

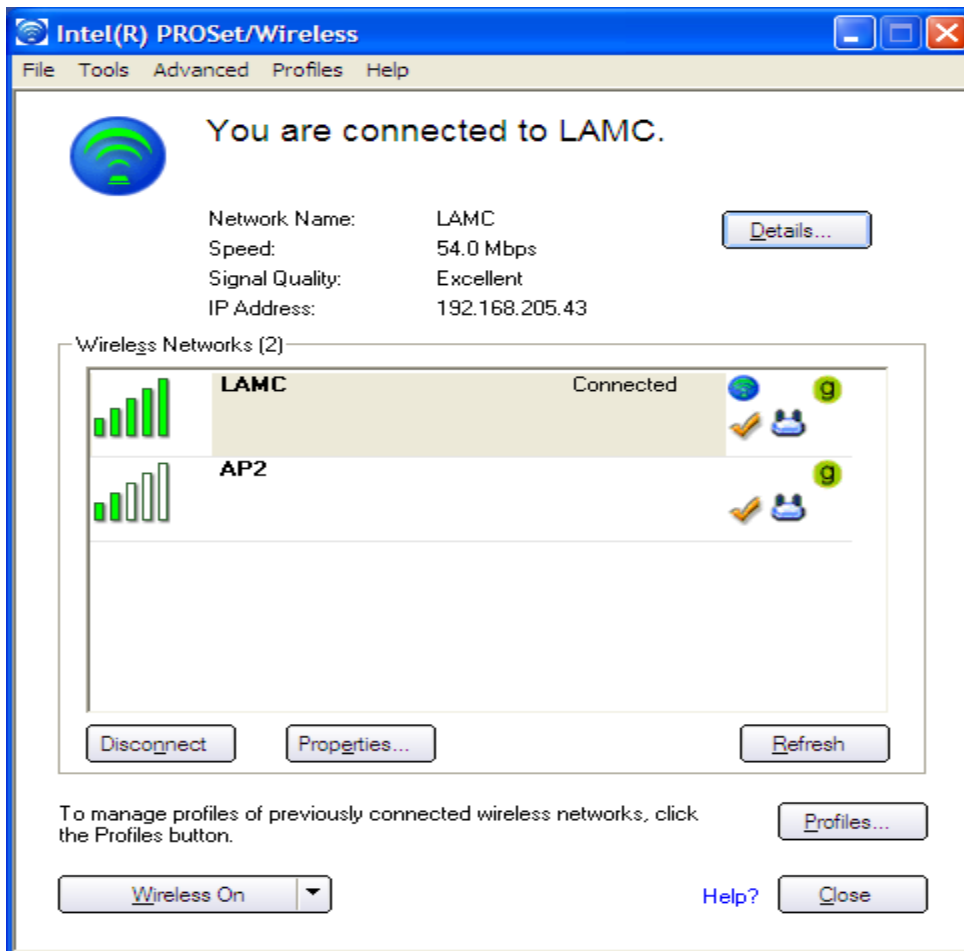
Los Angeles Mission College Wireless Network Authentication

All current students, faculty and staff are able to access to the LAMC wireless network.

To connect your laptop computer to the LAMC wireless network, you will need the complete the following steps:

Step 1: Get Connected!

Access the wireless settings on your laptop. (These settings will vary in appearance by type of laptop and/or operating system and may be different from the example shown below.) Choose LAMC and click on the **Connect** button.



Step 2: Security Alert Screen

Click on your favorite Internet browser. You will then be prompted with a Security Alert. Click on the **Yes** button to proceed.

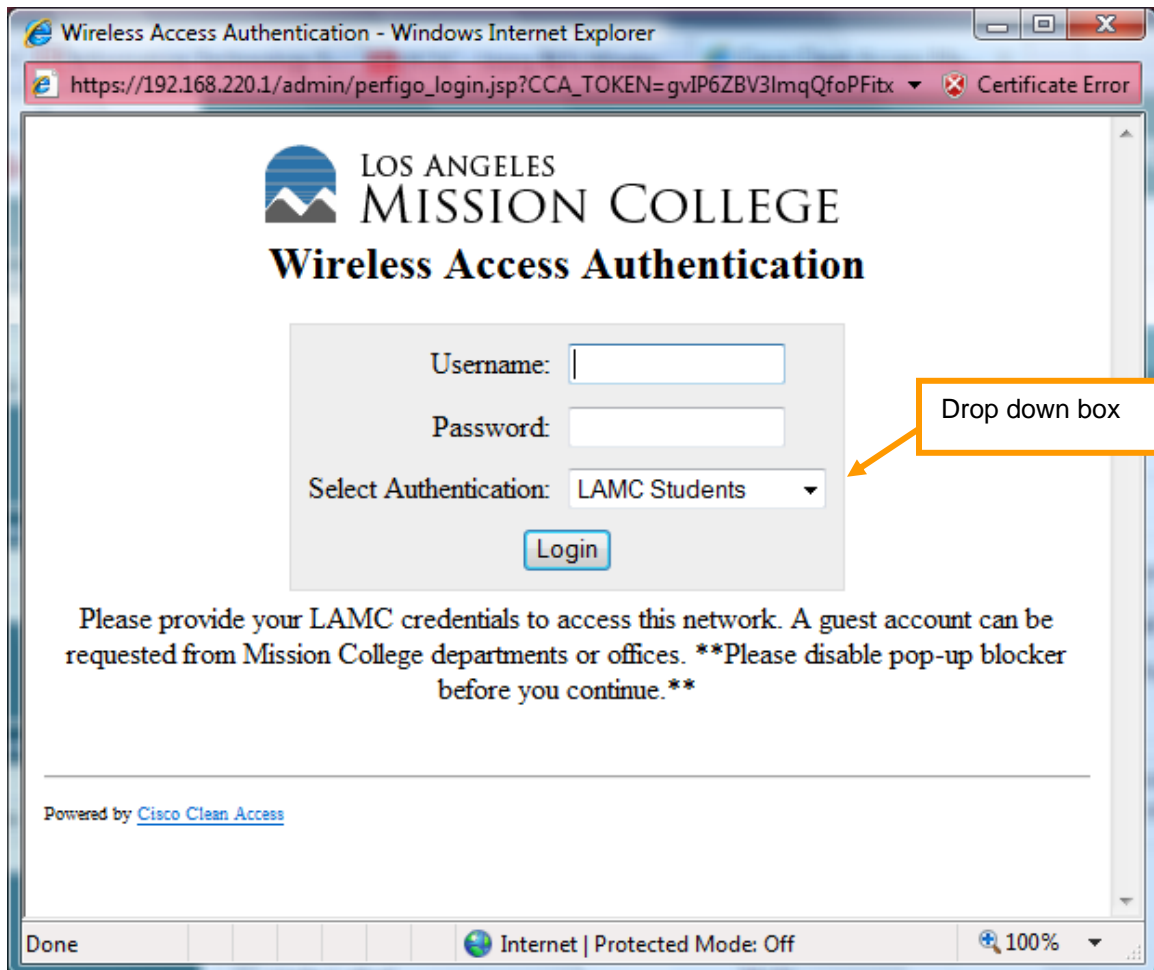


Step 3: Wireless Access Authentication screen.

If you are a **current student**, your user name is your student ID number and your password is your PIN number. Select **LAMC Students** from the Authentication drop down box.

If you are a **faculty or staff member**, your user name and password are the same as those used for your Outlook E-mail account. Select **LAMC Staff/Faculty** from the Authentication drop down box.

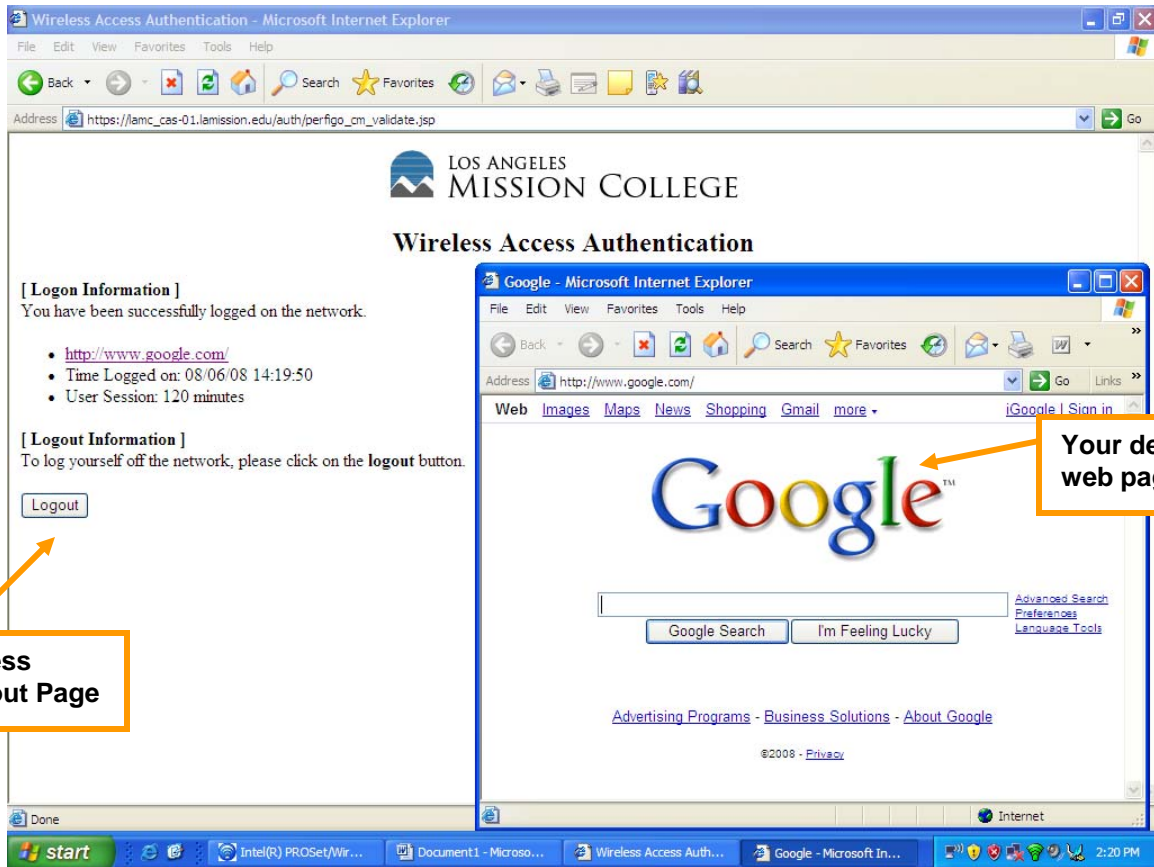
If you are a visitor and wish to access to the campus wireless network, the college IT department can issue a guest account. Requests for a guest account need to be made to the IT department through a sponsoring campus department or office. This request can be made through the IT Work Order System (http://support.lamission.edu/Tamis/default_IT.asp). Select **LAMC Guest** from the Authentication drop down box. Note that guest account credentials are only valid on the requested time/date.



Step 4: You are connected!


After successful login, your default web page will display along with LAMC Wireless Access Logout page.

Click on the logout button to disconnect your session. Your Internet wireless session will expire after 2 hours (120 minutes). To reconnect, repeat the authentication process beginning with Step 2.



File Edit View Favorites Tools Help

Home Page Safety Tools ?



Cisco Clean Access Standard Manager Version 4.1.3.1

Monitoring > Summary

Device Management

- CCA Servers
- Filters
- Clean Access

Switch Management

- Profiles
- Devices

User Management

- User Roles
- Auth Servers
- Local Users

Current Windows Clean Access Agent Version:	4.1.3.1	
Current Windows Clean Access Agent Patch Version:	4.1.6.0	
Current Macintosh Clean Access Agent Version:	4.1.3.1	
Current Cisco NAC Web Agent Version:	4.1.6.0	
Clean Access Servers configured:	2	
Global MAC addresses configured:	0 addresses / 0 ranges	
Global subnets configured:	0	
Online users:	<i>(In-Band / Out-of-Band)</i>	
Total:	619	0
Unique online users' names:	541	0
Unique online users' MAC addresses:	611	0
Online users in Unauthenticated Role:	0	0
Online users in Temporary Role:	0	0
Online users in Quarantine Role:	0	0
Online users in Students:	549	0
Online users in Staff:	70	0
Online users in Guest:	0	0

Management of Access points

Browser: https://192.168.200.230/screens/frar Certificate error LAMC-WLC3

Navigation: Save Configuration | Ping | Logout | Refresh

Menu: MONITOR | WLANs | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK

Monitor

802.11a/n Radios

Entries 1 - 25 of 94

Current Filter: None [\[Change Filter\]](#) [\[Clear Filter\]](#)

AP Name	Radio Slot#	Base Radio MAC	Sub Band	Operational Status	Load Profile	Radio Role	Noise Profile	Interference Profile	Coverage Profile	CleanAir Admin Status	Clean Oper Status
IA-1.WAP1	1	00:1d:a2:87:a1:00	-	UP	Passed	NA	Passed	Passed	Passed	NA	NA
IA-1.WAP7	1	00:1d:a2:87:f1:e0	-	UP	Passed	NA	Passed	Passed	Passed	NA	NA
LRC-1.WAP1	1	00:1d:a2:87:94:40	-	UP	Passed	NA	Passed	Passed	Passed	NA	NA
LRC-0.WAP1	1	00:1d:a2:88:27:c0	-	UP	Passed	NA	Passed	Passed	Passed	NA	NA
CC-2.WAP4	1	00:1d:a2:87:9a:10	-	UP	Passed	NA	Passed	Passed	Passed	NA	NA
PLANT-1.WAP1	1	00:23:ab:26:36:20	-	UP	Passed	NA	Passed	Passed	Passed	NA	NA
Sheriff-1.WAP1	1	00:1d:a2:87:96:e0	-	UP	Passed	NA	Passed	Passed	Passed	NA	NA
IA-2.WAP3	1	00:1d:a2:87:9b:30	-	UP	Passed	NA	Passed	Passed	Passed	NA	NA
CDC-1.WAP1	1	00:21:d8:92:6e:e0	-	UP	Passed	NA	Passed	Passed	Passed	NA	NA
IA-1.WAP3	1	00:1d:a2:87:7c:a0	-	UP	Passed	NA	Passed	Passed	Passed	NA	NA
CSB-2.WAP3	1	00:1d:a2:87:8b:20	-	UP	Passed	NA	Passed	Passed	Passed	NA	NA
PE-1.WAP5	1	58:bc:27:0f:6b:b0	-	UP	Passed	NA	Passed	Passed	Passed	NA	NA
FCSB-2.WAP1	1	58:bc:27:0f:9c:00	-	UP	Passed	NA	Passed	Passed	Passed	NA	NA
LRC-2.WAP2	1	00:1d:a2:88:23:e0	-	UP	Passed	NA	Passed	Passed	Passed	NA	NA
LRC-2.WAP1	1	00:1d:a2:88:22:20	-	UP	Passed	NA	Passed	Passed	Passed	NA	NA
CC-1.WAP3	1	00:1d:a2:87:76:20	-	UP	Passed	NA	Passed	Passed	Passed	NA	NA
LRC-1.WAP3	1	00:1d:a2:87:98:d0	-	UP	Passed	NA	Passed	Passed	Passed	NA	NA
CC-1.WAP2	1	00:1d:a2:87:93:20	-	UP	Passed	NA	Passed	Passed	Passed	NA	NA
FCSB-1.WAP1	1	58:bc:27:12:05:c0	-	UP	Passed	NA	Passed	Passed	Passed	NA	NA
CSB-1.WAP3	1	00:1d:a2:87:93:30	-	UP	Passed	NA	Passed	Passed	Passed	NA	NA
FCSB-2.WAP3	1	58:bc:27:0f:70:00	-	UP	Passed	NA	Passed	Passed	Passed	NA	NA
IA-1.WAP8	1	00:1d:a2:87:e7:70	-	UP	Passed	NA	Passed	Passed	Passed	NA	NA
CDC-2.WAP2	1	00:21:d8:c0:ee:00	-	UP	Passed	NA	Passed	Passed	Passed	NA	NA
CS-1.WAP1	1	00:1d:a2:88:25:a0	-	UP	Passed	NA	Passed	Passed	Passed	NA	NA
CS-1.WAP2	1	00:1e:13:06:06:90	-	UP	Passed	NA	Passed	Passed	Passed	NA	NA

100%

Management of Wireless Contrllers

Browser: <https://192.168.200.230/s> | Tab: LAMC-WLC3

Navigation: Save Configuration | Ping | Logout | Refresh


Menu: MONITOR | WLANs | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK

Monitor

- Summary
- Access Points
- Cisco CleanAir
- Statistics
- CDP
- Rogues
- Clients
- Multicast
- Applications

Summary

100 Access Points Supported



Controller Summary		Rogue Summary	
Management IP Address	192.168.200.230	Active Rogue APs	56 Detail
Service Port IP Address	0.0.0.0	Active Rogue Clients	9 Detail
Software Version	7.4.110.0	Adhoc Rogues	0 Detail
Field Recovery Image Version	6.0.182.0	Rogues on Wired Network	0
System Name	LAMC-WLC3		
Up Time	27 days, 3 hours, 21 minutes		
System Time	Wed Jan 6 14:30:53 2016		
Redundancy Mode	Disabled		
Internal Temperature	+40 C		
802.11a Network State	Enabled		
802.11b/g Network State	Enabled		
Local Mobility Group	LAMC-MOB		
CPU(s) Usage	0%		
Individual CPU Usage	0%/1%, 0%/1%, 0%/1%, 8%/3%, 0%/1%, 0%/1%, 0%/1%, 0%/1%, 0%/0%, 0%/0%, 0%/1%, 0%/0%		
Memory Usage	49%		

Top WLANs			
Profile Name	# of Clients		
LAMC-Wireless	213	Detail	
LAMC-WLP	12	Detail	

Most Recent Traps

- Coverage hole pre alarm for client[1] fc:db:b3:01:e4:ea on 802.11b/g interface of AP 00:1d:a2:87:83:
- Coverage hole cleared for Base Radio MAC: 00:1d:a2:87:8e:20 and slotNo: 0
- Coverage Hole Detected for AP IA-1.WAP5 whose Base Radio MAC is 00:1d:a2:87:8e:20. Number of Fa
- Coverage hole pre alarm for client[1] 9c:fc:01:5e:07:90 on 802.11b/g interface of AP 00:1d:a2:87:8e:
- Coverage hole pre alarm for client[1] 7c:01:91:96:85:a7 on 802.11b/g interface of AP 00:1d:a2:87:8e:

Access Point Summary

	Total	Up	Down	
802.11a/n Radios	94	94	0	Detail
802.11b/g/n Radios	94	94	0	Detail
Dual-Band Radios	0	0	0	Detail
All APs	94	94	0	Detail

Client Summary

Current Clients	225	Detail
-----------------	-----	------------------------

Footer: <https://192.168.200.230/screens/frameMonitor.html> | 100%