

# ワイヤレス LAN コントローラ モジュールのトラブルシューティング

## 目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[背景説明](#)

[トラブルシューティング](#)

[ISR で WLCM を認識しない](#)

[WLCM のブートフラッシュをアップグレードできますか。](#)

[WLCM はホットスワップ可能ですか。](#)

[WLCM でサポートされている LAP](#)

[WLCM のファスト イーサネットにアクセスできない](#)

[WLCM のステータスの確認](#)

[CLI コンフィギュレーション ウィザードで修正を実行する方法](#)

[LAP が ISR WLCM に登録されない - 正しくない証明書が付属した WLCM](#)

[LAP が WLCM に登録されない - システム時刻未設定](#)

[WLCM のパスワード回復](#)

[Cisco WLCM LED](#)

[コントローラのファームウェアのアップグレードが失敗](#)

[CDP をイネーブルにできない](#)

[ip-helper address コマンドおよび ip-forward protocol コマンドを使用した LAP の WLCM への登録](#)

[WLCM のトラブルシューティング コマンド](#)

[関連情報](#)

## [はじめに](#)

このドキュメントでは、Cisco ワイヤレス LAN コントローラ モジュール ( WLCM ) の基本的な問題のトラブルシューティング手順について説明します。

## [前提条件](#)

### [要件](#)

次の項目に関する知識が推奨されます。

- Lightweight Access Point Protocol ( LWAPP; Lightweight アクセス ポイント プロトコル ) に関する知識
- WLCM のモジュールを Cisco Unified Wireless Network に参加するように設定する方法の基本的な知識。注: 新規ユーザであり、WLCM での作業を未経験の場合は、『[Cisco WLAN コントローラ ネットワーク モジュール機能ガイド](#)』を参照してください。

## [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。

- バージョン 3.2.116.21 を実行する WLCM を使用するバージョン 12.4(11) T を実行する Cisco 2811 サービス統合型ルータ ( ISR )
- Cisco 1030 および Cisco 1232 AG Lightweight AP ( LAP )
- バージョン 2.5 を実行する Cisco 802.11a/b/g ワイヤレス LAN ( WLAN ) クライアント アダプタ
- バージョン 3.2 を実行する Cisco Secure Access Control Server ( ACS )

注: 次に示すコンポーネントは、この文書の作成に使用されたデバイスだけです。WLCM をサポートしている ISR および WLCM でサポートしている LAP の完全なリストについてはこのドキュメント内の「[トラブルシューティング](#)」を参照してください。

本書の情報は、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、初期 ( デフォルト ) 設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

## [表記法](#)

ドキュメント表記の詳細は、『[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。

## [背景説明](#)

Cisco WLCM は、Cisco 2800 および Cisco 3800 シリーズ ISR および Cisco 3700 シリーズ ルータ用の 802.11 無線ネットワークのソリューションを中小企業 ( SMB ) および企業のブランチ オフィスのお客様に提供するように設計されています。

Cisco WLCM を使用すると Cisco ISR および Cisco 3700 シリーズ ルータで最大 6 台の WLAN アクセス ポイント ( AP ) を管理でき、WLAN の導入や管理が簡素化されます。このオペレーティング システムでは、すべてのデータ クライアント、通信、およびシステム管理の機能を管理し、無線リソース管理 ( RRM ) 機能を実行し、オペレーティング システム セキュリティ ( OSS ) を使用してシステム全体のモビリティ ポリシーを管理し、OSS フレームワークを使用してすべてのセキュリティ機能を調整します。

Cisco WLCM では Cisco Aironet LAP、シスコ ワイヤレス コントロール システム ( WCS )、および Cisco Wireless Location Appliance と連携して、ミッション クリティカルなワイヤレス データ、音声、およびビデオ アプリケーションをサポートします。

## [トラブルシューティング](#)

ここでは、WLCM に関連する基本的な問題のトラブルシューティング手順を説明します。

## ISR で WLCM を認識しない

WLCM は、次の ISR プラットフォームだけでサポートされています。

- Cisco 3725 および 3745 ルータ
- Cisco 2811、2821、2851 ISR
- Cisco 3825 および 3845 ISR

このリストで指定されたもの以外の ISR がある場合は、WLCM が検出されません。適切なハードウェアを使用していることを確認します。

注: WLCM はネットワーク モジュール スロットでのみサポートされます。Cisco 2821 および 2851 ISR で使用できる EVM スロットではサポートされていません。

注: 1 つのルータ シャーシに設置できる Cisco WLCM は 1 台だけです。

WLCM に関する複数の最小ソフトウェア要件もあります。

ISR で WLCM を認識するには、ISR では、Cisco IOS<sup>®</sup>ソフトウェア リリース 12.4(2)XA1 ( ルータ ソフトウェア ) 以降を使用する必要があります。

## WLCM のブートフラッシュをアップグレードできますか。

Cisco WLCM は、取り付けられている付属の 256 MB Compact Flash メモリ カードがから起動します。Compact Flash メモリ カードにはブートローダ、Linux カーネル、Cisco WLCM と AP の実行可能ファイル、および Cisco WLCM 設定が格納されています。

Cisco WLCM の Compact Flash メモリ カードは、現場交換可能ではありません。

## WLCM はホットスワップ可能ですか。

WLCM は一部の ISR プラットフォームではホットスワップ可能ではありません。コントローラ モジュールの活性挿抜 ( OIR ) は、Cisco 3745 ルータおよび Cisco 3845 ISR でのみサポートされています。

## WLCM でサポートされている LAP

すべての LWAPP 対応 Cisco Aironet AP がサポートされており、これには Cisco Aironet 1000、1100、および 1200 シリーズが含まれます。HWIC-AP インターフェイス カードはサポートされていません。

## WLCM のファスト イーサネットにアクセスできない

これは、正常な動作です。Cisco WLCM の前面プレートにある外部ファスト イーサネット ポートはサポートされていません。NM-WLC ( WLCM モジュール ) には内部的にホスト ルータに接続された 1 つのファスト イーサネット ポートのみがあり、NM の前面プレートにある外部ファスト イーサネット ポートはディセーブルにされており使用不可能です。

## WLCM のステータスの確認

WLCM がルータに認識されており、正しく設置されているかどうかを確認するには、ISR から

**show version** コマンドを発行します。

```
2800-ISR-TSWEB#show version
```

```
Cisco IOS Software, 2800 Software (C2800NM-ADVSECURITYK9-M), Version 12.4(11)T,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Sat 18-Nov-06 17:16 by prod_rel_team
```

```
ROM: System Bootstrap, Version 12.4(1r) [hqluong 1r], RELEASE SOFTWARE (fc1)
```

```
2800-ISR-TSWEB uptime is 50 minutes
System returned to ROM by power-on
System image file is "flash:c2800nm-advsecurityk9-mz.124-11.T.bin"
```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:  
<http://www.cisco.com/wvl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to [export@cisco.com](mailto:export@cisco.com).

```
Cisco 2811 (revision 53.50) with 249856K/12288K bytes of memory.
Processor board ID FTX1014A34X
2 FastEthernet interfaces
1 terminal line
1 Virtual Private Network (VPN) Module
1 cisco Wireless LAN Controller(s)
```

```
DRAM configuration is 64 bits wide with parity enabled.
239K bytes of non-volatile configuration memory.
62720K bytes of ATA CompactFlash (Read/Write)
```

```
Configuration register is 0x2102
```

WLCM のステータスを調べるには、**service-module wlan-controller slot/port status** コマンドを発行します。

```
2800-ISR-TSWEB#service-module wlan-controller 1/0 status
Service Module is Cisco wlan-controller1/0
Service Module supports session via TTY line 66
Service Module is in Steady state
Getting status from the Service Module, please wait..
```

```
Cisco WLAN Controller 3.2.116.21
```

**service-module wlan-controller 1/0 statistics** コマンドを発行して WLCM のモジュール リセット統計情報を調べることもできます。

```
2800-ISR-TSWEB#service-module wlan-controller 1/0 statistics
Module Reset Statistics:
```

```
CLI reset count = 0
CLI reload count = 0
Registration request timeout reset count = 0
Error recovery timeout reset count = 0
Module registration count = 4
```

場合によっては、このエラーが表示されます。

```
Router#service-module wlan-controller 4/0 status
Service Module is Cisco wlan-controller4/0
Service Module supports session via TTY line 258
Service Module is trying to recover from error
Service Module status is not available
```

Or this:

```
Router#service-module wlan-controller 1/0 status
Service Module is Cisco wlan-controller1/0
Service Module supports session via TTY line 66
Service Module is failed
Service Module status is not available
```

このエラーは、ハードウェアの問題が原因である可能性があります。TAC のサービス リクエストをオープンして、この問題のトラブルシューティングを続けてください。TAC ケースを開くには、シスコとの契約が必要です。Cisco TAC に連絡するには、[テクニカル サポート](#)を参照してください。

WLCM の詳細な情報を表示するには **show sysinfo** コマンドを発行します。

```
(Cisco Controller) >show sysinfo
```

```
Manufacturer's Name..... Cisco Systems, Inc
Product Name..... Cisco Controller
Product Version..... 3.2.116.21
RTOS Version..... 3.2.116.21
Bootloader Version..... 3.2.116.21
Build Type..... DATA + WPS

System Name..... WLCM
System Location.....
System Contact.....
System ObjectID..... 1.3.6.1.4.1.14179.1.1.4.5
IP Address..... 60.0.0.2
System Up Time..... 0 days 0 hrs 39 mins 18 secs

Configured Country..... United States

State of 802.11b Network..... Enabled
State of 802.11a Network..... Enabled
Number of WLANs..... 1
3rd Party Access Point Support..... Disabled
Number of Active Clients..... 0
```

## [CLI コンフィギュレーション ウィザードで修正を実行する方法](#)

CLI コンフィギュレーション ウィザードを使用して WLCM を初めて (またはデフォルトへのリセット後に) 設定する場合、設定に変更を行うには - キーを使用します。次に例を示します。

ここでは、ユーザは **admin** と入力する代わりに、これを修正するために **adminn** を入力します。次のプロンプトで、を入力し、[Enter] をクリックします。システムが前のプロンプトに戻ります

o

(Cisco Controller)

Welcome to the Cisco Wizard Configuration Tool

Use the '-' character to backup

System Name [Cisco\_e8:38:c0]: **adminn**

*!--- The user enters adminn instead of admin.*

Enter Administrative User Name (24 characters max): -

*!--- In order to make the corrections, the user enters -.*

System Name [Cisco\_e8:38:c0] (31 characters max): **admin**

*!--- The user is again prompted for the system name and !--- then enters the correct system name admin.*

## LAP が ISR WLCM に登録されない - 正しくない証明書が付属した WLCM

NM-AIR-WLC6-K9 および NM-AIR-WLC6-K9= の WLCM には誤った証明書が付属しています。これが原因で、WLCNM は Cisco と Airespace の AP によって認証されません。2006 年 2 年 1 日から 2006 年 3 月 22 日の間に出荷された WLCM に影響があります。製造工程での不具合により、無線 LAN コントローラのネットワーク モジュールのデバイスに正しい証明書がコピーされていません。誤った証明書により RSA キーの不一致が発生し、LWAPP ベースの AP では、WLCNM に対する加入、関連付け、登録が失敗します。

詳細については、『[Field Notice : FN 62379 - ワイヤレス LAN コントローラ ネットワーク モジュールが Cisco と Airespace のアクセス ポイントで認証されない - ハードウェア アップグレード](#)』を参照してください。この Field Notice には、回避策に加え、影響を受けるネットワーク モジュールの部品番号とシリアル番号が含まれています。

## LAP が WLCM に登録されない - システム時刻未設定

WLCM にシステムの日付と時刻を設定する必要があります。手動で設定することも、NTP サーバを使用するように WLCM を設定することもできます。時刻と日付が設定されていない場合、LAP は WLCM に登録されません。CLI ウィザードで、システムの日付と時刻を入力するよう促されます。日時を入力しない場合、次の警告メッセージが表示されます。

```
Warning! No AP will come up unless the time is set
Please see documentation for more details.
```

時刻を手動で設定するには、WLCM の CLI から次のコマンドを発行します。

```
Warning! No AP will come up unless the time is set
Please see documentation for more details.
```

WLCM で NTP サーバを使用する場合は、このコマンドを発行します。

```
Warning! No AP will come up unless the time is set
```

Please see documentation for more details.

## [WLCM のパスワード回復](#)

WLCM にログインするためのパスワードを忘れた場合、WLCM にアクセスする唯一の方法は、WLCM をデフォルト設定にリセットすることです。この場合、WLCM の設定もすべてリセットされるので、最初から設定しなおす必要があります。

出荷時の初期状態に WLCM をリセットする方法については、「[WLCM をデフォルト設定にリセット](#)」を参照してください。

## [Cisco WLCM LED](#)

次の表は、Cisco WLCM の LED とその意味を示します。

LED	意味
CF	Compact Flash のメモリ カードがアクティブです。
EN	モジュールはセルフテストに合格し、ルータで使用できます。
PWR	電源はコントローラのモジュールで使用できます。

## [コントローラのファームウェアのアップグレードが失敗](#)

アップグレードプロセスの実行中に、アップグレードプロセスに影響のあるエラーが発生する場合があります。このセクションでは、エラーメッセージの意味およびエラーをなくしてコントローラをアップグレードする方法について説明します。

- 「Code file transfer failed-No reply from the TFTP server」：このエラーメッセージが表示されるのは、TFTP サーバがアクティブではない場合です。サーバの TFTP サービスがイネーブルになっているかどうかを確認します。
- 「Code file transfer failed - Error from server:」 「File was not found.」 「Aborting transfer」：OS ファイルが TFTP サーバのデフォルト ディレクトリに存在しない場合、このエラーメッセージが表示されます。このエラーをなくするには、TFTP サーバのデフォルト ディレクトリにイメージ ファイルをコピーします。
- 「TFTP Failure while storing in flash!」：TFTP サーバに問題がある場合にこのエラーが発生します。一部の TFTP サーバでは、転送できるファイルのサイズが制限されています。別の TFTP サーバ ユーティリティを使用してください。使用可能な無料の TFTP サーバ ユーティリティは多数提供されています。Tftpd32 バージョン 2.0 という TFTP サーバを使用することをお勧めします。TFTP、[Tftpd32](#)
- The install partitions are destroyed or the image is corrupted：ソフトウェアをアップグレードしようとしても引き続き失敗する場合は、イメージが破損している可能性があります。[シスコのテクニカル サポート](#)に連絡して、サポートを依頼してください。

WLCM のファームウェアをアップグレードする方法の詳細については、「[Cisco WLAN コントローラ モジュール ソフトウェアのアップグレード](#)」を参照してください。

## CDP をイネーブルにできない

3750 ISR にインストールされている WLCM 上の Cisco Discovery Protocol ( CDP ) をユーザがイネーブルにできません。 次のメッセージが表示されます。

```
Warning! No AP will come up unless the time is set
Please see documentation for more details.
```

ユーザが CDP をイネーブルにするために `config cdp enable` コマンドを発行しても、この同じメッセージが表示されます。

```
Warning! No AP will come up unless the time is set
Please see documentation for more details.
```

これは、Cisco Bug ID CSCsg67615 が原因で発生します。 3750G に付属している統合ワイヤレス LAN コントローラでは CDP をサポートしていませんが、このコントローラに対して CDP CLI コマンドを使用できません。 これは 4.0.206.0 で解決されています。

## ip-helper address コマンドおよび ip-forward protocol コマンドを使用した LAP の WLCM への登録

WLCM を使用すると、LAP が IP サブネットのブロードキャストにより、WLCM を検出することは困難です。 これは、ISR のバックプレーンに対する WLCM の統合方法と、通常は別の IP サブネットに配置されている LAP の配置方法 ( 推奨 ) が理由です。 IP サブネットのブロードキャストの検出を正常に実行するには、`ip helper-address` と `ip forward-protocol udp 12223` コマンドを発行します。

一般に、これらのコマンドの目的は、IP ブロードキャストである可能性のあるフレームを転送またはリレーすることです。 このリレーと WLC 管理インターフェイスへの方向付けは、WLC の応答が確実に LAP に戻るために十分である必要があります。

`ip helper-address` コマンドは、LAP が接続されているインターフェイスの下で発行する必要があります。 `ip helper-address` コマンドは、WLC の管理インターフェイスを指す必要があります。

```
Warning! No AP will come up unless the time is set
Please see documentation for more details.
```

`ip forward-protocol` コマンドはグローバル コンフィギュレーション コマンドです。

```
Warning! No AP will come up unless the time is set
Please see documentation for more details.
```

## WLCM のトラブルシューティング コマンド

ここでは、WLCM 設定をトラブルシューティングするために使用できる `debug` コマンドを示し

ます。

## コントローラに登録する LAP を確認する debug コマンド

LAP が WLCM に登録されているかどうかを確認するには、次の debug コマンドを使用します。

- **debug mac addr <AP-MAC-address xx: xx: xx: xx: xx: xx>** : LAP の MAC アドレスのデバッグを設定します。
- **debug lwapp events enable** : LWAPP イベントとエラー メッセージのデバッグを設定します。
- **debug pm pki enable** : セキュリティ ポリシー マネージャモジュールのデバッグを設定します。

LAP を WLCM に登録するときの **debug lwapp events enable** コマンドの出力例を次に示します。

```
Mon Mar 12 16:23:39 2007: Received LWAPP DISCOVERY REQUEST from AP 00:0b:85:51:5a:e0
to 00:15:2c:e8:38:c0 on port '1'
Mon Mar 12 16:23:39 2007: Successful transmission of LWAPP Discovery-Response to
AP 00:0b:85:51:5a:e0 on Port 1
Mon Mar 12 16:23:52 2007: Received LWAPP JOIN REQUEST from AP 00:0b:85:51:5a:e0 to
00:15:2c:e8:38:c0 on port '1'
Mon Mar 12 16:23:52 2007: LWAPP Join-Request MTU path from AP 00:0b:85:51:5a:e0
is 1500, remote debug mode is 0
Mon Mar 12 16:23:52 2007: Successfully added NPU Entry for AP 00:0b:85:51:5a:e0
(index 49)Switch IP: 60.0.0.3, Switch Port:
12223, intIfNum 1, vlanId 0 AP IP: 10.77.244.221, AP Port: 5550,
next hop MAC: 00:17:94:06:62:98
Mon Mar 12 16:23:52 2007: Successfully transmission of LWAPP Join-Reply to
AP 00:0b:85:51:5a:e0
Mon Mar 12 16:23:52 2007: Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 0
Mon Mar 12 16:23:52 2007: Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 1
Mon Mar 12 16:23:53 2007: Received LWAPP CONFIGURE REQUEST from AP 00:0b:85:51:5a:e0
to 00:15:2c:e8:38:c0
Mon Mar 12 16:23:53 2007: Updating IP info for AP 00:0b:85:51:5a:e0 --
static 0, 10.77.244.221/255.255.255.224, gtw 10.77.244.220
Mon Mar 12 16:23:53 2007: Updating IP 10.77.244.221 ==> 10.77.244.221 for
AP 00:0b:85:51:5a:e0
Mon Mar 12 16:23:53 2007: spamVerifyRegDomain RegDomain set for slot 0 code 0
regstring -A regDfromCb -A
Mon Mar 12 16:23:53 2007: spamVerifyRegDomain RegDomain set for slot 1 code 0
regstring -A regDfromCb -A
Mon Mar 12 16:23:53 2007: spamEncodeDomainSecretPayload:Send domain secret
WLCM-Mobility<bc,73,45,ec,a2,c8,55,ef,14,1e,5d,99,75,f2,f9,63,af,74,d9,02> to
AP 00:0b:85:51:5a:e0
Mon Mar 12 16:23:53 2007: Successfully transmission of LWAPP Config-Message to
AP 00:0b:85:51:5a:e0
Mon Mar 12 16:23:53 2007: Running spamEncodeCreateVapPayload for SSID 'WLCM-TSWEB'
Mon Mar 12 16:23:53 2007: Running spamEncodeCreateVapPayload for SSID 'WLCM-TSWEB'
Mon Mar 12 16:23:53 2007: AP 00:0b:85:51:5a:e0 associated. Last AP failure was due to
AP reset
Mon Mar 12 16:23:53 2007: Received LWAPP CHANGE_STATE_EVENT from AP 00:0b:85:51:5a:e0
Mon Mar 12 16:23:53 2007: Successfully transmission of LWAPP Change-State-Event
Response to AP 00:0b:85:51:5a:e0
Mon Mar 12 16:23:53 2007: Received LWAPP Up event for AP 00:0b:85:51:5a:e0 slot 0!
Mon Mar 12 16:23:53 2007: Received LWAPP CONFIGURE COMMAND RES from AP 00:0b:85:51:5a:e0
Mon Mar 12 16:23:53 2007: Received LWAPP CHANGE_STATE_EVENT from AP 00:0b:85:51:5a:e0
Mon Mar 12 16:23:53 2007: Successfully transmission of LWAPP Change-State-Event
Response to AP 00:0b:85:51:5a:e0
Mon Mar 12 16:23:53 2007: Received LWAPP Up event for AP 00:0b:85:51:5a:e0 slot 1!
Mon Mar 12 16:23:54 2007: Received LWAPP CONFIGURE COMMAND RES from AP 00:0b:85:51:5a:e0
```

Mon Mar 12 16:23:54 2007: Received LWAPP CONFIGURE COMMAND RES from AP 00:0b:85:51:5a:e0  
Mon Mar 12 16:23:54 2007: Received LWAPP CONFIGURE COMMAND RES from AP 00:0b:85:51:5a:e0  
Mon Mar 12 16:23:54 2007: Received LWAPP CONFIGURE COMMAND RES from AP 00:0b:85:51:5a:e0  
Mon Mar 12 16:23:54 2007: Received LWAPP CONFIGURE COMMAND RES from AP 00:0b:85:51:5a:e0  
Mon Mar 12 16:23:54 2007: Received LWAPP CONFIGURE COMMAND RES from AP 00:0b:85:51:5a:e0

LAP を WLCM に登録するときの debug pm pki enable コマンドの出力例を次に示します。

```
Mon Mar 12 16:30:40 2007: sshpmGetIssuerHandles: locking ca cert table
Mon Mar 12 16:30:40 2007: sshpmGetIssuerHandles: calling x509_alloc() for user cert
Mon Mar 12 16:30:40 2007: sshpmGetIssuerHandles: calling x509_decode()
Mon Mar 12 16:30:40 2007: sshpmGetIssuerHandles: <subject> C=US, ST=California,
L=San Jose, O=airespace Inc, CN=000b85515ae0,
MAILTO=support@airespace.com
Mon Mar 12 16:30:40 2007: sshpmGetIssuerHandles: <issuer> C=US, ST=California,
L=San Jose, O=airespace Inc, OU=none, CN=ca,
MAILTO=support@airespace.com
Mon Mar 12 16:30:40 2007: sshpmGetIssuerHandles: Mac Address in subject is
00:0b:85:51:5a:e0
Mon Mar 12 16:30:40 2007: sshpmGetIssuerHandles: Cert is issued by Airespace Inc.
Mon Mar 12 16:30:40 2007: sshpmGetCID: called to evaluate <bsnDefaultCaCert>
Mon Mar 12 16:30:40 2007: sshpmGetCID: comparing to row 0, CA cert >bsnOldDefaultCaCert<
Mon Mar 12 16:30:40 2007: sshpmGetCID: comparing to row 1, CA cert >bsnDefaultRootCaCert<
Mon Mar 12 16:30:40 2007: sshpmGetCID: comparing to row 2, CA cert >bsnDefaultCaCert<
Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: called to get cert for CID 2816f436
Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: comparing to row 0, certname
>bsnOldDefaultCaCert<
Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: comparing to row 1, certname
>bsnDefaultRootCaCert<
Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: comparing to row 2, certname
>bsnDefaultCaCert<
Mon Mar 12 16:30:40 2007: ssphmUserCertVerify: calling x509_decode()
Mon Mar 12 16:30:40 2007: ssphmUserCertVerify: failed to verify AP cert
>bsnDefaultCaCert<
Mon Mar 12 16:30:40 2007: sshpmGetCID: called to evaluate <bsnOldDefaultCaCert>
Mon Mar 12 16:30:40 2007: sshpmGetCID: comparing to row 0, CA cert
>bsnOldDefaultCaCert<
Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: called to get cert for CID 226b9636
Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: comparing to row 0, certname
>bsnOldDefaultCaCert<
Mon Mar 12 16:30:40 2007: ssphmUserCertVerify: calling x509_decode()
Mon Mar 12 16:30:40 2007: ssphmUserCertVerify: user cert verified using
>bsnOldDefaultCaCert<
Mon Mar 12 16:30:40 2007: sshpmGetIssuerHandles: ValidityString (current):
2007/03/12/16:30:40
Mon Mar 12 16:30:40 2007: sshpmGetIssuerHandles: AP sw version is 0x3027415,
send a Cisco cert to AP.
Mon Mar 12 16:30:40 2007: sshpmGetCID: called to evaluate <cscDefaultIdCert>
Mon Mar 12 16:30:40 2007: sshpmGetCID: comparing to row 0, CA cert >bsnOldDefaultCaCert<
Mon Mar 12 16:30:40 2007: sshpmGetCID: comparing to row 1, CA cert >bsnDefaultRootCaCert<
Mon Mar 12 16:30:40 2007: sshpmGetCID: comparing to row 2, CA cert >bsnDefaultCaCert<
Mon Mar 12 16:30:40 2007: sshpmGetCID: comparing to row 3, CA cert >bsnDefaultBuildCert<
Mon Mar 12 16:30:40 2007: sshpmGetCID: comparing to row 4, CA cert
>cscDefaultNewRootCaCert<
Mon Mar 12 16:30:40 2007: sshpmGetCID: comparing to row 5, CA cert >cscDefaultMfgCaCert<
Mon Mar 12 16:30:40 2007: sshpmGetCID: comparing to row 0, ID cert >bsnOldDefaultIdCert<
Mon Mar 12 16:30:40 2007: sshpmGetCID: comparing to row 1, ID cert >bsnDefaultIdCert<
Mon Mar 12 16:30:40 2007: sshpmGetCID: comparing to row 2, ID cert >cscDefaultIdCert<
Mon Mar 12 16:30:40 2007: sshpmGetCertFromHandle: calling sshpmGetCertFromCID()
with CID 0x15b4c76e
Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: called to get cert for CID 15b4c76e
Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: comparing to row 0, certname
>bsnOldDefaultCaCert<
```

```

Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: comparing to row 1, certname
>bsnDefaultRootCaCert<
Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: comparing to row 2, certname
>bsnDefaultCaCert<
Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: comparing to row 3, certname
>bsnDefaultBuildCert<
Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: comparing to row 4, certname
>cscscoDefaultNewRootCaCert<
Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: comparing to row 5, certname
>cscscoDefaultMfgCaCert<
Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: comparing to row 0, certname
>bsnOldDefaultIdCert<
Mon Mar 12 16:30:44 2007: sshpmGetCertFromCID: comparing to row 1, certname
>bsnDefaultIdCert<
Mon Mar 12 16:30:44 2007: sshpmGetCertFromCID: comparing to row 2, certname
>cscscoDefaultIdCert<
Mon Mar 12 16:30:44 2007: ssphmPublicKeyEncrypt: called to encrypt 16 bytes
Mon Mar 12 16:30:44 2007: ssphmPublicKeyEncrypt: successfully encrypted, out is 192 bytes
Mon Mar 12 16:30:44 2007: sshpmPrivateKeyEncrypt: called to encrypt 196 bytes
Mon Mar 12 16:30:44 2007: sshpmGetOpensslPrivateKeyFromCID: called to get key for
CID 15b4c76e
Mon Mar 12 16:30:44 2007: sshpmGetOpensslPrivateKeyFromCID: comparing to row 0, certname
>bsnOldDefaultIdCert<
Mon Mar 12 16:30:44 2007: sshpmGetOpensslPrivateKeyFromCID: comparing to row 1, certname
>bsnDefaultIdCert<
Mon Mar 12 16:30:44 2007: sshpmGetOpensslPrivateKeyFromCID: comparing to row 2, certname
>cscscoDefaultIdCert<
Mon Mar 12 16:30:44 2007: sshpmGetOpensslPrivateKeyFromCID: match in row 2
Mon Mar 12 16:30:44 2007: sshpmPrivateKeyEncrypt: calling RSA_private_encrypt
with 196 bytes
Mon Mar 12 16:30:44 2007: sshpmPrivateKeyEncrypt: RSA_private_encrypt returned 256
Mon Mar 12 16:30:44 2007: sshpmPrivateKeyEncrypt: encrypted bytes: 256

```

## Web 認証を検証する debug コマンド

Web 認証が WLCM で想定どおりに動作しているかどうかを確認するには、次の debug コマンドを使用します。

- **debug aaa all enable** : すべての AAA メッセージのデバッグを設定します。
- **debug pem state enable** : Policy Manager ステート マシンのデバッグを設定します。
- **debug pem events enable** : ポリシー マネージャ イベントのデバッグを設定します。
- **debug pm ssh-appgw enable** : アプリケーション ゲートウェイのデバッグを設定します。
- **debug pm ssh-tcp enable** : ポリシー マネージャ tcp 処理のデバッグを設定します。

これらの debug コマンドの一部のサンプル出力を次に示します。

```
(Cisco Controller) >debug aaa all enable
```

```

User user1 authenticated
00:40:96:ac:e6:57 Returning AAA Error 'Success' (0) for mobile 00:40:96:ac:e6:57
AuthorizationResponse: 0xbadff97c
  structureSize.....70
  resultCode.....0
  protocolUsed.....0x00000008
  proxyState.....00:40:96:AC:E6:57-00:00
  Packet contains 2 AVPs:
    AVP[01] Service-Type.....0x00000001 (1) (4 bytes)
    AVP[02] Airespace / WLAN-Identifier.....0x00000001 (1) (4 bytes)
00:40:96:ac:e6:57 Applying new AAA override for station 00:40:96:ac:e6:57
00:40:96:ac:e6:57 Override values for station 00:40:96:ac:e6:57 source: 48,

```

valid bits: 0x1 qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1  
dataAvgC: -1, rTAVgC: -1, dataBurstC: -1, rTimeBurstC: -1 vlanIfName: '', aclName:  
00:40:96:ac:e6:57 Unable to apply override policy for  
station 00:40:96:ac:e6:57 - VapAllowRadiusOverride is FALSE

AccountingMessage Accounting Start: 0xa62700c

Packet contains 13 AVPs:

AVP[01] User-Name.....user1 (5 bytes)  
AVP[02] Nas-Port.....0x00000001 (1) (4 bytes)  
AVP[03] Nas-Ip-Address.....0x0a4df4d2 (172881106) (4 bytes)  
AVP[04] NAS-Identifier.....0x574c4331 (1464615729) (4 bytes)  
AVP[05] Airespace / WLAN-Identifier.....0x00000001 (1) (4 bytes)  
AVP[06] Acct-Session-Id.....45e84f50/00:40:96:ac:e6:57/9 (28 bytes)  
AVP[07] Acct-Authentic.....0x00000002 (2) (4 bytes)  
AVP[08] Tunnel-Type.....0x0000000d (13) (4 bytes)  
AVP[09] Tunnel-Medium-Type.....0x00000006 (6) (4 bytes)  
AVP[10] Tunnel-Group-Id.....0x3330 (13104) (2 bytes)  
AVP[11] Acct-Status-Type.....0x00000001 (1) (4 bytes)  
AVP[12] Calling-Station-Id.....10.0.0.1 (8 bytes)  
AVP[13] Called-Station-Id.....10.77.244.210 (13 bytes)

when web authentication is closed by user:

(Cisco Controller) >

AccountingMessage Accounting Stop: 0xa627c78

Packet contains 20 AVPs:

AVP[01] User-Name.....user1 (5 bytes)  
AVP[02] Nas-Port.....0x00000001 (1) (4 bytes)  
AVP[03] Nas-Ip-Address.....0x0a4df4d2 (172881106) (4 bytes)  
AVP[04] NAS-Identifier.....0x574c4331 (1464615729) (4 bytes)  
AVP[05] Airespace / WLAN-Identifier.....0x00000001 (1) (4 bytes)  
AVP[06] Acct-Session-Id.....45e84f50/00:40:96:ac:e6:57/9 (28 bytes)  
AVP[07] Acct-Authentic.....0x00000002 (2) (4 bytes)  
AVP[08] Tunnel-Type.....0x0000000d (13) (4 bytes)  
AVP[09] Tunnel-Medium-Type.....0x00000006 (6) (4 bytes)  
AVP[10] Tunnel-Group-Id.....0x3330 (13104) (2 bytes)  
AVP[11] Acct-Status-Type.....0x00000002 (2) (4 bytes)  
AVP[12] Acct-Input-Octets.....0x0001820e (98830) (4 bytes)  
AVP[13] Acct-Output-Octets.....0x00005206 (20998) (4 bytes)  
AVP[14] Acct-Input-Packets.....0x000006ee (1774) (4 bytes)  
AVP[15] Acct-Output-Packets.....0x00000041 (65) (4 bytes)  
AVP[16] Acct-Terminate-Cause.....0x00000001 (1) (4 bytes)  
AVP[17] Acct-Session-Time.....0x000000bb (187) (4 bytes)  
AVP[18] Acct-Delay-Time.....0x00000000 (0) (4 bytes)  
AVP[19] Calling-Station-Id.....10.0.0.1 (8 bytes)  
AVP[20] Called-Station-Id.....10.77.244.210 (13 bytes)

(Cisco Controller) >**debug pem state enable**

Fri Mar 2 16:27:39 2007: 00:40:96:ac:e6:57 10.0.0.1  
**WEBAUTH\_REQD (8) Change state to START (0)**  
Fri Mar 2 16:27:39 2007: 00:40:96:ac:e6:57 10.0.0.1  
**START (0) Change state to AUTHCHECK (2)**  
Fri Mar 2 16:27:39 2007: 00:40:96:ac:e6:57 10.0.0.1  
**AUTHCHECK (2) Change stateto L2AUTHCOMPLETE (4)**  
Fri Mar 2 16:27:39 2007: 00:40:96:ac:e6:57 10.0.0.1  
L2AUTHCOMPLETE (4) Change state to WEBAUTH\_REQD (8)  
Fri Mar 2 16:28:16 2007: 00:16:6f:6e:36:2b 0.0.0.0  
START (0) Change state to AUTHCHECK (2)  
Fri Mar 2 16:28:16 2007: 00:16:6f:6e:36:2b 0.0.0.0  
AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4)  
Fri Mar 2 16:28:16 2007: 00:16:6f:6e:36:2b 0.0.0.0

```
L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7)
Fri Mar  2 16:28:19 2007: 00:40:96:ac:e6:57 10.0.0.1
WEBAUTH_REQD (8) Change state to WEBAUTH_NOL3SEC (14)
Fri Mar  2 16:28:19 2007: 00:40:96:ac:e6:57 10.0.0.1
WEBAUTH_NOL3SEC (14) Change state to RUN (20)
Fri Mar  2 16:28:20 2007: 00:16:6f:6e:36:2b 0.0.0.0
START (0) Change state to AUTHCHECK (2)
Fri Mar  2 16:28:20 2007: 00:16:6f:6e:36:2b 0.0.0.0
AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4)
Fri Mar  2 16:28:20 2007: 00:16:6f:6e:36:2b 0.0.0.0
L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7)
Fri Mar  2 16:28:24 2007: 00:40:96:af:a3:40 0.0.0.0
START (0) Change state to AUTHCHECK (2)
Fri Mar  2 16:28:24 2007: 00:40:96:af:a3:40 0.0.0.0
AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4)
Fri Mar  2 16:28:24 2007: 00:40:96:af:a3:40 0.0.0.0
L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7)
Fri Mar  2 16:28:25 2007: 00:40:96:af:a3:40 40.0.0.1
DHCP_REQD (7) Change stateto RUN (20)
Fri Mar  2 16:28:30 2007: 00:16:6f:6e:36:2b 0.0.0.0
START (0) Change state to AUTHCHECK (2)
Fri Mar  2 16:28:30 2007: 00:16:6f:6e:36:2b 0.0.0.0
AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4)
Fri Mar  2 16:28:30 2007: 00:16:6f:6e:36:2b 0.0.0.0
L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7)
Fri Mar  2 16:28:34 2007: 00:16:6f:6e:36:2b 30.0.0.2
DHCP_REQD (7) Change stateto WEBAUTH_REQD (8)
```

(Cisco Controller) >**debug pem events enable**

```
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1
START (0) Initializing policy
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1
L2AUTHCOMPLETE (4)Plumbed mobile LWAPP rule on AP 00:0b:85:5b:fb:d0
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1
WEBAUTH_REQD (8) Adding TMP rule
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1
WEBAUTH_REQD (8) Replacing Fast Path rule
    type = Temporary Entry on AP 00:0b:85:5b:fb:d0, slot 0,
interface = 1 ACL Id = 255,
Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 1506
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1
WEBAUTH_REQD (8) Successfully plumbed mobile rule (ACL ID 255)
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1
WEBAUTH_REQD (8) Deleting mobile policy rule 27
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57
Adding Web RuleID 28 for mobile 00:40:96:ac:e6:57
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1
WEBAUTH_REQD (8)Adding TMP rule
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1
WEBAUTH_REQD (8)ReplacingFast Path rule type = Temporary Entry
on AP 00:0b:85:5b:fb:d0, slot 0, interface = 1 ACL Id = 255,
Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 1506
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1
WEBAUTH_REQD (8)Successfully plumbed mobile rule (ACL ID 255)
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 Removed NPU entry.
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 Added NPU entry of type 8
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 Added NPU entry of type 8
```

## **DHCP の動作を確認する debug コマンド**

DHCP のクライアントとサーバのアクティビティを確認するには、次の debug コマンドを使用します。

- **debug dhcp message enable** : DHCP クライアントのアクティビティに関するデバッグ情報を表示し、DHCP パケットのステータスをモニタします。
- **debug dhcp packet enable** : DHCP のパケット レベル情報を表示します。

これらの debug コマンドのサンプル出力を次に示します。

```
(Cisco Controller) >debug dhcp message enable
00:40:96:ac:e6:57 dhcp option len,including the magic cookie = 64
00:40:96:ac:e6:57 dhcp option: received DHCP REQUEST msg
00:40:96:ac:e6:57 dhcp option: skipping option 61, len 7
00:40:96:ac:e6:57 dhcp option: requested ip = 10.0.0.1
00:40:96:ac:e6:57 dhcp option: skipping option 12, len 3
00:40:96:ac:e6:57 dhcp option: skipping option 81, len 7
00:40:96:ac:e6:57 dhcp option: vendor class id = MSFT5.0 (len 8)
00:40:96:ac:e6:57 dhcp option: skipping option 55, len 11
00:40:96:ac:e6:57 dhcpParseOptions: options end, len 64, actual 64
00:40:96:ac:e6:57 Forwarding DHCP packet (332 octets)from 00:40:96:ac:e6:57
-- packet received on direct-connect port requires forwarding to external DHCP server.
   Next-hop is 10.0.0.50
00:40:96:ac:e6:57 dhcp option len, including the magic cookie = 64
00:40:96:ac:e6:57 dhcp option: received DHCP ACK msg
00:40:96:ac:e6:57 dhcp option: server id = 10.0.0.50
00:40:96:ac:e6:57 dhcp option: lease time (seconds) =86400
00:40:96:ac:e6:57 dhcp option: skipping option 58, len 4
00:40:96:ac:e6:57 dhcp option: skipping option 59, len 4
00:40:96:ac:e6:57 dhcp option: skipping option 81, len 6
00:40:96:ac:e6:57 dhcp option: netmask = 255.0.0.0
00:40:96:ac:e6:57 dhcp option: gateway = 10.0.0.50
00:40:96:ac:e6:57 dhcpParseOptions: options end, len 64, actual 64
```

```
(Cisco Controller) >debug dhcp packet enable
```

```
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57 dhcpProxy: Received packet:
Client 00:40:96:ac:e6:57 DHCP Op: BOOTREQUEST(1), IP len: 300,
switchport: 1, encaps: 0xec03
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57 dhcpProxy: dhcp request,
client: 00:40:96:ac:e6:57: dhcp op: 1, port: 1, encaps 0xec03,
old mscb port number: 1
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57 Determing relay for 00:40:96:ac:e6:57
dhcpServer: 10.0.0.50, dhcpNetmask: 255.0.0.0, dhcpGateway: 10.0.0.50,
dhcpRelay: 10.0.0.10 VLAN: 30
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57 Relay settings for 00:40:96:ac:e6:57
Local Address: 10.0.0.10, DHCP Server: 10.0.0.50, Gateway Addr: 10.0.0.50,
VLAN: 30, port: 1
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57 DHCP Message Type received: DHCP REQUEST msg
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57   op: BOOTREQUEST,
htype: Ethernet,hlen: 6, hops: 1
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57   xid: 1674228912, secs: 0, flags: 0
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57   chaddr: 00:40:96:ac:e6:57
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57   ciaddr: 10.0.0.1, yiaddr: 0.0.0.0
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57   siaddr: 0.0.0.0, giaddr: 10.0.0.10
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57 DHCP request to 10.0.0.50,
len 350,switchport 1, vlan 30
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57 dhcpProxy: Received packet:
Client 00:40:96:ac:e6:57 DHCP Op: BOOTREPLY(2), IP len: 300,
switchport: 1, encaps: 0xec00
Fri Mar  2 16:06:35 2007: DHCP Reply to AP client: 00:40:96:ac:e6:57,
frame len412, switchport 1
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57   DHCP Message Type received: DHCP ACK msg
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57   op: BOOTREPLY, htype: Ethernet,
hlen: 6, hops: 0
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57   xid: 1674228912, secs: 0, flags: 0
```

```
Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 chaddr: 00:40:96:ac:e6:57
Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 ciaddr: 10.0.0.1, yiaddr: 10.0.0.1
Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 siaddr: 0.0.0.0, giaddr: 0.0.0.0
Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 server id: 1.1.1.1
rcvd server id: 10.0.0.50
```

## TFTP アップグレードを確認する debug コマンド

- **show msglog** : Cisco ワイヤレス LAN コントローラのデータベースに書き込まれたメッセージ ログを表示します。15 エントリを超える場合は、例に示すメッセージを表示するよう求められます。
- **debug transfer trace** : 転送またはアップグレードのデバッグを設定します。

次に **debug transfer trace** コマンドの例を示します。

```
Cisco Controller) >debug transfer trace enable
```

```
(Cisco Controller) >transfer download start
```

```
Mode..... TFTP
Data Type..... Code
TFTP Server IP..... 172.16.1.1
TFTP Packet Timeout..... 6
TFTP Max Retries..... 10
TFTP Path..... d:\WirelessImages/
TFTP Filename..... AIR-WLC2006-K9-3-2-78-0.aes
```

This may take some time.

Are you sure you want to start? (y/n) y

```
Mon Feb 13 14:06:56 2006: RESULT_STRING: TFTP Code transfer starting.
```

```
Mon Feb 13 14:06:56 2006: RESULT_CODE:1
```

TFTP Code transfer starting.

```
Mon Feb 13 14:06:59 2006: Still waiting! Status = 2
```

```
Mon Feb 13 14:07:00 2006: Locking tftp semaphore, pHost=172.16.1.1
```

```
pFilename=d:\WirelessImages/AIR-WLC2006-K9-3-2-78-0.aes
```

```
Mon Feb 13 14:07:00 2006: Semaphore locked, now unlocking, pHost=172.16.1.1
```

```
pFilename=d:\WirelessImages/AIR-WLC2006-K9-3-2-78-0.aes
```

```
Mon Feb 13 14:07:00 2006: Semaphore successfully unlocked, pHost=172.16.1.1
```

```
pFilename=d:\WirelessImages/AIR-WLC2006-K9-3-2-78-0.aes
```

```
Mon Feb 13 14:07:02 2006: Still waiting! Status = 1
```

```
Mon Feb 13 14:07:05 2006: Still waiting! Status = 1
```

```
Mon Feb 13 14:07:08 2006: Still waiting! Status = 1
```

```
Mon Feb 13 14:07:11 2006: Still waiting! Status = 1
```

```
Mon Feb 13 14:07:14 2006: Still waiting! Status = 1
```

```
Mon Feb 13 14:07:17 2006: Still waiting! Status = 1
```

```
Mon Feb 13 14:07:19 2006: tftp rc=0, pHost=172.16.1.1 pFilename=d:\WirelessImages/
AIR-WLC2006-K9-3-2-78-0.aes pLocalFilename=/mnt/download/local.tgz
```

```
Mon Feb 13 14:07:19 2006: tftp = 6, file_name=d:\WirelessImages/
```

```
AIR-WLC2006-K9-3-2-78-0.aes, ip_address=172.16.1.1
```

```
Mon Feb 13 14:07:19 2006: upd_get_code_via_tftp = 6 (target=268435457)
```

```
Mon Feb 13 14:07:19 2006: RESULT_STRING: TFTP receive complete... extracting components.
```

```
Mon Feb 13 14:07:19 2006: RESULT_CODE:6
```

TFTP receive complete... extracting components.

```
Mon Feb 13 14:07:20 2006: Still waiting! Status = 2
```

```
Mon Feb 13 14:07:23 2006: Still waiting! Status = 1
```

```
Mon Feb 13 14:07:23 2006: Still waiting! Status = 1
```

```
Mon Feb 13 14:07:23 2006: Still waiting! Status = 1
```

```
Mon Feb 13 14:07:25 2006: RESULT_STRING: Executing init script.
```

```
Mon Feb 13 14:07:25 2006: RESULT_STRING: Executing backup script.
```

```

Executing backup script.
Mon Feb 13 14:07:26 2006: Still waiting! Status = 2
Mon Feb 13 14:07:29 2006: Still waiting! Status = 1
Mon Feb 13 14:07:31 2006: RESULT_STRING: Writing new bootloader to flash disk.

Writing new bootloader to flash disk.
Mon Feb 13 14:07:32 2006: Still waiting! Status = 2
Mon Feb 13 14:07:33 2006: RESULT_STRING: Executing install_bootloader script.

Executing install_bootloader script.
Mon Feb 13 14:07:35 2006: Still waiting! Status = 2
Mon Feb 13 14:07:35 2006: RESULT_STRING: Writing new RTOS to flash disk.
Mon Feb 13 14:07:36 2006: RESULT_STRING: Executing install_rtos script.
Mon Feb 13 14:07:36 2006: RESULT_STRING: Writing new Code to flash disk.

Writing new Code to flash disk.
Mon Feb 13 14:07:38 2006: Still waiting! Status = 2
Mon Feb 13 14:07:41 2006: Still waiting! Status = 1
Mon Feb 13 14:07:42 2006: RESULT_STRING: Executing install_code script.

Executing install_code script.
Mon Feb 13 14:07:44 2006: Still waiting! Status = 2
Mon Feb 13 14:07:47 2006: Still waiting! Status = 1
Mon Feb 13 14:07:48 2006: RESULT_STRING: Writing new APIB to flash disk.

Writing new APIB to flash disk.
Mon Feb 13 14:07:50 2006: Still waiting! Status = 2
Mon Feb 13 14:07:51 2006: RESULT_STRING: Executing install_apib script.

Executing install_apib script.
Mon Feb 13 14:07:53 2006: Still waiting! Status = 2
Mon Feb 13 14:07:53 2006: Still waiting! Status = 1
Mon Feb 13 14:07:53 2006: Still waiting! Status = 1
Mon Feb 13 14:07:53 2006: Still waiting! Status = 1
Mon Feb 13 14:07:53 2006: Still waiting! Status = 1
Mon Feb 13 14:07:54 2006: RESULT_STRING: Writing new APIB to flash disk.
Mon Feb 13 14:07:56 2006: RESULT_STRING: Executing install_apib script.

Executing install_apib script.
Mon Feb 13 14:07:56 2006: Still waiting! Status = 2
Mon Feb 13 14:07:59 2006: RESULT_STRING: Writing new APIB to flash disk.

Writing new APIB to flash disk.
Mon Feb 13 14:08:00 2006: Still waiting! Status = 2
Mon Feb 13 14:08:00 2006: RESULT_STRING: Executing install_apib script.

Executing install_apib script.
Mon Feb 13 14:08:03 2006: Still waiting! Status = 2
Mon Feb 13 14:08:03 2006: RESULT_STRING: Writing new Cert-patch to flash disk.
Mon Feb 13 14:08:03 2006: RESULT_STRING: Executing install_cert_patch script.
Mon Feb 13 14:08:03 2006: RESULT_STRING: Executing fini script.
Mon Feb 13 14:08:04 2006: RESULT_STRING: TFTP File transfer is successful.
Reboot the switch for update to complete.
Mon Feb 13 14:08:06 2006: Still waiting! Status = 2
Mon Feb 13 14:08:08 2006: ummounting: <umount /mnt/download/> cwd = /mnt/application
Mon Feb 13 14:08:08 2006: finished umounting

```

## 802.1X/WPA/RSN/PMK キャッシングの debug コマンド

- **debug dot1x all enable** : 802.1X デバッグ情報を表示します。このコマンドの出力例を次に示します。

```
(Cisco Controller) >debug dot1x all enable
```

Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57  
Adding AAA\_ATT\_USER\_NAME(1) index=0  
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57  
Adding AAA\_ATT\_CALLING\_STATION\_ID(31) index=1  
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57  
Adding AAA\_ATT\_CALLED\_STATION\_ID(30) index=2  
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57  
Adding AAA\_ATT\_NAS\_PORT(5) index=3  
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57  
Adding AAA\_ATT\_NAS\_IP\_ADDRESS(4) index=4  
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57  
Adding AAA\_ATT\_NAS\_IDENTIFIER(32) index=5  
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57  
Adding AAA\_ATT\_VAP\_ID(1) index=6  
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57  
Adding AAA\_ATT\_SERVICE\_TYPE(6) index=7  
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57  
Adding AAA\_ATT\_FRAMED\_MTU(12) index=8  
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57  
Adding AAA\_ATT\_NAS\_PORT\_TYPE(61) index=9  
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57  
Adding AAA\_ATT\_EAP\_MESSAGE(79) index=10  
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57  
Adding AAA\_ATT\_MESS\_AUTH(80) index=11  
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57  
**AAA EAP Packet created request = 0xbbdfe944.. !!!!**  
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57  
**AAA Message 'Interim Response' received for mobile 00:40:96:ac:e6:57**  
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57  
**Received EAP Attribute (code=1, length=24,id=1, dot1xcb->id = 1)  
for mobile 00:40:96:ac:e6:57**  
**Fri Mar 23 21:35:01 2007: 00000000: 01 01 00 18 11 01 00 08 38 93 8c 47 64 99  
e1 d0 .....8..Gd...  
00000010: 45 41 50 55 53 45 52 31** **EAPUSER1**  
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57  
Skipping AVP (0/80) for mobile 00:40:96:ac:e6:57  
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57  
Adding AAA\_ATT\_USER\_NAME(1) index=0  
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57  
Adding AAA\_ATT\_CALLING\_STATION\_ID(31) index=1  
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57  
Adding AAA\_ATT\_CALLED\_STATION\_ID(30) index=2  
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57  
Adding AAA\_ATT\_NAS\_PORT(5) index=3  
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57  
Adding AAA\_ATT\_NAS\_IP\_ADDRESS(4) index=4  
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57  
Adding AAA\_ATT\_NAS\_IDENTIFIER(32) index=5  
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57  
Adding AAA\_ATT\_VAP\_ID(1) index=6  
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57  
Adding AAA\_ATT\_SERVICE\_TYPE(6) index=7  
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57  
Adding AAA\_ATT\_FRAMED\_MTU(12) index=8  
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57  
Adding AAA\_ATT\_NAS\_PORT\_TYPE(61) index=9  
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57  
Adding AAA\_ATT\_EAP\_MESSAGE(79) index=10  
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57  
Adding AAA\_ATT\_MESS\_AUTH(80) index=11  
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57  
AAA EAP Packet created request = 0xbbdfe944.. !!!!  
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57

```

AAA Message 'Interim Response' received for mobile 00:40:96:ac:e6:57
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Received EAP Attribute (code=3, length=4,id=1, dot1xcb->id = 1)
for mobile 00:40:96:ac:e6:57
Fri Mar 23 21:35:01 2007: 00000000: 03 01 00 04
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57 Skipping AVP (0/80)
for mobile 00:40:96:ac:e6:57
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_USER_NAME(1) index=0
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_CALLING_STATION_ID(31) index=1
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_CALLED_STATION_ID(30) index=2
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_NAS_PORT(5) index=3
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_NAS_IDENTIFIER(32) index=5
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_VAP_ID(1) index=6
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_SERVICE_TYPE(6) index=7
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_FRAMED_MTU(12) index=8
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_NAS_PORT_TYPE(61) index=9
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_EAP_MESSAGE(79) index=10
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_MESS_AUTH(80) index=11
Fri Mar 23 21:35:05 2007: 00:40:96:ac:e6:57
AAA EAP Packet created request = 0xbbdfe944.. !!!!
Fri Mar 23 21:35:05 2007: 00:40:96:ac:e6:57
AAA Message 'Success' received for mobile 00:40:96:ac:e6:57

```

....

- **debug dot11 all enable** : 無線の機能のデバッグをイネーブルにします。
- **show client summary <mac>** : MAC アドレスによりクライアントの要約情報を表示します。  
このコマンドの出力例を次に示します。  
(Cisco Controller) >**show client summary**

```

Number of Clients..... 1

MAC Address          AP Name              Status              WLAN  Auth  Protocol  Port
-----
00:40:96:ac:e6:57   AP0015.63e5.0c7e    Associated          1     Yes   802.11a   1

```

## 関連情報

- [Cisco ワイヤレス LAN コントローラ コマンド リファレンス](#)
- [Cisco WLAN コントローラ ネットワーク モジュール機能ガイド](#)
- [Wireless LAN Controller Module \( WLCM \) の設定例](#)
- [ワイヤレス LAN コントローラの Web 認証の設定例](#)
- [WLAN Controller \( WLC \) での EAP 認証の設定例](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)