



Set Up Your Wireless LAN Controller Module

Home > Work With My Wireless Devices > Cisco Aironet 1100 and 1200 Series Access Points > Set Up Your Wireless LAN Controller Module

Service Requests

[Open a service request](#)

[Update a service request](#)

Feedback

Please rate this site:

++ + +/- - --

Suggestions for improvement:

Step 5: Configure the Cisco Wireless LAN Controller Module

Step 1: [SMB Support Assistant Site Survey](#)

Step 2: [Set Up Your Cisco Wireless LAN Controller Module Hardware](#)

Step 3: [Configure Your Router for the Wireless LAN Controller Module](#)

Step 4: [Complete Initial Setup for the Cisco Wireless LAN Controller Module](#)

Step 5: Configure the Cisco Wireless LAN Controller Module

[Introduction](#)

Requirements

Configure the Controller

[Connect to the Device Manager](#)

[Switch Settings](#)

[Configure Interfaces](#)

[WLAN Settings](#)

[Enable Telnet/SSH](#)

[Wireless Security](#)

[Configure WLAN Security for a Pre-Shared Key](#)

[Configure Wireless Security for an External RADIUS Server](#)

Next Step

Troubleshoot the Procedure

[Install the Certificate](#)

Related Information

Step 6: [Set Up a RADIUS Server for the Wireless LAN Controller Module](#)

Step 7: [Add a Lightweight Access Point to Your Wireless Network](#)

Download PDF



[Step 5: Configure the Cisco Wireless LAN Controller Module](#)



[Set Up Your Wireless LAN Controller Module](#)

If Cisco may contact you for more details or for future feedback opportunities, please enter your contact information:

Full

Name:

Email:

Introduction

This document provides instructions on how to configure the Wireless LAN Controller Module (WLCM) installed in your Cisco 2800 and 3800 Integrated Services Router.

This document shows how to configure the WLCM solution with these subnets:

VLAN	IP Address

Wireless LAPs	192.168.14.0
WLAN Controller Management	192.168.15.0
Wireless Default	192.168.16.0
Wireless Guest	192.168.17.0

If you want to set up a WLCM at more than one site, the [Wireless LAN Controller Module IP Addressing Plan](#) provides additional subnets that you can use for up to 30 sites. To set up an additional site, replace the VLAN subnets used in this document with the appropriate subnets for your site.

[Back to Top](#)

Requirements

To configure the Cisco WLCM, you need these items:

- A straight-through Ethernet cable. For more information about cables, refer to [Cable Descriptions](#).
- Completed worksheets from the [Site Survey](#):
 - LAN Addressing Worksheet
 - ISR Router Worksheet

In addition, you must have completed the steps in the [Complete Initial Setup for the Cisco Wireless LAN Controller Module](#) document.

[Back to Top](#)

Configure the Controller

Follow these steps to configure the Cisco WLCM:

Connect to the Device Manager

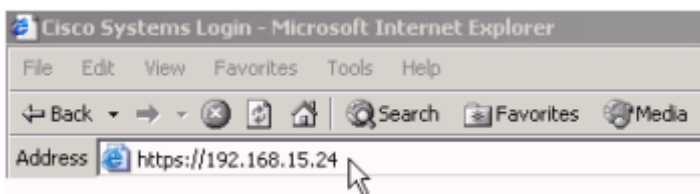
Follow these steps to connect to the Cisco WLAN Controller web user interface:

1. Connect a [straight-through Ethernet cable](#) from a PC to the Management port listed in field S5 of the ISR Router Worksheet.

2. Configure your PC with these values:

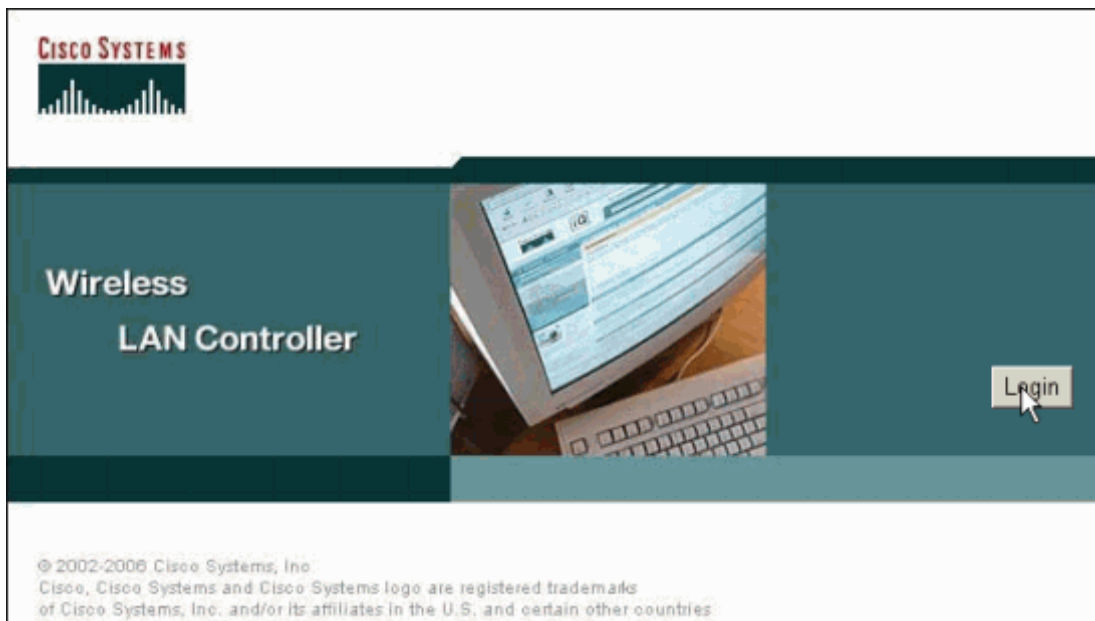
- o IP Address: **192.168.14.100**
- o Subnet Mask: **255.255.255.0**
- o Default Gateway: **192.168.14.1**

For detailed instructions on how to configure an IP address on your PC, refer to [Configure an IP Address on Your PC](#).

3. In a web browser, open **https://192.168.15.24**.4. Click **Yes** to accept the security certificate from the WLCM.

Note: If you would like to permanently install the certificate in order to skip this step in the future, see [Install the Certificate](#).

5. Click **Login**.



6. In the Enter Network Password dialog box, enter the username **admin** and the password that you entered in fields W24 of the ISR Router Worksheet.



7. The WLCM Monitor screen displays.

Cisco Systems | Save Configuration | Ping | Logout | Refresh

MONITOR | WLANs | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP

Monitor

Summary

Statistics

Controller

Ports

Wireless

Rogue APs

Known Rogue APs

Rogue Clients

Adhoc Rogues

802.11a Radios

802.11b/g Radios

Clients

RADIUS Servers

Summary

Controller Summary

Management IP Address: 192.168.10.252

Software Version: 3.2.78.0

System Name: Cisco_33-52-4444a0

Up Time: 0 days, 1 hours, 1 minutes

System Time: Thu Feb 9 05:48:19 2006

802.11a Network State: Enabled

802.11b/g Network State: Enabled

Rogue Summary

Active Rogue APs: 0 [Detail](#)

Active Rogue Clients: 0 [Detail](#)

Adhoc Rogues: 0 [Detail](#)

Rogues on Wired Network: 0

Top WLANs

WLAN	# of Clients by SSID	Detail
smbsa	0	Detail

Most Recent Traps

Cold Start:

Link Up: Slot: 0 Part: 4

Link Down: Slot: 0 Part: 4

[View All](#)

This page refreshes every 30 seconds.

Access Point Summary

	Total	Up	Down	Detail
802.11a Radios	0	0	0	Detail
802.11b/g Radios	0	0	0	Detail
All APs	0	0	0	Detail

Client Summary

Current Clients	0	Detail
Excluded Clients	0	Detail
Disabled Clients	0	Detail

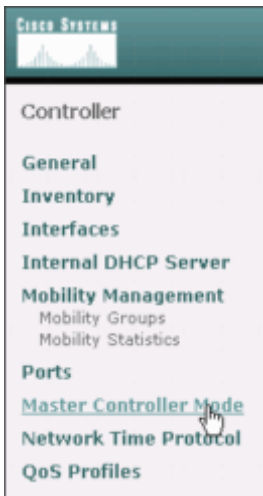
Switch Settings

Follow these steps to configure the switch settings on the Wireless Controller:

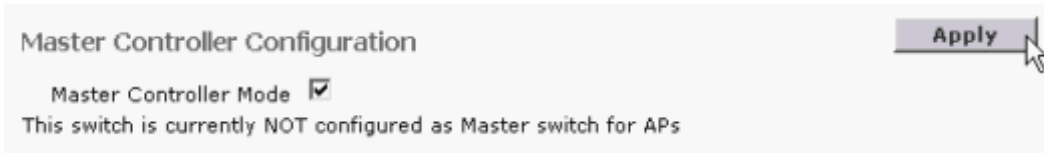
1. Click **Controller**.



2. Follow these steps to set the WLCM in master controller mode:
 - a. Click **Master Controller Mode**.



- b. Check **Master Controller Mode** and click **Apply**.



- 3. Follow these steps to configure a time server:

- a. Click **Network Time Protocol**.



- b. Click **New**.



NTP Servers

Apply New...

NTP Polling Interval seconds 86400

Server Index	Server Address
--------------	----------------

c. On the NTP Servers > New screen, enter these values:

- Server Index (Priority): 1
- Server IP Address: Enter the router IP address that you entered in field L6A of the LAN Addressing Worksheet.

Click **Apply**.



NTP Servers > New

< Back Apply

Server Index (Priority) 1

Server IPAddress 192.168.10.1

Configure Interfaces

Follow these steps to configure VLAN interfaces on the WLCM:

1. Click **Controller**.



2. Click **Interfaces**.



3. Follow these steps to create a VLAN interface for wireless users on the default network:

a. Click **New**.



b. Enter these values to create the Guest VLAN interface:

- Interface Name: Vlan26
- VLAN ID: **26**

Click **Apply**.



c. On the Interfaces > Edit screen, make these changes to the default values:

- Interface Address:
 - IP Address: **192.168.16.254**
 - Netmask: **255.255.255.0**
 - Gateway: **192.168.16.1**

- DHCP Information:
 - Primary DHCP Server: **192.168.16.1**

Click **Apply**.

The screenshot shows the Cisco configuration interface for editing a VLAN interface. The navigation bar at the top includes: MONITOR, WLANS, CONTROLLER (highlighted), WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The breadcrumb trail is "Interfaces > Edit". There are "< Back" and "Apply" buttons. The configuration is organized into sections: General Information, Interface Address, Physical Information, DHCP Information, and Access Control List. A red note at the bottom states: "Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients."

General Information	
Interface Name	Vlan26

Interface Address	
VLAN Identifier	26
IP Address	192.168.16.254
Netmask	255.255.255.0
Gateway	192.168.16.1

Physical Information	
Port Number	1

DHCP Information	
Primary DHCP Server	192.168.16.1
Secondary DHCP Server	0.0.0.0

Access Control List	
ACL Name	none

Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

4. Follow these steps to create a VLAN interface for wireless users on the guest network:

- a. Click **New**.
- b. Enter these values to create the Guest VLAN interface:
 - Interface Name: Vlan27
 - VLAN ID: **27**

Click **Apply**.

- c. Click **Interfaces > Edit**.
- d. On the Interfaces > Edit screen, make these changes to the default values:
 - Interface Address:

- IP Address: **192.168.17.254**

- Netmask: **255.255.255.0**
- Gateway: **192.168.17.1**
- DHCP Information:
 - Primary DHCP Server: **192.168.17.1**

Click **Apply**.

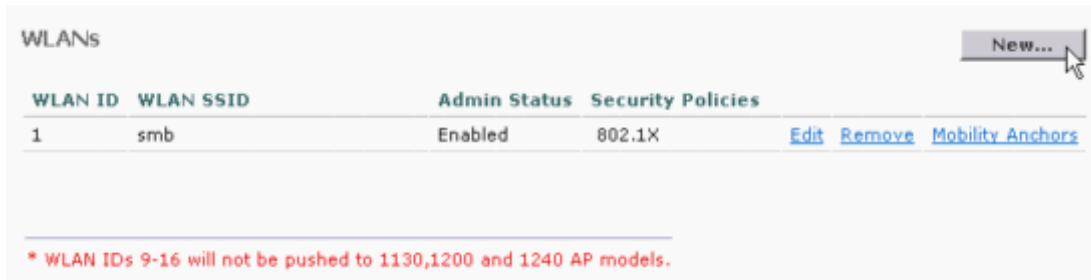
WLAN Settings

Follow these steps to configure Wireless LAN interfaces (WLANs) on the WLCM:

1. Click **WLANs**.



2. Click **New**.



3. Enter these values to create a WLAN for guest users:

- WLAN ID: **3**
- WLAN SSID: **wlan3**

Click **Apply**.



4. On the WLANs > Edit screen, make these changes to the default values:

- General Policies:
 - Admin Status: **Enabled**
 - DHCP Server: Check **Override** and enter **192.168.17.1**.
 - DHCP Addr. Assignment: **Required**
 - Interface Name: **Vlan 27**
- Security Policies:
 - Layer 2 Security: **None**
 - Layer 3 Security: **None**

Note: Instructions to apply security policies are provided later in this document.

Click **Apply**.

The screenshot shows the Cisco WLAN configuration interface. The top navigation bar includes MONITOR, WLANs (selected), CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The main heading is "WLANs > Edit" with "< Back" and "Apply" buttons. The configuration is for WLAN ID 3, WLAN SSID wlan3.

General Policies:

- Radio Policy: All
- Admin Status: Enabled
- Session Timeout (secs): 1800
- Quality of Service (QoS): Silver (best effort)
- WMM Policy: Disabled
- 7920 Phone Support: Client CAC Limit AP CAC Limit
- Broadcast SSID: Enabled
- Allow AAA Override: Enabled
- External Policy Validation: Enabled
- Client Exclusion: Enabled ** 60 (Timeout Value (secs))
- DHCP Server: Override 192.168.17.1 (DHCP Server IP Addr)
- DHCP Addr. Assignment: Required
- Interface Name: vlan27

Security Policies:

- Layer 2 Security: None
 - MAC Filtering
- Layer 3 Security: None
 - Web Policy *

Radius Servers:

	Authentication Servers	Accounting Servers
Server 1	none	none
Server 2	none	none
Server 3	none	none

Footnotes:

- * Web Policy cannot be used in combination with IPsec and L2TP.
- ** When client exclusion is enabled, a timeout value of zero means infinity (will require administrative override to reset excluded clients)

Enable Telnet/SSH

The controller can be configured to accept telnet and SSH connections through the controller web-interface. Follow these steps to enable Telnet and SSH:

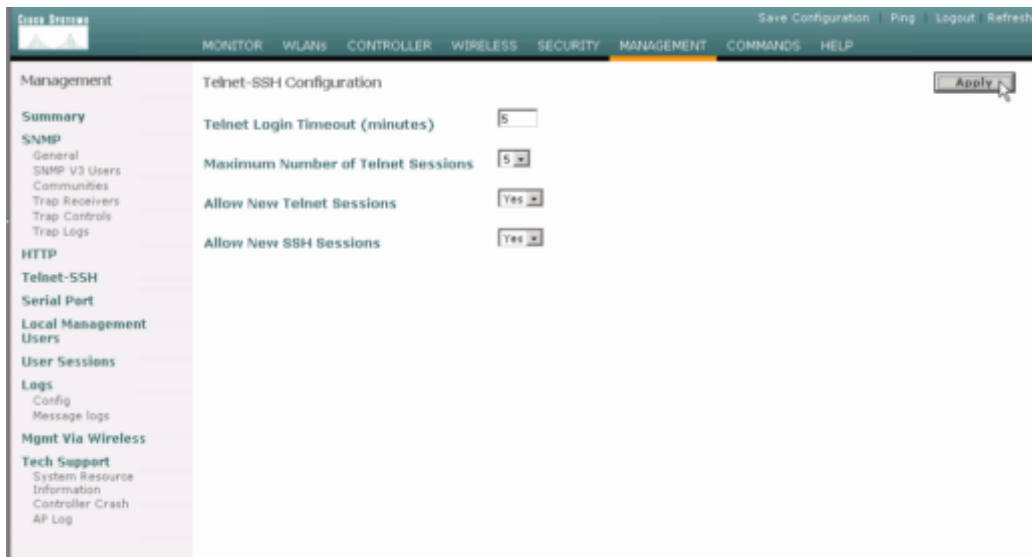
1. Click Management.



2. Click Telnet-SSH.



3. In the Telnet-SSH screen, make these changes to the defaults:
 - o For the Allow New Telnet Sessions, select **Yes** from the drop-down menu.
 - o For the Allow New SSH Sessions, select **Yes** from the drop-down menu.
 - o Click **Apply**.



Wireless Security

Two security options are available for the WLCM:

- **External RADIUS Server:** The wireless network uses an external RADIUS server to authenticate users. This option provides greater security and requires that you provide an external RADIUS server.

Note: Cisco provides the parameters required to set up the RADIUS server, but does not provide full instructions for any particular RADIUS implementation.

- **WPA2 Pre-Shared Key:** A pre-shared password or passphrase is used to provide access to the wireless network. This option is less secure and requires that you create a [strong password](#) for the wireless network.

To configure wireless security to use a pre-shared key, proceed to [Configure Wireless Security for a Pre-Shared Key](#). To configure wireless security to use an external RADIUS server, proceed to [Configure Wireless Security for an External RADIUS Server](#).

Configure WLAN Security for a Pre-Shared Key

Follow these steps to configure wireless security to use a WPA2 Pre-Shared Key:

1. Click **WLANs**.



2. Follow these steps to configure security on the default WLAN:
 - a. Click **Edit** next to the WLAN SSID for the default network that you entered in field W26 of the ISR Router Worksheet.

WLAN ID	WLAN SSID	Admin Status	Security Policies	
1	smb	Enabled	802.1X	Edit Remove Mobility Anchors
3	wlan3	Enabled		Edit Remove Mobility Anchors

* WLAN IDs 9-16 will not be pushed to 1130,1200 and 1240 AP models.

b. On the WLANs > Edit screen, make these changes to the default values:

a. Security Policies:

- Layer 2 Security: Choose **WPA2**.
- Layer 3 Security: **None**.

b. WPA2 Parameters:

- WPA2 Compatibility Mode: Check **WPA2 Compatibility Mode**.
- Allow WPA2 TKIP Clients: **Check Allow WPA2 TKIP Clients**.
- Pre-Shared Key: **Check Pre-Shared Key**.
- Check **Please set the WPA2 Pre-Shared Key of length between 8 and 63 characters** and enter the Pre-Shared Key that you entered in field W27 of the ISR Router Worksheet.

Click **Apply**.

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

WLANs > Edit < Back Apply

WLAN ID 1
WLAN SSID smb

General Policies

Radio Policy
 Admin Status Enabled
 Session Timeout (secs)
 Quality of Service (QoS)
 WMM Policy
 7920 Phone Support Client CAC Limit AP CAC Limit
 Broadcast SSID Enabled
 Allow AAA Override Enabled
 External Policy Validation Enabled
 Client Exclusion Enabled **
 Timeout Value (secs)
 DHCP Server Override
 DHCP Server IP Addr
 DHCP Addr. Assignment Required
 Interface Name

Security Policies

Layer 2 Security
 MAC Filtering

Layer 3 Security
 Web Policy *

* Web Policy cannot be used in combination with IPsec and L2TP.
 ** When client exclusion is enabled, a timeout value of zero means infinity(will require administrative override to reset excluded clients)

Radius Servers

	Authentication Servers	Accounting Servers
Server 1	<input type="text" value="none"/>	<input type="text" value="none"/>
Server 2	<input type="text" value="none"/>	<input type="text" value="none"/>
Server 3	<input type="text" value="none"/>	<input type="text" value="none"/>

WPA2 Parameters

WPA Compatibility Mode Enable
 Allow WPA2 TKIP Clients Enable
 Pre-Shared Key Enabled (WPA2 passphrase has been set)
 Please set the WPA2 Pre-Shared Key of length between 8 and 63 characters

3. Follow these steps to configure security on the Guest WLAN:

a. Click **Edit** next to **wlan3**.

b. On the WLANs > Edit screen, make these changes to the default values:

a. Security Policies:

- Layer 2 Security: Choose **WPA2**.
- Layer 3 Security: **None**.

b. WPA2 Parameters:

- WPA2 Compatibility Mode: Check **WPA2 Compatibility Mode**.
- Allow WPA2 TKIP Clients: **Check Allow WPA2 TKIP Clients**.

- Pre-Shared Key: **Check Pre-Shared Key.**
- Check **Please set the WPA2 Pre-Shared Key of length between 8 and 63 characters** and enter the Pre-Shared Key that you entered in field W27 of the ISR Router Worksheet.

Click **Apply**.

4. Click **Save Configuration** to save your configuration. Click **OK** to confirm.



5. Proceed to the [Next Step](#).

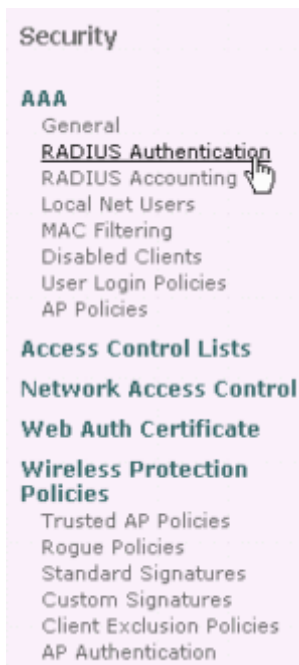
Configure Wireless Security for an External RADIUS Server

Follow these steps to configure wireless security with an external RADIUS server:

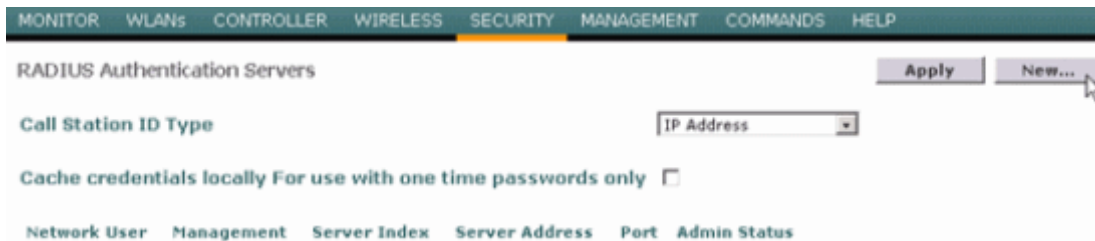
1. Follow these steps to configure the WLCM to use the RADIUS server:
 - a. Click **Security**.



- b. Click **Radius Authentication**.



c. Click **New**.



d. On the RADIUS Authentication Servers > New screen, make these changes to the default values:

- Server IP Address: Enter the IP address of the RADIUS server that you entered in the field W22 of the Wireless Worksheet.
- Shared Secret: Enter the shared secret key that you entered in field W18 of the Wireless Worksheet.
- Confirm Shared Secret: Re-enter the shared secret key that you entered in field W18 of the Wireless Worksheet.
- Network User: **Enable**

Click **Apply**.

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

RADIUS Authentication Servers > New [< Back](#) [Apply](#)

Server Index (Priority)

Server IPAddress

Shared Secret Format

Shared Secret

Confirm Shared Secret

Port Number

Server Status

Support for RFC 3576

Retransmit Timeout seconds

Network User Enable

Management Enable

2. Follow these steps to configure WLAN security for the RADIUS server:

a. Click **WLANs**.



b. Follow these steps to configure WLAN security for users on the default network:

a. Click **Edit** next to the WLAN SSID for the default network that you entered in field W26 of the ISR Router Worksheet.

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

WLANs [New...](#)

WLAN ID	WLAN SSID	Admin Status	Security Policies	
1	smb	Enabled	802.1X	Edit Remove Mobility Anchors
3	wlan3	Enabled		Edit Remove Mobility Anchors

* WLAN IDs 9-16 will not be pushed to 1130,1200 and 1240 AP models.

b. On the WLANs > Edit screen, make these changes to the default values:

a. Security Policies:

- Layer 2 Security: Choose **WPA2**.
- Layer 3 Security: **None**.

b. RADIUS servers:

- Server 1: Choose the RADIUS server IP Address that you entered in field W22 of the ISR Router Worksheet.

Click **Apply**.

MONITOR **WLANs** CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

WLANs > Edit < Back Apply

WLAN ID: 1
WLAN SSID: smb

General Policies

Radio Policy: All
Admin Status: Enabled
Session Timeout (secs): 1800
Quality of Service (QoS): Silver (best effort)
WMM Policy: Disabled
7920 Phone Support: Client CAC Limit AP CAC Limit
Broadcast SSID: Enabled
Allow AAA Override: Enabled
External Policy Validation: Enabled
Client Exclusion: Enabled ** 60
DHCP Server: Override 192.168.16.1
DHCP Addr. Assignment: Required
Interface Name: vlan26

Security Policies

Layer 2 Security: WPA2
 MAC Filtering

Layer 3 Security: None
 Web Policy *

* Web Policy cannot be used in combination with IPsec and L2TP.
** When client exclusion is enabled, a timeout value of zero means infinity(will require administrative override to reset excluded clients)

Radius Servers

	Authentication Servers	Accounting Servers
Server 1	IP:192.168.14.5, Port:1812	none
Server 2	none	none
Server 3	none	none

WPA2 Parameters

WPA Compatibility Mode: Enable
Allow WPA2 TKIP Clients: Enable
Pre-Shared Key: Enabled (WPA2 passphrase has been set)

c. Follow these steps to configure WLAN security for Guest users:

a. Click **Edit** next to **wlan3**.

b. On the WLANs > Edit screen, make these changes to the default values:

a. Security Policies:

- Layer 2 Security: Choose **WPA2**.
- Layer 3 Security: **None**.

b. RADIUS servers:

- Server 1: Choose the RADIUS server IP Address that you entered in field W22 of the ISR Router Worksheet.

Click **Apply**.

d. Click **Save Configuration** to save your configuration. Click **OK** to confirm.



[Back to Top](#)

Next Step

You have completed this procedure.

If you set up wireless security for a pre-shared key, proceed to [Add a Lightweight Access Point to Your Wireless Network](#).

If you set up wireless security for an external RADIUS server, proceed to [Set Up a RADIUS Server for the Wireless LAN Controller Module](#).

To make further changes to the wireless network, refer to the [Wireless Support Page](#).

To configure other devices in your network, refer to the [Configuration Overview Page](#).

[Back to Top](#)

Troubleshoot the Procedure

This section provides information about common problems that you may encounter. If this information does not solve your problem, contact the [SMB Technical Assistance Center \(SMB TAC\)](#) for assistance.

Problem	Cause(s) and Suggested Solution(s)

You are not able to connect to the WLCM.

- Ensure that you type **https** before the WLCM IP address in your browser.
- Ensure that your PC is connected to the management port that you configured in [Configure Your Router for the Wireless LAN Controller Module](#).
- For further assistance, contact the [SMB Technical Assistance Center \(SMB TAC\)](#).

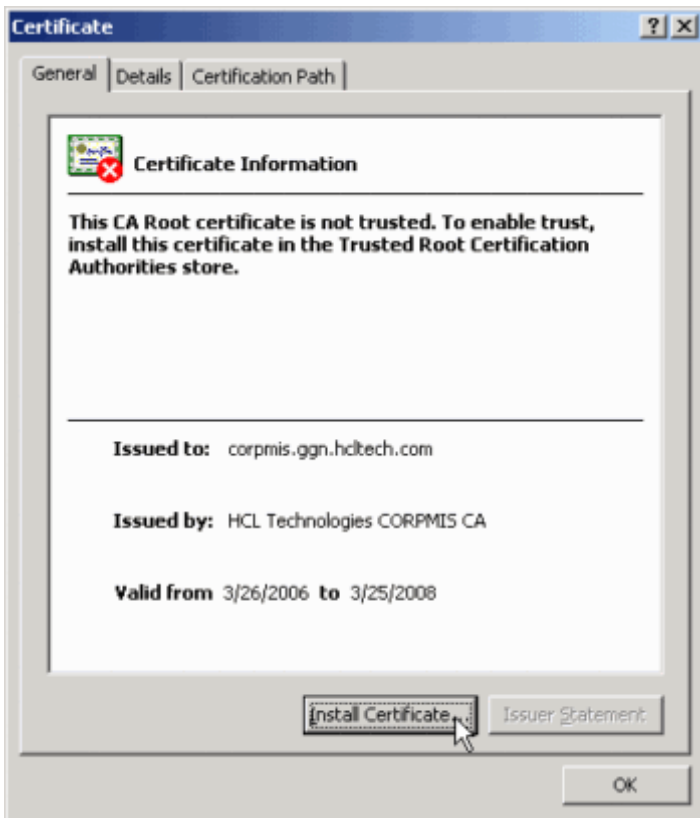
Install the Certificate

If you want to install a certificate from the WLCM on your PC, follow these steps:

1. Click **View Certificate**.



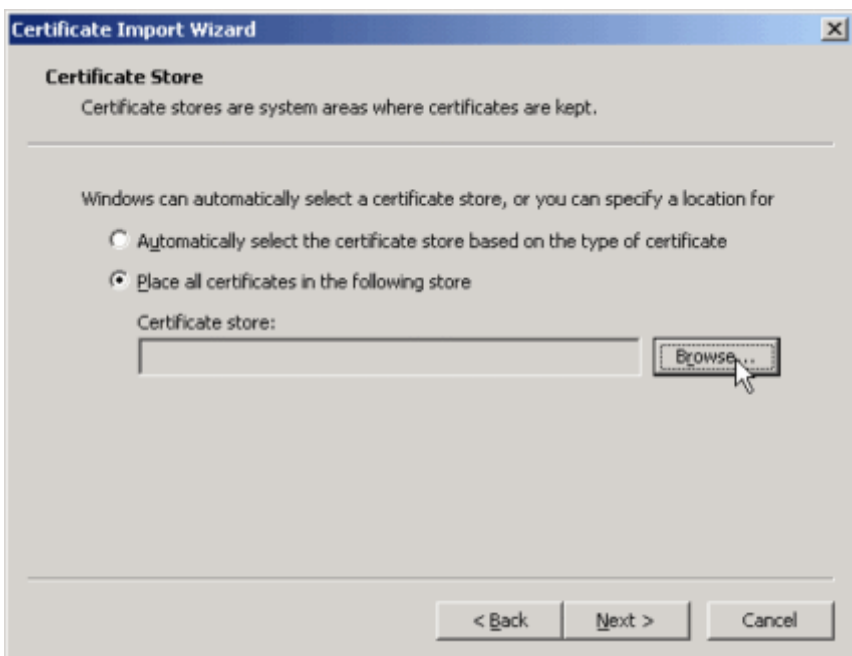
2. On the Certificate screen, click **Install Certificate**.



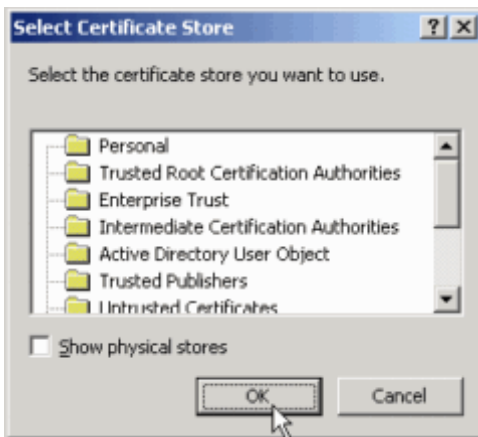
3. On the Certificate Import Wizard screen, click **Next**.



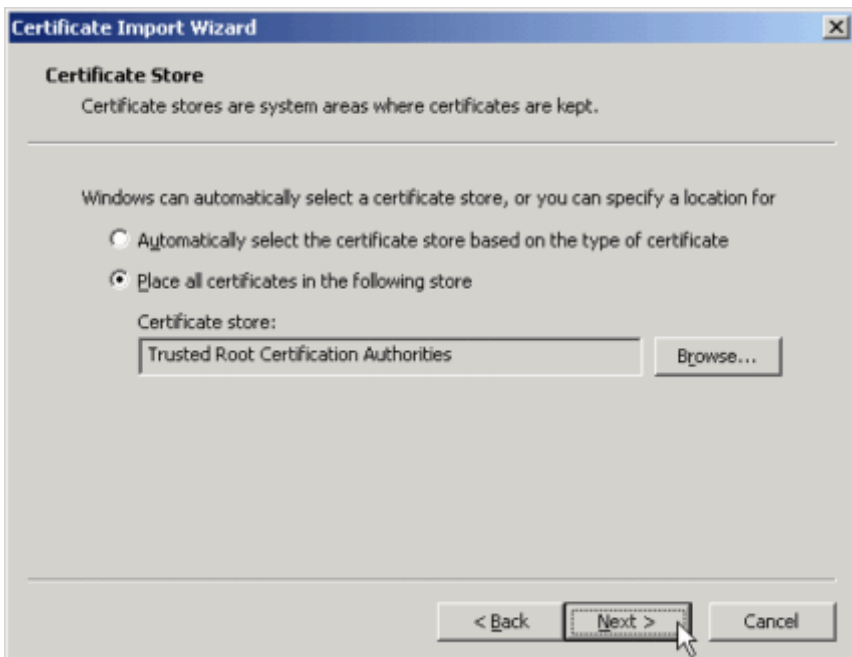
4. On the Certificate Store screen, choose **Place all certificates in the following store** and click **Browse**.



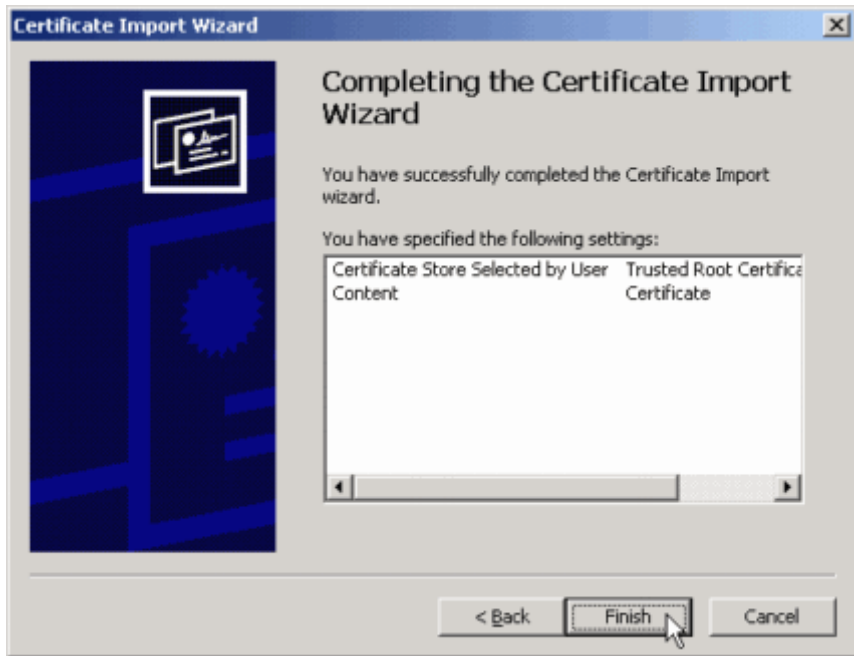
5. On the Select Certificate Store screen, click **Trusted Root Certificate Authorities** and click **OK**.



6. The Certificate Store screen displays **Trusted Root Certification Authorities**. Click **Next**.



7. Click **Finish**.



8. The browser displays a security warning. Click **OK**.
9. The browser displays an alert that indicates that the certificate import was successful. Click **OK**.

[Back to Top](#)

Related Information

- [Site Survey](#)
- [Complete Initial Setup for the Cisco Wireless LAN Controller Module](#)
- [Cable Descriptions](#)
- [Add a Lightweight Access Point to Your Wireless Network](#)
- [Wireless LAN Controller Module IP Addressing Plan](#)
- [Set Up a RADIUS Server for the Wireless LAN Controller Module](#)