Authentification EAP avec le serveur RADIUS

Contenu

Introduction

Ce document fournit un exemple de configuration d'un point d'accès basé sur Cisco IOS® pour l'authentification Extensible Authentication Protocol (EAP) des utilisateurs sans fil contre une base de données consultée par un serveur RADIUS.

En raison du rôle passif que le point d'accès joue dans l'EAP (relie des paquets sans fil du client dans des paquets câblés destinés au serveur d'authentification, et vice versa), cette configuration est utilisée avec pratiquement toutes les méthodes d'EAP. Ces méthodes incluent (mais ne sont pas limités à) LEAP, Protected EAP (PEAP) - MS-Challenge Handshake Authentication Protocol (CHAP) version 2, PEAP-Generic Token Card (GTC), EAP-Flexible Authentication par l'intermédiaire de Secure Tunneling (FAST), EAP-Transport Layer Security (TLS) et EAP-Tunneled TLS (TTL). Vous devez configurer convenablement le serveur d'authentification pour chacune de ces méthodes d'EAP.

Ce document couvre comment configurer le point d'accès (AP) et le serveur RADIUS, qui est Cisco Secure ACS dans l'exemple de configuration de ce document.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Vous êtes familiarisé avec la GUI ou CLI de Cisco IOS.
- Vous êtes au courant des concepts derrière l'authentification EAP.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Les produits Cisco Aironet qui exécutent Cisco IOS.
- Le principe qu'il n'y a qu'un seul LAN virtuel (VLAN) dans le réseau.
- Un produit de serveur d'authentification RADIUS qui s'intègre avec succès dans une base de données utilisateur.Voici les serveurs d'authentification pris en charge pour Cisco LEAP et EAP-FAST :Cisco Secure Access Control Server (ACS)Cisco Access Registrar (CAR)Funk Steel Belted RADIUSInterlink MeritVoici les serveurs d'authentification pris en charge pour Microsoft PEAP-MS-CHAP version 2 et PEAP-GTC :Microsoft Internet Authentication Service (IAS)Cisco Secure ACSFunk Steel Belted RADIUSInterlink MeritTout serveur d'authentification supplémentaire Microsoft peut autoriser.**Remarque:** GTC ou One-Time Passwords exigent des services supplémentaires qui ont besoin d'un logiciel supplémentaire côté client et côté serveur, ainsi que des générateurs de jetons de matériel ou de logiciel.Consultez le constructeur du supplicant client pour des détails sur les serveurs d'authentification pris en charge avec leurs produits pour EAP-TLS, EAP-TTLS et d'autres méthodes d'EAP.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configurer

Cette configuration décrit comment configurer l'authentification EAP sur un AP basé sur IOS. Dans l'exemple de ce document, LEAP est utilisé comme méthode d'authentification EAP avec le serveur RADIUS.

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Comme avec la plupart des algorithmes basés sur une authentification par mot de passe, Cisco LEAP est vulnérable aux attaques de dictionnaire. Ce n'est pas une nouvelle attaque ou une nouvelle vulnérabilité de Cisco LEAP. La création d'une forte politique de mot de passe est la méthode la plus efficace d'atténuer les attaques par dictionnaire. Ceci inclut l'utilisation de mots de passe forts et l'expiration périodique des mots de passe. Référez-vous à Attaque par dictionnaire sur Cisco LEAP pour obtenir des informations sur les attaques par dictionnaire et la façon de les prévenir.

Ce document utilise cette configuration pour GUI et CLI :

- L'adresse IP de l'AP est 10.0.0.106.
- L'adresse IP du serveur RADIUS (ACS) est 10.0.0.3.

Network EAP ou l'authentification ouverte avec EAP

Dans n'importe quelle méthode d'authentification basée sur EAP/802.1x, vous pouvez interroger ce que sont les différences entre Network-EAP et l'authentification ouverte avec EAP. Ces éléments se rapportent aux valeurs dans le domaine d'algorithme d'authentification dans les en-têtes des paquets de gestion et d'association. La plupart des constructeurs des clients sans fil définissent cette zone sur la valeur 0 (authentification ouverte), puis signalent un désir de faire l'authentification EAP plus tard dans le processus d'association. Cisco définit la valeur différemment, depuis le début de l'association avec l'indicateur Network EAP.

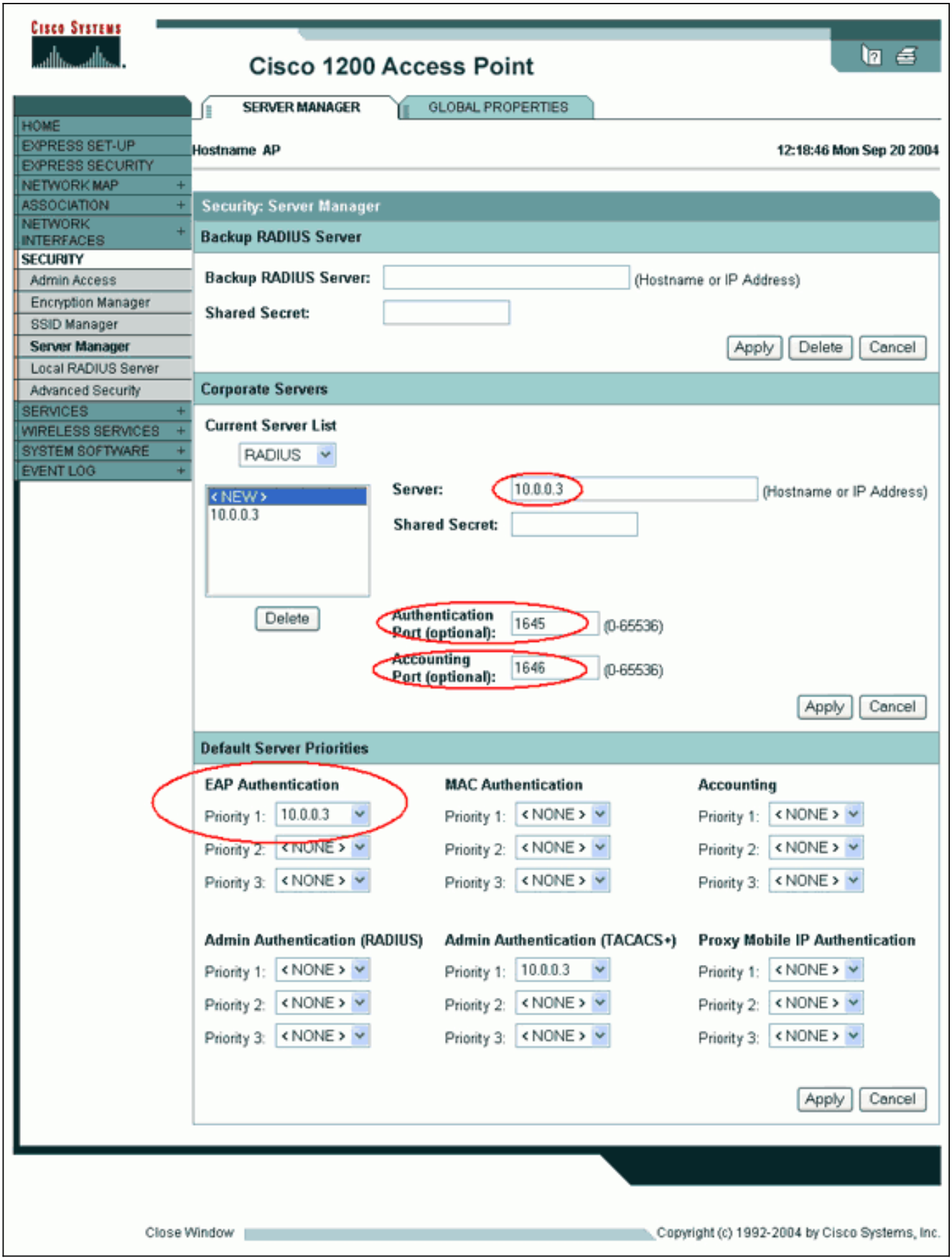
Si votre réseau a des clients qui sont :

- clients Cisco - Utilisez Network-EAP.
- Clients de tiers (inclut les produits compatibles CCX) - utilisez Open avec EAP.
- Une combinaison du client Cisco et tiers - choisissez Network-EAP et l'authentification ouverte avec EAP.

Définir le serveur d'authentification

La première étape dans la configuration d'EAP est de définir le serveur d'authentification et d'établir une relation avec lui.

1. Dans l'onglet du gestionnaire du serveur du point d'accès (sous l'élément de menu **Security > Server Manager**), complétez ces étapes :Présentez l'adresse IP du serveur d'authentification dans le domaine du serveur.Spécifiez le secret partagé et les ports.Cliquez sur **Apply** pour créer la définition et peupler les listes déroulantes.Définissez le champ de la priorité 1 du type d'authentification EAP sur l'adresse IP du serveur sous Default Server Priorities (priorités du serveur par défaut).Cliquez sur **Apply**.

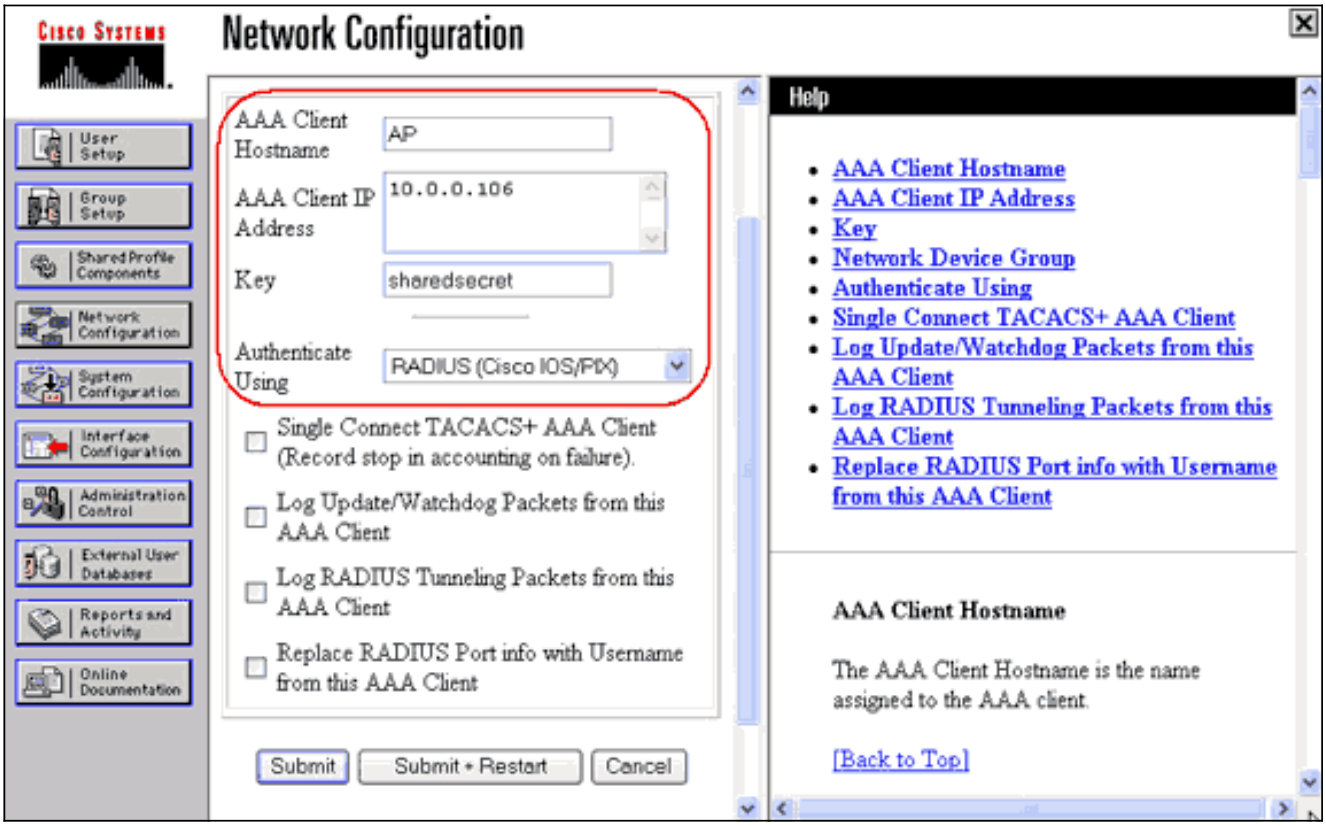


Vous pouvez également émettre ces commandes de la CLI :

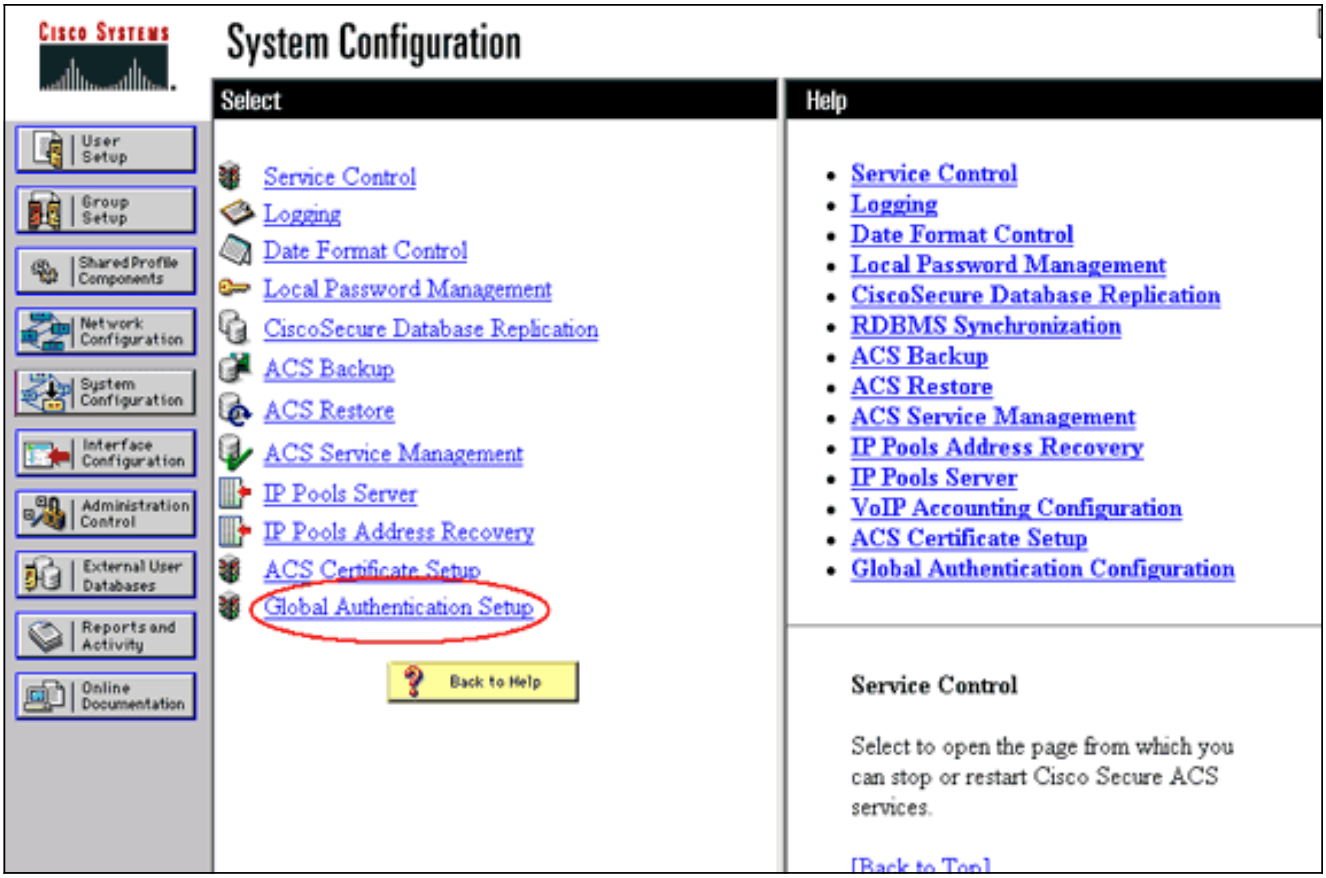
```
AP#configure terminal

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
```

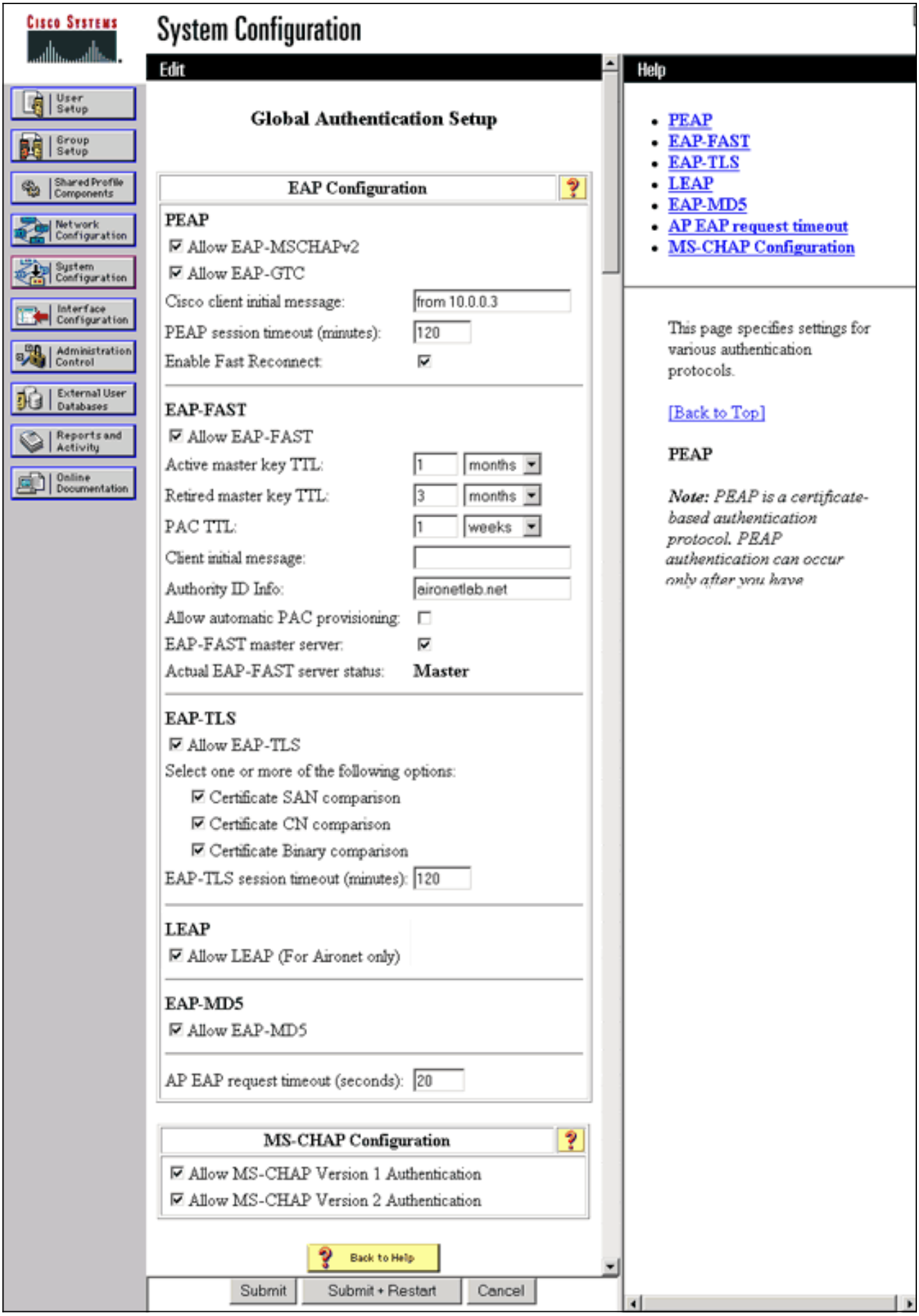
2. Le point d'accès doit être configuré dans le serveur d'authentification comme un client AAA.Par exemple, dans Cisco Secure ACS, ceci se produit à la page de Configuration du réseau où le nom du point d'accès, l'adresse IP, le secret partagé et la méthode d'authentification (RADIUS Cisco Aironet ou RADIUS Cisco IOS/PIX) sont définis. Référez-vous à la documentation du constructeur pour d'autres serveurs d'authentification non-ACS.



Assurez-vous que le serveur d'authentification est configuré pour exécuter la méthode d'authentification EAP désirée. Par exemple, pour un Cisco Secure ACS qui fait LEAP, configurez l'authentification LEAP sur la page Configuration du système - Configuration d'authentification globale. Cliquez sur la **System Configuration (Configuration système)**, puis cliquez sur **Global Authentication Setup (Configuration d'authentification globale)**. Référez-vous à la documentation du constructeur pour d'autres serveurs d'authentification non-ACS ou d'autres méthodes
d'EAP.



Cette image montre Cisco Secure ACS configuré pour PEAP, EAP-FAST, EAP-TLS, LEAP et EAP-
MD5.

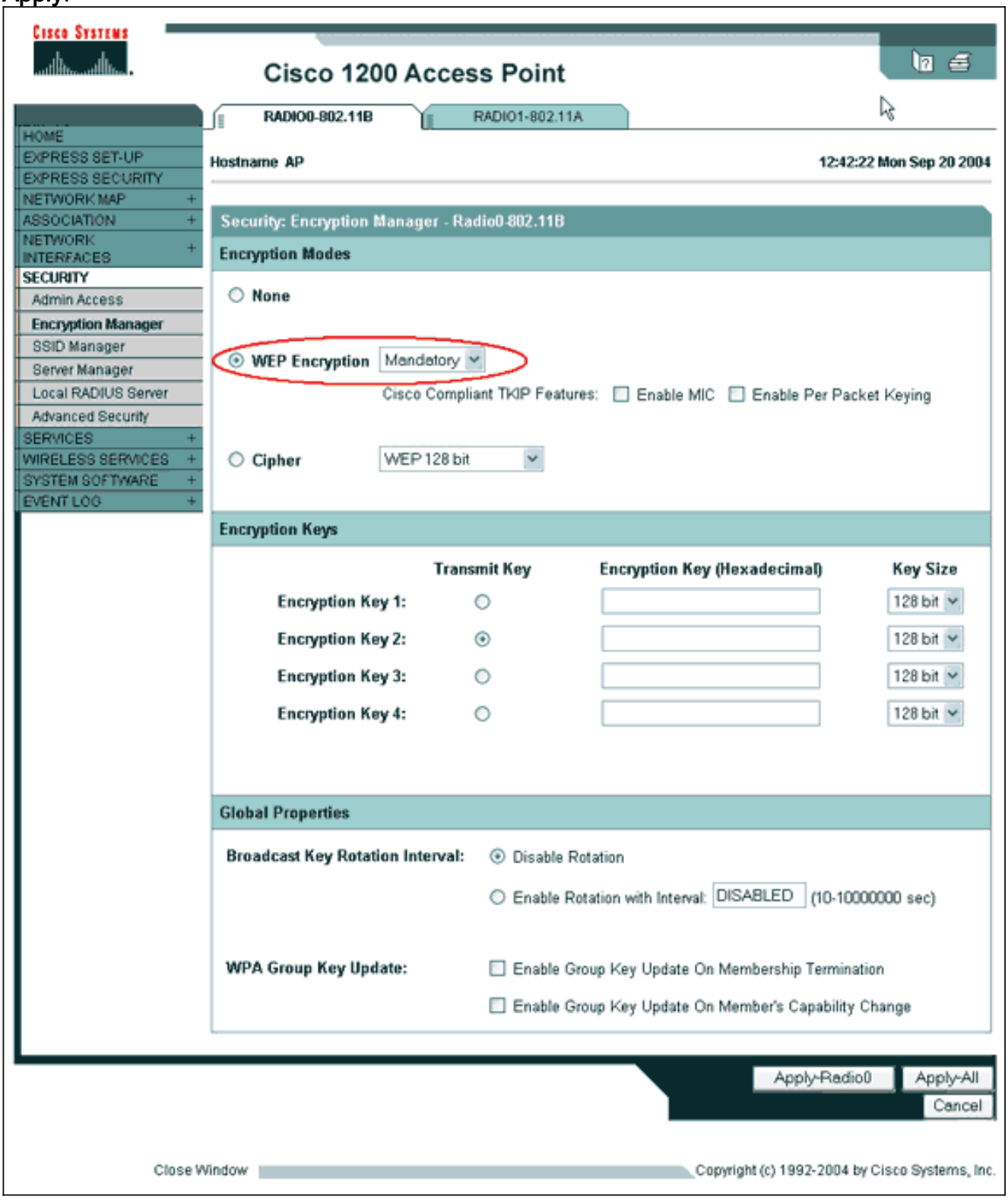


[Définir les méthodes d'authentification du client]

Une fois que le point d'accès sait où envoyer les demandes d'authentification du client, configurez-le pour qu'il accepte ces méthodes.

Remarque: Ces instructions sont pour une installation basée sur WEP. Pour WPA (qui utilise des chiffres au lieu de WEP), référez-vous à Aperçu de la configuration de WPA.

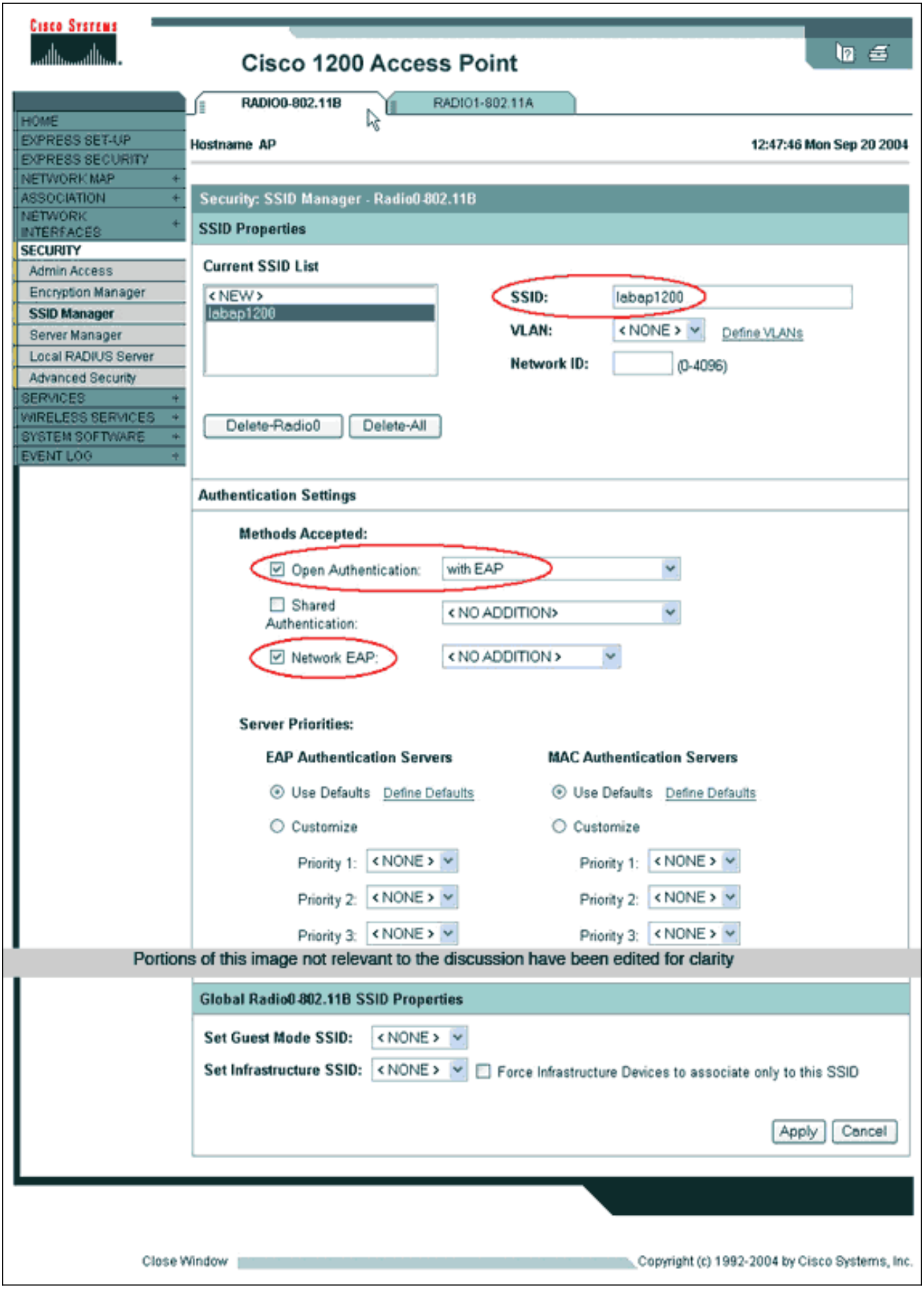
1. Dans l'onglet du gestionnaire de cryptage du point d'accès (sous l'élément de menu **Security > Encryption Manager**), complétez ces étapes :Spécifiez que vous voulez utiliser le **cryptage WEP**.Spécifiez que WEP est **obligatoire**.Vérifiez que la taille de la clé est définie sur **128-bits**.Cliquez sur
Apply.



Vous pouvez également émettre ces commandes de la 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. Complétez ces étapes dans l'onglet du gestionnaire SSID du point d'accès (sous l'élément de menu **Security > SSID Manager**) :Sélectionnez le SSID désiré.Sous Authentication Methods Accepted, cochez la case étiquetée **Open** et utilisez la liste déroulante pour choisir **With EAP**.Cochez la case étiquetée **Network-EAP** si vous avez des cartes client Cisco. Voyez la discussion de la section Network EAP ou authentification ouverte avec EAP.Cliquez sur **Apply**.



Vous pouvez également émettre ces commandes de la 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
```

Une fois que vous confirmez la fonctionnalité de base avec une configuration EAP de base, vous pouvez ajouter des fonctionnalités supplémentaires et la gestion des clés ultérieurement. Posez des fonctions plus complexes au-dessus des bases fonctionnelles afin de faciliter le dépannage.

Vérifier

Cette section fournit des informations qui vous permettront de vérifier que votre configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

- **show radius server-group tout** - Affiche une liste de tous les groupes de serveurs RADIUS configurés sur l'AP.

Dépanner

Procédure de dépannage

Complétez ces étapes afin de dépanner votre configuration.

1. Dans l'utilitaire ou le logiciel côté client, créez un nouveau profil ou nouvelle connexion avec les mêmes paramètres ou des paramètres similaires afin de vous assurer que rien n'a été altéré dans la configuration du client.
2. Afin d'éliminer la possibilité de problèmes RF qui empêchent la réussite de l'authentification, désactivez temporairement l'authentification comme indiqué dans ces étapes :Depuis CLI, utilisez les commandes **no authentication open eap eap_methods**, **no authentication network-eap eap_methods** et **authentication open**.Depuis GUI, sur la page du gestionnaire SSID, décochez **Network-EAP**, cochez **Open** et définissez la liste déroulante sur **No Addition**.Si le client s'associe avec succès, alors RF ne contribue pas au problème d'association.
3. Vérifiez que les mots de passe secrets partagés sont synchronisés entre le point d'accès et le serveur d'authentification. Sinon, vous pouvez recevoir ce message d'erreur :
   ```
   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
```

Depuis CLI, vérifiez la ligne radius-server host x.x.x.x auth-port x acct-port x key <shared_secret>.Depuis GUI, sur la page du gestionnaire de serveur, ressaisissez le secret partagé pour le serveur adéquat dans la case étiquetée Shared Secret.L'entrée de secret partagée pour le point d'accès sur le serveur RADIUS doit contenir le même mot de passe secret partagé que ceux précédemment mentionnés.

4. Supprimez tout groupe d'utilisateurs du serveur RADIUS. Parfois des conflits peuvent se produire entre les groupes d'utilisateurs définis par le serveur RADIUS et les groupes d'utilisateurs dans le domaine sous-jacent. Examinez les tentatives ayant échoué dans les journaux du serveur RADIUS et les raisons de ces échecs.

Dépannage des commandes

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

Le débogage des authentifications fournit une quantité importante de détails sur la façon de recueillir et d'interpréter la sortie des débogages liés à EAP.

Remarque: Avant d'émettre des commandes **debug**, reportez-vous à Informations importantes sur les commandes de débogage.

- **debug dotale aga authenticité state-machine** - Affiche les principales divisions (ou états) de la négociation entre le client et le serveur d'authentification. Voici la sortie d'une authentification **réussie**:

```
*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)
```

Remarque: Dans les versions du logiciel Cisco IOS antérieures à 12.2(15)JA, la syntaxe de cette commande **debug** est **debug dot11 aaa dot1x state-machine**.

- **debug dot11 aaa authenticator process** - Affiche les différentes entrées de dialogue de la négociation entre le client et le serveur d'authentification.**Remarque:** Dans les versions du logiciel Cisco IOS antérieures à 12.2(15)JA, la syntaxe de cette commande de débogage est **debug dot11 aaa dot1x process**.
- **debug radius authentification** - Affiche les négociations de RADIUS entre le serveur et le client, qui sont tous deux reliés par l'AP. Ceci est la sortie d'un **échec d'authentification** :

```
*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** - Affiche les négociations d'AAA pour l'authentification entre le périphérique client et le serveur d'authentification.

Informations connexes

- Déboguer les authentifications
- Configuration des types d'authentification
- Authentification LEAP sur un serveur RADIUS local
- Configuration des serveurs RADIUS et TACACS+
- Configuration de l'accélérateur de contenu sécurisé Cisco Secure pour Windows v3.2 avec authentification PEAP-MS-CHAPv2
- Cisco Secure ACS pour Windows v3.2 avec l'authentification de machine d'EAP-TLS
- Configuration de PEAP/EAP sur Microsoft IAS
- Dépannage de Microsoft IAS en tant que serveur RADIUS
- Authentification du client Microsoft 802.1x
- Support et documentation techniques - Cisco Systems