

MAC Filters with Wireless LAN Controllers (WLCs) Configuration Example

Document ID: 91901

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

MAC Address Filter (MAC Authentication) on WLCs

Configure Local MAC Authentication on WLCs

- Configure a WLAN and Enable MAC Filtering
- Configure the Local Database on the WLC with Client MAC Addresses

Configure MAC Authentication using a RADIUS Server

- Configure a WLAN and Enable MAC Filtering
- Configure the RADIUS Server with Client MAC Addresses
- Use the CLI to Configure the MAC Filter on WLC
- Verify

Troubleshoot

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document explains how to configure MAC filters with wireless LAN controllers (WLCs) with a configuration example. This document also discusses how to authorize lightweight access points (LAPs) against an AAA server.

Prerequisites

Requirements

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

- Basic knowledge of the configuration of LAPs and Cisco WLCs
- Basic knowledge of Cisco Unified Wireless Security Solutions

Components Used

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

- Cisco 4400 WLC that runs software version 5.2.178.0
- Cisco 1230AG Series LAPs
- 802.11 a/b/g wireless client adapter with firmware 4.4
- Aironet Desktop Utility (ADU) version 4.4

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 Cisco Technical Tips Conventions for more information on document conventions.

MAC Address Filter (MAC Authentication) on WLCs

When you create a MAC address filter on WLCs, users are granted or denied access to the WLAN network based on the MAC address of the client they use.

There are two types of MAC authentication that are supported on WLCs:

- Local MAC authentication
- MAC authentication using a RADIUS server

With local MAC authentication, user MAC addresses are stored in a database on the WLC. When a user tries to access the WLAN that is configured for MAC filtering, the client MAC address is validated against the local database on the WLC, and the client is granted access to the WLAN if the authentication is successful.

By default, the WLC local database supports up to 512 user entries.

The local user database is limited to a maximum of 2048 entries and is set to a default value of 512 entries. The local database stores entries for these items:

- MAC filters (clients)
- AP MIC/SSC (AP authorization list)
- Dynamic Interfaces
- Management users
- Local net users
- Excluded Clients

Together, all of these types of users cannot exceed the configured database size.

In order to increase the local database to 2048, use this command from the CLI:

```
<Cisco Controller>config database size ?  
<count>          Enter the maximum number of entries (512-2048)
```

Alternatively, MAC address authentication can also be performed using a RADIUS server. The only difference is that the users MAC address database is stored in the RADIUS server instead of the WLC. When a user database is stored on a RADIUS server the WLC forwards the MAC address of the client to the RADIUS server for client validation. Then, the RADIUS server validates the MAC address based on the database it has. If the client authentication is successful, the client is granted access to the WLAN. Any RADIUS server which supports MAC address authentication can be used.

Configure Local MAC Authentication on WLCs

Complete these steps in order to configure local MAC authentication on the WLCs:

1. Configure a WLAN and Enable MAC Filtering
2. Configure the Local Database on the WLC with Client MAC Addresses

Note: Before you configure MAC authentication, you must configure the WLC for basic operation and register the LAPs to the WLC. This document assumes that the WLC is already configured for

basic operation and that the LAPs are registered to the WLC. If you are a new user trying to set up the WLC for basic operation with LAPs, refer to Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC).

Note: There is no special configuration needed on the wireless client in order to support MAC authentication.

Configure a WLAN and Enable MAC Filtering

Complete these steps in order to configure a WLAN with MAC filtering:

1. Click **WLANs** from the controller GUI in order to create a WLAN.

The WLANs window appears. This window lists the WLANs configured on the controller.

2. Click **New** in order to configure a new WLAN.

In this example, the WLAN is named *MAC-WLAN* and the WLAN ID is *1*.

WLANs > New

Type	WLAN
Profile Name	MAC-WLAN
SSID	MAC-WLAN
ID	1

3. Click **Apply**.

4. In the WLAN > Edit window, define the parameters specific to the WLAN.

WLANs > Edit

General **Security** **QoS** **Advanced**

Layer 2 **Layer 3** **AAA Servers**

Layer 2 Security **Z** None

MAC Filtering

- a. Under Security Policies > Layer 2 Security, check the **MAC Filtering** check box.

This enables MAC authentication for the WLAN.

b. Under General Policies > Interface Name, select the interface to which the WLAN is mapped.

In this example, the WLAN is mapped to the management interface.

c. Select the other parameters, which depend on the design requirements of the WLAN.

d. Click **Apply**.

WLANs > Edit

The screenshot shows the 'WLANs > Edit' configuration page with the 'Security' tab selected. The configuration is as follows:

Field	Value
Profile Name	MAC-WLAN
Type	WLAN
SSID	MAC-WLAN
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	MAC Filtering
Radio Policy	All
Interface	management
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

(Modifications done under security tab will appear after applying the

The next step is to configure the local database on the WLC with the client MAC addresses.

Refer to VLANs on Wireless LAN Controllers Configuration Example for information on how to configure dynamic interfaces (VLANs) on WLCs.

Configure the Local Database on the WLC with Client MAC Addresses

Complete these steps in order to configure the local database with a client MAC address on the WLC:

1. Click **Security** from the controller GUI, and then click **MAC Filtering** from the left side menu.

The MAC Filtering window appears.

MAC Filtering

RADIUS Compatibility Mode

Cisco ACS

(In the Radius Access Request MAC address.)

MAC Delimiter

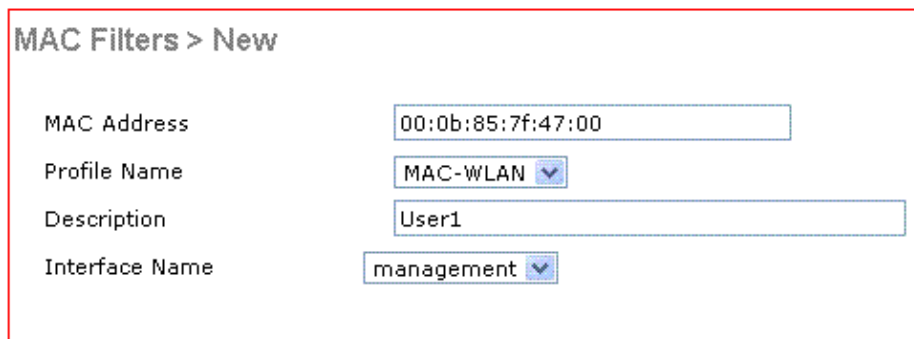
No Delimiter

Local MAC Filters

MAC Address	Profile Name	Interface	Description
-------------	--------------	-----------	-------------

2. Click **New** in order to create a local database MAC address entry on the WLC.
3. In the MAC Filters > New window, enter the MAC address, Profile Name, Description and the Interface Name for the client.

Here is an example:



MAC Filters > New

MAC Address: 00:0b:85:7f:47:00

Profile Name: MAC-WLAN

Description: User1

Interface Name: management

4. Click **Apply**.
5. Repeat steps 2–4 in order to add more clients to the local database.

Now, when clients connect to this WLAN, the WLC validates the clients MAC address against the local database and if the validation is successful, the client is granted access to the network.

Note: In this example, only a MAC address filter without any other Layer 2 Security mechanism was used. Cisco recommends that MAC address authentication should be used along with other Layer 2 or Layer 3 security methods. It is not advisable to use only MAC address authentication to secure your WLAN network because it does not provide a strong security mechanism.

Configure MAC Authentication using a RADIUS Server

Complete these steps in order to configure MAC authentication using a RADIUS server. In this example, the Cisco Secure ACS server is used as the RADIUS server.

1. Configure a WLAN and Enable MAC Filtering
2. Configure the RADIUS Server with Client MAC Addresses

Configure a WLAN and Enable MAC Filtering

Complete these steps in order to configure a WLAN with MAC filtering:

1. Click **WLANs** from the controller GUI in order to create a WLAN.

The WLANs window appears. This window lists the WLANs configured on the controller.

2. Click **New** in order to configure a new WLAN.

In this example, the WLAN is named *MAC-ACS-WLAN* and the WLAN ID is 2.

WLANs > New

Type	WLAN
Profile Name	MAC-ACS-WLAN
SSID	MAC-ACS-WLAN
ID	2

3. Click **Apply**.

4. In the **WLAN > Edit** window, define the parameters specific to the WLAN.

- a. Under **Security Policies > Layer 2 Security**, check the **MAC Filtering** check box.

This enables MAC authentication for the WLAN.

- b. Under **General Policies > Interface Name**, select the interface to which the WLAN is mapped.
- c. Under **RADIUS servers**, select the RADIUS server that will be used for MAC authentication.

WLANs > Edit

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Select AAA servers below to override use of default servers on this WLAN

Radius Servers

	Authentication Servers	Accounting Servers
Server 1	IP:10.77.244.196, Port:1812	None <input checked="" type="checkbox"/> Enabled
Server 2	None	None
Server 3	None	None

Note: Before you can select the RADIUS server from the **WLAN > Edit** window, you should define the RADIUS server in the **Security > Radius Authentication** window and enable the RADIUS server.

RADIUS Authentication Servers

Call Station ID Type

Use AES Key Wrap (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Network User	Management	Server Index	Server Address	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	10.77.244.196	1812	Enabled	Enabled <input checked="" type="checkbox"/>

- d. Select the other parameters, which depend on the design requirements of the WLAN.
- e. Click **Apply**.

WLANs > Edit

General | **Security** | QoS | Advanced

Profile Name: MAC-ACS-WLAN
Type: WLAN
SSID: MAC-ACS-WLAN

Status: Enabled

Security Policies: **MAC Filtering**
(Modifications done under security tab will appear after applying the

Radio Policy: All
Interface: management
Broadcast SSID: Enabled

5. Click **Security > MAC Filtering**.
6. In the MAC Filtering window, choose the type of RADIUS server under RADIUS Compatibility Mode.

This example uses Cisco ACS.

7. From the MAC Delimiter pull down menu, choose the MAC delimiter.

This example uses Colon.

8. Click **Apply**.

MAC Filtering

RADIUS Compatibility Mode (In the Radius Access Request MAC address.)

MAC Delimiter

The next step is to configure the ACS server with the client MAC addresses.

Configure the RADIUS Server with Client MAC Addresses

Complete these steps in order to add a MAC address to the ACS:

1. Define the WLC as an AAA client on the ACS server. Click **Network Configuration** from the ACS GUI.
2. When the Network Configuration window appears, define the name of the WLC, the IP address, the shared secret and the authentication method (RADIUS Cisco Aironet or RADIUS Airespace).

Refer to the documentation from the manufacturer for other non-ACS authentication servers.

The screenshot displays the Cisco Systems Network Configuration GUI. The main window is titled "Add AAA Client" and is divided into two panes: "Edit" and "Help".

Edit Pane:

- AAA Client Hostname:** WirelessLANController
- AAA Client IP Address:** 10.77.244.210
- Key:** cisco
- Authenticate Using:** RADIUS (Cisco Aironet)
- Single Connect TACACS+ AAA Client (Record stop in accounting on failure).
- Log Update/Watchdog Packets from this AAA Client
- Log RADIUS Tunneling Packets from this AAA Client
- Replace RADIUS Port info with Username from this AAA Client

Buttons at the bottom: Submit, Submit + Restart, Cancel, and a Back to Help button.

Help Pane:

- [AAA Client Hostname](#)
- [AAA Client IP Address](#)
- [Key](#)
- [Network Device Group](#)
- [Authenticate Using](#)
- [Single Connect TACACS+ AAA Client](#)
- [Log Update/Watchdog Packets from this AAA Client](#)
- [Log RADIUS Tunneling Packets from this AAA Client](#)
- [Replace RADIUS Port info with Username from this AAA Client](#)

AAA Client Hostname
The AAA Client Hostname is the name assigned to the AAA client.
[\[Back to Top\]](#)

AAA Client IP Address
The AAA Client IP Address is the IP address assigned to the AAA client.
If you want to designate more than one AAA client with a single AAA client entry in Cisco Secure ACS, you can specify the IP address for each AAA client to be represented by this AAA client entry. To separate each IP

Note: The shared secret key that you configure on the WLC and the ACS server must match. The shared secret is case sensitive.

3. From the ACS main menu, click **User Setup**.
4. In the User text box, enter the MAC address in order to add to the user database.

Select

User: 00:40:96:AC:E6:57

Find Add/Edit

List users beginning with letter/number:

A B C D E F G H I J K L M N
 O P Q R S T U V W X Y Z
 0 1 2 3 4 5 6 7 8 9

List All Users

Back to Help

Help

- [User Setup and External User Databases](#)
- [Finding a Specific User in the CiscoSecure User Database](#)
- [Adding a User to the CiscoSecure User Database](#)
- [Listing Usernames that Begin with a Particular Character](#)
- [Listing All Usernames in the CiscoSecure User Database](#)
- [Changing a Username in the CiscoSecure User Database](#)

User Setup enables you to configure individual user information, add users, and delete users in the database.

User Setup and External User Databases

Before Cisco Secure ACS can authenticate users with an external user database:

- You must have the database up and running on the external server. For example, if you are using token card authentication, your token server must be running and properly configured.
- You must have configured the applicable parameters in the External User Databases section.

Note: User Setup configuration overrides Group Setup configuration.

If you rely on the Unknown User Policy in the External User Databases section to create entries in the

Note: The MAC address must be exactly as it is sent by the WLC for both the username and the password. If authentication fails, check the failed attempts log to see how the MAC is reported by the WLC. Do not cut and paste the MAC address, as this can introduce phantom characters.

5. In the User Setup window, enter the MAC address in the Secure-PAP password text box.

Edit

User: 00:40:96:AC:E6:57 (New User)

Account Disabled

User Setup

Password Authentication: CiscoSecure Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password

Confirm

Password

Separate (CHAP/MS-CHAP/ARAP)

Password

Confirm

Password

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:

Help

- [Account Disabled](#)
- [Deleting a Username](#)
- [Supplementary User Info](#)
- [Password Authentication](#)
- [Group to which the user is assigned](#)
- [Callback](#)
- [Client IP Address Assignment](#)
- [Advanced Settings](#)
- [Network Access Restrictions](#)
- [Max Sessions](#)
- [Usage Quotas](#)
- [Account Disable](#)
- [Downloadable ACLs](#)
- [Advanced TACACS+ Settings](#)
- [TACACS+ Enable Control](#)
- [TACACS+ Enable Password](#)
- [TACACS+ Outbound Password](#)
- [TACACS+ Shell Command Authorization](#)
- [Command Authorization for Network Device Management Applications](#)
- [TACACS+ Unknown Services](#)
- [IETF RADIUS Attributes](#)
- [RADIUS Vendor-Specific Attributes](#)

Account Disabled Status

Select the Account Disabled check box to disable this

Note: The MAC address must be exactly as it is sent by the WLC for both the username and the password. If authentication fails, check the failed attempts log to see how the MAC is reported by the AP. Do not cut and paste the MAC address, as this can introduce phantom characters.

6. Click **Submit**.
7. Repeat steps 2–5 in order to add more users to the ACS database.

Now, when clients connect to this WLAN, the WLC passes the credentials to the ACS server. The ACS server validates the credentials against the ACS database. If the client MAC address is present in the database, the ACS RADIUS server returns an authentication success to the WLC and the client will be granted access to the WLAN.

Use the CLI to Configure the MAC Filter on WLC

This document previously discussed how to use the WLC GUI to configure MAC filters. You can also use the CLI in order to configure MAC filters on the WLC. You can use these commands in order to configure the MAC filter on WLC:

- **config macfilter add** command:

The **config macfilter add** command lets you add a macfilter, interface, description, and so forth.

Use the **config macfilter add** command in order to create a MAC filter entry on the Cisco Wireless LAN controller. Use this command in order to add a client locally to a wireless LAN on the Cisco Wireless LAN controller. This filter bypasses the RADIUS authentication process.

```
config macfilter add MAC_address wlan_id [interface_name]
[description] [IP address]
```

Example:

Enter a static MAC-to-IP address mapping. This can be done to support a *passive client*, that is, one that does not use DHCP and does not transmit unsolicited IP packets.

```
>config macfilter add 00:E0:77:31:A3:55 1 lab02 "labconnect" 10.92.125.51
```

- **config macfilter ip-address** command

The **config macfilter ip-address** command lets you map an existing MAC-filter to an IP address. Use this command in order to configure an IP address into the local MAC filter database:

```
config macfilter ip-address
MAC_address IP address
```

Example:

```
>config macfilter add 00:E0:77:31:A3:55 1 lab02 "labconnect" 10.92.125.51
```

Verify

Use these commands in order to verify if the MAC filter is configured correctly:

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

- **show macfilter summary** Displays a summary of all MAC filter entries.
- **show macfilter detail <client MAC Address>** Detailed display of a MAC filter entry.

Here is an example of the **show macfilter summary** command:

```
(Cisco Controller) >show macfilter summary

MAC Filter RADIUS Compatibility mode..... Cisco ACS
MAC Filter Delimiter..... None
```

Local Mac Filter Table

MAC Address	WLAN Id	Description
00:40:96:ac:e6:57	1	Guest

```
(Cisco Controller) >show macfilter detail 00:40:96:ac:e6:57
```

Here is an example of the **show macfilter detail** command:

```
(Cisco Controller) >show macfilter detail 00:40:96:ac:e6:57

MAC Address..... 00:40:96:ac:e6:57
WLAN Identifier..... 1
Interface Name..... mac-client
Description..... Guest
```

Troubleshoot

You can use these commands to troubleshoot your configuration:

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

- **debug aaa all enable** Provides debugging of all AAA messages.
- **debug mac addr <Client-MAC-address xx:xx:xx:xx:xx:xx>** In order to configure MAC debugging, use the **debug mac** command.

Here is an example of the **debug aaa all enable** command:

```
Wed May 23 11:13:55 2007: Looking up local blacklist 004096ace657
Wed May 23 11:13:55 2007: Looking up local blacklist 004096ace657
Wed May 23 11:13:55 2007: User 004096ace657 authenticated
Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57 Returning AAA Error 'Success' (0)
for mobile 00:40:96:ac:e6:57
Wed May 23 11:13:55 2007: AuthorizationResponse: 0xbadff97c
Wed May 23 11:13:55 2007: structureSize.....76
Wed May 23 11:13:55 2007: resultCode.....0
Wed May 23 11:13:55 2007: protocolUsed.....0x00000008
Wed May 23 11:13:55 2007: proxyState.....
00:40:96:AC:E6:57-00:00
Wed May 23 11:13:55 2007: Packet contains 2 AVPs:
Wed May 23 11:13:55 2007: AVP[01] Service-Type.....
0x0000000a (10) (4 bytes)
Wed May 23 11:13:55 2007: AVP[02] Airespace / Interface-Name.....
staff-vlan (10 bytes)
Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57 processing avps[0]: attribute 6
Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57 processing avps[1]: attribute 5
Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57 Applying new AAA override for
station 00:40:96:ac:e6:57
Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57 Override values for station 00:40:96:ac:e6:57
source: 2, valid bits: 0x200 qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff,
sessionTimeout: -1 dataAvgC: -1, rTAvgC: -1, dataBurstC:
-1, rTimeBurstC: -1 vlanIfName: 'mac-client'
```

When a wireless client is not present in the MAC address database on the WLC (local database) or on the RADIUS server tries to associate to the WLAN, that client will be excluded. Here is an example of the **debug aaa all enable** command for an unsuccessful MAC authentication:

```
Wed May 23 11:05:06 2007: Unable to find requested user entry for 004096ace657
Wed May 23 11:05:06 2007: AuthenticationRequest: 0xa620e50
Wed May 23 11:05:06 2007: Callback.....0x807e724
Wed May 23 11:05:06 2007: protocolType.....0x00000001
Wed May 23 11:05:06 2007: proxyState.....
00:40:96:AC:E6:57-00:00
Wed May 23 11:05:06 2007: Packet contains 14 AVPs (not shown)
Wed May 23 11:05:06 2007: 00:40:96:ac:e6:57 Returning AAA Error 'No Server' (-7)
for mobile 00:40:96:ac:e6:57
Wed May 23 11:05:06 2007: AuthorizationResponse: 0xbadff7e4
Wed May 23 11:05:06 2007: structureSize.....28
Wed May 23 11:05:06 2007: resultCode.....-7
Wed May 23 11:05:06 2007: protocolUsed.....0xffffffff
Wed May 23 11:05:06 2007: proxyState.....
00:40:96:AC:E6:57-00:00
Wed May 23 11:05:06 2007: Packet contains 0 AVPs:
```

Wireless Clients that Try to Authenticate by MAC Address are Rejected; Failed Authentication Report Shows Internal Errors

When you use ACS 4.1 that runs on a Microsoft Windows 2003 Enterprise server, clients that try to authenticate by the MAC address are rejected. This occurs when an AAA client sends the Service-Type=10 attribute value to the AAA server. This is because of Cisco bug ID CSCsh62641 (registered customers only). AAA clients affected by this bug include WLCs and switches that use MAC Authentication Bypass.

The workarounds are:

- Downgrade to ACS 4.0.
- or
- Add the MAC addresses to be authenticated to a Network Access Protection (NAP) under the internal ACS DB MAC address table.

Not able to add a MAC filter using the WLC GUI

This can happen because of the Cisco bug ID CSCsj98722 (registered customers only). The bug is fixed in 4.2 release of code. If you are running versions earlier than 4.2, you can upgrade the firmware to 4.2 or use these two workarounds for this issue.

- Use the CLI in order to configure the MAC Filter with this command:

```
config macfilter add <MAC address> <WLAN ID#> <Interface>
```

- From the Web GUI of the controller, choose **Any WLAN** under the Security tab and enter the MAC address to be filtered.

Silent client not placed in run state

If DHCP required is not configured on the controller, the APs learn the IP address of wireless clients when the wireless clients send out the first IP packet or ARP. If the wireless clients are passive devices, for example, devices that do not initiate a communication, then the APs fails to learn the IP address of the wireless devices. As a result, the controller waits ten seconds for the client to send an IP packet. If there is no response from the packet from the client, then the controller drops any packets to the passive wireless clients. This issue is documented in Cisco bug ID CSCsq46427 (registered customers only)

As a recommended workaround for passive devices like printers, wireless PLC pumps and so forth, you need to set the WLAN for MAC filtering and have AAA override checked in order to allow these devices to be connected.

A MAC address filter can be created on the controller that maps the MAC address of the wireless device to an IP address.

Note: This requires MAC address filtering to be enabled on the WLAN configuration for Layer 2 Security. It also requires Allow AAA Override to be enabled in the advance settings of the WLAN configuration.

From the CLI, enter this command in order to create the MAC address filter:

```
config macfilter add <STA MAC addr> <WLAN id> [interface name] [description] [STA IP address]
```

Here is an example:

```
config macfilter add 00:01:02:03:04:05 1 my_interface "Zebra Printer"  
192.168.1.1
```

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Wireless
Wireless – Mobility: WLAN Radio Standards
Wireless – Mobility: Security and Network Management
Wireless – Mobility: Getting Started with Wireless
Wireless – Mobility: General

Related Information

- [ACLs on Wireless LAN Controller Configuration Example](#)
- [Authentication on Wireless LAN Controllers Configuration Examples](#)
- [VLANs on Wireless LAN Controllers Configuration Example](#)
- [Cisco Wireless LAN Controller Configuration Guide, Release 4.1](#)
- [Wireless Support Page](#)
- [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: Mar 13, 2009

Document ID: 91901
