

内部 RADIUS サーバで使用するコンバージド アクセス 5760、3850、および 3650 シリーズ WLS EAP-FAST の設定例

TAC

Document ID: 117664

Updated: 2014 年 4 月 18 日

著者 : Cisco TAC エンジニア、Surendra BG



[PDF のダウンロード](#)



[印刷](#)

[フィードバック](#)

関連製品

- [ワイヤレス LAN \(WLAN \)](#)

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[設定の概要](#)

[CLI で WLC を設定して下さい](#)

[GUI で WLC を設定して下さい](#)

[確認](#)

[トラブルシューティング](#)

[Cisco サポート コミュニティ - 特集対話](#)

概要

この資料にクライアント認証のためのセキュアなプロトコルによって Cisco 拡張可能認証プロトコル適用範囲が広い認証を（この例で、EAP-FAST な）行う RADIUSサーバとして機能するために Cisco をアクセス 5760、3850、および 3650 シリーズ ワイヤレス LAN コントローラ（WLCs）設定する方法をコンバートしました記述されています。

通常場合によっては実行可能なソリューションではない外部の RADIUSサーバはユーザを認証するために使用されます。この場合、コンバージしたアクセス WLC はユーザが WLC で設定されるローカルデータベースに対して認証される RADIUSサーバとして機能できます。これをローカル RADIUS サーバ機能と呼びます。

前提条件

要件

この設定を開始する前に、次の項目に関する知識を得ておくことを推奨します。

- コンバージしたアクセス 5760、3850、および 3650 シリーズ WLC の Cisco IOS[®] GUI か CLI
- Extensible Authentication Protocol (EAP) 概念
- サービス セット ID (SSID) の設定
- RADIUS

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco 5760 シリーズ WLC リリース 3.3.2 (次世代 ワイヤリング クローゼット[NGWC])
- Cisco 3602 シリーズ Lightweight アクセスポイント (AP)
- Microsoft Windows XP と Intel PROset サプリカント
- Cisco Catalyst 3560 シリーズ スイッチ

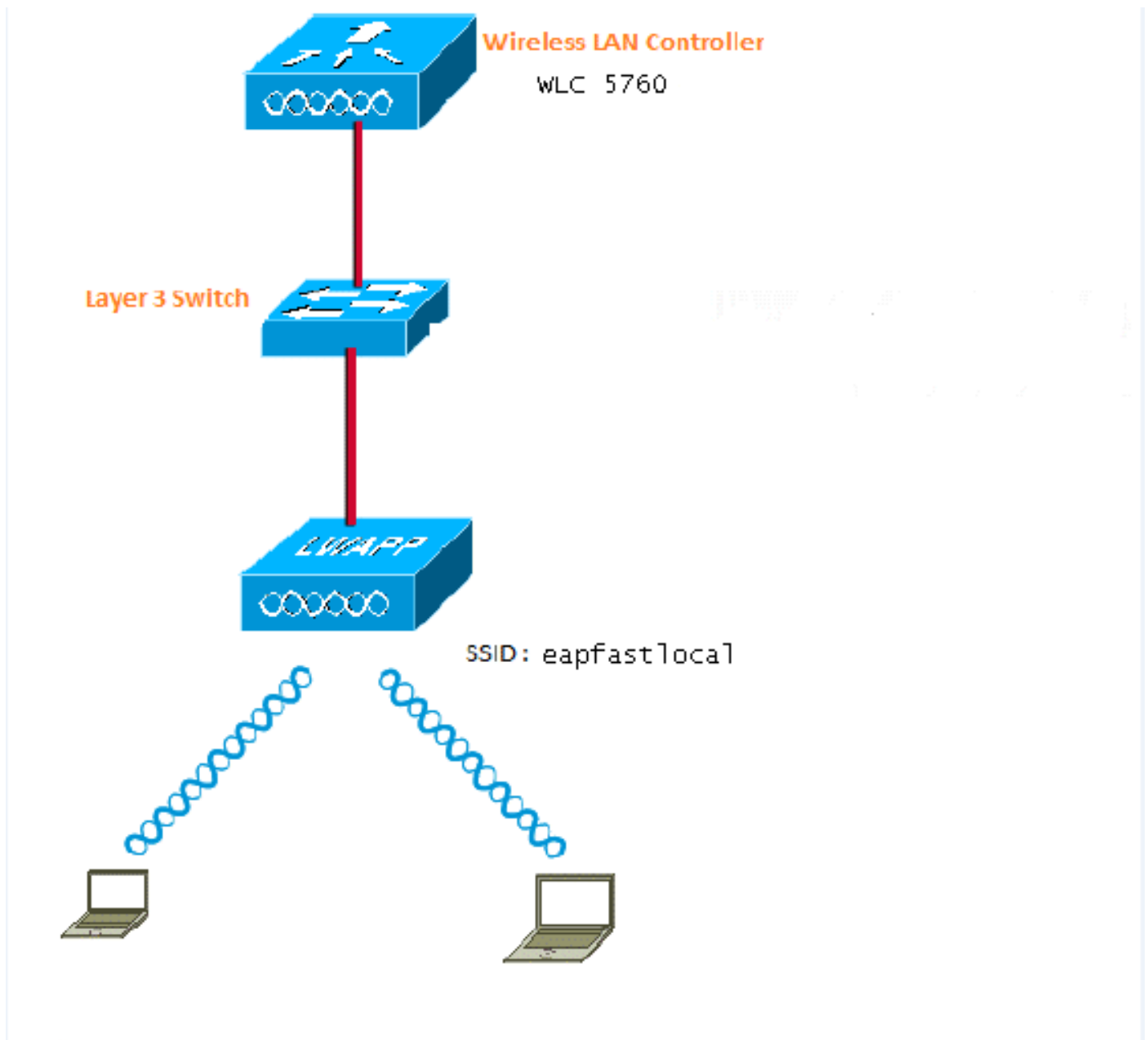
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

設定

注: このセクションで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#) ([登録ユーザ専用](#)) を使用してください。

ネットワーク図

次の画像は、ネットワーク ダイアグラムの例を示しています。



設定の概要

この設定は 2 つのステップで完了します:

1. CLI か GUI でローカル EAP 方式および関連認証 および 権限プロファイルのための WLC を設定して下さい。
2. WLAN を設定し、認証 および 権限プロファイルがあるメソッドリストをマッピングして下さい。

CLI で WLC を設定して下さい

CLI で WLC を設定するためにこれらのステップを完了して下さい:

1. WLC の AAA モデルを有効に して下さい:

```
aaa new-model
```

2. 認証 および 権限を定義して下さい:

```
aaa local authentication eapfast authorization eapfast

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

3. ローカル EAP プロファイルおよび方式を設定して下さい (この例で使用されます EAP-FAST な):

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

4. 高度 EAP-FAST な パラメータを設定して下さい:

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

5. WLAN を設定し、WLAN にローカル許可 プロファイルをマッピングして下さい:

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

6. クライアント 接続をサポートするためにインフラストラクチャを設定して下さい:

```
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
```

GUI で WLC を設定して下さい

GUI で WLC を設定するためにこれらのステップを完了して下さい:

1. 認証のためのメソッドリストを設定して下さい:

Dot1x で eapfast 型を設定して下さい。

ローカルで eapfast グループ タイプを設定して下さい。

Security		Authentication						
<ul style="list-style-type: none"> AAA <ul style="list-style-type: none"> Method Lists <ul style="list-style-type: none"> General Authentication Accounting Authorization Server Groups RADIUS 		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. 許可のためのメソッドリストを設定して下さい:

資格情報ダウンロードで **eapfast** 型を設定して下さい。

ローカルで **eapfast** グループ タイプを設定して下さい。

Security		Authorization						
<ul style="list-style-type: none"> AAA <ul style="list-style-type: none"> Method Lists <ul style="list-style-type: none"> General Authentication Accounting Authorization Server Groups 		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. ローカル EAP プロファイルを設定して下さい:

Local EAP	
<input type="checkbox"/> Local EAP Profiles	
<input type="checkbox"/> EAP-FAST Parameters	

4. 新しいプロファイルを作成し、EAP 型を選択して下さい:

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

Profile Name は **eapfast** であり、『eap』を選択された型は **EAP-FAST** です:

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. EAP-FAST なメソッド パラメーターを設定して下さい:

EAP-FAST Method Parameters

New Remove

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

サーバキーは Cisco123 で設定されます。

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. Dot1x システム Auth コントロール チェックボックスをチェックし、メソッドリストに **eapfast** を選択して下さい。これはローカル EAP 認証を行うのを助けます。

Security	General
▼ 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. WPA2 AES 暗号化のための WLAN を設定して下さい:

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

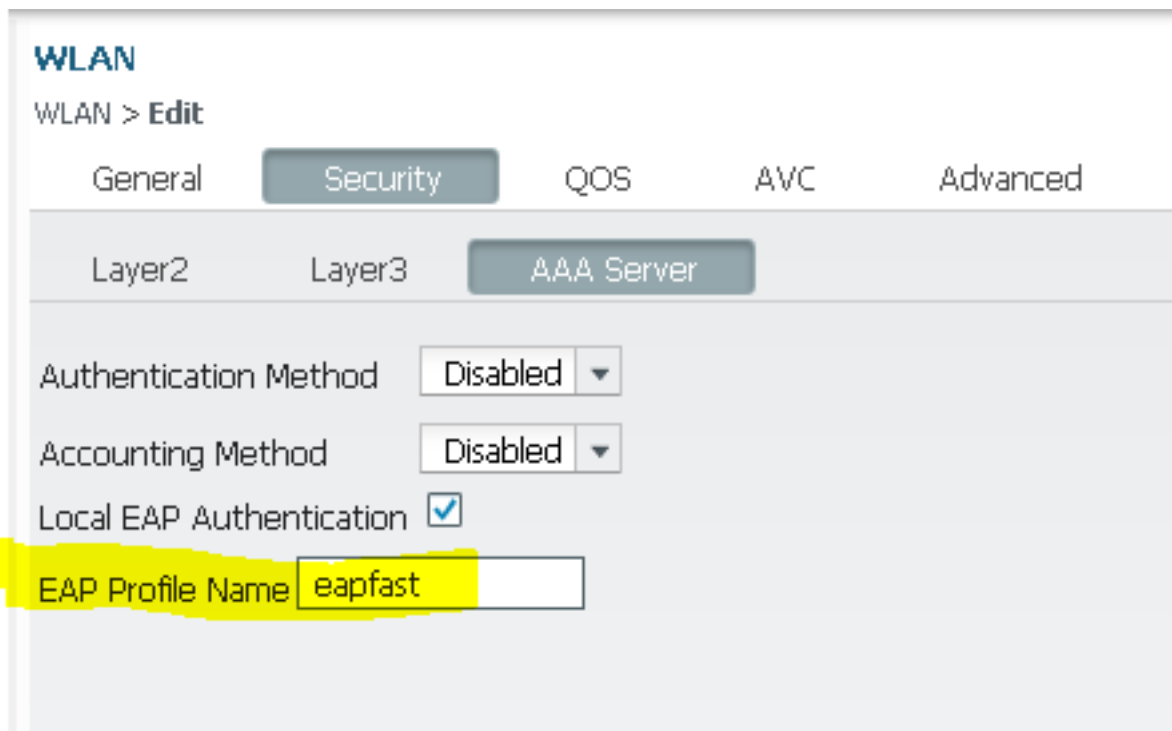
General Security QOS AVC Advanced

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 ▾

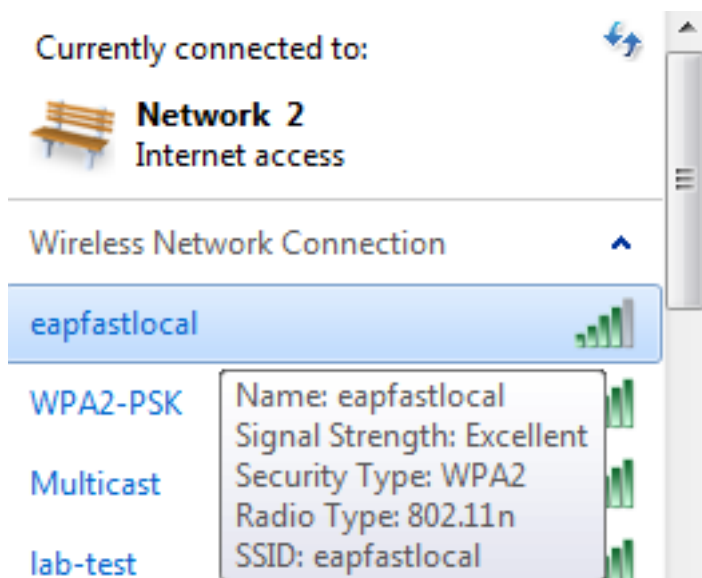
8. AAAサーバタブで、WLANにEAP Profile Name **eapfast** をマッピングして下さい:



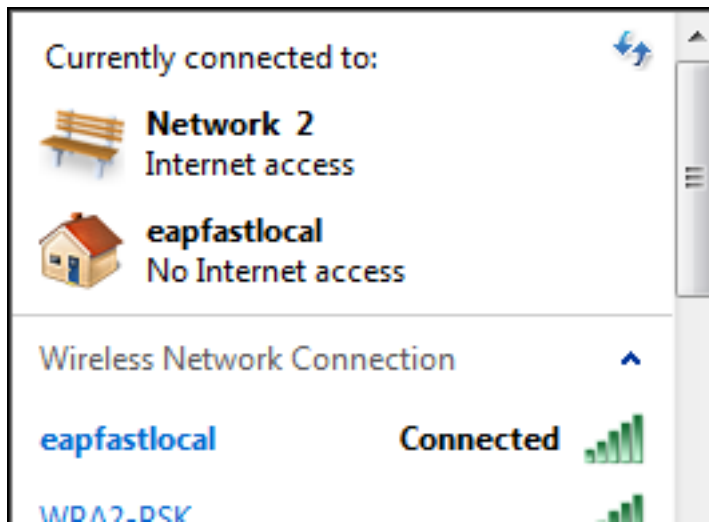
確認

設定がきちんと機能することを確認するためにこれらのステップを完了して下さい:

1. WLAN にクライアントを接続して下さい:



2. ポップアップ保護されたアクセス 資格情報 (PAC) が出ること、そして認証に成功するために受け入れる必要があることを確認して下さい:



トラブルシューティング

無線の問題のトラブルシューティングを行う際はトレースを使用することを推奨します。トレースは循環バッファに保存されているため、プロセッサに負荷はかかりません。

レイヤ2 (L2) auth ログを得ることをこれらのトレースが可能にしてください:

- **set trace group-wireless-secure level debug**
- **トレースグループワイヤレスセキュアフィルタ mac0021.6a89.51ca を設定して下さい**

DHCP イベント ログを得ることをこれらのトレースが可能にしてください:

- **set trace dhcp events level debug**
- **トレース dhcp イベント フィルタ MAC 0021.6a89.51ca を設定して下さい**

正常なトレースのいくつかの例はここにあります:

```
[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 (0x57ca400000048): 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
```

このドキュメントは有用でしたか。 [はいいいえ](#)

フィードバックいただき、ありがとうございました。

[サポートケースのオープン](#) ([シスコ サービス契約< ts generic='1' nval='P%1,2%%'が必要ですか](#))。

Cisco サポート コミュニティ - 特集対話

[Cisco サポート コミュニティ](#)では、フォーラムに参加して情報交換することができます。

このドキュメントで使用されている表記法の詳細は、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

Updated: 2014 年 4 月 18 日

Document ID: 117664