Exemplo de Configuração de WLC EAP-FAST de Acesso Convergente das Séries 5760, 3850 e 3650 com Servidor RADIUS Interno

Contents

Introduction

Este documento descreve como configurar os Cisco Converged Access 5760, 3850 e 3650 Series Wireless LAN Controllers (WLCs) para atuar como servidores RADIUS que executam o Cisco Extensible Authentication Protocol-Flexible Authentication via Secure Protocol (EAP-FAST, neste exemplo) para autenticação de cliente.

Geralmente, um servidor RADIUS externo é usado para autenticar usuários, o que não é uma solução viável em alguns casos. Nessas situações, uma WLC de Acesso Convergente pode atuar como um servidor RADIUS, onde os usuários são autenticados no banco de dados local configurado na WLC. Isso é chamado de recurso de servidor RADIUS local.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos antes de tentar esta configuração:

- Cisco IOS® GUI ou CLI com o WLC de acesso convergido 5760, 3850 e 3650 Series
- Conceitos do Extensible Authentication Protocol (EAP)
- Configuração do Service Set Identifier (SSID)
- RADIUS

Componentes Utilizados

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

- WLC Cisco 5760 Series versão 3.3.2 (Next Generation Wiring Closet [NGWC])
- Access Point (AP) Lightweight Cisco 3602 Series
- Microsoft Windows XP com Intel PROset Supplicant
- Cisco Catalyst 3560 Series Switches

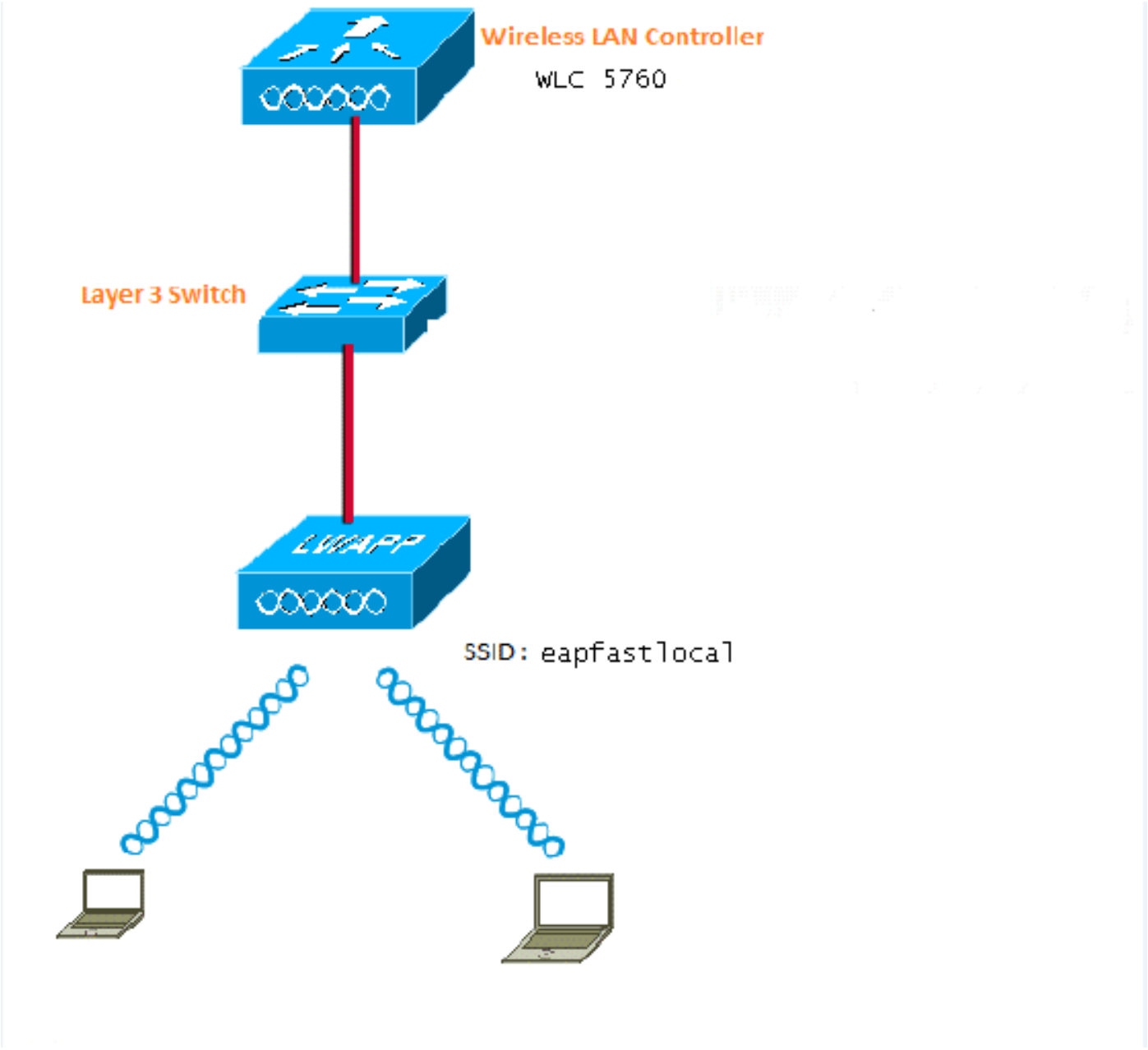
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

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

Diagrama de Rede

A imagem fornece um exemplo de um diagrama de rede:



Visão geral sobre a configuração

Essa configuração é concluída em duas etapas:

1. Configure a WLC para o método EAP local e os perfis de autenticação e autorização relacionados com a CLI ou GUI.

2. Configure a WLAN e mapeie a lista de métodos que tem os perfis de autenticação e autorização.

Configurar a WLC com a CLI

Conclua estes passos para configurar a WLC com a CLI:

1. Ative o modelo AAA na WLC:

```
aaa new-model
```

2. Defina a autenticação e a autorização:

```
aaa local authentication eapfast authorization eapfast

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

3. Configure o perfil EAP local e o método (EAP-FAST é usado neste exemplo):

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

4. Configure os parâmetros EAP-FAST avançados:

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

5. Configure a WLAN e mapeie o perfil de autorização local para a WLAN:

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

6. Configure a infraestrutura para suportar a conectividade do cliente:

```
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
```

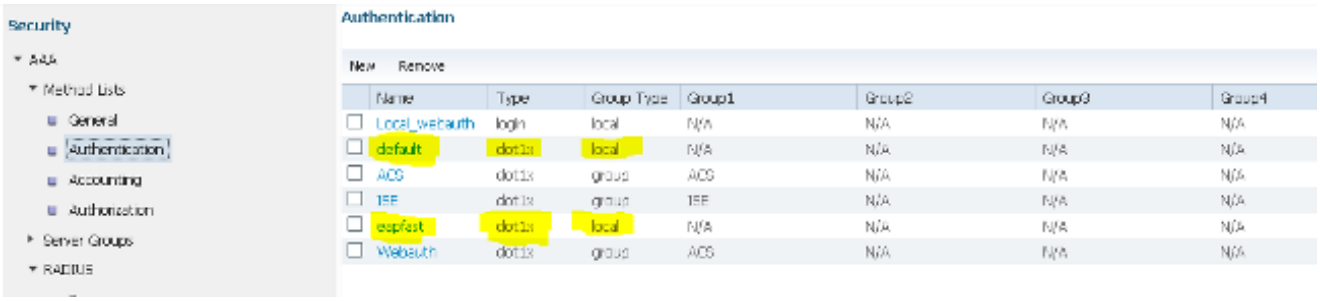
Configurar o WLC com a GUI

Conclua estes passos para configurar a WLC com a GUI:

1. Configure a lista de métodos para Autenticação:

Configure o **eapfast** Type como **Dot1x**.

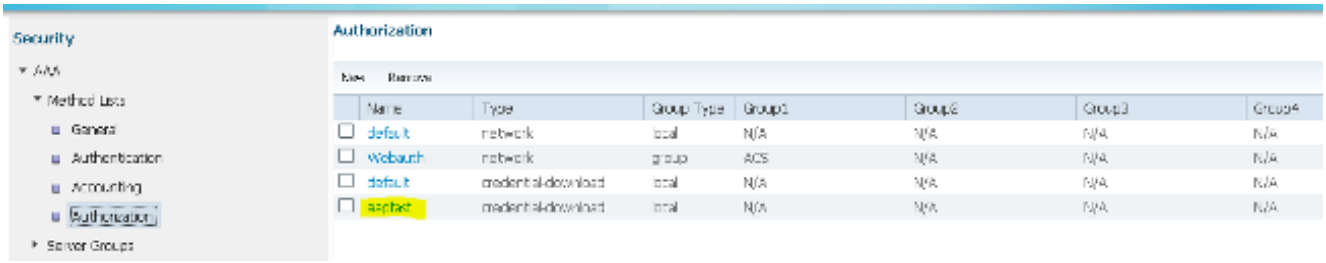
Configure o tipo de grupo **eapfast** como **Local**.



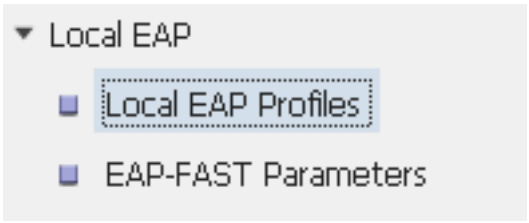
2. Configure a lista de métodos para autorização:

Configure o **eapfast** Type como **Credential-Download**.

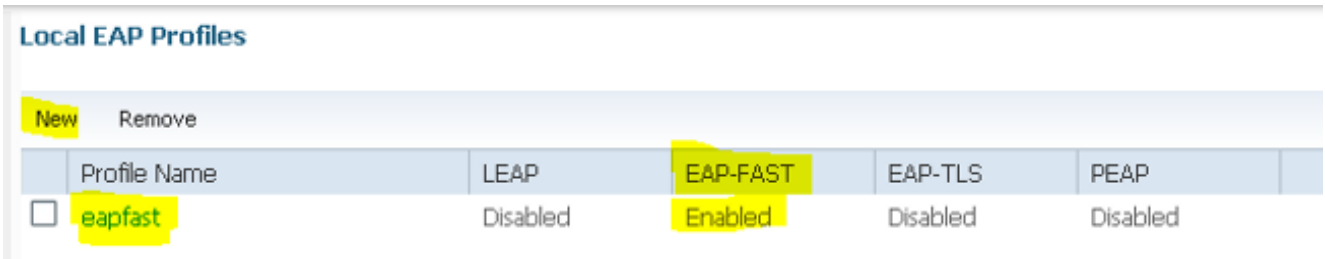
Configure o tipo de grupo **eapfast** como **Local**.



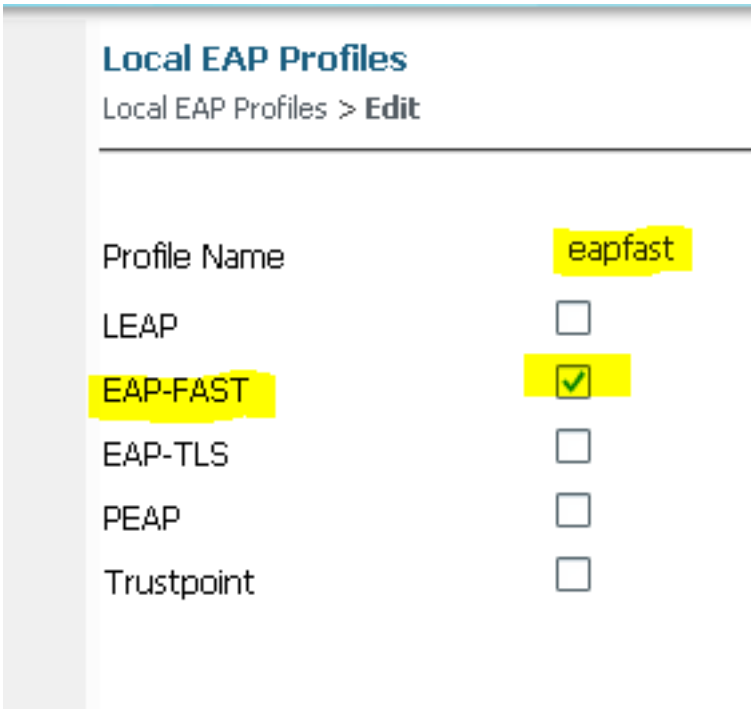
3. Configurar o perfil EAP local:



4. Crie um novo perfil e selecione o tipo de EAP:

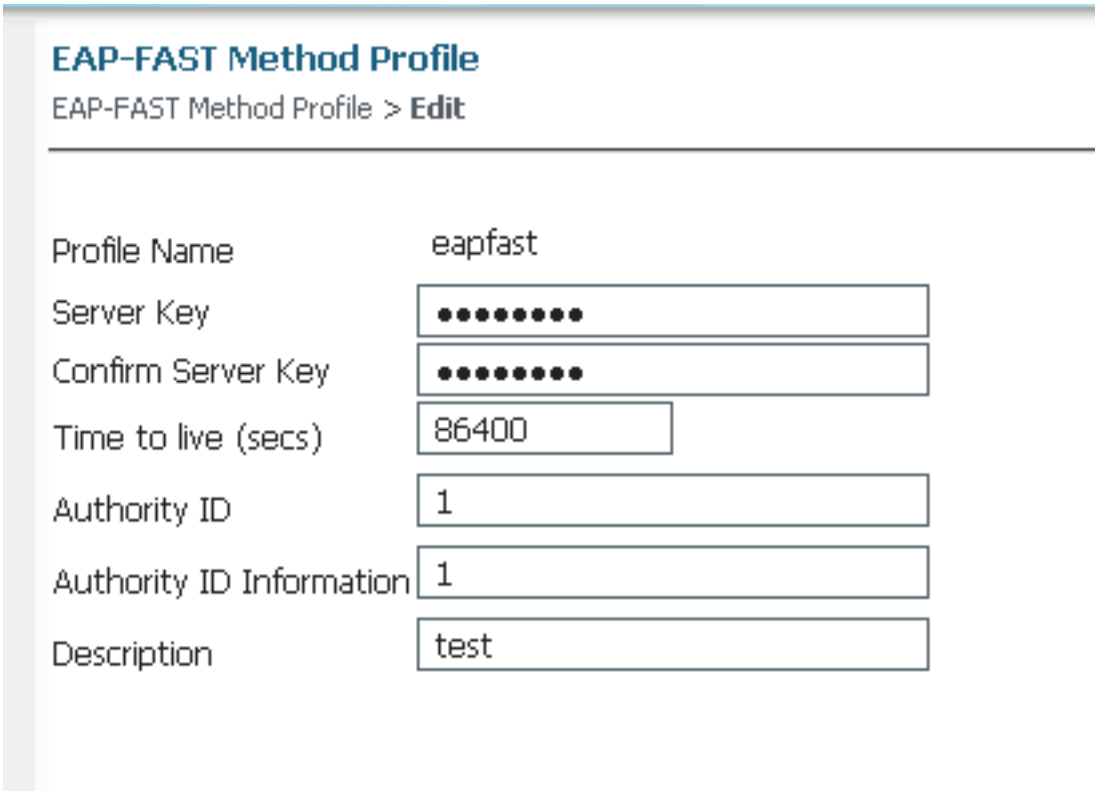


O nome do perfil é **eapfast** e o tipo de EAP selecionado é **EAP-FAST**:

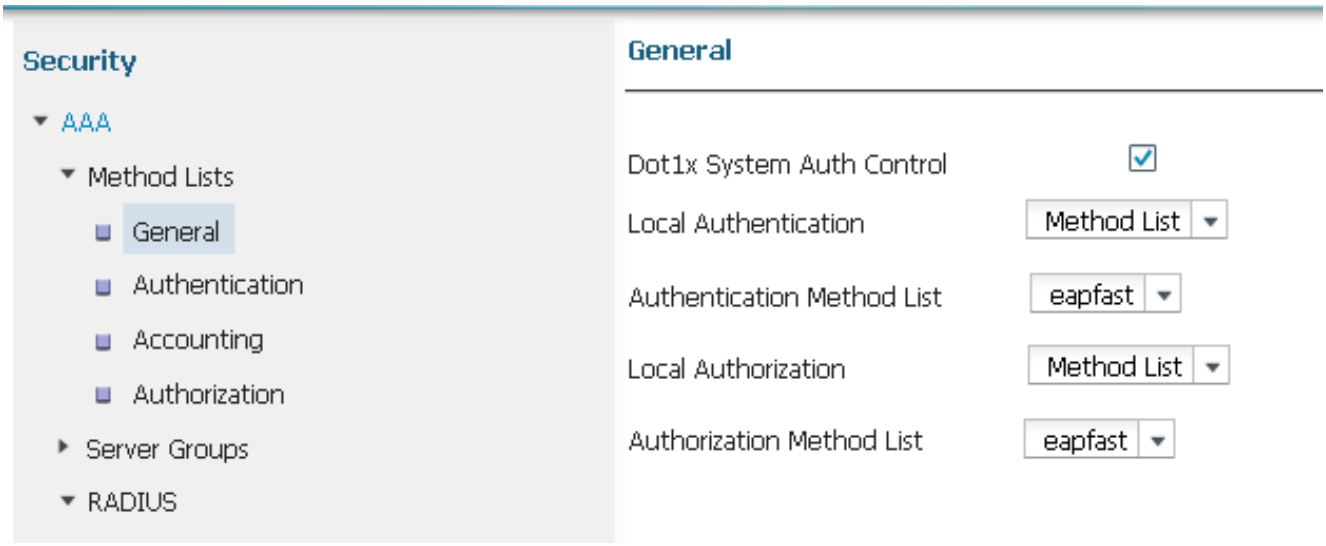


5. Configure os parâmetros do método EAP-FAST:

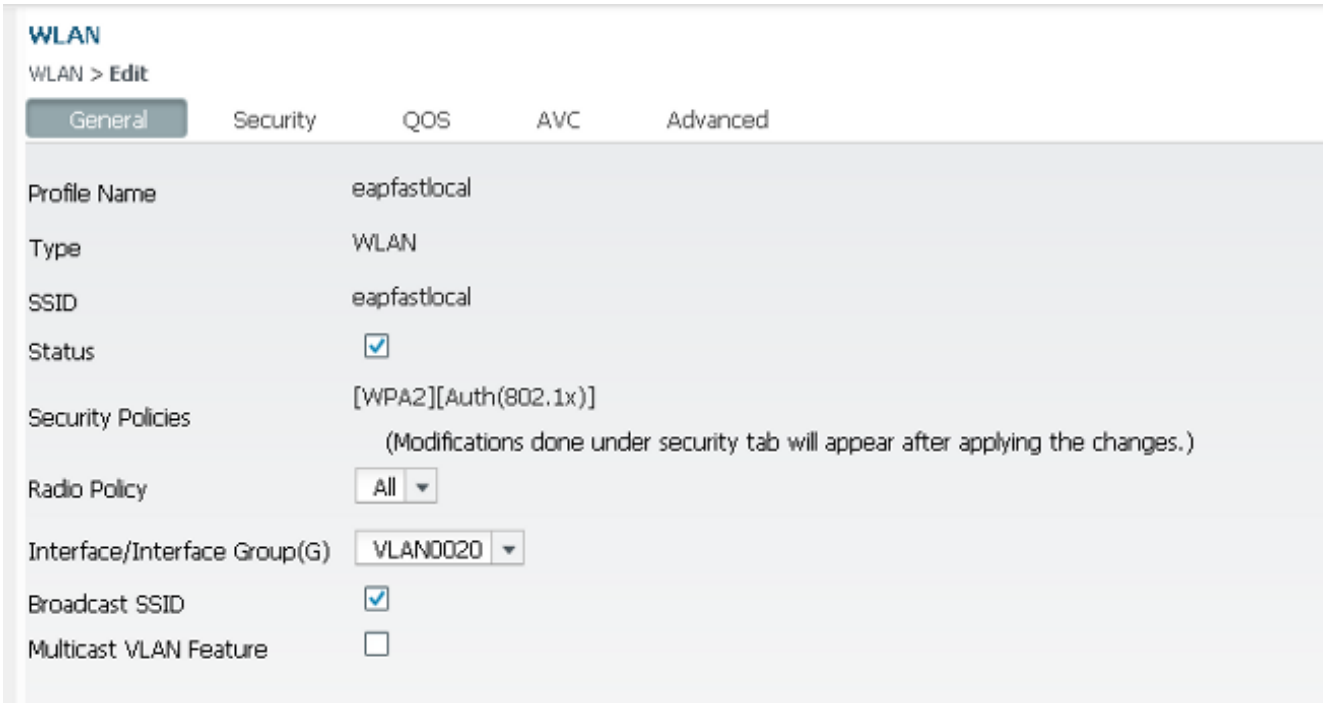
A Chave do Servidor está configurada como **Cisco123**.

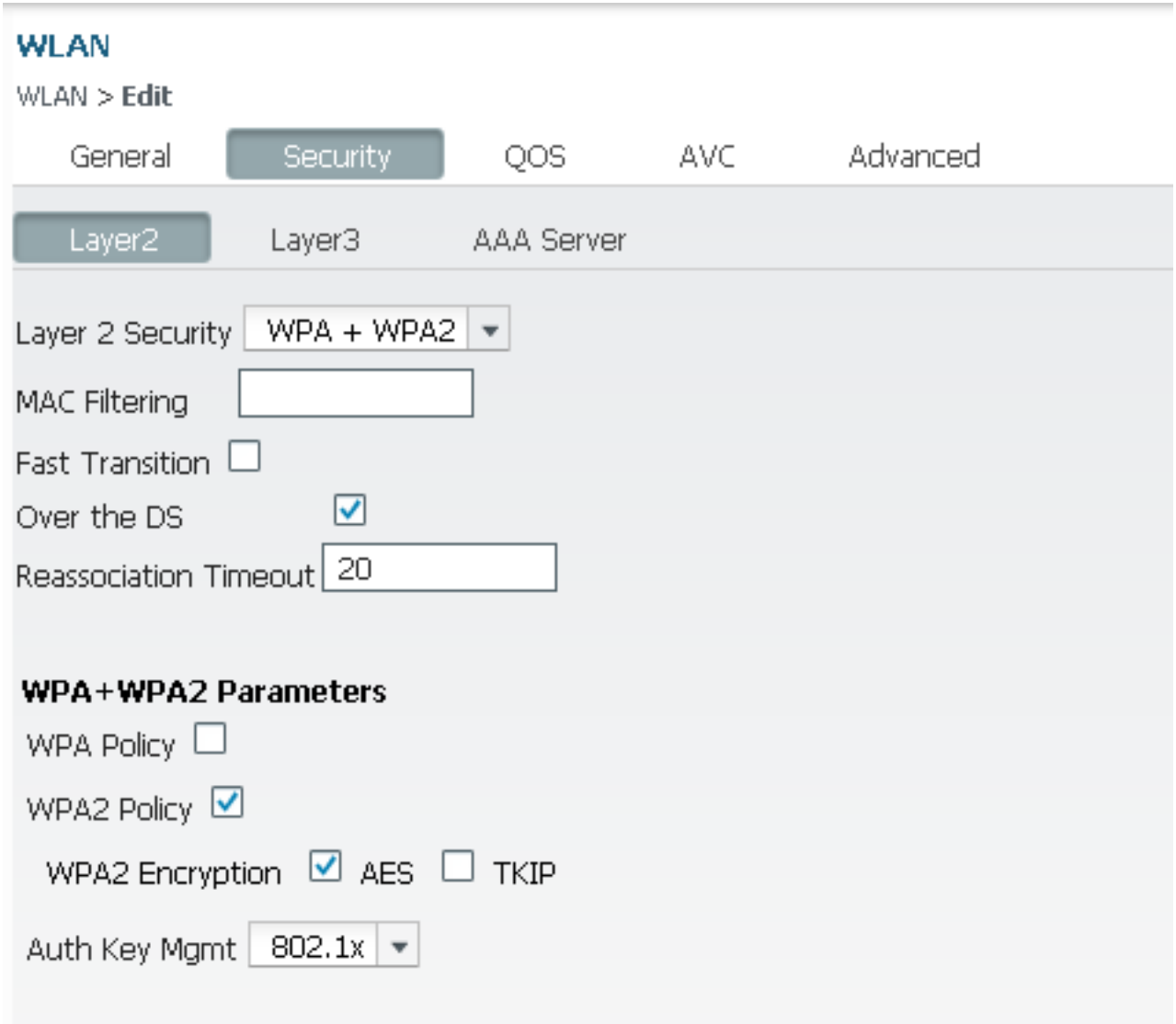


6. Marque a caixa de seleção **Dot1x System Auth Control** e selecione **eapfast** para as listas de métodos. Isso ajuda a executar a autenticação EAP local.

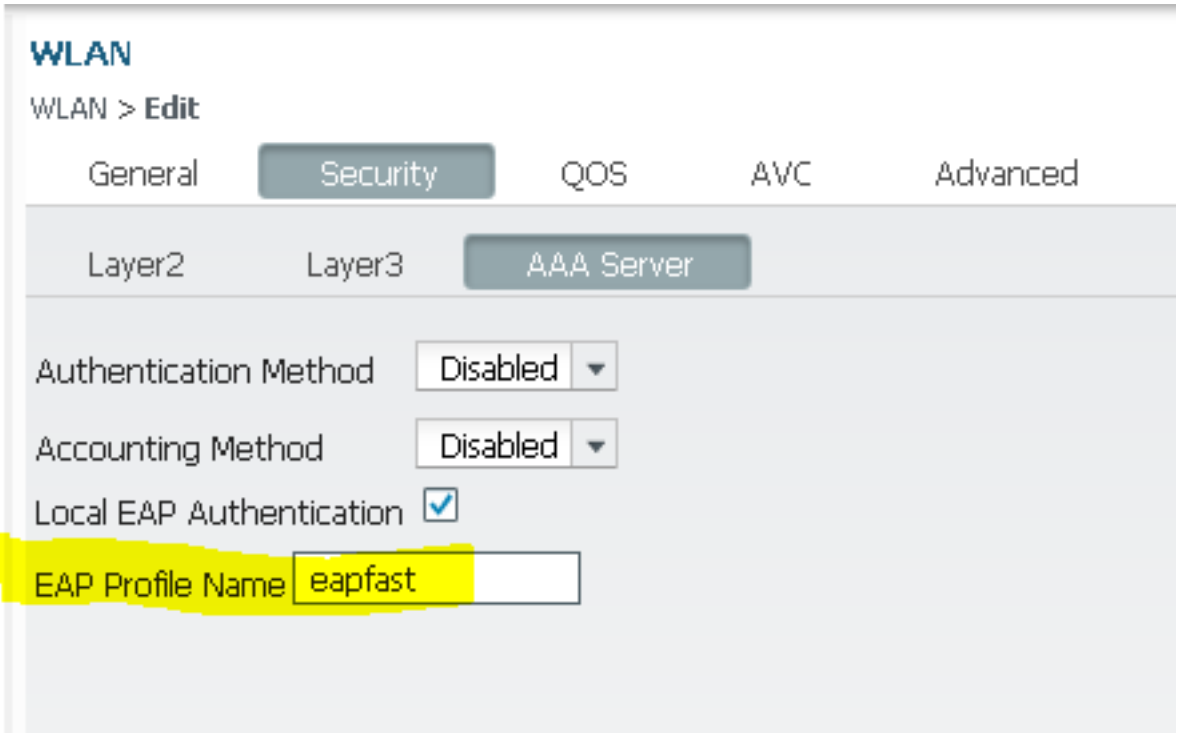


7. Configure a WLAN para a criptografia WPA2 AES:





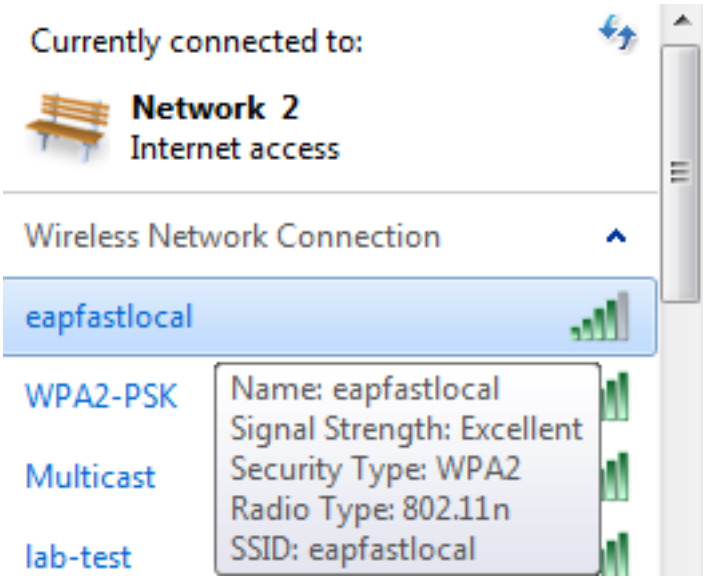
8. Na guia **AAA Server**, mapeie o nome do perfil EAP **rapidamente** para a WLAN:



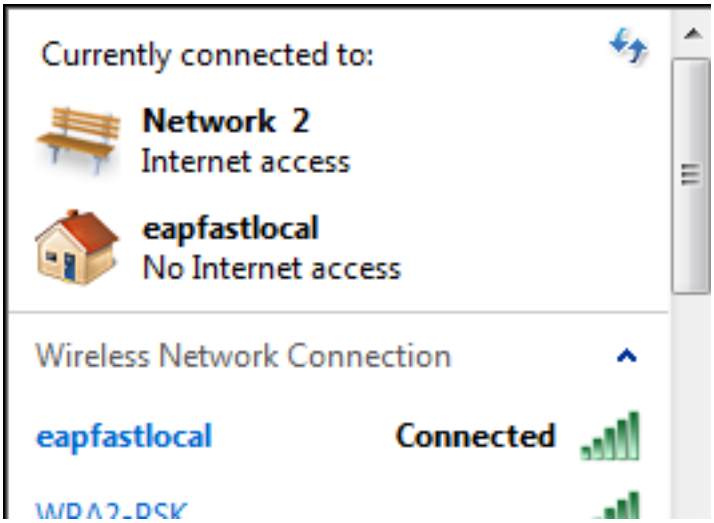
Verificar

Conclua estes passos para verificar se sua configuração funciona corretamente:

1. Conecte o cliente à WLAN:



2. Verifique se o pop-up PAC (Protected Access Credentials) é exibido e se você deve aceitar para autenticar com êxito:



Troubleshoot

A Cisco recomenda que você use rastreamentos para solucionar problemas de conexões sem fio. Os rastreamentos são salvos no buffer circular e não exigem muito do processador.

Ative estes rastreamentos para obter os registros de autenticação da Camada 2 (L2):

- **set trace group-wireless-secure level debug**
- **set trace group-wireless-secure filter mac0021.6a89.51ca**

Ative estes rastreamentos para obter os registros de eventos DHCP:

- **set trace dhcp events level debug**
- **set trace dhcp events filter mac 0021.6a89.51ca**

Aqui estão alguns exemplos de rastreamentos bem-sucedidos:

```
[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