Self−Signed Certificate Manual Addition to the Controller for LWAPP−Converted APs

Document ID: 70341

Contents

Introduction
Prerequisites
Requirements
Components Used
Conventions
Background Information
Locate the SHA1 Key Hash
Add the SSC to the WLC
Task
GUI Configuration
CLI Configuration
Verify
Troubleshoot
Related Information

Introduction

This document explains the methods that you can use in order to manually add self−signed certificates (SSCs) to a Cisco Wireless LAN (WLAN) Controller (WLC).

The SSC of an access point (AP) should exist on all WLCs in the network to which the AP has permission to register. As a general rule, apply the SSC to all WLCs in the same mobility group. When addition of the SSC to the WLC does not occur through the upgrade utility, you must manually add the SSC to the WLC with use of the procedure in this document. You also need this procedure when an AP is moved to a different network or when additional WLCs are added to the existing network.

You can recognize this problem when a Lightweight AP Protocol (LWAPP)−converted AP does not associate to the WLC. When you troubleshoot the association problem, you see these outputs when you issue these debugs:

- When you issue the **debug pm pki enable** command, you see:

```
(Cisco Controller) >debug pm pki enable
Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: locking ca cert table
Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: calling x509_alloc() for user cert
Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: calling x509_decode()
Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: <subject> L=San Jose, ST=
California, C=US, O=Cisco Systems, MAILTO=support@cisco.com, CN=C1130−00146a1b3744
Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: <issuer>  L=San Jose, ST=
California, C=US, O=Cisco Systems, MAILTO=support@cisco.com, CN=C1130−00146a1b3744
Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: Mac Address in subject is
00:XX:XX:XX:XX
Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: Cert is issued by Cisco Systems.
Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: SSC is not allowed by config;
bailing...
Thu Jan 26 20:22:50 2006: sshpmFreePublicKeyHandle: called with (nil)
Thu Jan 26 20:22:50 2006: sshpmFreePublicKeyHandle: NULL argument.
```

- When you issue the **debug lwapp events enable** command, you see:

```
(Cisco Controller) >debug lwapp errors enable
....
Thu Jan 26 20:23:27 2006: Received LWAPP DISCOVERY REQUEST from AP
00:13:5f:f8:c3:70 to ff:ff:ff:ff:ff:ff on port '1'
Thu Jan 26 20:23:27 2006: Successful transmission of LWAPP Discovery−Response to
AP 00:13:5f:f8:c3:70 on Port 1
Thu Jan 26 20:23:27 2006: Received LWAPP JOIN REQUEST from AP 00:13:5f:f9:dc:b0 to
06:0a:10:10:00:00 on port '1'
Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: locking ca cert table
Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: calling x509_alloc() for user cert
Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: calling x509_decode()
Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: <subject> L=San Jose, ST=
California, C=US, O=Cisco Systems, MAILTO=support@cisco.com, CN=C1130−00146a1b321a
Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: <issuer>  L=San Jose, ST=
California, C=US, O=Cisco Systems, MAILTO=support@cisco.com, CN=C1130−00146a1b321a
Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: Mac Address in subject is
00:14:6a:1b:32:1a

Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: Cert is issued by Cisco Systems.
Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: SSC is not allowed by config;
bailing...
Thu Jan 26 20:23:27 2006: LWAPP Join−Request does not include valid certificate
in CERTIFICATE_PAYLOAD from AP 00:13:5f:f9:dc:b0.
Thu Jan 26 20:23:27 2006: sshpmFreePublicKeyHandle: called with (nil)
Thu Jan 26 20:23:27 2006: sshpmFreePublicKeyHandle: NULL argument.
Thu Jan 26 20:23:27 2006: Unable to free public key for AP  00:13:5F:F9:DC:B0
Thu Jan 26 20:23:27 2006: spamDeleteLCB: stats timer not initialized for AP
00:13:5f:f9:dc:b0
Thu Jan 26 20:23:27 2006: spamProcessJoinRequest : spamDecodeJoinReq failed
```

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- The WLC does not contain the SSC that the upgrade utility generated.
- The APs contain an SSC.
- Telnet is enabled on the WLC and the AP.
- The minimum version of pre−LWAPP Cisco IOS® Software code is on the AP to be upgraded.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 2006 WLC that runs firmware 3.2.116.21 with no SSC installed
- Cisco Aironet 1230 Series AP with an SSC

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

Conventions

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

Background Information

In the Cisco Centralized WLAN architecture, APs operate in lightweight mode. The APs associate to a Cisco WLC with use of the LWAPP. LWAPP is an Internet Engineering Task Force (IETF) draft protocol that defines the control messaging for setup and path authentication and run−time operations. LWAPP also defines the tunneling mechanism for data traffic.

A lightweight AP (LAP) discovers a WLC with use of LWAPP discovery mechanisms. The LAP then sends the WLC an LWAPP join request. The WLC sends the LAP an LWAPP join response that allows the LAP to join the WLC. When the LAP is joined to the WLC, the LAP downloads the WLC software if the revisions on the LAP and the WLC do not match. Subsequently, the LAP is completely under the control of the WLC.

LWAPP secures the control communication between the AP and the WLC by means of a secure key distribution. The secure key distribution requires already provisioned X.509 digital certificates on both the LAP and the WLC. Factory−installed certificates are referenced with the term "MIC", which is an acronym for Manufacturing Installed Certificate. Aironet APs that shipped before July 18, 2005, do not have MICs. So these APs create an SSC when they are converted to operate in lightweight mode. Controllers are programmed to accept SSCs for the authentication of specific APs.

This is the upgrade process:

1. The user runs an upgrade utility that accepts an input file with a list of APs and their IP addresses, in addition to their login credentials.
2. The utility establishes Telnet sessions with the APs and sends a series of Cisco IOS Software commands in the input file in order to prepare the AP for the upgrade. These commands include the commands to create the SSCs. Also, the utility establishes a Telnet session with the WLC in order to program the device to allow the authorization of specific SSC APs.
3. The utility then loads Cisco IOS Software Release 12.3(7)JX onto the AP so that the AP can join the WLC.
4. After the AP joins the WLC, the AP downloads a complete Cisco IOS Software version from the WLC. The upgrade utility generates an output file that includes the list of APs and corresponding SSC key−hash values that can be imported into the Wireless Control System (WCS) management software.
5. The WCS can then send this information to other WLCs on the network.

After an AP joins a WLC, you can reassign the AP to any WLC on your network, if necessary.

Locate the SHA1 Key Hash

If the computer that performed the AP conversion is available, you can obtain the Secure Hash Algorithm 1 (SHA1) Key Hash from the .csv file that is in the Cisco Upgrade Tool directory. If the .csv file is unavailable, you can issue a **debug** command on the WLC in order to retrieve the SHA1 Key Hash.

Complete these steps:

1. Turn on the AP and connect it to the network.
2. Enable the debugging on the WLC command−line interface (CLI).

   The command is **debug pm pki enable**.

```
(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
>cscoDefaultNewRootCaCert<
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 5, CA cert
>cscoDefaultMfgCaCert<
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
bc1acc13 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
280cbed1 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
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
```

Add the SSC to the WLC

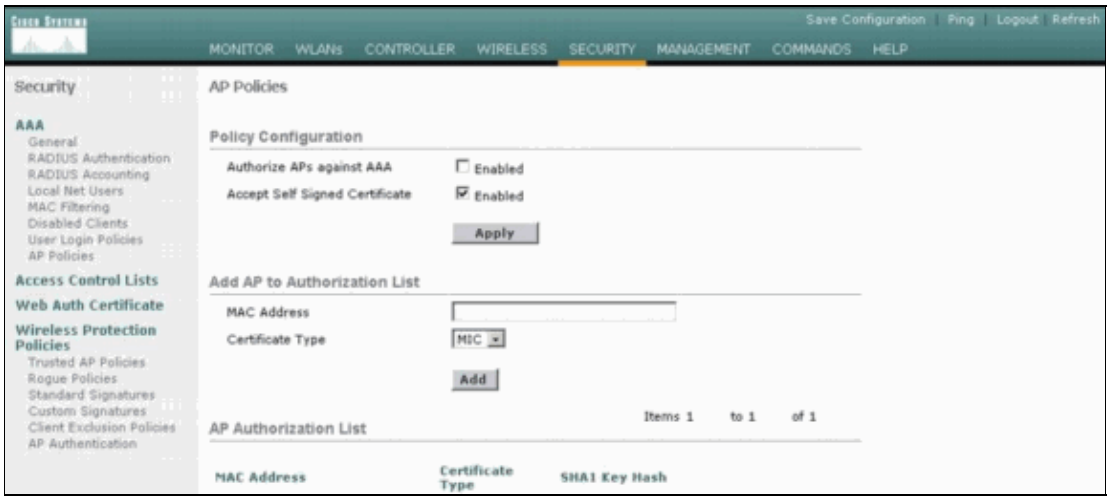
Task

In this section, you are presented with the information to configure the features described in this document.

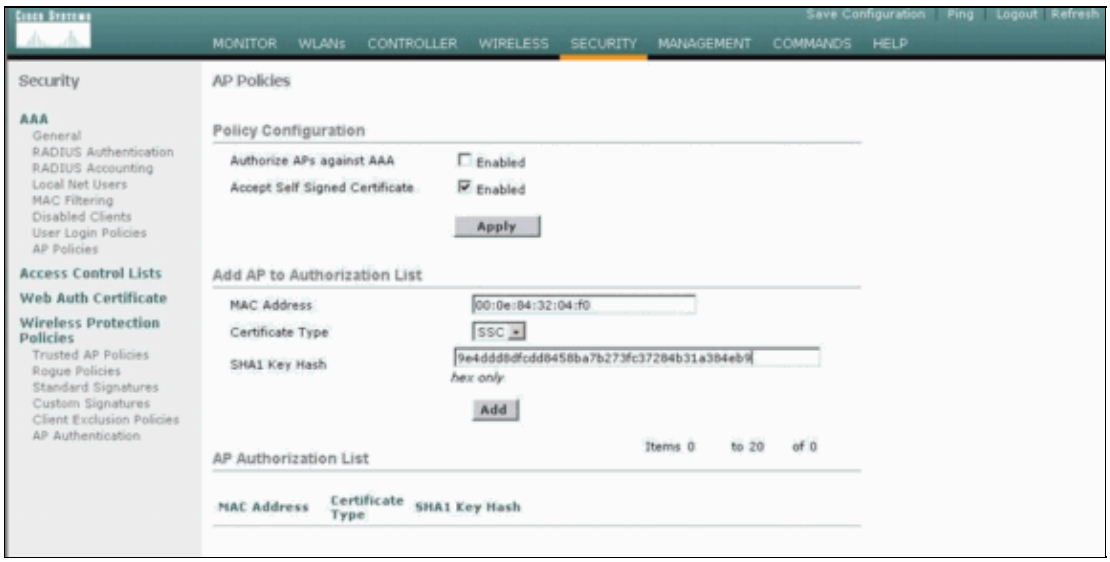
GUI Configuration

Complete these steps from the GUI:

1. Choose **Security > AP Policies** and click **Enabled** beside Accept Self Signed Certificate.



2. Select **SSC** from the Certificate Type drop−down menu.



3. Enter the MAC address of the AP and the hash key, and click **Add**.

CLI Configuration

Complete these steps from the CLI:

1. Enable Accept Self Signed Certificate on the WLC.

   The command is **config auth−list ap−policy ssc enable**.

   ```
   (Cisco Controller) >config auth-list ap-policy ssc enable
   ```

2. Add the AP MAC address and hash key to the authorization list.

The command is **config auth−list add ssc** *AP_MAC AP_key* .

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

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

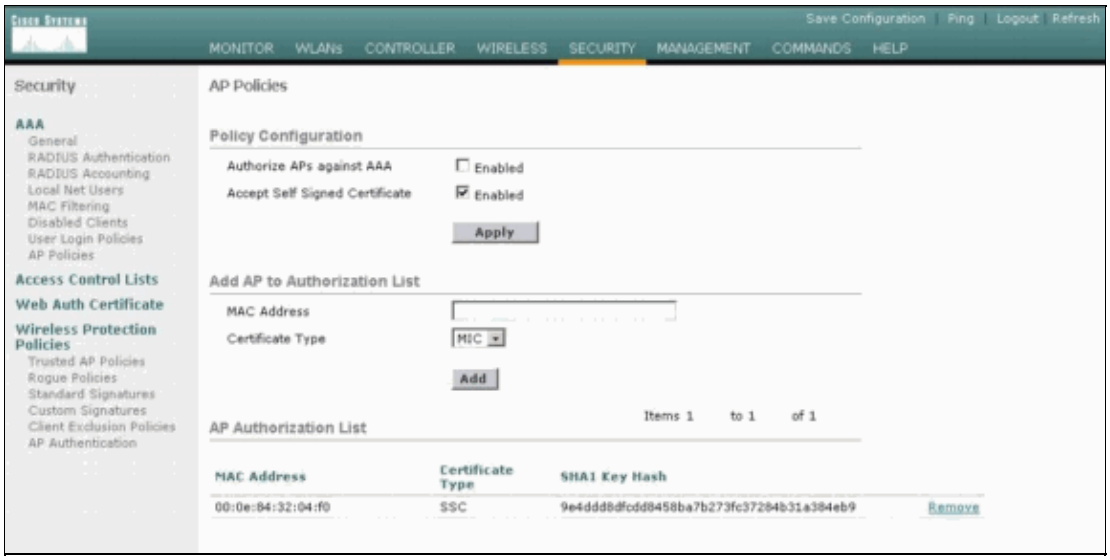
Verify

Use this section to confirm that your configuration works properly.

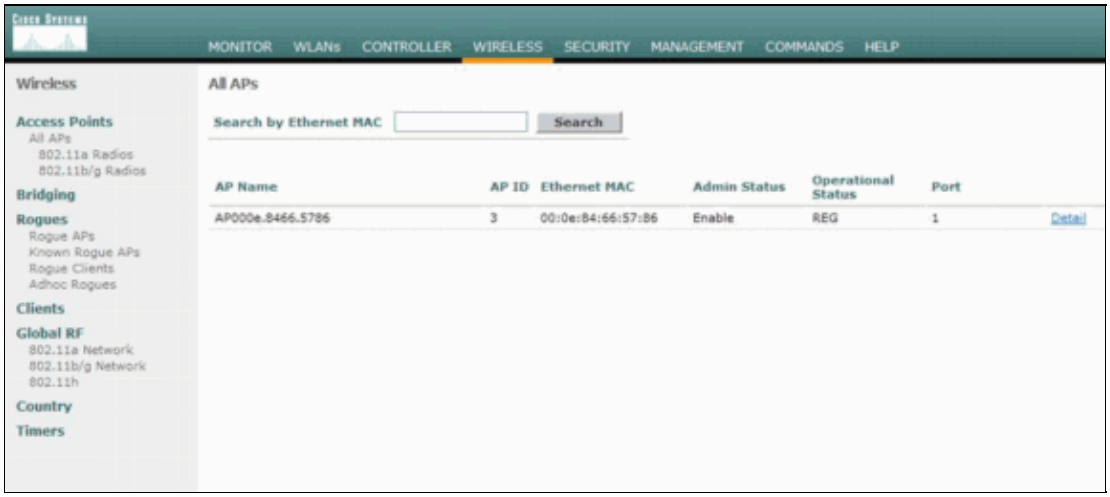
GUI Verification

Complete these steps:

1. In the AP Policies window, verify that the AP MAC address and SHA1 Key Hash appear in the AP Authorization List area.



2. In the All APs window, verify that all APs are registered with the WLC.



CLI Verification

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show auth−list** Displays the AP authorization list.
- **show ap summary** Displays a summary of all connected APs.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **Wireless LAN Controller (WLC) Troubleshoot FAQ**
- **Cisco Wireless LAN Controller Configuration Guide, Release 3.2**
- **Wireless LAN Controller and Lightweight Access Point Basic Configuration Example**
- **Technical Support & Documentation − Cisco Systems**

Contacts & Feedback | Help | Site Map
© 2013 − 2014 Cisco Systems, Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems, Inc.

Updated: Aug 04, 2008 Document ID: 70341