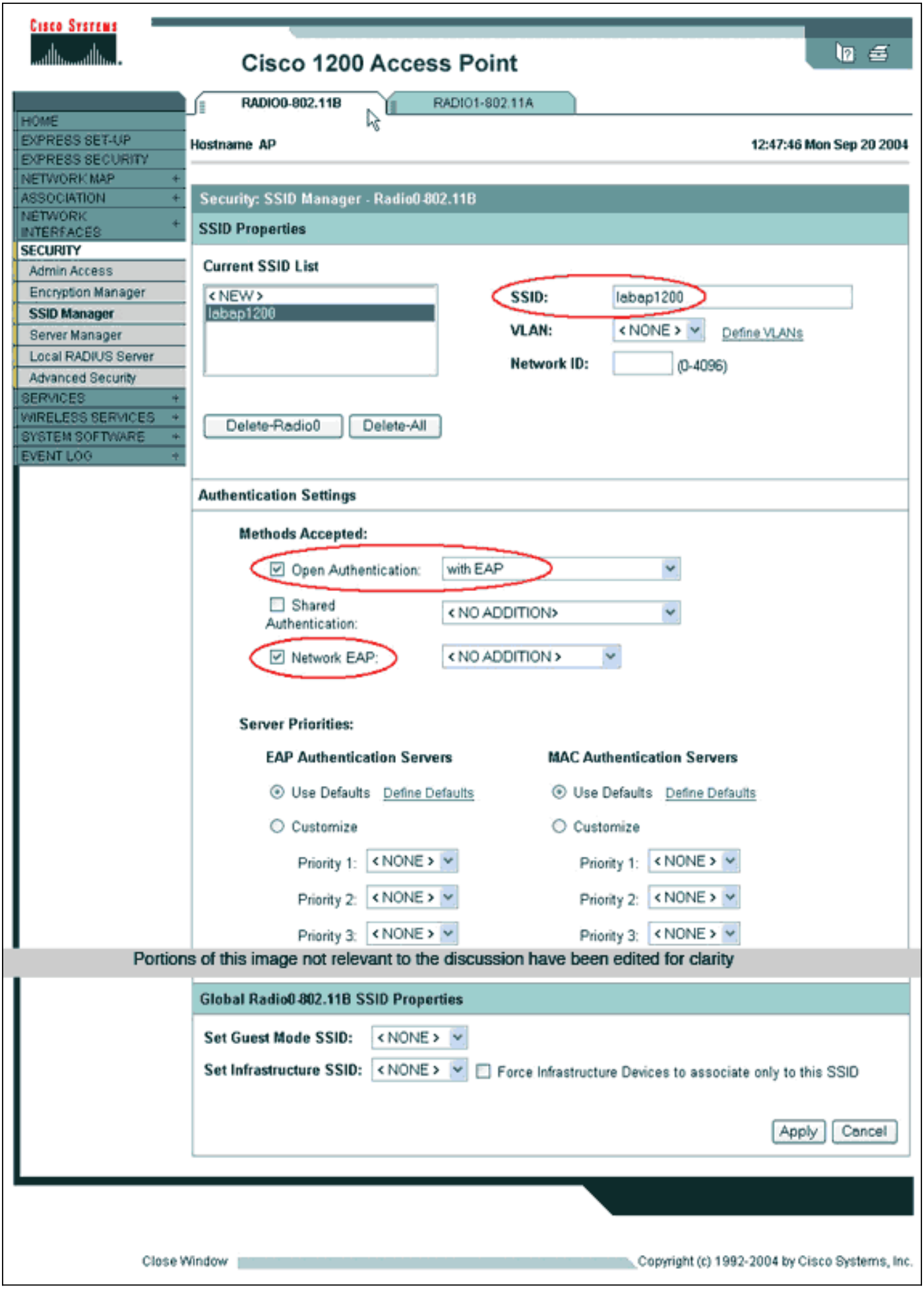
1. Na guia Gerenciador de criptografia do ponto de acesso (no item de menu **Segurança > Gerenciador de criptografia**), faça o seguinte:Especifique que pretende utilizar a **encriptação WEP**.Especifique se WEP é **obrigatório**.Verifique se o tamanho da chave está definido como **128 bits**.Clique em
   Apply.



Você também pode emitir estes comandos a partir da CLI:

```
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. Conclua estas etapas na guia Gerenciador de SSID do ponto de acesso (sob o item de menu **Segurança > Gerenciador de SSID**):Selecione o SSID desejado.Em "Authentication Methods Accepted", marque a caixa **Open** e use a lista suspensa para escolher **With EAP**.Marque a caixa rotulada **Network-EAP** se você tiver placas de cliente Cisco. Consulte a discussão na seção EAP de rede ou Autenticação aberta com EAP.Clique em Apply.



Você também pode emitir estes comandos a partir da CLI:

```
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
```

Depois de confirmar a funcionalidade básica com uma configuração básica de EAP, você poderá adicionar recursos adicionais e gerenciamento de chaves posteriormente. A camada funciona de forma mais complexa sobre as bases funcionais para facilitar a solução de problemas.

Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração funciona adequadamente.

A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

- **show radius server-group all** — Exibe uma lista de todos os grupos de servidores RADIUS configurados no AP.

Troubleshoot

Procedimento de solução de problemas

Execute estes passos para fazer troubleshoot da sua configuração.

1. No utilitário ou software do lado do cliente, crie um novo perfil ou conexão com os mesmos parâmetros ou parâmetros semelhantes para garantir que nada seja corrompido na configuração do cliente.
2. Para eliminar a possibilidade de problemas de RF que impeçam a autenticação bem-sucedida, desative temporariamente a autenticação como mostrado nestas etapas:Na CLI, use os comandos **no authentication open eap eap_methods**, **no authentication network-eap eap_methods** e **authentication open**.Na GUI, na página do SSID Manager, desmarque **Network-EAP**, marque **Open** e defina a lista suspensa de volta para **No Add**.Se o cliente se associar com êxito, o RF não contribui para o problema de associação.
3. Verifique se as senhas secretas compartilhadas estão sincronizadas entre o ponto de acesso e o servidor de autenticação. Caso contrário, você poderá receber esta mensagem de erro:
   ```
   Invalid message authenticator in EAP request
   ```

Na CLI, verifique a linha `radius-server host x.x.x.x auth-port x acct-port x key <shared_secret>`.Na GUI, na página Gerenciador do servidor, digite novamente o segredo compartilhado para o servidor apropriado na caixa intitulada "Segredo compartilhado".A entrada de segredo compartilhado para o ponto de acesso no servidor RADIUS deve conter a mesma senha secreta compartilhada que as mencionadas anteriormente.

4. Remova todos os grupos de usuário do servidor RADIUS. Às vezes, podem ocorrer conflitos entre grupos de usuários definidos pelo servidor RADIUS e grupos de usuários no domínio subjacente. Verifique os registros do servidor RADIUS em busca de tentativas com falha e os motivos dessa falha.

Comandos de solução de problemas

A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

Debugging Authentications fornece uma quantidade significativa de detalhes sobre como coletar e interpretar a saída de depurações relacionadas ao EAP.

Observação: antes de emitir comandos **debug**, consulte Informações importantes sobre comandos debug.

- **debug dot11 aaa authenticator state-machine** — Exibe as principais divisões (ou estados) da negociação entre o cliente e o servidor de autenticação. Aqui está uma saída de uma autenticação **bem-sucedida**:

```
*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)
```

Observação: nas versões do Cisco IOS Software anteriores a 12.2(15)JA, a sintaxe deste comando **debug** é **debug dot11 aaa dot1x state-machine**.

- **debug dot11 aaa authenticator process** — Exibe as entradas de diálogo individuais da negociação entre o cliente e o servidor de autenticação.**Observação:** nas versões do Cisco IOS Software anteriores a 12.2(15)JA, a sintaxe deste comando debug é o **processo debug dot11 aaa dot1x**.
- **debug radius authentication** — Exibe as negociações RADIUS entre o servidor e o cliente, ambas ligadas pelo AP. Esta é uma saída para autenticação **com falha**:

```
*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** —Exibe as negociações AAA para autenticação entre o dispositivo cliente e o servidor de autenticação.

Informações Relacionadas

- Autenticações de depuração
- Configurando tipos de autenticação
- Autenticação LEAP em um servidor RADIUS local
- Configuração de servidores RADIUS e TACACS+
- Configurando o Cisco Secure ACS para Windows v3.2 com autenticação de máquina PEAP-MS-CHAPv2
- Cisco Secure ACS para Windows v3.2 com autenticação de máquina EAP-TLS
- Configurando PEAP/EAP no Microsoft IAS
- Troubleshooting do Microsoft IAS como um servidor RADIUS
- Cliente de Autenticação do Microsoft 802.1X
- Suporte Técnico e Documentação - Cisco Systems