

LWAPP Upgrade Tool Troubleshooting Tips

Document ID: 69339

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Upgrade Process – Overview

Upgrade Tool – Basic Operation

- Important notes

Types of Certificates

Problem

- Symptom

Solutions

- Cause 1

- Cause 2

- Cause 3

- Cause 4

- Cause 5

- Cause 6

- Cause 7

- Cause 8

Troubleshoot Tips

Related Information

Introduction

This document discusses some of the key issues that might occur when you use the upgrade tool in order to upgrade autonomous access points (APs) to lightweight mode. This document also provides information on how to rectify these issues.

Prerequisites

Requirements

APs must run Cisco IOS® Software Release 12.3(7)JA or later before you can perform the upgrade.

Cisco controllers must run a minimum of software version 3.1.

Cisco Wireless Control System (WCS) (if used) must run a minimum of version 3.1.

The upgrade utility is supported on the Windows 2000 and Windows XP platforms. Either of these Windows operating system versions must be used.

Components Used

The information in this document is based on these Access Points and Wireless LAN Controllers.

The APs that support this migration are:

- All 1121 access points
- All 1130AG access points
- All 1240AG access points
- All 1250 series access points
- For all IOS-based 1200 series modular access point (1200/1220 Cisco IOS Software Upgrade, 1210 and 1230 AP) platforms, it depends on the radio:
 - ◆ if 802.11G, MP21G and MP31G are supported
 - ◆ if 802.11A, RM21A and RM22A are supported

The 1200 series access points can be upgraded with any combination of supported radios: G only, A only, or both G and A. For an access point that contains dual radios, if one of the two radios is an LWAPP-supported radio, the upgrade tool still performs the upgrade. The tool adds a warning message to the detailed log that indicates which radio is unsupported.

- All 1310 AG access points
- Cisco C3201 Wireless Mobile Interface Card (WMIC)

Note: The second-generation 802.11a radios contain two part numbers.

Access points must run Cisco IOS Release 12.3(7)JA or later before you can perform the upgrade.

For Cisco C3201WMIC, access points must run Cisco IOS Release 12.3(8)JK or later before you can perform the upgrade.

These Cisco wireless LAN controllers support autonomous access points upgraded to lightweight mode:

- 2000 series controllers
- 2100 series controllers
- 4400 series controllers
- Cisco Wireless Services Modules (WiSMs) for Cisco Catalyst 6500 Series Switches
- Controller Network Modules within the Cisco 28/37/38xx Series Integrated Services Routers
- Catalyst 3750G Integrated Wireless LAN Controller Switches

Cisco controllers must run a minimum of software version 3.1.

Cisco Wireless Control System (WCS) must run a minimum of version 3.1. The upgrade utility is supported on the Windows 2000 and Windows XP platforms.

You can download the latest version of the upgrade utility from the Cisco Software Downloads page.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Upgrade Process – Overview

The user runs an upgrade utility that accepts an input file with a list of access points and their credentials. The utility telnets to the access points in the input file a series of Cisco IOS commands to prepare the access point for the upgrade, which includes the commands to create the self-signed certificates. Also, the utility telnets to the controller to program the device to allow authorization of specific self-signed certificate access points. It then loads Cisco IOS Software Release 12.3(11)JX1 onto the access point so that it can join the controller. After the access point joins the controller, it downloads a complete Cisco IOS version from it. The upgrade utility generates an output file that includes the list of access points and corresponding self-signed certificate

key-hash values that can be imported into the WCS management software. The WCS can then send this information to other controllers on the network.

Refer to the Upgrade Procedure section of *Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode* for more information.

Upgrade Tool – Basic Operation

This upgrade tool is used to upgrade an autonomous AP to lightweight mode provided the AP is compatible for this upgrade. The upgrade tool performs the basic tasks necessary to upgrade from autonomous to lightweight mode. These tasks include:

- Basic condition checking Verifies whether the AP is a supported one, whether it runs a minimum software revision, and whether the radio types are supported.
- Preparation of the autonomous AP for conversion Adds the Public Key Infrastructure (PKI) configuration and certificate hierarchy so that the AP authentication to the Cisco controllers can occur, and self-signed certificates (SSCs) can be generated for the AP. If the AP has a manufacturing-installed certificate (MIC), then SSCs are not used.
- Downloads an Autonomous to Lightweight Mode Upgrade Image, such as 12.3(11)JX1 or 12.3(7)JX, which allows the AP to join a controller. On a successful download, this reboots the AP.
- Generates an output file that consists of AP MAC addresses, the certificate type, and a secure key-hash, and automatically updates the controller. The output file can be imported into WCS and exported to other controllers.

Important notes

Before you use this utility, consider these important notes:

- Access points converted with this tool do not connect to 40xx, 41xx, or 3500 controllers.
- You cannot upgrade access points with 802.11b-only or first-generation 802.11a radios.
- If you want to retain the static IP address, netmask, hostname, and default gateway of access points after conversion and reboot, you must load one of these autonomous images on the access points before you convert the access points to LWAPP:
 - ◆ 12.3(7)JA
 - ◆ 12.3(7)JA1
 - ◆ 12.3(7)JA2
 - ◆ 12.3(7)JA3
 - ◆ 12.3(7)JA4
 - ◆ 12.3(8)JA
 - ◆ 12.3(8)JA1
 - ◆ 12.3(8)JA2
 - ◆ 12.3(8)JEA
 - ◆ 12.3(8)JEA1
 - ◆ 12.3(8)JEA2
 - ◆ 12.3(8)JEB
 - ◆ 12.3(8)JEB1
 - ◆ 12.4(3g) JA
 - ◆ 12.4(3g) JA1
- If you upgrade access points to LWAPP from one of these autonomous images, the converted access points do not retain their static IP address, netmask, hostname, and default gateway:
 - ◆ 12.3(11)JA

- ◆ 12.3(11)JA1
- ◆ 12.3(11)JA2
- ◆ 12.3(11)JA3
- The LWAPP upgrade tool does not release Windows operating system memory resources when the upgrade process is complete. Memory resources are released only after you exit the upgrade tool. If you upgrade several batches of access points, you must exit the tool in between batches to release memory resources. If you do not exit the tool in between batches, performance of the upgrade station quickly degrades because of excessive memory consumption.

Types of Certificates

There are two different kinds of APs:

- APs with a MIC
- APs that need to have a SSC

Factory installed certificates are referenced by the term MIC, which is an acronym for Manufacturing Installed Certificate. Cisco Aironet access points shipped before July 18, 2005, do not have MIC, so these access points create a self-signed certificate when upgraded to operate in lightweight mode. Controllers are programmed to accept self-signed certificates for authentication of specific access points.

You must treat Cisco Aironet MIC APs that use Lightweight Access Point Protocol (LWAPP), such as Aironet 1000 APs, and troubleshoot accordingly. In other words, check the IP connectivity, debug the LWAPP state machine, and then check the crypto.

The upgrade tool logs show you whether the AP is a MIC AP or SSC AP. This is an example of a detailed log from the upgrade tool:

```

2006/08/21 16:59:07 INFO          172.16.1.60      Term Length configured.
2006/08/21 16:59:07 INFO          172.16.1.60      Upgrade Tool supported AP
2006/08/21 16:59:07 INFO          172.16.1.60      AP has two radios
2006/08/21 16:59:07 INFO          172.16.1.60      AP has Supported Radio
2006/08/21 16:59:07 INFO          172.16.1.60      AP has 12.3(7)JA Image or greater
2006/08/21 16:59:07 INFO          172.16.1.60      Station role is Root AP
2006/08/21 16:59:07 INFO          172.16.1.60      MIC is already configured in the AP
2006/08/21 16:59:07 INFO          172.16.1.60      Hardware is PowerPC405GP Ethernet,
                               address is 0015.63e5.0c7e (bia 0015.63e5.0c7e)
2006/08/21 16:59:08 INFO          172.16.1.60      Inside Shutdown function
2006/08/21 16:59:10 INFO          172.16.1.60      Shutdown the Dot11Radio1
2006/08/21 16:59:11 INFO          172.16.1.60      Shutdown the Dot11Radio0
2006/08/21 16:59:12 INFO          172.16.1.60      Updating the AP with Current System Time
2006/08/21 16:59:13 INFO          172.16.1.60      Saving the configuration into memory
2006/08/21 16:59:13 INFO          172.16.1.60      Getting AP Name
2006/08/21 16:59:58 INFO          172.16.1.60      Successfully Loaded the LWAPP Recovery
                               Image on to the AP
2006/08/21 16:59:58 INFO          172.16.1.60      Executing Write Erase Command
2006/08/21 17:00:04 INFO          172.16.1.60      Flash contents are logged
2006/08/21 17:00:06 INFO          172.16.1.60      Environmental Variables are logged
2006/08/21 17:00:06 INFO          172.16.1.60      Reloading the AP
2006/08/21 17:00:08 INFO          172.16.1.60      Successfully executed the Reload command

```

In this log, the highlighted line specifies that the AP has a MIC installed with it. Refer to the Upgrade Process Overview section of *Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode* for more information on the certificates and the upgrade process.

In the case of the SSC APs, no certificate is created on the controller. The upgrade tool has the AP generate a Rivest, Shamir, and Adelman (RSA) key pair that is used to sign a self-generated certificate (the SSC). The

upgrade tool adds an entry to the controller authentication list with the MAC address of the AP and public key–hash. The controller needs the public key–hash in order to validate the SSC signature.

If the entry has not been added to the controller, check the output CSV file. There should be entries for each AP. If you find the entry, import that file into the controller. If you use the controller command–line interface (CLI) (with use of the **config auth–list** command) or the switch web, you must import one file at a time. With a WCS, you can import the whole CSV file as a template.

Also, check the regulatory domain.

Note: If you have a LAP AP but you want Cisco IOS functionality, you need to load an autonomous Cisco IOS image on it. Conversely, if you have an autonomous AP and want to convert it to LWAPP, you can install an LWAPP recovery image over autonomous IOS.

You can complete the steps to change AP image with the MODE button or CLI **archive download** commands. Refer to Troubleshooting for more information on how to use the MODE button image reload, which works with autonomous IOS or recovery image named to AP model default filename.

The next section discusses some of the commonly seen issues in the upgrade operation and the steps to resolve these issues.

Problem

Symptom

The AP does not join the controller. The Solutions section of this document provides the causes in order of probability.

Solutions

Use this section to solve this problem.

Cause 1

The AP cannot find the controller via LWAPP discovery, or the AP cannot reach the controller.

Troubleshoot

Complete these steps:

1. Issue the **debug lwapp events enable** command at the controller CLI.

Look for the LWAPP discovery > discovery response > join request > join response sequence. If you do not see the LWAPP discovery request, it means the AP cannot or does not find the controller.

Here is an example of a successful JOIN REPLY from the Wireless LAN Controller (WLC) to the converted Lightweight AP (LAP). This is the output of the **debug lwapp events enable** command:

```
Thu May 25 06:53:54 2006: Received LWAPP DISCOVERY REQUEST from AP
00:15:63:e5:0c:7e to 00:0b:85:33:84:a0 on port '1'
Thu May 25 06:53:54 2006: Successful transmission of LWAPP Discovery-Response to AP
00:15:63:e5:0c:7e on Port 1
Thu May 25 06:53:54 2006: Received LWAPP DISCOVERY REQUEST from AP 00:15:63:e5:0c:7e
to 00:0b:85:33:84:a0 on port '1'
```

```

Thu May 25 06:53:54 2006: Successful transmission of LWAPP Discovery-Response to AP
00:15:63:e5:0c:7e on Port 1
Thu May 25 06:53:54 2006: Received LWAPP DISCOVERY REQUEST from AP 00:15:63:e5:0c:7e
to ff:ff:ff:ff:ff:ff on port '1'
Thu May 25 06:53:54 2006: Successful transmission of LWAPP Discovery-Response to
AP 00:15:63:e5:0c:7e on Port 1
Thu May 25 06:54:05 2006: Received LWAPP JOIN REQUEST from AP 00:15:63:e5:0c:7e
to 00:0b:85:33:84:a0 on port '1'
Thu May 25 06:54:05 2006: LWAPP Join-Request MTU path from AP 00:15:63:e5:0c:7e
is 1500, remote debug mode is 0
Thu May 25 06:54:05 2006: Successfully added NPU Entry for AP 00:15:63:e5:0c:7e
(index 51)Switch IP: 172.16.1.11, Switch Port: 12223,
intIfNum 1, vlanId 0AP IP: 172.16.1.60, AP Port: 20679,
next hop MAC: 00:15:63:e5:0c:7e
Thu May 25 06:54:05 2006: Successfully transmission of LWAPP Join-Reply to AP
00:15:63:e5:0c:7e
.....
.....
..... // the debug output continues for
full registration process.

```

2. Check for IP connectivity between the AP network and the controller. If the controller and the AP reside in the same subnet, ensure that they are properly interconnected. If they reside in different subnets, ensure that a router is used in between them and routing is properly enabled between the two subnets.
3. Verify that the discovery mechanism is correctly configured.

If the Domain Name System (DNS) option is used for discovering the WLC, ensure that the DNS server is correctly configured to map CISCO-LWAPP-CONTROLLER.local-domain with the WLC IP address. Hence, if the AP can resolve the name, it issues an LWAPP join message to the resolved IP address.

If option 43 is used as the discovery option, ensure that it is properly configured on the DHCP server.

Refer to Register the LAP with the WLC for more information on the discovery process and sequence.

Refer to DHCP OPTION 43 for Lightweight Cisco Aironet Access Points Configuration Example for more information on how to configure DHCP option 43.

Note: Remember that when you convert statically-addressed APs, the only Layer 3 discovery mechanism that works is the DNS because the static address is preserved during the upgrade.

On the AP, you can issue the **debug lwapp client events** command and the **debug ip udp** command in order to receive enough information to determine exactly what occurs. You should see a User Datagram Protocol (UDP) packet sequence such as this:

- a. Sourced from the AP IP with the controller management interface IP.
- b. Sourced from the controller AP manager IP to the AP IP.
- c. Series of packets that are sourced from the AP IP to the AP manager IP.

Note: In some situations, there can be more than one controller and the AP might try to join a different controller on the basis of the LWAPP discovery state machine and algorithms. This situation might occur because of the default dynamic AP load balancing that the controller performs. This situation can be worth examination.

Note: This is an example output of the **debug ip udp** command:

```
Dec 16 00:32:08.228: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12222)
```

```

length=78
*Dec 16 00:32:08.777: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223)
length=60
*Dec 16 00:32:08.777: UDP: sent src=172.16.1.60(20679), dst=172.16.1.10(12223)
length=75
*Dec 16 00:32:08.778: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679)
length=22
*Dec 16 00:32:08.779: UDP: rcvd src=172.16.1.10(12223), dst=172.16.1.60(20679)
length=59
*Dec 16 00:32:09.057: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223)
length=180
*Dec 16 00:32:09.059: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679)
length=22
*Dec 16 00:32:09.075: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223)
length=89
*Dec 16 00:32:09.077: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679)
length=22
*Dec 16 00:32:09.298: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223)
length=209
*Dec 16 00:32:09.300: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679)
length=22
*Dec 16 00:32:09.300: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223)
length=164
*Dec 16 00:32:09.301: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679)
length=22
*Dec 16 00:32:09.302: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223)
length=209
*Dec 16 00:32:09.303: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679)
length=22
*Dec 16 00:32:09.303: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223)
length=287
*Dec 16 00:32:09.306: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679)
length=22
*Dec 16 00:32:09.306: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223)
length=89
*Dec 16 00:32:09.308: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679)
length=22
*Dec 16 00:32:09.308: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223)
length=222

```

Resolution

Complete these steps:

1. Review the manual.
2. Fix the infrastructure so that it correctly supports the LWAPP discovery.
3. Move the AP to the same subnet as the controller in order to prime it.
4. If necessary, issue the **lwapp ap controller ip address A.B.C.D** command in order to manually set the controller IP at the AP CLI:

The *A.B.C.D* part of this command is the management interface IP address of the WLC.

Note: This CLI command can be used on an AP that has never registered to a controller, or on an AP that had its default enable password changed while joined to a previous controller. Refer to Resetting the LWAPP Configuration on a Lightweight AP (LAP) for more information.

Cause 2

The controller time is outside the certificate validity interval.

Troubleshoot

Complete these steps:

1. Issue the **debug lwapp errors enable** and **debug pm pki enable** commands.

These **debug** commands show the debug of certificate messages that are passed between the AP and the WLC. The commands clearly show a message that the certificate is rejected as outside the validity interval.

Note: Make sure to account for the Coordinated Universal Time (UTC) offset.

This is the output from the **debug pm pki enable** command on the controller:

```
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: locking ca cert table
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: calling x509_alloc() for user cert
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: calling x509_decode()
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: <subject> C=US, ST=California,
L=San Jose, O=Cisco Systems, CN=C1200-001563e50c7e,
MAILTO=support@cisco.com
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: <issuer> O=Cisco Systems,
CN=Cisco Manufacturing CA
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: Mac Address in subject is
00:15:63:e5:0c:7e
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: Cert is issued by Cisco Systems.
.....
.....
.....
.....
Fri Apr 15 07:55:03 2005: ssphmUserCertVerify: calling x509_decode()
Fri Apr 15 07:55:03 2005: ssphmUserCertVerify: user cert verified using
>ciscoDefaultMfgCaCert<
Fri Apr 15 07:55:03 2005: sshpmGetIssuerHandles: ValidityString (current):
2005/04/15/07:55:03
Fri Apr 15 07:55:03 2005: sshpmGetIssuerHandles: Current time outside AP cert
validity interval: make sure the controller time is set.
Fri Apr 15 07:55:03 2005: sshpmFreePublicKeyHandle: called with (nil)
```

In this output, notice the highlighted information. This information clearly shows that the **controller time is outside the certificate validity interval of the AP**. Therefore, the AP cannot register with the controller. Certificates installed in the AP have a predefined validity interval. The controller time should be set in such a way that it is within the certificate validity interval of the AP.

2. Issue the **show crypto ca certificates** command from the AP CLI in order to verify the certificate validity interval set in the AP.

This is an example:

```
AP0015.63e5.0c7e#show crypto ca certificates
.....
.....
.....
.....
Certificate
Status: Available
Certificate Serial Number: 4BC6DAB8000000517AF
Certificate Usage: General Purpose
Issuer:
cn=Cisco Manufacturing CA
o=Cisco Systems
Subject:
Name: C1200-001563e50c7e
```

```

ea=support@cisco.com
cn=C1200-001563e50c7e
o=Cisco Systems
l=San Jose
st=California
c=US
CRL Distribution Point:
  http://www.cisco.com/security/pki/crl/cmca.crl
Validity Date:
  start date: 17:22:04 UTC Nov 30 2005
  end   date: 17:32:04 UTC Nov 30 2015
  renew date: 00:00:00 UTC Jan 1 1970
Associated Trustpoints: Cisco_IOS_MIC_cert
.....
.....
.....

```

The entire output is not listed as there can be many validity intervals associated with the output of this command. You need to consider only the validity interval specified by the **Associated Trustpoint: Cisco_IOS_MIC_cert** with the relevant AP name in the name field (**Here, Name: C1200-001563e50c7e**), as highlighted in this output example. **This is the actual certificate validity interval to be considered.**

3. Issue the **show time** command from the controller CLI in order to verify that the date and time set on your controller falls within this validity interval.

If the controller time is above or below this certificate validity interval, then change the controller time to fall within this interval.

Resolution

Complete this step:

Choose **Commands > Set Time** in the controller GUI mode or issue the **config time** command in the controller CLI in order to set the controller time.

Cause 3

With SSC APs, the SSC AP policy is disabled.

Troubleshoot

In such cases, you see this error message on the controller:

```

Wed Aug  9 17:20:21 2006 [ERROR] spam_lrad.c 1553: spamProcessJoinRequest
                        :spamDecodeJoinReq failed
Wed Aug  9 17:20:21 2006 [ERROR] spam_crypto.c 1509: Unable to free public key for
                        AP 00:12:44:B3:E5:60
Wed Aug  9 17:20:21 2006 [ERROR] spam_lrad.c 4880: LWAPP Join-Request does not include
                        valid certificate in CERTIFICATE_PAYLOAD from
                        AP 00:12:44:b3:e5:60.
Wed Aug  9 17:20:21 2006 [CRITICAL] sshpmpkiApi.c 1493: Not configured to accept
                        Self-signed AP cert

```

Complete these steps:

Perform one of these two actions:

- Issue the **show auth-list** command at the controller CLI in order to check for whether the controller

is configured to accept APs with SSCs.

This is a sample output of **show auth-list** command:

```
#show auth-list
```

```
Authorize APs against AAA ..... disabled
```

```
Allow APs with Self-signed Certificate (SSC) .... enabled
```

Mac Addr	Cert Type	Key Hash
-----	-----	-----
00:09:12:2a:2b:2c	SSC	1234567890123456789012345678901234567890

- Choose **Security > AP Policies** in the GUI.

- a. Check whether the **Accept Self Signed Certificate** check box is enabled. If not, enable it.
- b. Choose **SSC** as the certificate type.
- c. Add **AP** to the authorization list with MAC address and key-hash.

This key-hash can be obtained from the output of the **debug pm pki enable** command. See Cause 4 for information on getting the key-hash value.

Cause 4

The SSC public key-hash is wrong or missing.

Troubleshoot

Complete these steps:

1. Issue the **debug lwapp events enable** command.

Verify that the AP tries to join.

2. Issue the **show auth-list** command.

This command shows the public key-hash that the controller has in storage.

3. Issue the **debug pm pki enable** command.

This command shows the actual public key-hash. The actual public key-hash must match the public key-hash that the controller has in storage. A discrepancy causes the problem. This is a sample output of this debug message:

```
(Cisco Controller) >  
debug pm pki enable  
  
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: getting (old) aes ID cert handle..  
Mon May 22 06:34:10 2006: sshpmGetCID: called to evaluate <bsnOldDefaultIdCert>  
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 0, CA cert  
>bsnOldDefaultCaCert<  
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 1, CA cert  
>bsnDefaultRootCaCert<  
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 2, CA cert  
>bsnDefaultCaCert<  
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 3, CA cert
```

```

>bsnDefaultBuildCert<
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 4, CA cert
>cscscoDefaultNewRootCaCert<
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 5, CA cert
>cscscoDefaultMfgCaCert<
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 0, ID cert
>bsnOldDefaultIdCert<
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Calculate SHA1 hash on Public Key
Data
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 30820122 300d0609
2a864886 f70d0101
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 01050003 82010f00
3082010a 02820101
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 00c805cd 7d406ea0
cad8df69 b366fd4c
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 82fc0df0 39f2bff7
ad425fa7 face8f15
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data f356a6b3 9b876251
43b95a34 49292e11
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 038181eb 058c782e
56f0ad91 2d61a389
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data f81fa6ce cd1f400b
b5cf7cef 06ba4375
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data dde0648e c4d63259
774ce74e 9e2fde19
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 0f463f9e c77b79ea
65d8639b d63aa0e3
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 7dd485db 251e2e07
9cd31041 b0734a55
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 463fbacc 1a61502d
c54e75f2 6d28fc6b
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 82315490 881e3e31
02d37140 7c9c865a
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 9ef3311b d514795f
7a9bac00 d13ff85f
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 97e1a693 f9f6c5cb
88053e8b 7fae6d67
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data ca364f6f 76cf78bc
bclacc13 0d334aa6
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 031fb2a3 b5e572df
2c831e7e f765b7e5
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data fe64641f de2a6fe3
23311756 8302b8b8
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 1bfae1a8 eb076940
280cbcd1 49b2d50f
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data f7020301 0001
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: SSC Key Hash is
9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9

!--- This is the actual SSC key-hash value.

Mon May 22 06:34:14 2006: LWAPP Join-Request MTU path from AP 00:0e:84:32:04:f0
is 1500, remote debug mode is 0
Mon May 22 06:34:14 2006: spamRadiusProcessResponse: AP Authorization failure for
00:0e:84:32:04:f0

```

Resolution

Complete these steps:

1. Copy the public key-hash from the **debug pm pki enable** command output and use it to replace the public key-hash in the authentication list.
2. Issue the **config auth-list add ssc AP_MAC AP_key** command in order to add the AP MAC address and key-hash to the authorization list:

This is an example of this command:

```
(Cisco Controller)>config auth-list add ssc 00:0e:84:32:04:f0  
9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9
```

!--- This command should be on one line.

Cause 5

There is a certificate or public key corruption on the AP.

Troubleshoot

Complete this step:

Issue the **debug lwapp errors enable** and **debug pm pki enable** commands.

You see messages that indicate the certificates or keys that are corrupted.

Resolution

Use one of these two options in order to resolve the problem:

- MIC AP Request a return materials authorization (RMA).
- SSC AP Downgrade to Cisco IOS Software Release 12.3(7)JA.

Complete these steps in order to downgrade:

1. Use the reset button option.
2. Clear the controller settings.
3. Run the upgrade again.

Cause 6

The controller might be working in Layer 2 mode.

Troubleshoot

Complete this step:

Check the mode of operation of the controller.

Converted APs only support Layer 3 discovery. Converted APs do not support Layer 2 discovery.

Resolution

Complete these steps:

1. Set the WLC to be in Layer 3 mode.
2. Reboot and give the AP manager interface an IP address in the same subnet as the management interface.

If you have a service port, such as the service port on a 4402 or 4404, you should have it in a different supernet than the AP manager and management interfaces.

Cause 7

You see this error during the upgrade:

```
FAILED Unable to Load the LWAPP Recovery Image on to the AP
```

Troubleshoot

When you see this error, complete these steps:

1. Verify that your TFTP server is properly configured.

If you use the Upgrade Tool embedded TFTP server, a common culprit is personal firewall software, which blocks the incoming TFTP.

2. Check if you are using the correct image for the upgrade.

The upgrade to lightweight mode requires a special image and does not work with the normal upgrade images.

Cause 8

You receive this error message on the AP after the conversion:

```
*Mar 1 00:00:23.535: %LWAPP-5-CHANGED: LWAPP changed state to DISCOVERY
*Mar 1 00:00:23.550: LWAPP_CLIENT_ERROR_DEBUG: lwapp_crypto_init_ssc_keys_and_
certs no certs in the SSC Private File
*Mar 1 00:00:23.550: LWAPP_CLIENT_ERROR_DEBUG:
*Mar 1 00:00:23.551: lwapp_crypto_init: PKI_StartSession failed
*Mar 1 00:00:23.720: %SYS-5-RELOAD: Reload requested by LWAPP CLIENT.
Reload Reason: FAILED CRYPTO INIT.
*Mar 1 00:00:23.721: %LWAPP-5-CHANGED: LWAPP changed state to DOWN
```

The AP reloads after 30 seconds and starts the process over again.

Resolution

Complete this step:

You have an SSC AP. Once you convert to LWAPP AP, add the SSC and its MAC address under the AP Authentication list in the controller.

Troubleshoot Tips

These tips can be used when you upgrade from autonomous to LWAPP mode:

- If the NVRAM is not cleared when the controller tries to write to it after the conversion, problems are caused. Cisco recommends to clear the configuration before you convert an AP to LWAPP. In order to clear the configuration:
 - ◆ From the IOS GUI Go to **System Software > System Configuration > Reset to Defaults**, or **Reset to Defaults Except IP**.

- ◆ From CLI Issue the **write erase** and **reload** commands at the CLI and do not allow the configuration to be saved when prompted.

This also makes the text file of APs to be converted by the Upgrade Tool more simple to create as the entries become <ip address>,Cisco,Cisco,Cisco.

- Cisco recommends that you use the tftp32. You can download the latest TFTP server at <http://tftpd32.jounin.net/>.
- If a firewall or an access control list is enabled during the upgrade process, the upgrade tool can become unable to copy the file that contains environmental variables from a workstation to an AP.

If a firewall or access control list blocks the copy operation and you select the Use Upgrade Tool TFTP Server option, you cannot proceed with the upgrade because the tool cannot update the environmental variables, and the image upload to the AP fails.

- Double check the image you are trying to upgrade to. The upgrade from IOS to LWAPP images is different from the normal IOS images.

Under My Documents/My Computer--> Tools--> Folder Options, make sure you uncheck the **Hide file extensions for known file types** check box.

- Always make sure to use the latest available Upgrade Tool and Upgrade Recovery Image. The latest versions are available in the Wireless Software Center.
- An AP can not boot a **.tar** image file. It is an archive, similar to zip files. You need to unbundle the **.tar** file into AP flash with the **archive download** command, or else pull the bootable image out of the tar file first then put the bootable image into AP flash.

Related Information

- **Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode**
- **Resetting the LWAPP Configuration on a Lightweight AP (LAP)**
- **DHCP OPTION 43 for Lightweight Cisco Aironet Access Points Configuration Example**
- **Technical Support & Documentation – Cisco Systems**

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Aug 12, 2009

Document ID: 69339
