Accès convergé 5760, 3850, et EAP-FAST de la gamme 3650 WLC avec l'exemple de configuration de serveur RADIUS interne

Contenu

Introduction

Ce document décrit comment configurer Cisco a convergé accès 5760, 3850, et contrôleurs LAN Sans fil de gamme 3650 (WLCs) afin d'agir en tant que serveurs de RADIUS qui exécutent l'authentification Protocol-flexible d'authentification extensible de Cisco par l'intermédiaire du protocole sécurisé (EAP-FAST, dans cet exemple) pour l'authentification client.

Habituellement un serveur RADIUS externe est utilisé afin d'authentifier des utilisateurs, qui n'est pas une solution faisable dans certains cas. Dans ces situations, Access convergé WLC peut agir en tant que serveur de RADIUS, où des utilisateurs sont authentifiés contre la base de données locale qui est configurée dans le WLC. Ceci s'appelle une caractéristique locale de serveur de RADIUS.

Conditions préalables

Exigences

Cisco recommande de posséder des connaissances sur les sujets suivants avant de tenter cette configuration :

- GUI ou CLI de Cisco IOS® avec l'accès convergé 5760, 3850, et la gamme 3650 WLC
- Concepts de Protocole EAP (Extensible Authentication Protocol)
- Configuration d'Identifiant SSID (Service Set Identifier)
- RADIUS

[Composants utilisés](#)

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

- Version 3.3.2 de la gamme Cisco 5760 WLC (local de câblage de nouvelle génération [NGWC])
- Point d'accès léger de gamme Cisco 3602 (AP)
- Microsoft Windows XP avec le suppliant d'Intel PROset
- Commutateurs Cisco Catalyst, série 3560

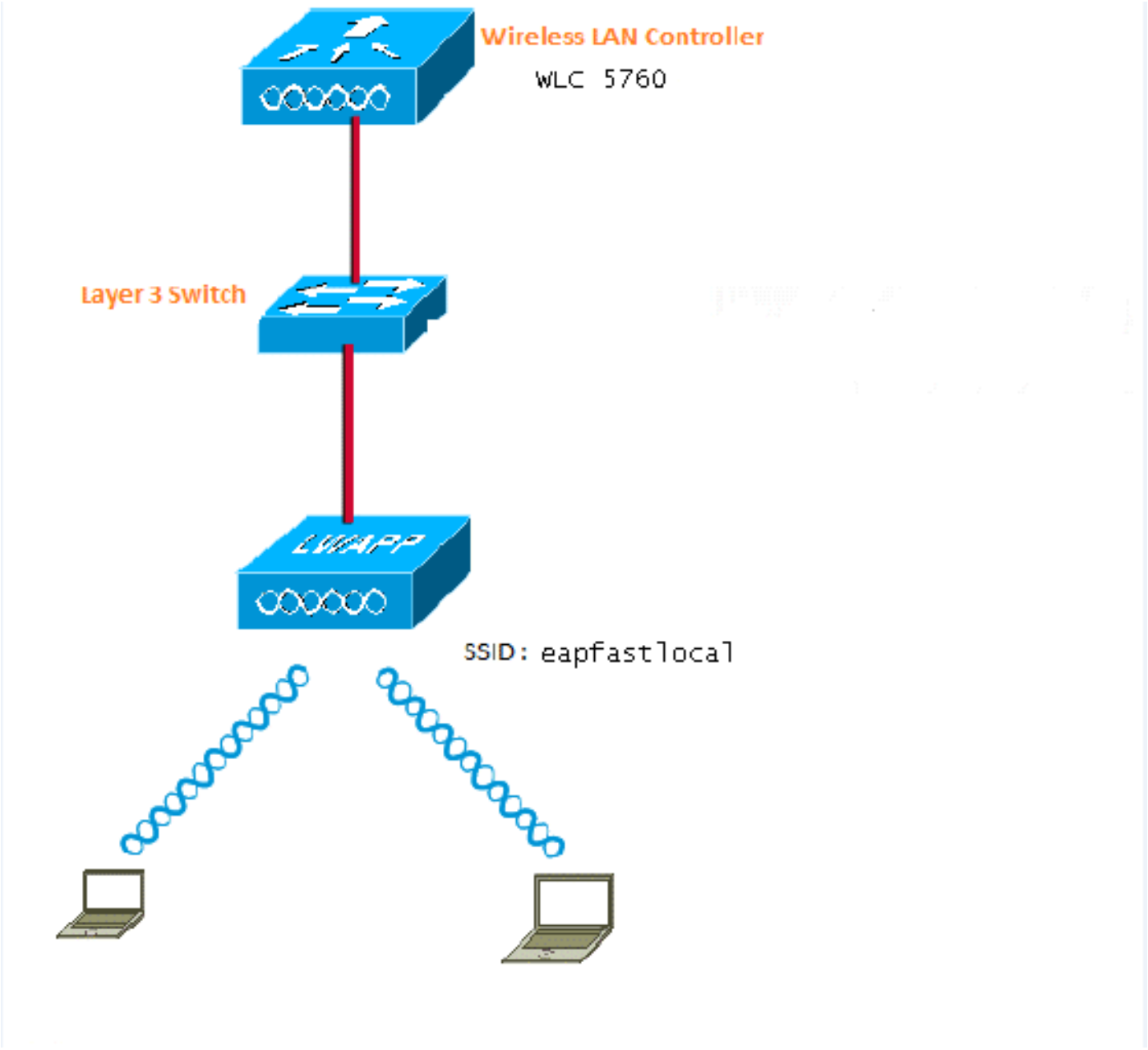
Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez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

Configurer

> Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Cette image fournit un exemple d'un schéma de réseau :



Vue d'ensemble de configuration

Cette configuration est terminée dans deux étapes :

1. Configurez le WLC pour la méthode locale d'EAP et les profils relatifs d'authentification et d'autorisation avec le CLI ou le GUI.

2. Configurez le WLAN et tracez la liste de méthode qui a les profils d'authentification et d'autorisation.

Configurez le WLC avec le CLI

Terminez-vous ces étapes afin de configurer le WLC avec le CLI :

1. Activez le modèle d'AAA sur le WLC :

```
aaa new-model
```

2. Définissez l'authentification et l'autorisation :

```
aaa local authentication eapfast authorization eapfast

aaa authentication dot1x eapfast local
aaa authorization credential-download eapfast local
aaa authentication dot1x default local
```

3. Configurez l'eap profile local et la méthode (l'EAP-FAST est utilisé dans cet exemple) :

```
eap profile eapfast
 method fast
!
```

4. Configurez les paramètres avancés d'EAP-FAST :

```
eap method fast profile eapfast
 description test
 authority-id identity 1
 authority-id information 1
 local-key 0 cisco123
```

5. Configurez le WLAN et tracez le profil local d'autorisation au WLAN :

```
wlan eapfastlocal 13 eapfastlocal
 client vlan VLAN0020
 local-auth eapfast
 session-timeout 1800
 no shutdown
```

6. Configurez l'infrastructure afin de prendre en charge la Connectivité de client :

```
ip dhcp snooping vlan 12,20,30,40,50
ip dhcp snooping
!
ip dhcp pool vlan20
 network 20.20.20.0 255.255.255.0
 default-router 20.20.20.251
 dns-server 20.20.20.251



interface TenGigabitEthernet1/0/1
 switchport trunk native vlan 12
 switchport mode trunk
 ip dhcp relay information trusted
 ip dhcp snooping trust
```

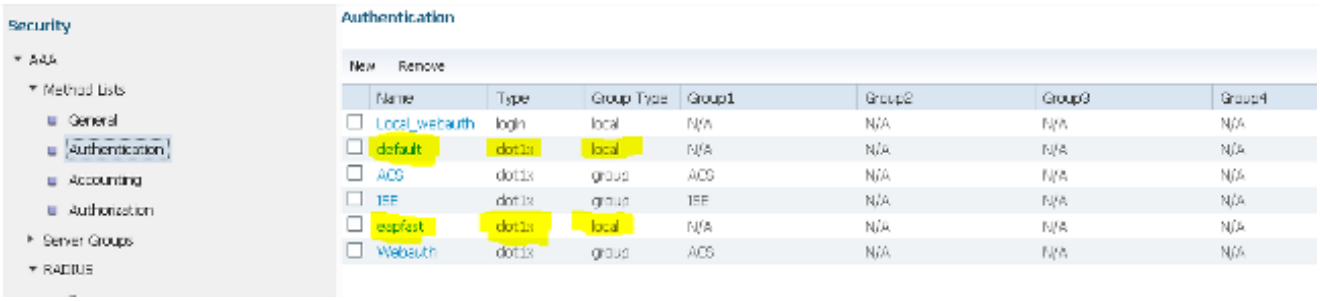
Configurez le WLC avec le GUI

Terminez-vous ces étapes afin de configurer le WLC avec le GUI :

1. Configurez la liste de méthode pour l'authentification :

Configurez le type d'**eapfast** comme **dot1x**.

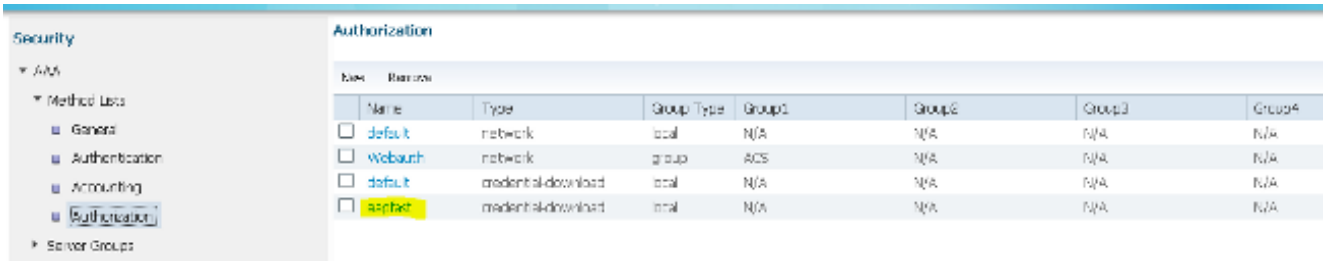
Configurez le type de groupe d'**eapfast** comme **gens du pays**.



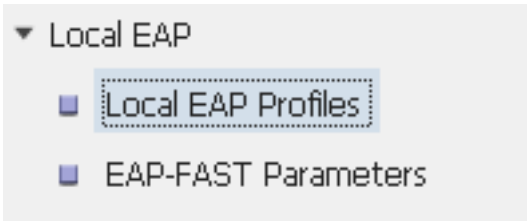
2. Configurez la liste de méthode pour l'autorisation :

Configurez le type d'**eapfast** comme Laisser-passer-**téléchargement**.

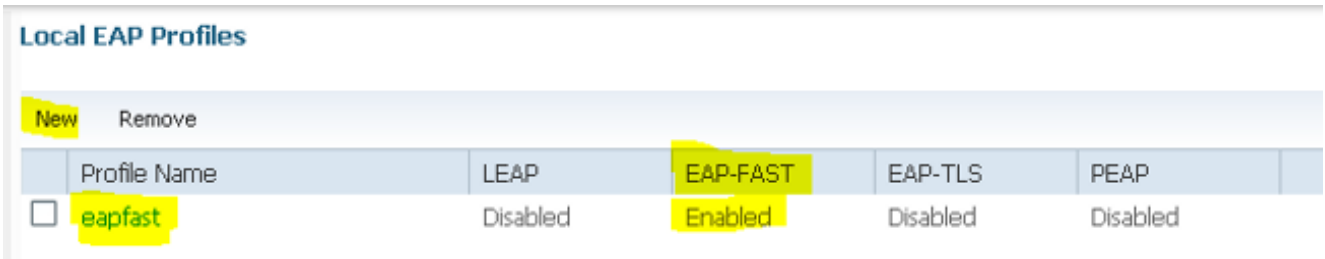
Configurez le type de groupe d'**eapfast** comme **gens du pays**.



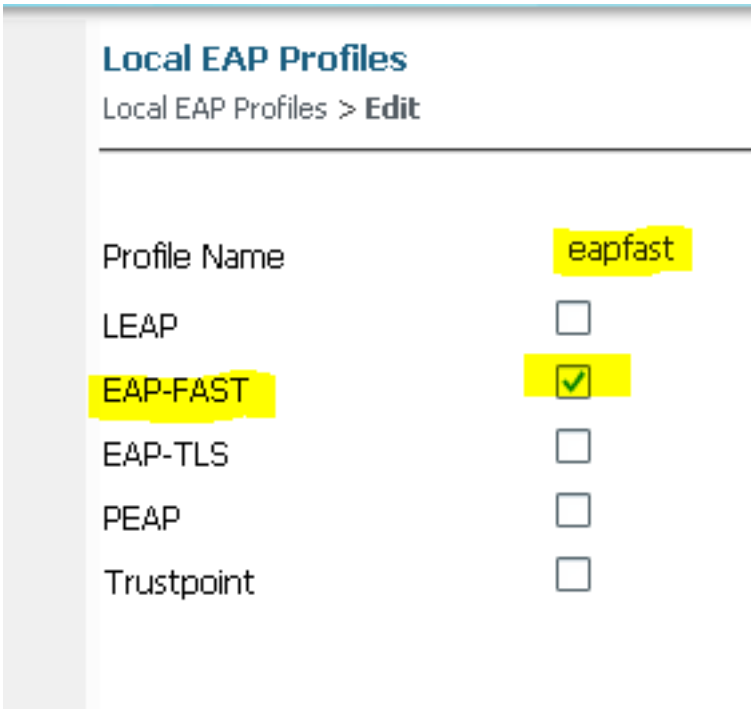
3. Configurez l'eap profile local :



4. Créez un nouveau profil et sélectionnez le type d'EAP :

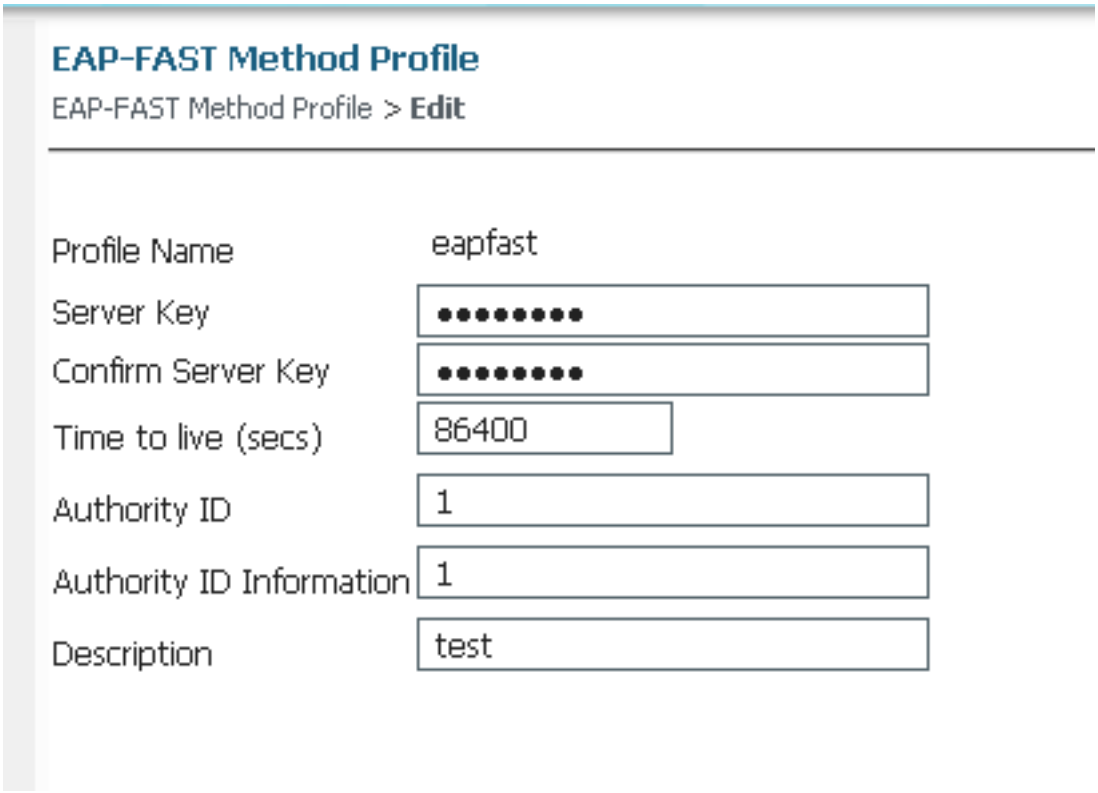


Le nom de profil est **eapfast** et le type sélectionné d'EAP est **EAP-FAST** :

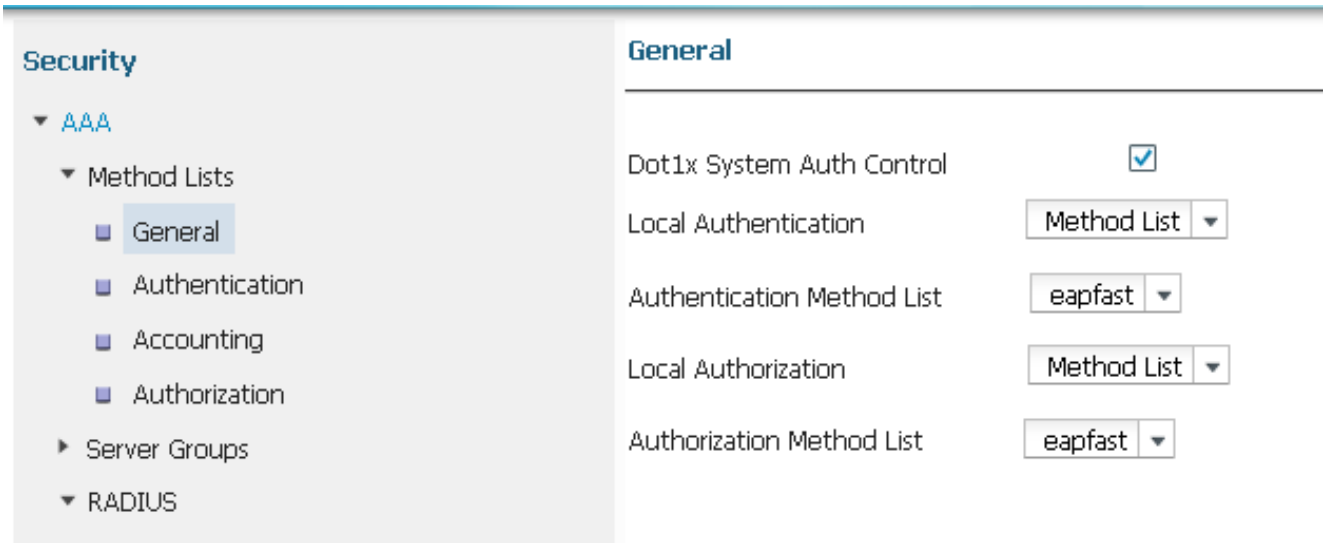


5. Configurez les paramètres de méthode d'EAP-FAST :

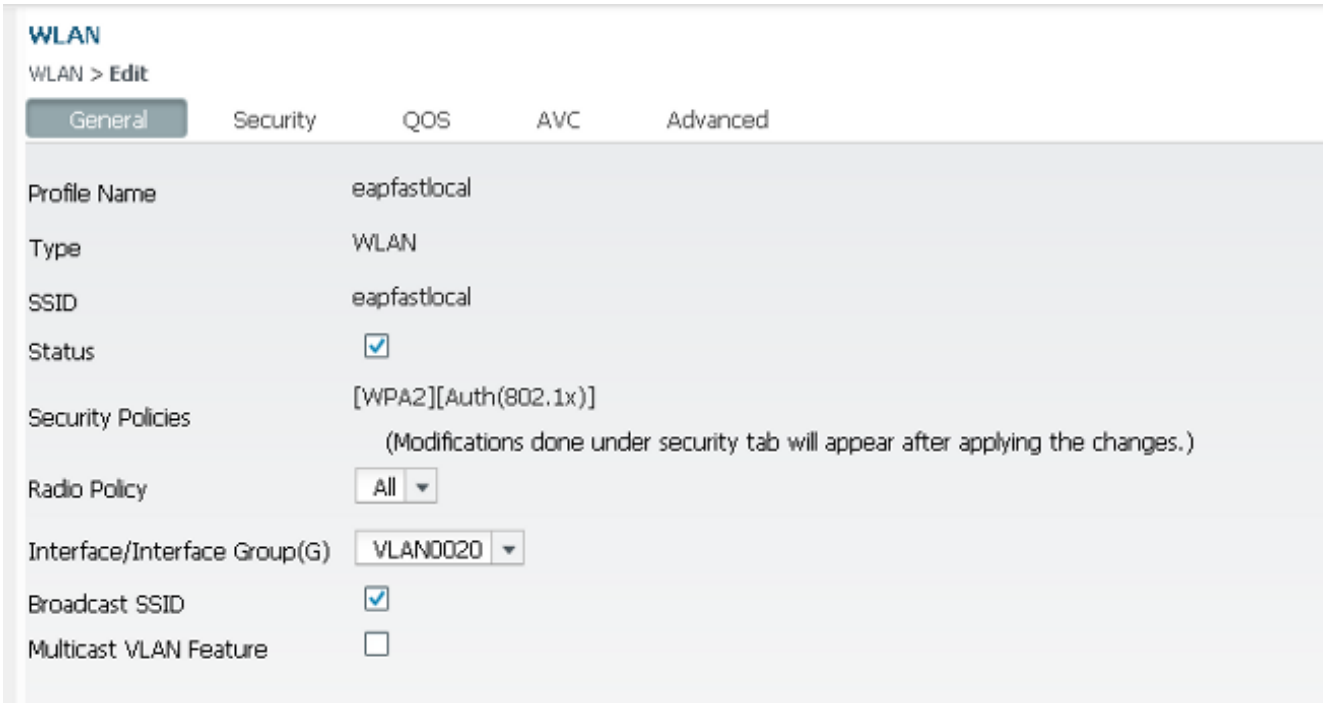
La clé de serveur est configurée comme **Cisco123**.

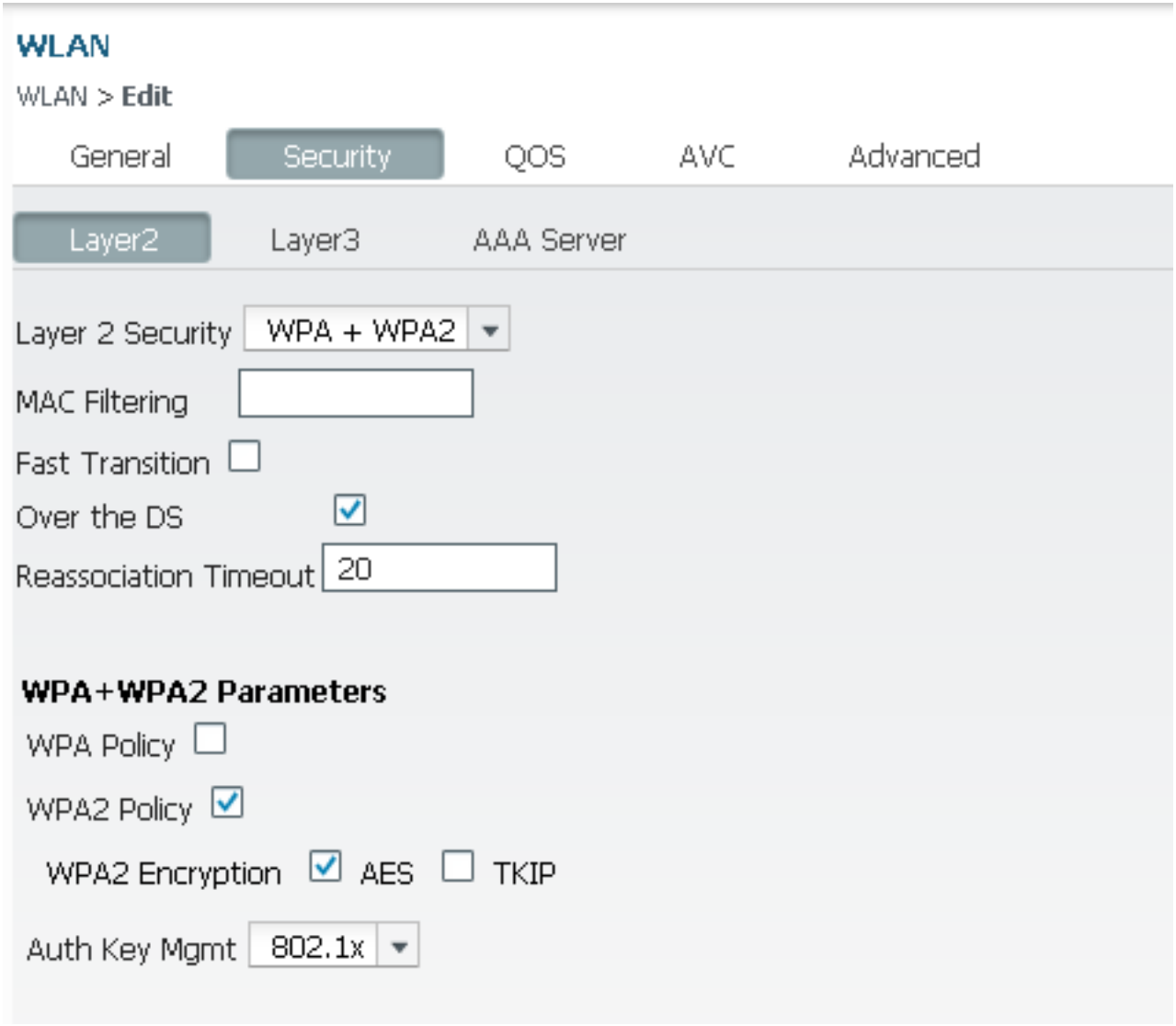


6. Cochez la case **authentique de contrôle de système de dot1x** et l'**eapfast** choisi pour les listes de méthode. Ceci vous aide à exécuter l'authentification EAP locale.

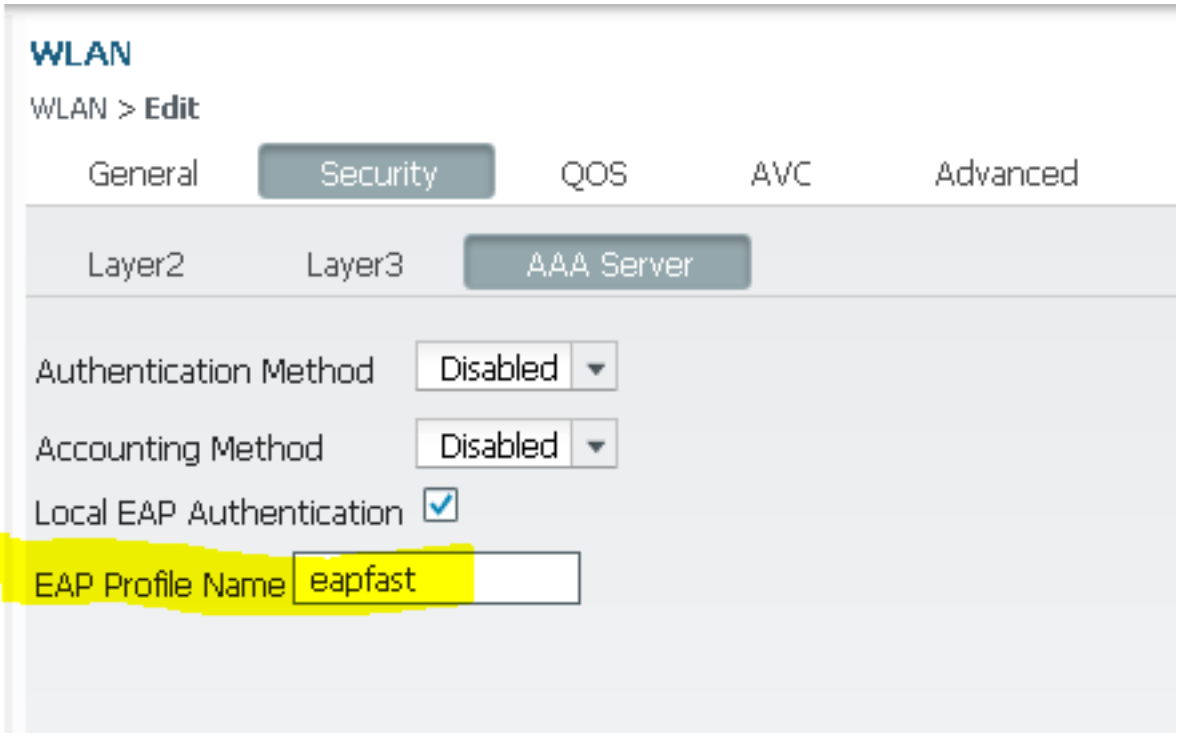


7. Configurez le WLAN pour le cryptage WPA2 AES :





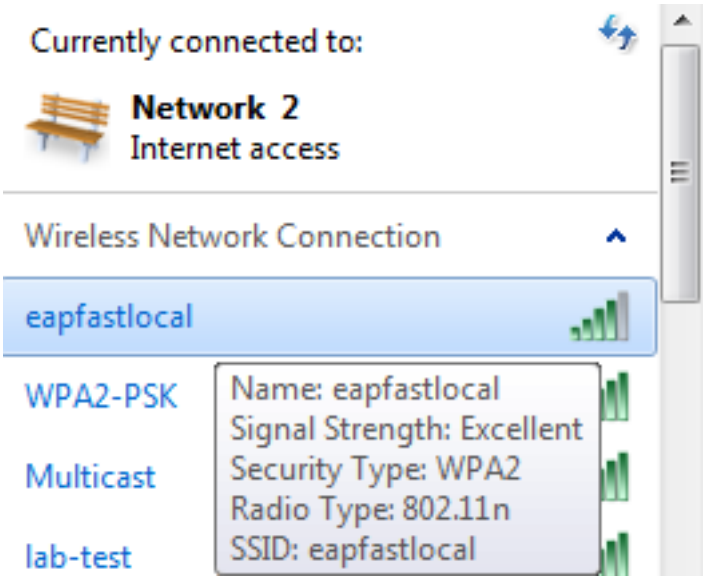
8. Sur l'onglet de **serveur d'AAA**, tracez l'**eapfast de** nom d'eap profile au WLAN :



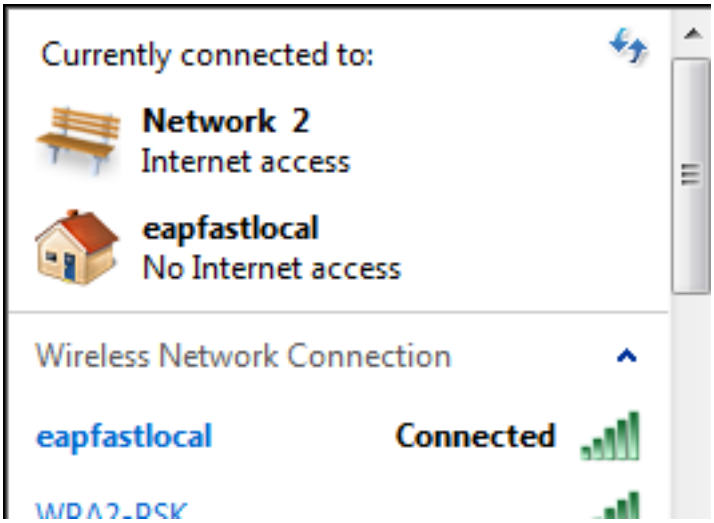
Vérifiez

Terminez-vous ces étapes afin de vérifier que votre configuration fonctionne correctement :

1. Connectez le client au WLAN :



2. Vérifiez que les qualifications de Protected Access (PAC) instantanées paraît et que vous devez recevoir afin d'authentifier avec succès :



Dépanner

Cisco recommande que vous employiez des suivis afin de dépanner les questions Sans fil. Des suivis sont enregistrés dans la mémoire tampon circulaire et ne sont pas processeur intensif.

Permettez à ces suivis afin d'obtenir les logs authentiques de la couche 2 (L2) :

- **débogage de niveau groupe-radio-sécurisé de set trace**
- **filtre groupe-radio-sécurisé mac0021.6a89.51ca de set trace**

Permettez à ces suivis afin d'obtenir les journaux d'événements DHCP :

- **les événements DHCP de set trace nivellent le débogage**
- **MAC 0021.6a89.51ca de filtre d'événements DHCP de set trace**

Voici quelques exemples des suivis réussis :

```
[04/10/14 18:49:50.719 IST 3 8116] 0021.6a89.51ca Association received from
 mobile on AP  c8f9.f983.4260

[04/10/14 18:49:50.719 IST 4 8116] 0021.6a89.51ca qos upstream policy is
 unknown and downstream policy is unknown
[04/10/14 18:49:50.719 IST 5 8116] 0021.6a89.51ca apChanged 1 wlanChanged 0
 mscb ipAddr 20.20.20.6, apf RadiusOverride 0x0, numIPv6Addr=0
[04/10/14 18:49:50.719 IST 6 8116] 0021.6a89.51ca Applying WLAN policy on MSCB.
[04/10/14 18:49:50.719 IST 7 8116] 0021.6a89.51ca Applying WLAN ACL policies
 to client

[04/10/14 18:49:50.719 IST 9 8116] 0021.6a89.51ca Applying site-specific IPv6
 override for station  0021.6a89.51ca  - vapId 13, site 'default-group',
 interface 'VLAN0020'
[04/10/14 18:49:50.719 IST a 8116] 0021.6a89.51ca Applying local bridging
 Interface Policy for station  0021.6a89.51ca  - vlan 20, interface 'VLAN0020'
[04/10/14 18:49:50.719 IST b 8116] 0021.6a89.51ca STA - rates (8):
 140 18 152 36 176 72 96 108 48 72 96 108 0 0 0 0

[04/10/14 18:49:50.727 IST 2f 8116] 0021.6a89.51ca Session Manager Call Client
```

57ca4000000048, uid 42, capwap id 50b94000000012,Flag 4, Audit-Session ID 0a6987b253468efb0000002a, method list

[04/10/14 18:49:50.727 IST 30 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF: [0021.6a89.51ca, Ca3] Session update from Client[1] for 0021.6a89.51ca, ID list 0x00000000
[04/10/14 18:49:50.727 IST 31 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF: [0021.6a89.51ca, Ca3] (UPD): method: Dot1X, method list: none, aaa id: 0x0000002A
[04/10/14 18:49:50.727 IST 32 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF: [0021.6a89.51ca, Ca3] (UPD): eap profile: eapfast

[04/10/14 18:49:50.728 IST 4b 278] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3] Posting AUTH_START for 0xF700000A
[04/10/14 18:49:50.728 IST 4c 278] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3] 0xF700000A:entering request state
[04/10/14 18:49:50.728 IST 4d 278] ACCESS-METHOD-DOT1X-NOTF:[0021.6a89.51ca,Ca3] Sending EAPOL packet
[04/10/14 18:49:50.728 IST 4e 278] ACCESS-METHOD-DOT1X-INFO:[0021.6a89.51ca,Ca3] Platform changed src mac of EAPOL packet
[04/10/14 18:49:50.728 IST 4f 278] ACCESS-METHOD-DOT1X-INFO:[0021.6a89.51ca,Ca3] EAPOL packet sent to client 0xF700000A
[04/10/14 18:49:50.728 IST 50 278] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3] 0xF700000A:idle request action
[04/10/14 18:49:50.761 IST 51 8116] 0021.6a89.51ca 1XA: Received 802.11 EAPOL message (len 5) from mobile
[04/10/14 18:49:50.761 IST 52 8116] 0021.6a89.51ca 1XA: Received EAPOL-Start from mobile
[04/10/14 18:49:50.761 IST 53 8116] 0021.6a89.51ca 1XA: EAPOL-Start - EAPOL start message from mobile as mobile is in Authenticating state, restart authenticating

[04/10/14 18:49:50.816 IST 95 278] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3] 0xF700000A:entering response state
[04/10/14 18:49:50.816 IST 96 278] ACCESS-METHOD-DOT1X-NOTF:[0021.6a89.51ca,Ca3] Response sent to the server from 0xF700000A
[04/10/14 18:49:50.816 IST 97 278] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3] 0xF700000A:ignore response action
[04/10/14 18:49:50.816 IST 98 203] Parsed CLID MAC Address = 0:33:106:137:81:202
[04/10/14 18:49:50.816 IST 99 203] AAA SRV(00000000): process authen req
[04/10/14 18:49:50.816 IST 9a 203] AAA SRV(00000000): Authen method=LOCAL

[04/10/14 18:49:50.846 IST 11d 181] ACCESS-CORE-SM-CLIENT-SPI-NOTF: [0021.6a89.51ca, Ca3] Session authz status notification sent to Client[1] for 0021.6a89.51ca with handle FE000052, list 630007B2
[04/10/14 18:49:50.846 IST 11e 181]ACCESS-METHOD-DOT1X-NOTF:[0021.6a89.51ca,Ca3] Received Authz Success for the client 0xF700000A (0021.6a89.51ca)
[04/10/14 18:49:50.846 IST 11f 271] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3] Posting AUTHZ_SUCCESS on Client 0xF700000A
[04/10/14 18:49:50.846 IST 120 271] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3] 0xF700000A:entering authenticated state
[04/10/14 18:49:50.846 IST 121 271]ACCESS-METHOD-DOT1X-NOTF:[0021.6a89.51ca,Ca3] EAPOL success packet was sent earlier.

[04/10/14 18:49:50.846 IST 149 8116] 0021.6a89.51ca 1XA:authentication succeeded
[04/10/14 18:49:50.846 IST 14a 8116] 0021.6a89.51ca 1XK: Looking for BSSID c8f9.f983.4263 in PMKID cache
[04/10/14 18:49:50.846 IST 14b 8116] 0021.6a89.51ca 1XK: Looking for BSSID c8f9.f983.4263 in PMKID cache
[04/10/14 18:49:50.846 IST 14c 8116] 0021.6a89.51ca **Starting key exchange with mobile - data forwarding is disabled**
[04/10/14 18:49:50.846 IST 14d 8116] 0021.6a89.51ca 1XA: **Sending EAPOL message to mobile, WLAN=13 AP WLAN=13**
[04/10/14 18:49:50.858 IST 14e 8116] 0021.6a89.51ca 1XA: Received 802.11 EAPOL

message (len 123) from mobile
[04/10/14 18:49:50.858 IST 14f 8116] 0021.6a89.51ca 1XA: Received EAPOL-Key from mobile
[04/10/14 18:49:50.858 IST 150 8116] 0021.6a89.51ca 1XK: **Received EAPOL-key in PTK_START state (msg 2) from mobile**
[04/10/14 18:49:50.858 IST 151 8116] 0021.6a89.51ca 1XK: Stopping retransmission timer
[04/10/14 18:49:50.859 IST 152 8116] 0021.6a89.51ca 1XA**: Sending EAPOL message to mobile, WLAN=13 AP WLAN=13**
[04/10/14 18:49:50.862 IST 153 8116] 0021.6a89.51ca 1XA: Received 802.11 EAPOL message (len 99) from mobile
[04/10/14 18:49:50.862 IST 154 8116] 0021.6a89.51ca 1XA: Received EAPOL-Key from mobile
[04/10/14 18:49:50.862 IST 155 8116] 0021.6a89.51ca 1XK: **Received EAPOL-key in PTKINITNEGOTIATING state (msg 4) from mobile**

[04/10/14 18:49:50.863 IST 172 338] [WCDB] wcdb_ffcp_cb: client (0021.6a89.51ca) client (0x57ca4000000048): FFCP operation (UPDATE) return code (0)
[04/10/14 18:49:50.914 IST 173 273] dhcp pkt processing routine is called for pak with SMAC = 0021.6a89.51ca and SRC_ADDR = 0.0.0.0
[04/10/14 18:49:50.914 IST 174 219] sending dhcp packet outafter processing with SMAC = 0021.6a89.51ca and SRC_ADDR = 0.0.0.0
[04/10/14 18:49:50.914 IST 175 256] DHCPD: address 20.20.20.6 mask 255.255.255.0
[04/10/14 18:49:54.279 IST 176 273] dhcp pkt processing routine is called for pak with SMAC = 0021.6a89.51ca and SRC_ADDR = 20.20.20.6
[04/10/14 18:49:54.279 IST 177 219] sending dhcp packet outafter processing with SMAC = 0021.6a89.51ca and SRC_ADDR = 20.20.20.6