

# Konfigurationsbeispiel für konvergenten Zugriff auf WLC EAP-FAST der Serien 5760, 3850 und 3650 mit internem RADIUS-Server

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurationsübersicht](#)

[Konfigurieren des WLC mithilfe der CLI](#)

[Konfigurieren des WLC mithilfe der GUI](#)

[Überprüfen](#)

[Fehlerbehebung](#)

## Einführung

In diesem Dokument wird beschrieben, wie die Cisco WLCs (Converged Access 5760, 3850 und 3650) für die Client-Authentifizierung als RADIUS-Server konfiguriert werden, die Cisco Extensible Authentication Protocol-Flexible Authentication via Secure Protocol (in diesem Beispiel EAP-FAST) ausführen.

In der Regel wird ein externer RADIUS-Server für die Benutzerauthentifizierung verwendet, was in einigen Fällen nicht praktikabel ist. In diesen Situationen kann ein WLC für konvergenten Zugriff als RADIUS-Server fungieren, bei dem Benutzer anhand der im WLC konfigurierten lokalen Datenbank authentifiziert werden. Dies wird als Funktion für einen lokalen RADIUS-Server bezeichnet.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, vor dem Versuch dieser Konfiguration über Kenntnisse dieser Themen zu verfügen:

- Cisco IOS<sup>®</sup> GUI oder CLI mit dem WLC der Serien Converged Access 5760, 3850 und 3650
- EAP-Konzepte (Extensible Authentication Protocol)
- SSID-Konfiguration (Service Set Identifier)
- RADIUS

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco WLC Version 3.3.2 der Serie 5760 (Next Generation Wiring Closet [NGWC])
- Cisco Lightweight Access Point (AP) der Serie 3602
- Microsoft Windows XP mit Intel PROset-Komponente
- Cisco Catalyst Switches der Serie 3560

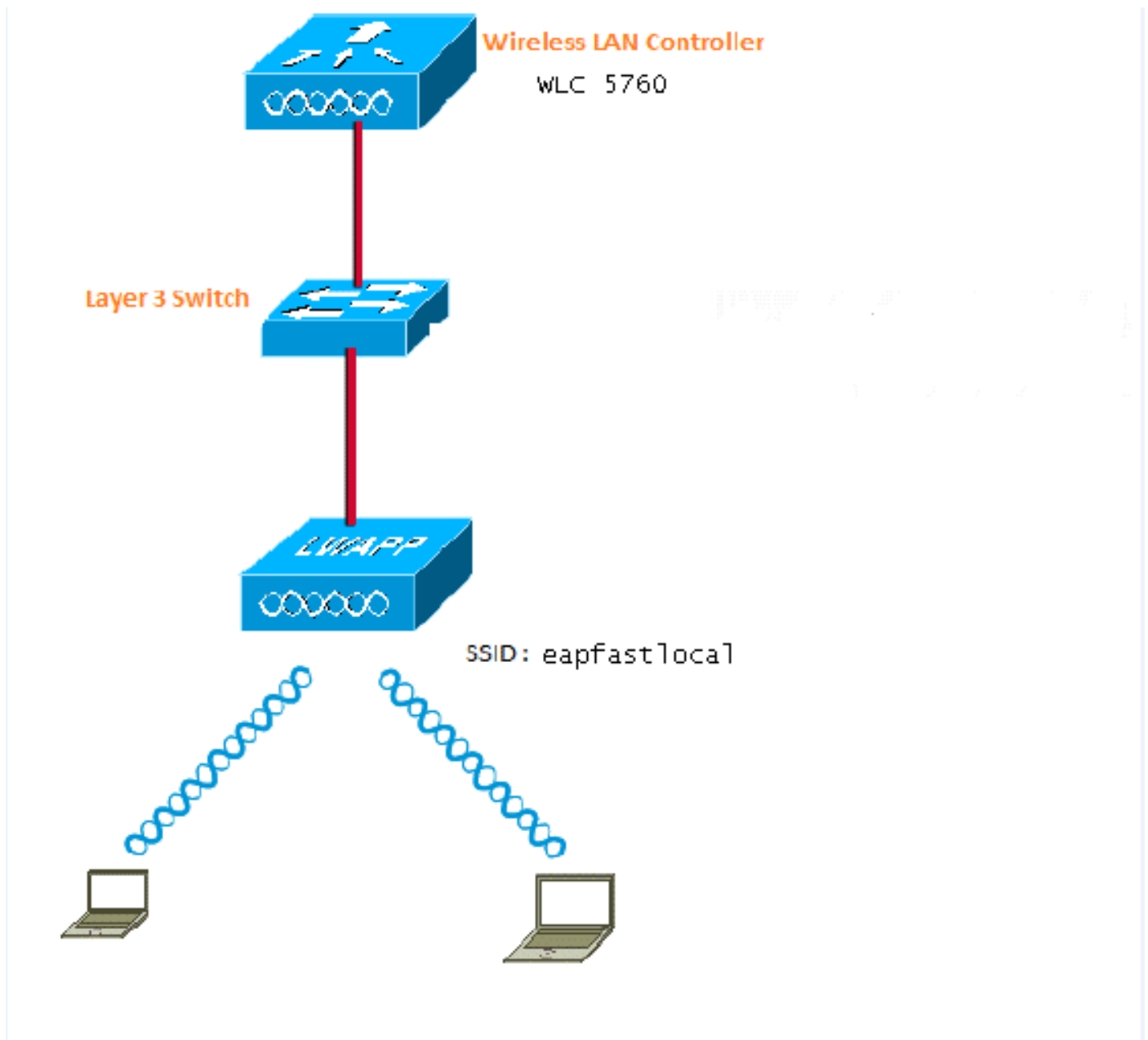
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Konfigurieren

**Hinweis:** Verwenden Sie das [Command Lookup Tool](#) (nur [registrierte](#) Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

## Netzwerkdiagramm

Dieses Bild enthält ein Beispiel für ein Netzwerkdiagramm:



## Konfigurationsübersicht

Diese Konfiguration ist in zwei Schritten abgeschlossen:

1. Konfigurieren Sie den WLC für die lokale EAP-Methode und die zugehörigen Authentifizierungs- und Autorisierungsprofile mithilfe der CLI oder GUI.
2. Konfigurieren Sie das WLAN, und ordnen Sie der Methodenliste die Authentifizierungs- und Autorisierungsprofile zu.

## Konfigurieren des WLC mithilfe der CLI

Gehen Sie wie folgt vor, um den WLC mit der CLI zu konfigurieren:

1. Aktivieren Sie das AAA-Modell auf dem WLC:

```
aaa new-model
```

## 2. Definieren Sie Authentifizierung und Autorisierung:

```
aaa local authentication eapfast authorization eapfast
```

```
aaa authentication dot1x eapfast local
```

```
aaa authorization credential-download eapfast local
```

```
aaa authentication dot1x default local
```

## 3. Konfigurieren Sie das lokale EAP-Profil und die Methode (in diesem Beispiel wird EAP-FAST verwendet):

```
eap profile eapfast
```

```
method fast
```

```
!
```

## 4. Konfigurieren Sie die erweiterten EAP-FAST-Parameter:

```
eap method fast profile eapfast
```

```
description test
```

```
authority-id identity 1
```

```
authority-id information 1
```

```
local-key 0 cisco123
```

## 5. Konfigurieren Sie das WLAN, und ordnen Sie das lokale Autorisierungsprofil dem WLAN zu:

```
wlan eapfastlocal 13 eapfastlocal
```

```
client vlan VLAN0020
```

```
local-auth eapfast
```

```
session-timeout 1800
```

```
no shutdown
```

## 6. Konfigurieren Sie die Infrastruktur, um die Client-Konnektivität zu unterstützen:

```
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
```

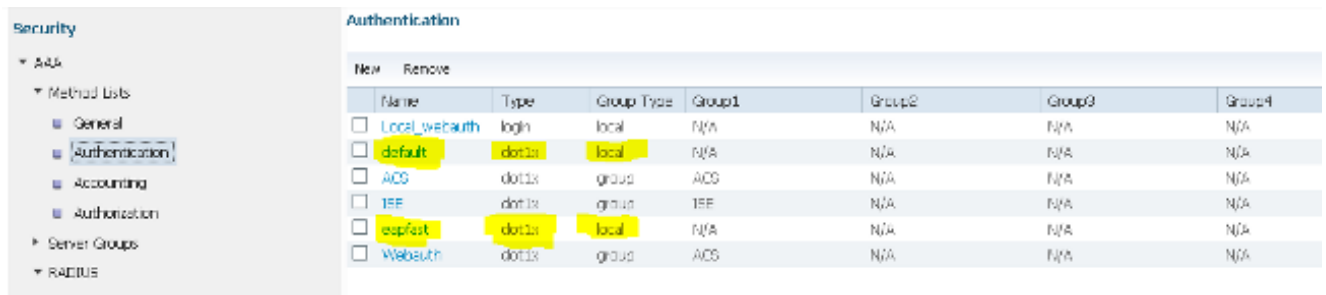
## Konfigurieren des WLC mithilfe der GUI

Gehen Sie wie folgt vor, um den WLC mit der GUI zu konfigurieren:

### 1. Konfigurieren Sie die Methodenliste für die Authentifizierung:

Konfigurieren Sie den **EasyFast**-Typ als **Dot1x**.

Konfigurieren Sie den **EasyFast**-Gruppentyp als **Local (Lokal)**.

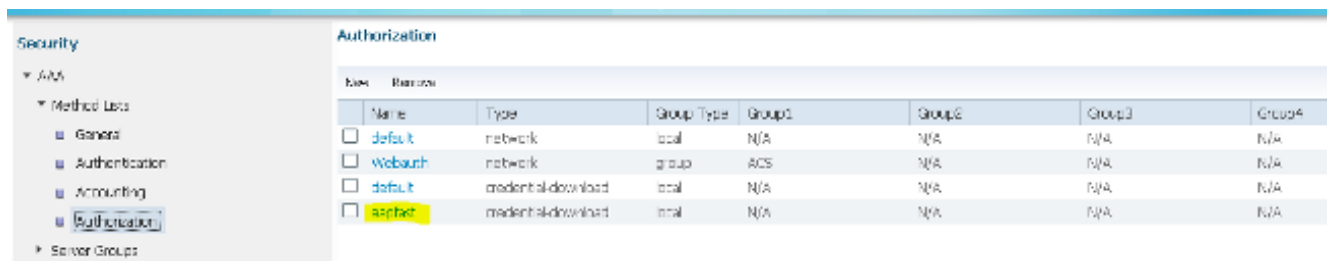


New		Remove					
Name	Type	Group Type	Group1	Group2	Group3	Group4	
<input type="checkbox"/> Local_webauth	login	local	N/A	N/A	N/A	N/A	
<input type="checkbox"/> default	dot1x	local	N/A	N/A	N/A	N/A	
<input type="checkbox"/> ACS	dot1x	group	ACS	N/A	N/A	N/A	
<input type="checkbox"/> TEF	dot1x	group	TEF	N/A	N/A	N/A	
<input type="checkbox"/> eapfast	dot1x	local	N/A	N/A	N/A	N/A	
<input type="checkbox"/> Webauth	dot1x	group	ACS	N/A	N/A	N/A	

2. Konfigurieren Sie die Methodenliste für die Autorisierung:

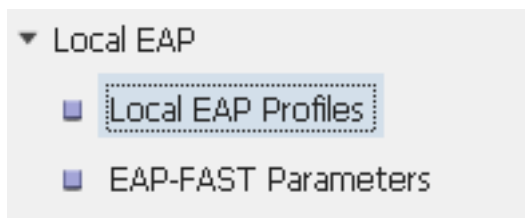
Konfigurieren Sie den **EasyFast**-Typ als **Credential-Download**.

Konfigurieren Sie den **EasyFast**-Gruppentyp als **Local (Lokal)**.




New		Remove					
Name	Type	Group Type	Group1	Group2	Group3	Group4	
<input type="checkbox"/> default	network	local	N/A	N/A	N/A	N/A	
<input type="checkbox"/> Webauth	network	group	ACS	N/A	N/A	N/A	
<input type="checkbox"/> default	credential-download	local	N/A	N/A	N/A	N/A	
<input type="checkbox"/> eapfast	credential-download	local	N/A	N/A	N/A	N/A	

3. Konfigurieren Sie das lokale EAP-Profil:



4. Erstellen Sie ein neues Profil, und wählen Sie den EAP-Typ aus:



Local EAP Profiles					
New		Remove			
Profile Name	LEAP	EAP-FAST	EAP-TLS	PEAP	
<input type="checkbox"/> eapfast	Disabled	Enabled	Disabled	Disabled	

Der Profilname ist **einfach** und der ausgewählte EAP-Typ **EAP-FAST**:

### Local EAP Profiles

Local EAP Profiles > Edit

---

Profile Name	eapfast
LEAP	<input type="checkbox"/>
EAP-FAST	<input checked="" type="checkbox"/>
EAP-TLS	<input type="checkbox"/>
PEAP	<input type="checkbox"/>
Trustpoint	<input type="checkbox"/>

5. Konfigurieren der EAP-FAST-Methodenparameter:

### EAP-FAST Method Parameters

New Remove

	Profile Name	Description
<input type="checkbox"/>	eapfast	test

Der Serverschlüssel wird als **Cisco123** konfiguriert.

## EAP-FAST Method Profile

EAP-FAST Method Profile > **Edit**

Profile Name	eapfast
Server Key	●●●●●●●●
Confirm Server Key	●●●●●●●●
Time to live (secs)	86400
Authority ID	1
Authority ID Information	1
Description	test

6. Aktivieren Sie das Kontrollkästchen **Dot1x System Auth Control** (Auth-Steuerung für Dot1x-System), und wählen Sie **Eapfast** für die Methodenlisten aus. So können Sie die lokale EAP-Authentifizierung durchführen.

<b>Security</b>	<b>General</b>
▼ AAA	
▼ Method Lists	
■ General	Dot1x System Auth Control <input checked="" type="checkbox"/>
■ Authentication	Local Authentication Method List ▼
■ Accounting	Authentication Method List eapfast ▼
■ Authorization	Local Authorization Method List ▼
▶ Server Groups	Authorization Method List eapfast ▼
▼ RADIUS	

7. WLAN für die WPA2 AES-Verschlüsselung konfigurieren:

**WLAN**  
WLAN > **Edit**

General Security QOS AVC Advanced

Profile Name eapfastlocal  
 Type WLAN  
 SSID eapfastlocal  
 Status   
 Security Policies [WPA2][Auth(802.1x)]  
 (Modifications done under security tab will appear after applying the changes.)  
 Radio Policy All ▾  
 Interface/Interface Group(G) VLAN0020 ▾  
 Broadcast SSID   
 Multicast VLAN Feature

**WLAN**  
WLAN > **Edit**

General Security QOS AVC Advanced

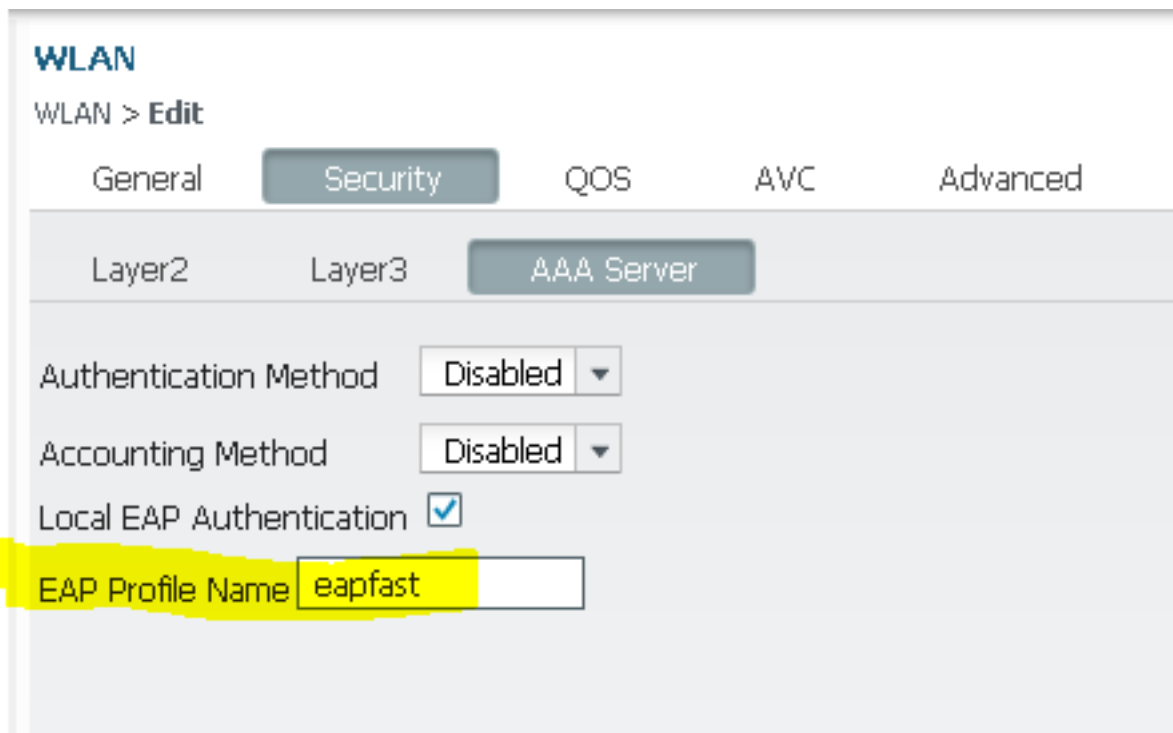
Layer2 Layer3 AAA Server

Layer 2 Security WPA + WPA2 ▾  
 MAC Filtering   
 Fast Transition   
 Over the DS   
 Reassociation Timeout 20

**WPA+WPA2 Parameters**  
 WPA Policy   
 WPA2 Policy   
 WPA2 Encryption  AES  TKIP  
 Auth Key Mgmt 802.1x ▾

8. Ordnen Sie auf der Registerkarte **AAA Server** den EAP-Profilnamen dem WLAN zu:

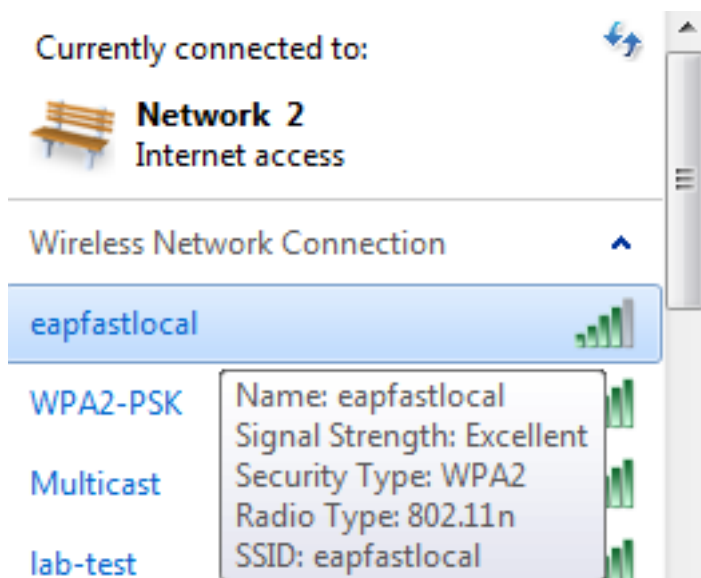




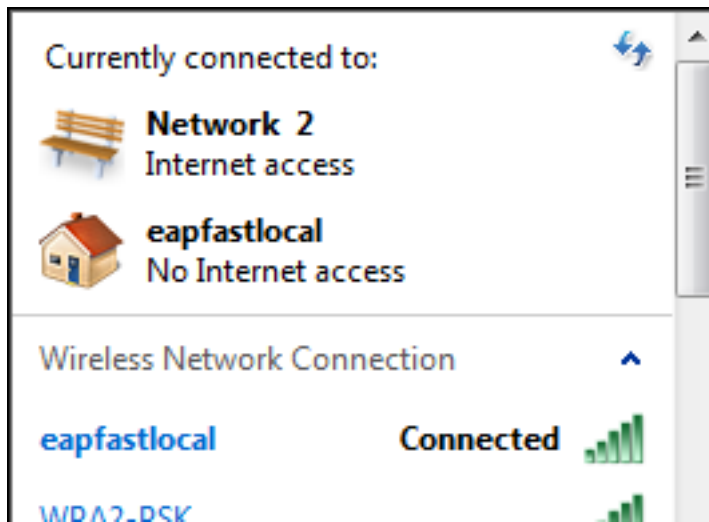
## Überprüfen

Gehen Sie wie folgt vor, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert:

1. Verbinden Sie den Client mit dem WLAN:



2. Überprüfen Sie, ob das Popup-Fenster "Protected Access Credentials (PAC)" angezeigt wird und Sie akzeptieren müssen, um sich erfolgreich zu authentifizieren:



## Fehlerbehebung

Cisco empfiehlt die Verwendung von Ablaufverfolgungen, um Wireless-Probleme zu beheben. Ablaufverfolgungen werden im runden Puffer gespeichert und sind nicht prozessorintensiv.

Aktivieren Sie diese Ablaufverfolgungen, um die Layer 2 (L2)-Authentifizierungsprotokolle zu erhalten:

- Ablaufverfolgungsgruppe - Debugging auf Wireless-Ebene festlegen
- `set trace group-wireless-secure filter mac0021.6a89.51ca`

Aktivieren Sie diese Ablaufverfolgungen, um die DHCP-Ereignisprotokolle abzurufen:

- Festlegen des Ablaufverfolgungs-DHCP-Ereignisebenendebuggens
- `set trace dhcp events filter mac 0021.6a89.51ca`

Hier einige Beispiele für erfolgreiche Ablaufverfolgungen:

```
[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**