Switch configuration

```
vlan 14
name wlc
vlan 50
name untrusted
vlan 51
name guest
vlan 53
name nas
vlan 54
name nam

int vlan 14
ip add 10.2.14.1 255.255.255.0
int vlan 51
ip add 10.2.51.1 255.255.255.0
int vlan 53
ip add 10.2.53.1 255.255.255.0
int vlan 54
ip add 10.2.54.1 255.255.255.0

int g0/1
connected to NAM
switchport mode access
switchport access vlan 54
spanning-tree portfast

int g0/2
connected to wlc
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 14,51-54

int g0/3
connected to NAS untrusted
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 50

int g0/4
connected to NAS trusted
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 14,51,54

int g0/6
connected to ap
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 14
```

switchport allowed vlan 14,50-54

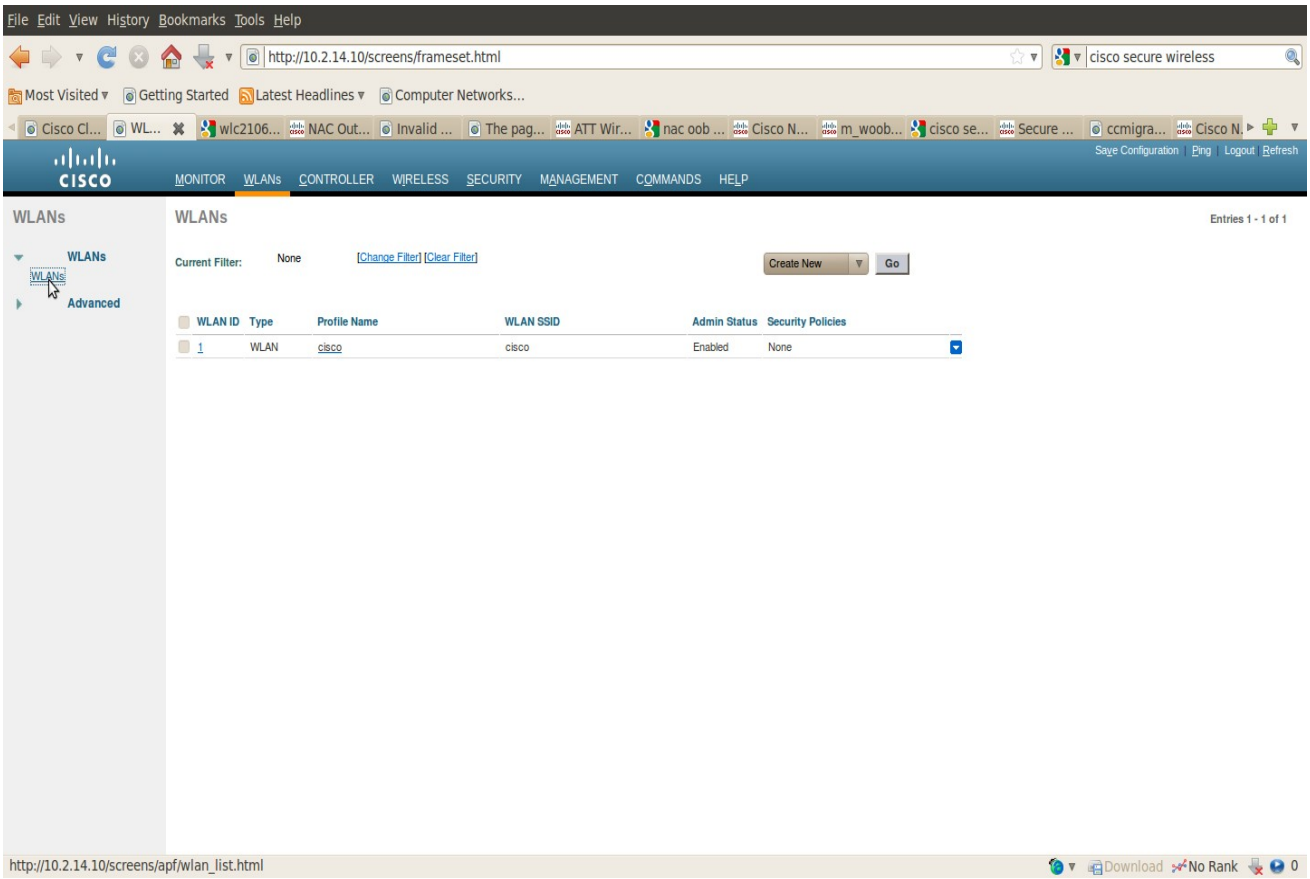
ip dhcp excluded-addresses 10.2.14.1
ip dhcp excluded-addresses 10.2.53.1
ip dhcp excluded-addresses 10.2.54.1
ip dhcp excluded-addresses 10.2.51.1
ip dhcp excluded-addresses 10.2.51.2
ip dhcp excluded-addresses 10.2.51.254

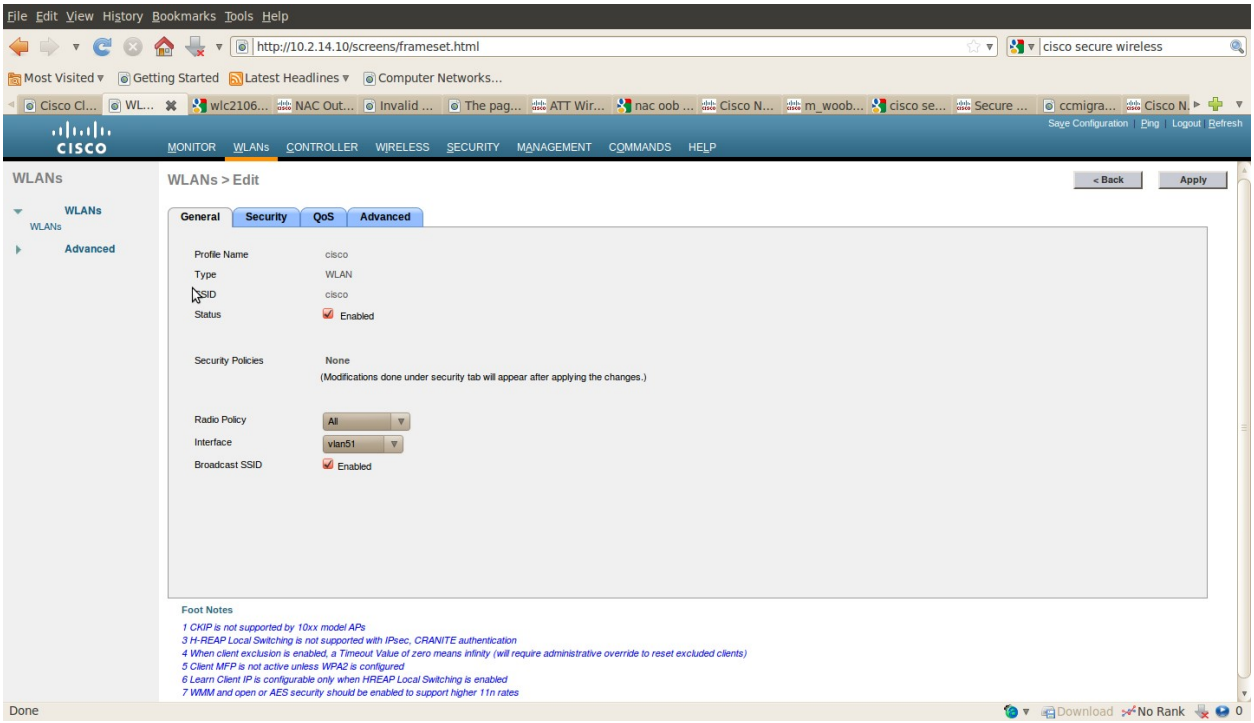
ip dhcp pool vlan51
network 10.2.51.0/24
default-router 10.2.51.1

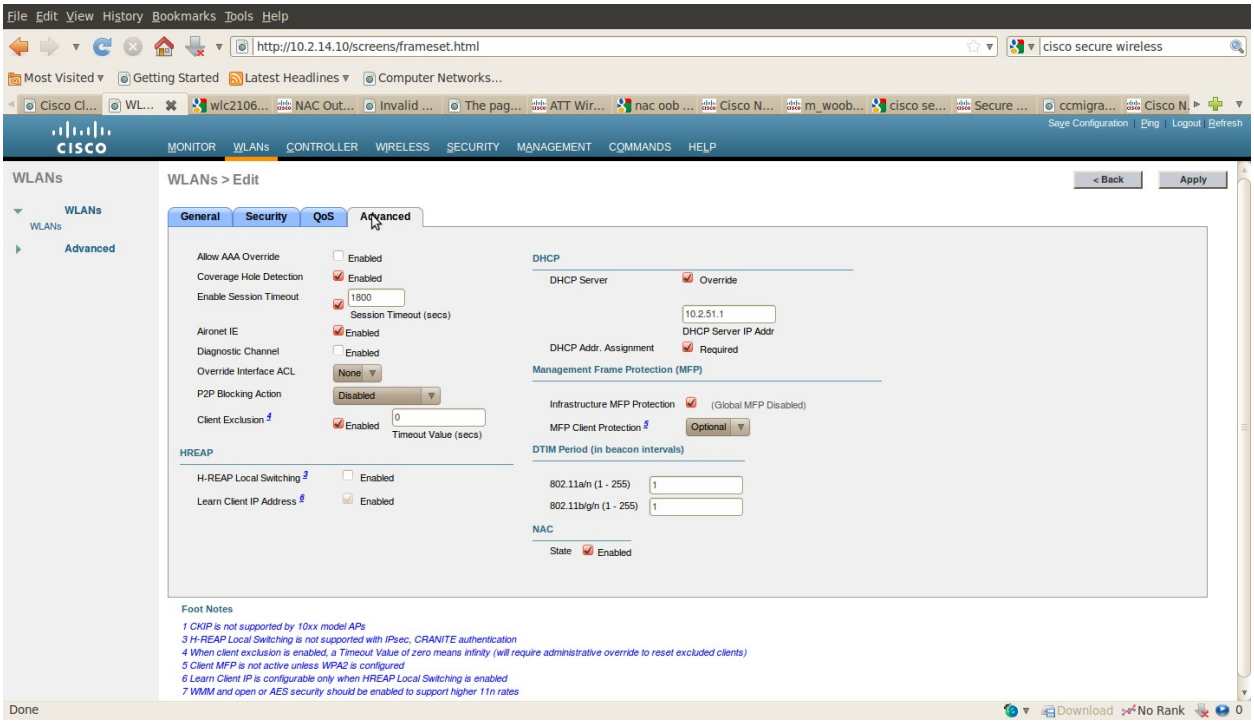
ip dhcp pool vlan14
network 10.2.14.0/24
default-router 10.2.14.1

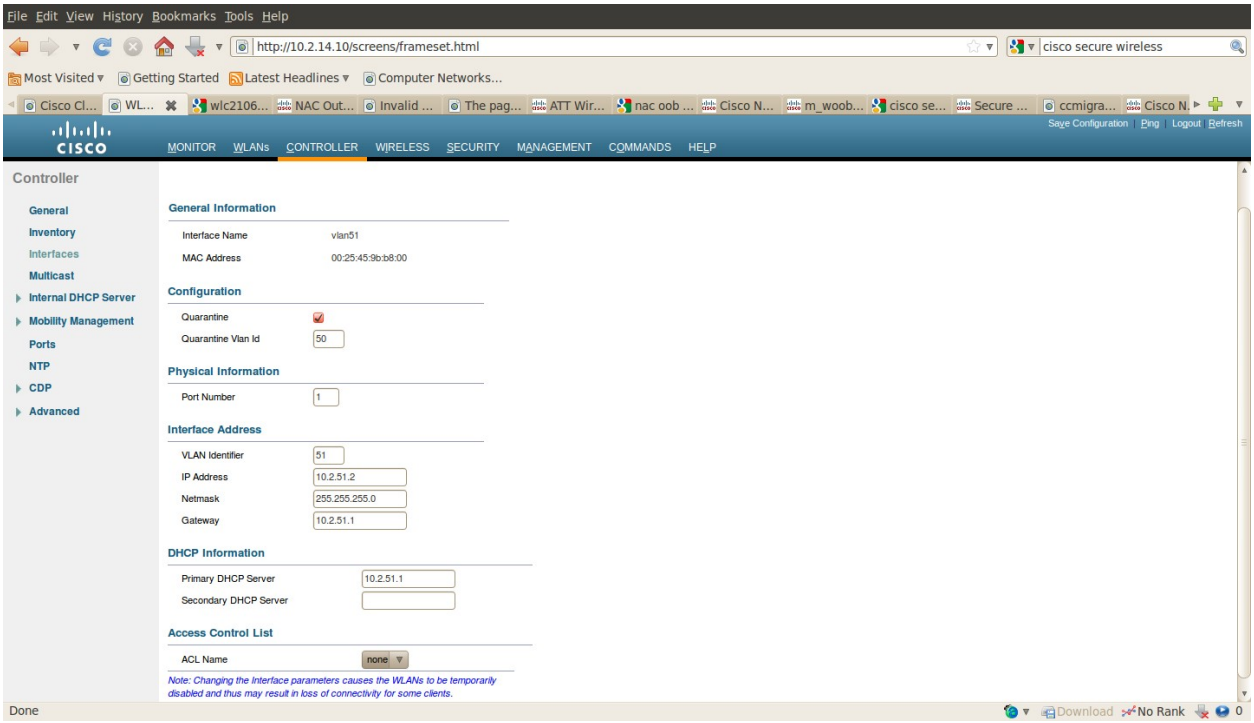
ip routing

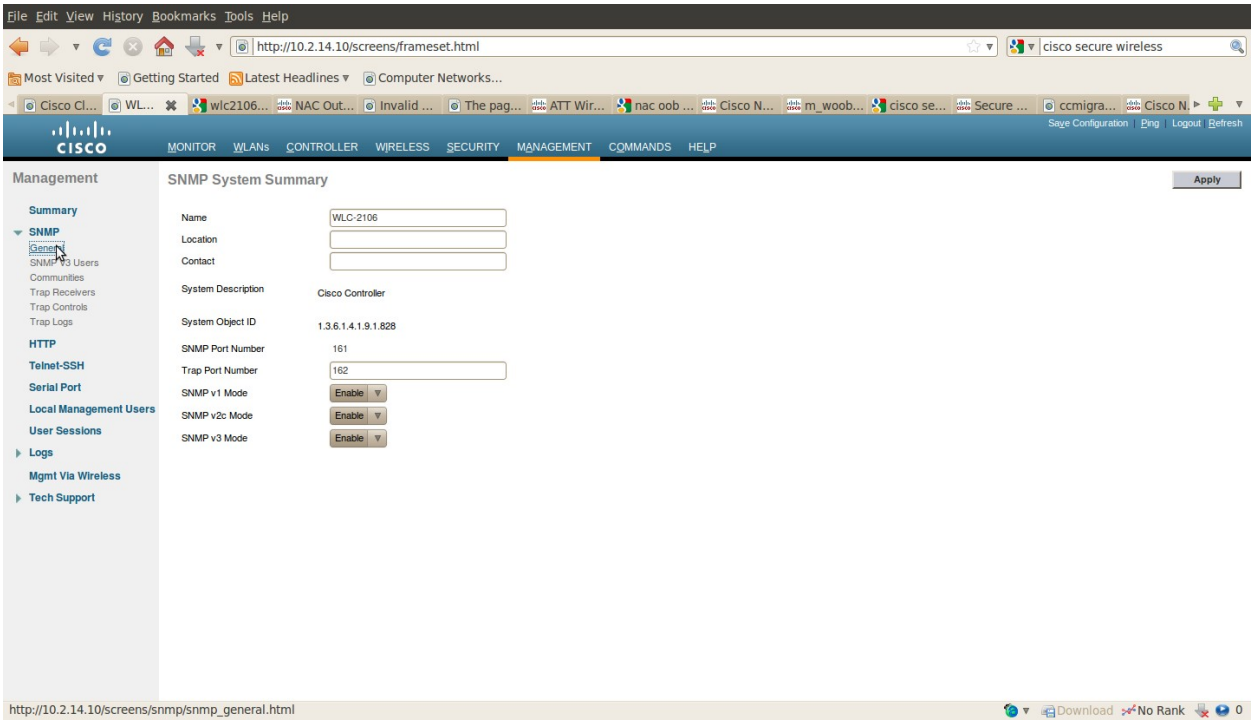
wlc configuration

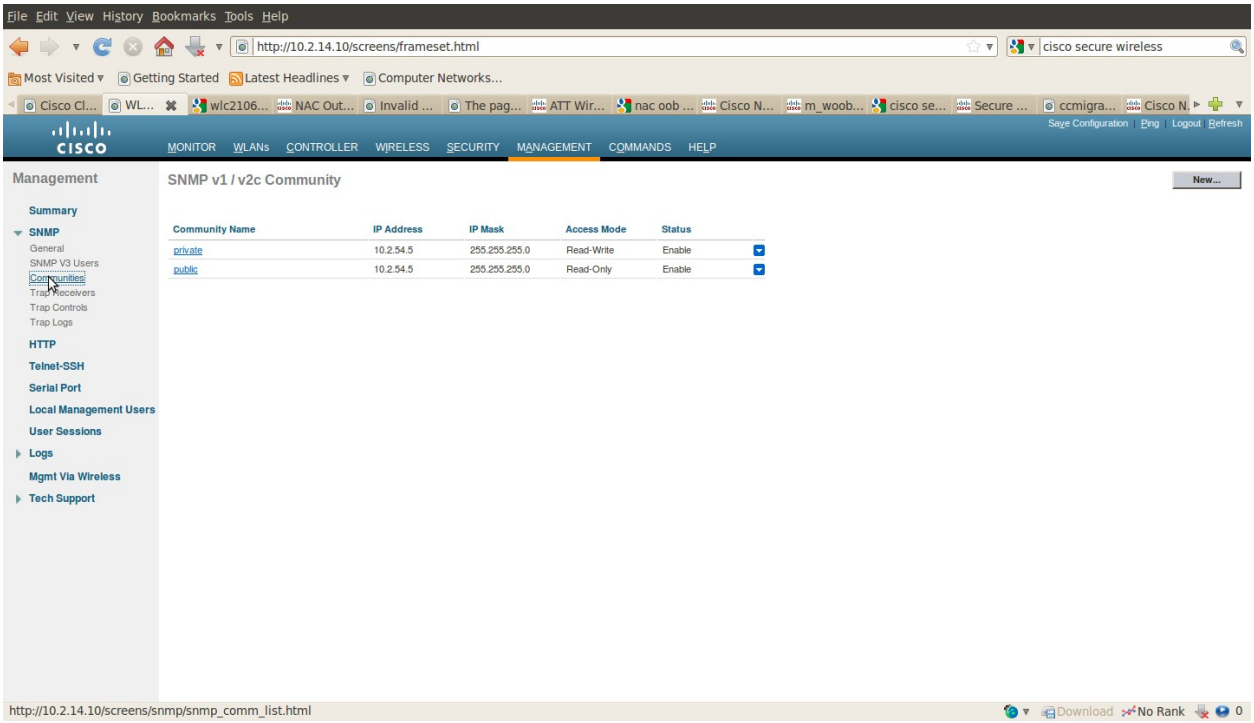


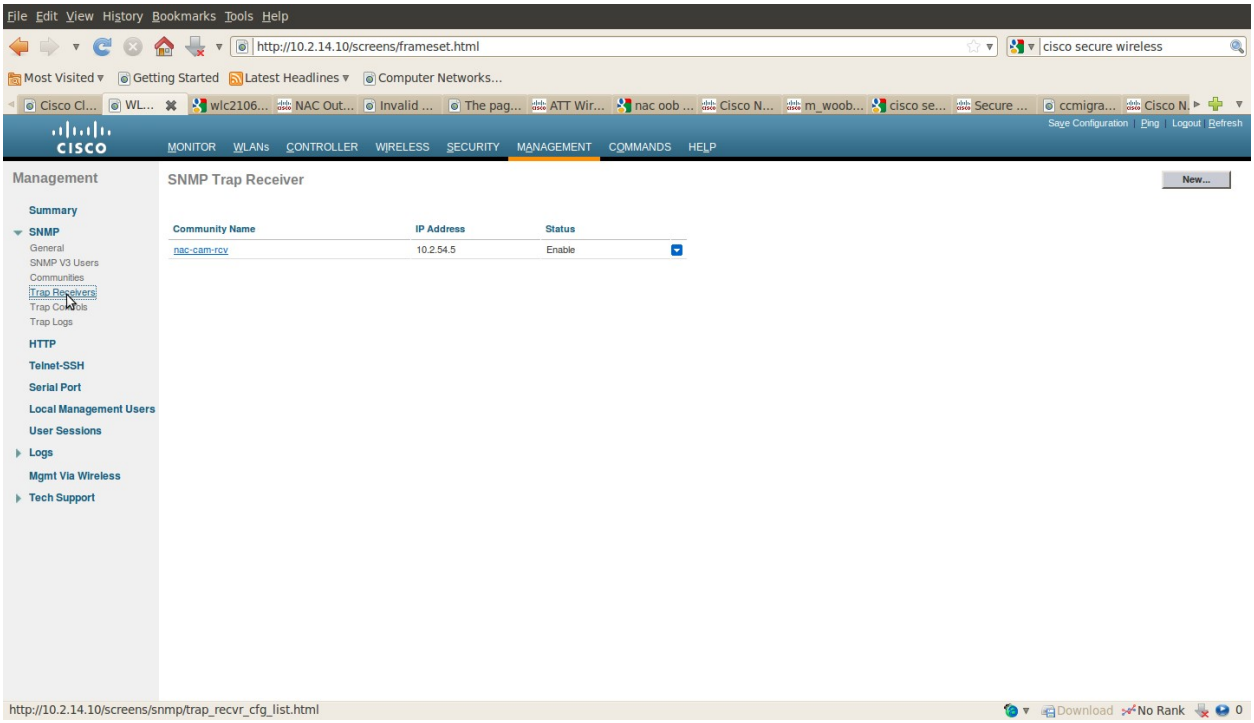

File Edit View History Bookmarks Tools Help
http://10.2.14.10/screens/frameset.html
cisco secure wireless
Most Visited
Getting Started
Latest Headlines
Computer Networks...
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
WLANs > Edit
< Back
Apply
General Security QoS Advanced
Profile Name cisco
Type WLAN
SSID cisco
Status Enabled
Security Policies None
(Modifications done under security tab will appear after applying the changes.)
Radio Policy All
Interface vlan51
Broadcast SSID Enabled
Foot Notes
1 CKIP is not supported by 10xx model APs
3 H-REAP Local Switching is not supported with IPsec, CRANITE authentication
4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
5 Client MFP is not active unless WPA2 is configured
6 Learn Client IP is configurable only when HREAP Local Switching is enabled
7 WMM and open or AES security should be enabled to support higher 11n rates
Done
Download
No Rank
0


File Edit View History Bookmarks Tools Help
http://10.2.14.10/screens/frameset.html
cisco secure wireless
Most Visited
Getting Started
Latest Headlines
Computer Networks...
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
WLANs > Edit
< Back
Apply
General Security QoS Advanced
Allow AAA Override Enabled
Coverage Hole Detection Enabled
Enable Session Timeout 1800
Session Timeout (secs)
Aironet IE Enabled
Diagnostic Channel Enabled
Override Interface ACL None
P2P Blocking Action Disabled
Client Exclusion 4 Enabled 0
Timeout Value (secs)
HREAP
H-REAP Local Switching 3 Enabled
Learn Client IP Address 6 Enabled
DHCP
DHCP Server Override
10.2.51.1
DHCP Server IP Addr
DHCP Addr. Assignment Required
Management Frame Protection (MFP)
Infrastructure MFP Protection (Global MFP Disabled)
MFP Client Protection 5 Optional
DTIM Period (in beacon intervals)
802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1
NAC
State Enabled
Foot Notes
1 CKIP is not supported by 10xx model APs
3 H-REAP Local Switching is not supported with IPsec, CRANITE authentication
4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
5 Client MFP is not active unless WPA2 is configured
6 Learn Client IP is configurable only when HREAP Local Switching is enabled
7 WMM and open or AES security should be enabled to support higher 11n rates
Done
Download
No Rank
0

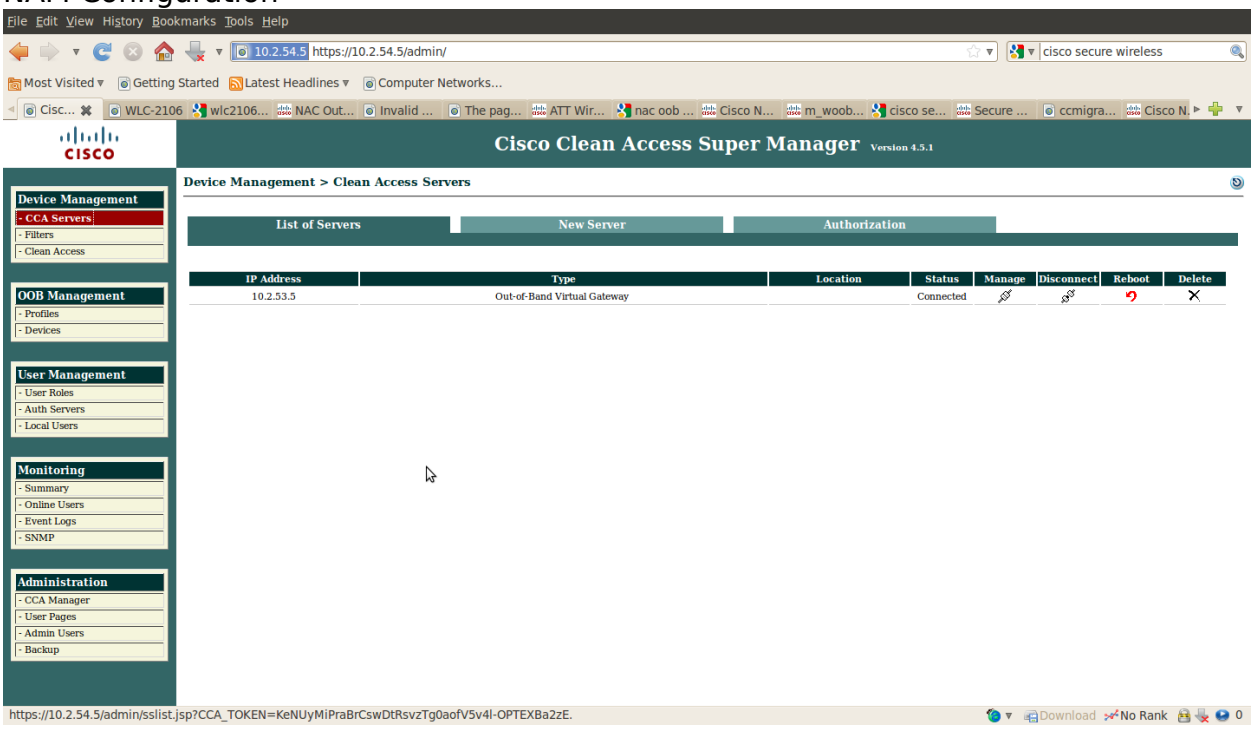

File Edit View History Bookmarks Tools Help
http://10.2.14.10/screens/frameset.html
cisco secure wireless
Most Visited
Getting Started
Latest Headlines
Computer Networks...
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Controller
General
Inventory
Interfaces
Multicast
Internal DHCP Server
Mobility Management
Ports
NTP
CDP
Advanced
General Information
Interface Name vlan51
MAC Address 00:25:45:9b:b8:00
Configuration
Quarantine
Quarantine Vlan Id 50
Physical Information
Port Number 1
Interface Address
VLAN Identifier 51
IP Address 10.2.51.2
Netmask 255.255.255.0
Gateway 10.2.51.1
DHCP Information
Primary DHCP Server 10.2.51.1
Secondary DHCP Server
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.
Done
Download
No Rank
0

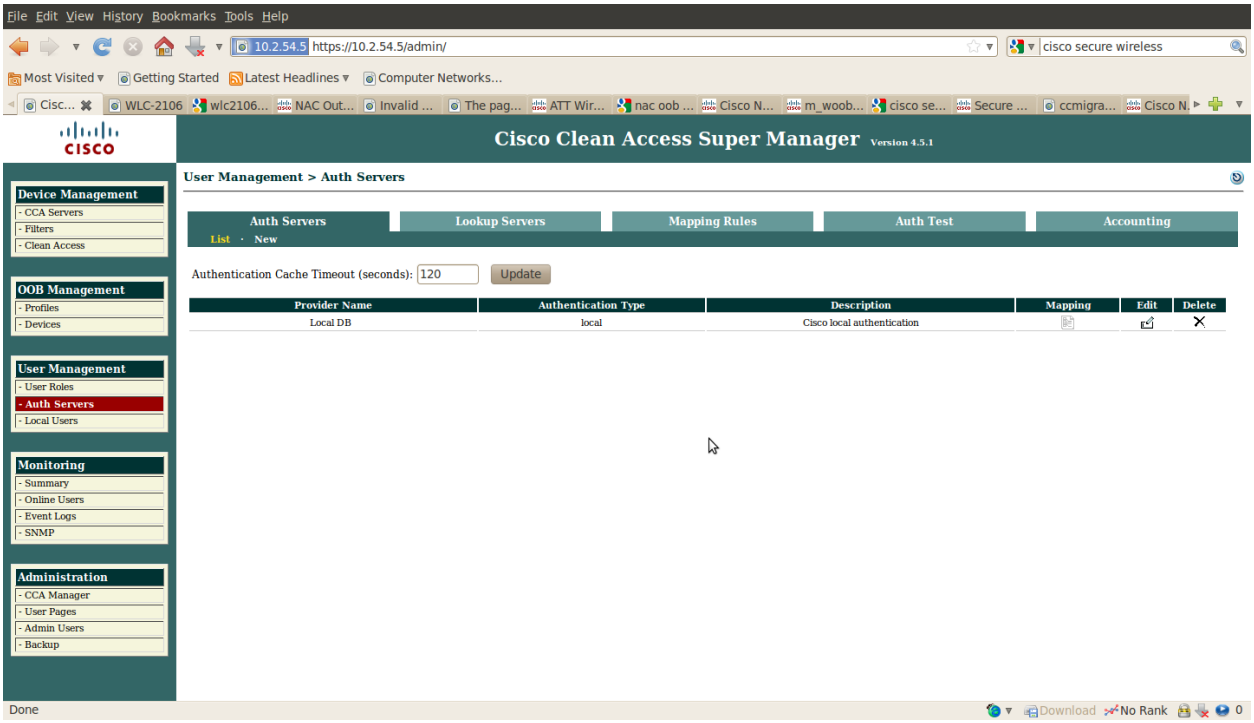

File Edit View History Bookmarks Tools Help
http://10.2.14.10/screens/frameset.html
cisco secure wireless
Most Visited
Getting Started
Latest Headlines
Computer Networks...
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Management
Summary
SNMP
General
SNMP V3 Users
Communities
Trap Receivers
Trap Controls
Trap Logs
HTTP
Telnet-SSH
Serial Port
Local Management Users
User Sessions
Logs
Mgmt Via Wireless
Tech Support
SNMP System Summary
Apply
Name WLC-2106
Location
Contact
System Description Cisco Controller
System Object ID 1.3.6.1.4.1.9.1.828
SNMP Port Number 161
Trap Port Number 162
SNMP v1 Mode Enable
SNMP v2c Mode Enable
SNMP v3 Mode Enable
http://10.2.14.10/screens/snmp/snmp_general.html
Download
No Rank
0

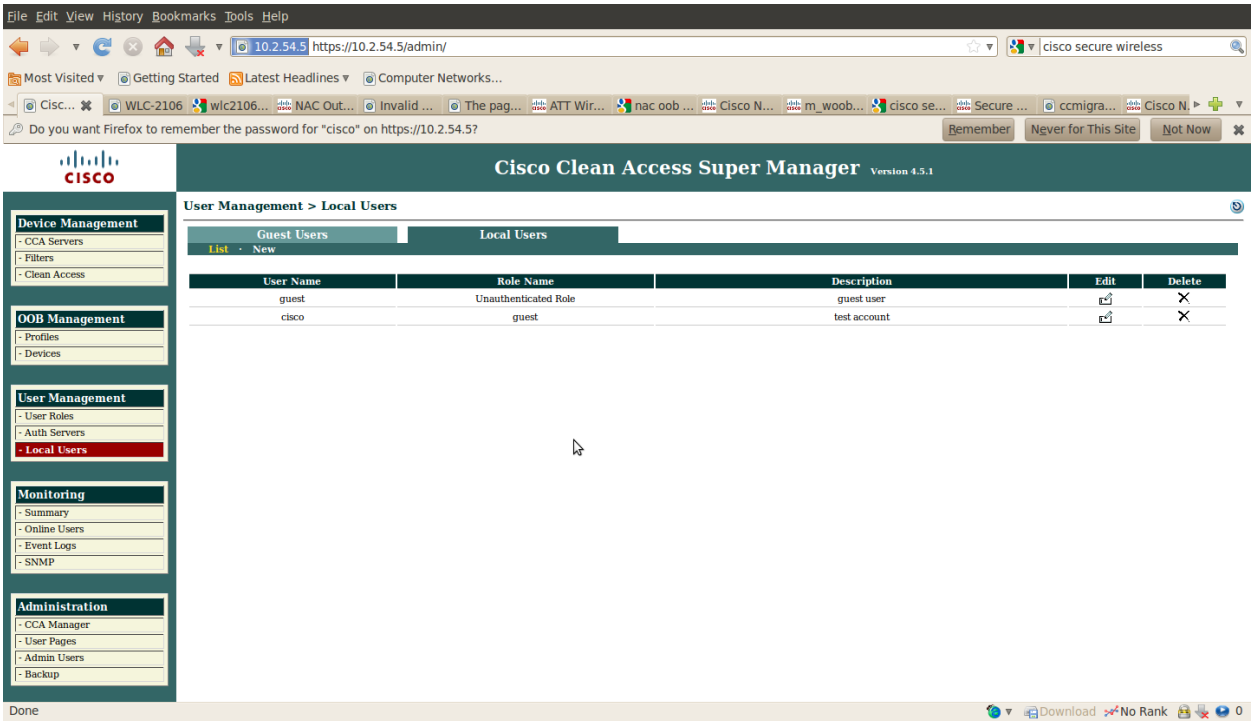

File Edit View History Bookmarks Tools Help
http://10.2.14.10/screens/frameset.html
cisco secure wireless
Most Visited
Getting Started
Latest Headlines
Computer Networks...
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Management
Summary
SNMP
General
SNMP V3 Users
Communities
Trap Receivers
Trap Controls
Trap Logs
HTTP
Telnet-SSH
Serial Port
Local Management Users
User Sessions
Logs
Mgmt Via Wireless
Tech Support
SNMP v1 / v2c Community
New...
Community Name
IP Address
IP Mask
Access Mode
Status
private
10.2.54.5
255.255.255.0
Read-Write
Enable
public
10.2.54.5
255.255.255.0
Read-Only
Enable
http://10.2.14.10/screens/snmp/snmp_comm_list.html
Download
No Rank
0

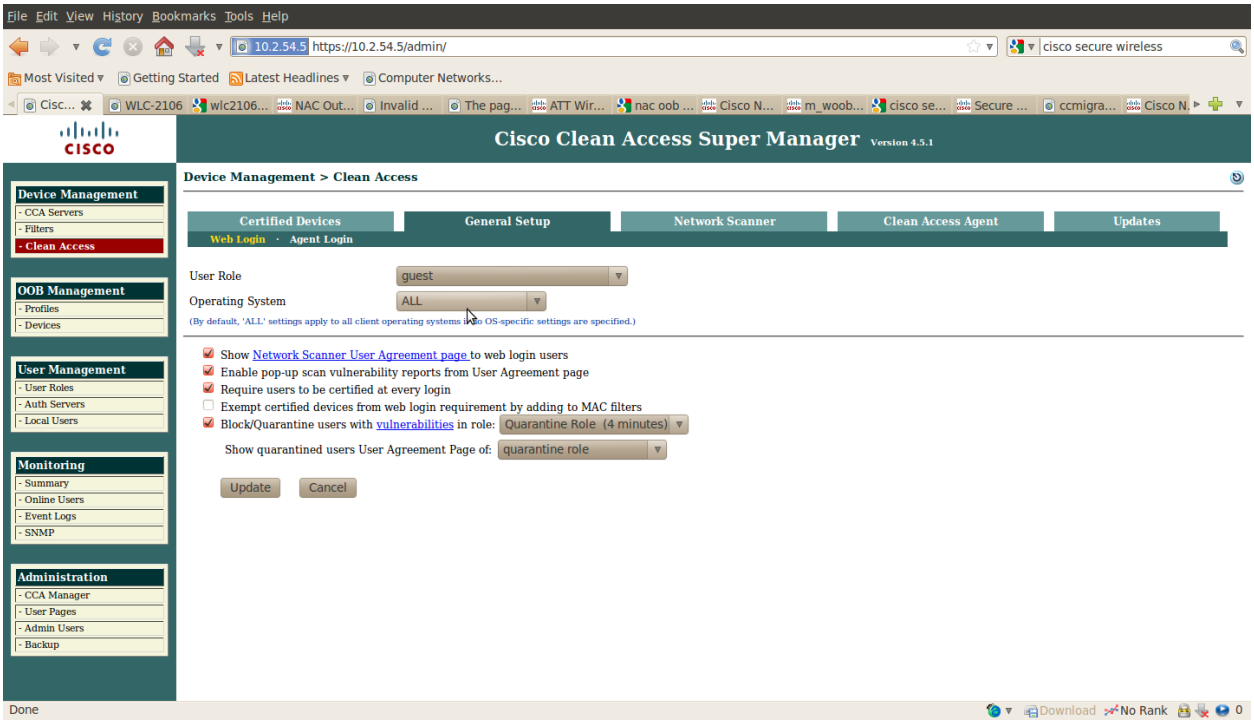

File Edit View History Bookmarks Tools Help
http://10.2.14.10/screens/frameset.html
cisco secure wireless
Most Visited
Getting Started
Latest Headlines
Computer Networks...
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Management
Summary
SNMP
General
SNMP V3 Users
Communities
Trap Receivers
Trap Controls
Trap Logs
HTTP
Telnet-SSH
Serial Port
Local Management Users
User Sessions
Logs
Mgmt Via Wireless
Tech Support
SNMP Trap Receiver
New...
Community Name
IP Address
Status
nac-cam-rcv
10.2.54.5
Enable
http://10.2.14.10/screens/snmp/trap_recvr_cfg_list.html
Download
No Rank
0

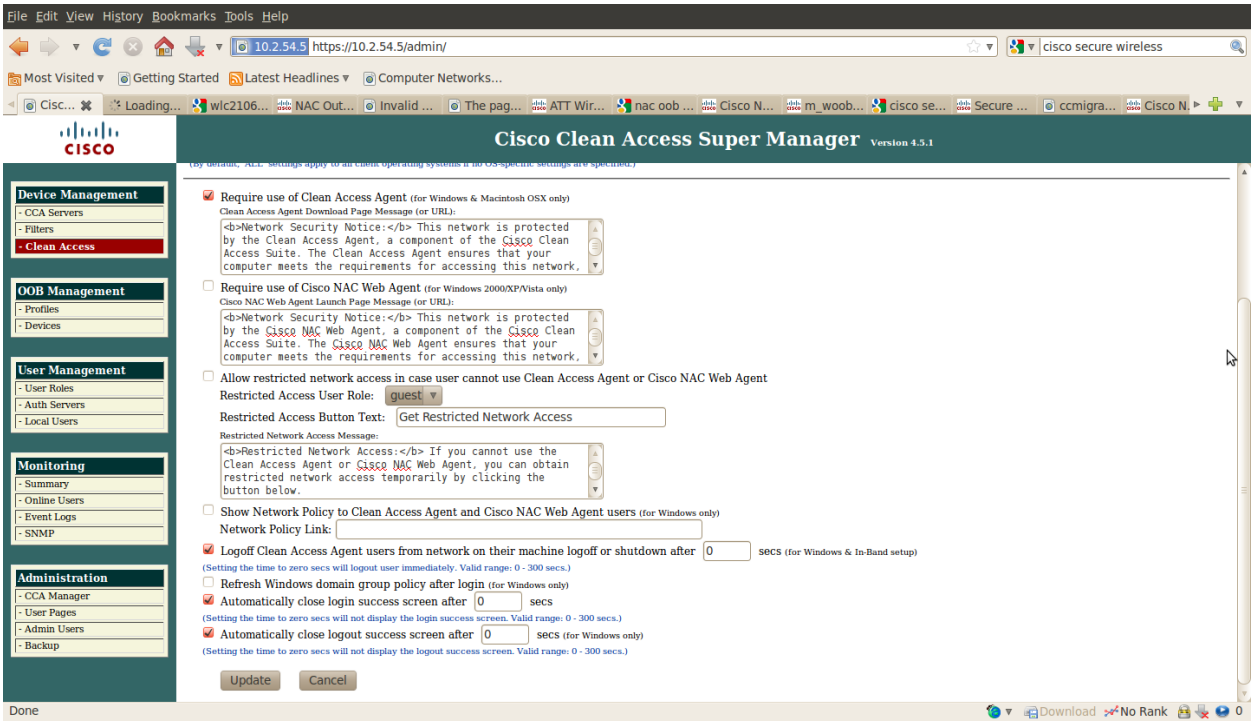
NAM Configuration

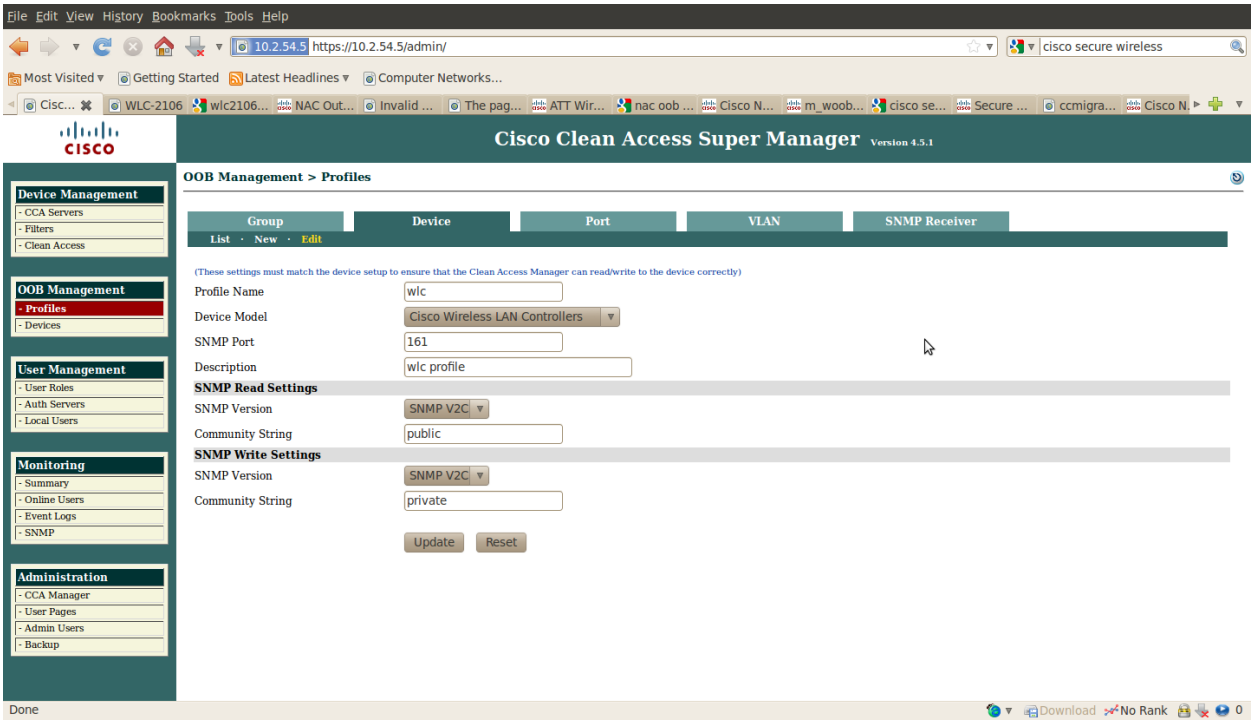


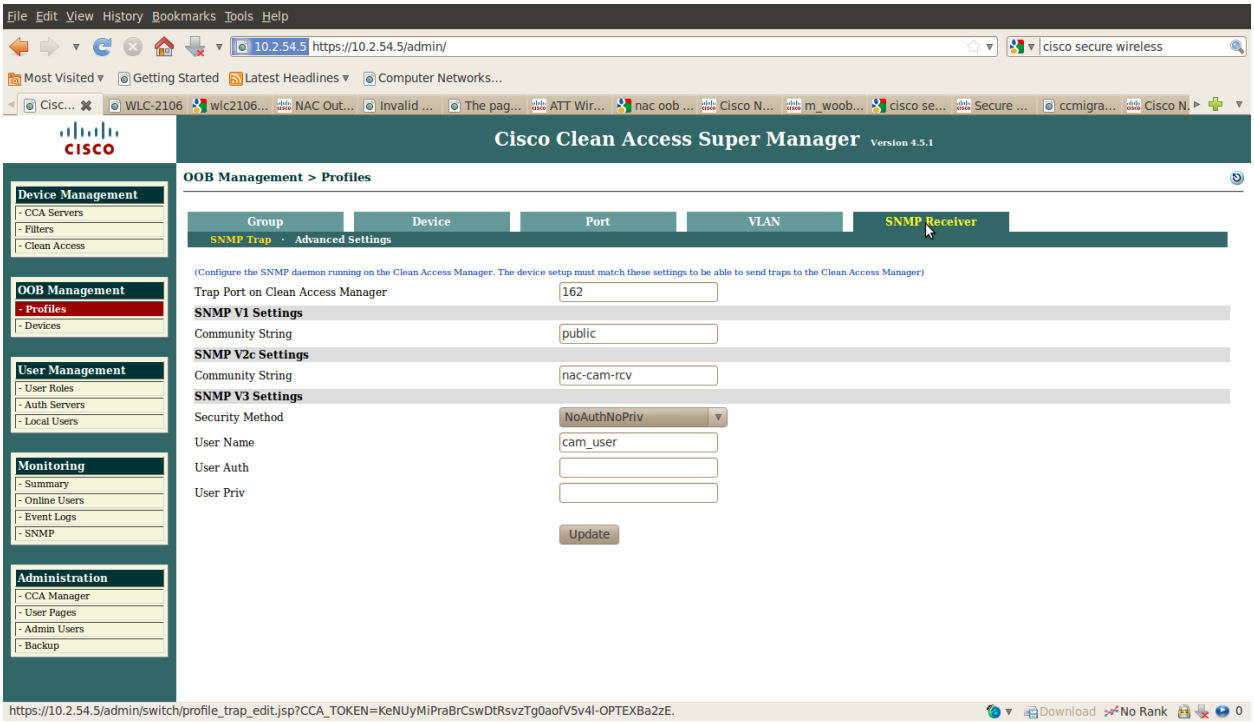


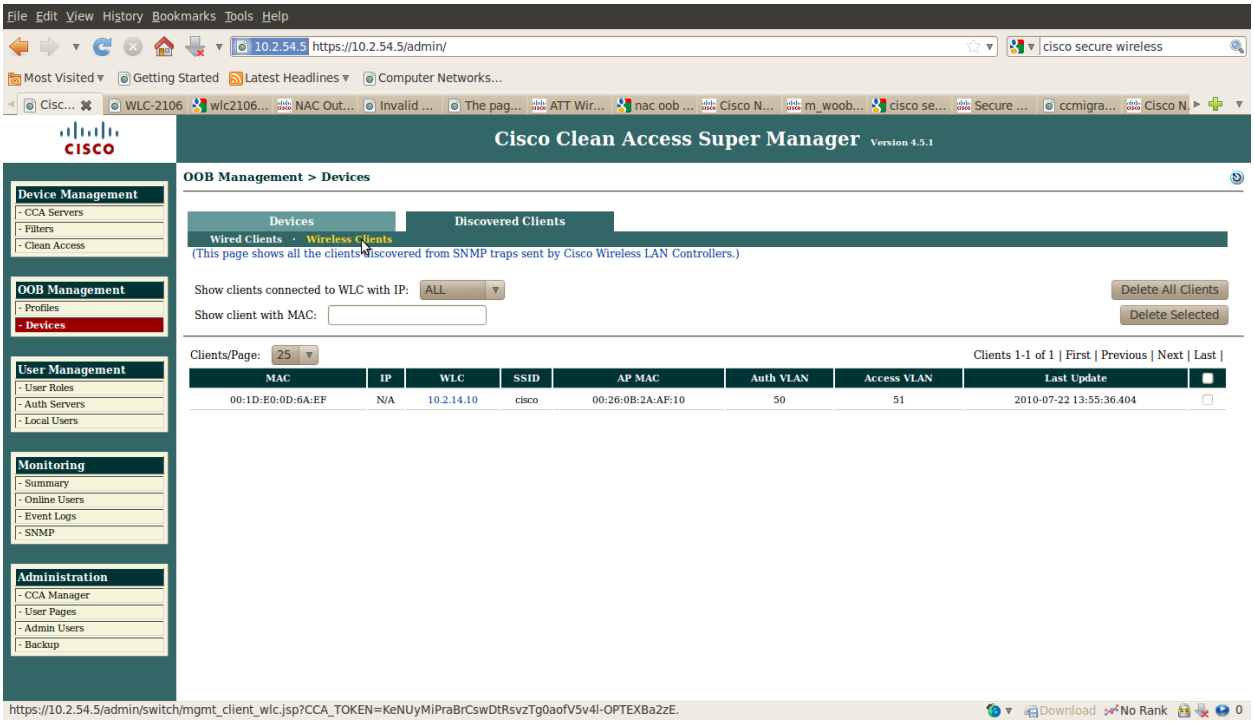

File Edit View History Bookmarks Tools Help
https://10.2.54.5/admin/
cisco secure wireless
Most Visited
Getting Started
Latest Headlines
Computer Networks...
Do you want Firefox to remember the password for "cisco" on https://10.2.54.5?
Remember
Never for This Site
Not Now
Cisco Clean Access Super Manager Version 4.5.1
User Management > Local Users
Guest Users
Local Users
List · New
User Name
Role Name
Description
Edit
Delete
guest
Unauthenticated Role
guest user
cisco
guest
test account
Device Management
- CCA Servers
- Filters
- Clean Access
OOB Management
- Profiles
- Devices
User Management
- User Roles
- Auth Servers
- Local Users
Monitoring
- Summary
- Online Users
- Event Logs
- SNMP
Administration
- CCA Manager
- User Pages
- Admin Users
- Backup
Done

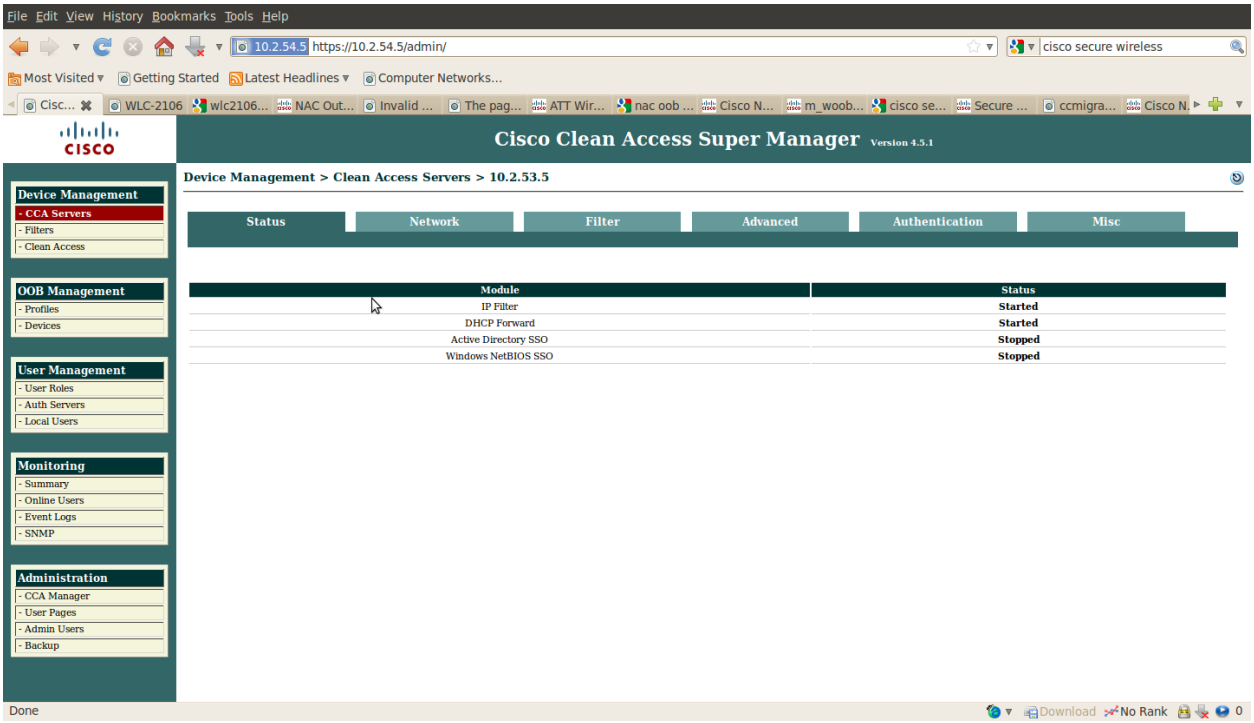

File Edit View History Bookmarks Tools Help
https://10.2.54.5/admin/
cisco secure wireless
Cisco Clean Access Super Manager Version 4.5.1
Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Updates
Web Login · Agent Login
User Role
guest
Operating System
ALL
(By default, 'ALL' settings apply to all client operating systems unless OS-specific settings are specified.)
Show Network Scanner User Agreement page to web login users
Enable pop-up scan vulnerability reports from User Agreement page
Require users to be certified at every login
Exempt certified devices from web login requirement by adding to MAC filters
Block/Quarantine users with vulnerabilities in role:
Quarantine Role (4 minutes)
Show quarantined users User Agreement Page of:
quarantine role
Update
Cancel
Device Management
- CCA Servers
- Filters
- Clean Access
OOB Management
- Profiles
- Devices
User Management
- User Roles
- Auth Servers
- Local Users
Monitoring
- Summary
- Online Users
- Event Logs
- SNMP
Administration
- CCA Manager
- User Pages
- Admin Users
- Backup
Done

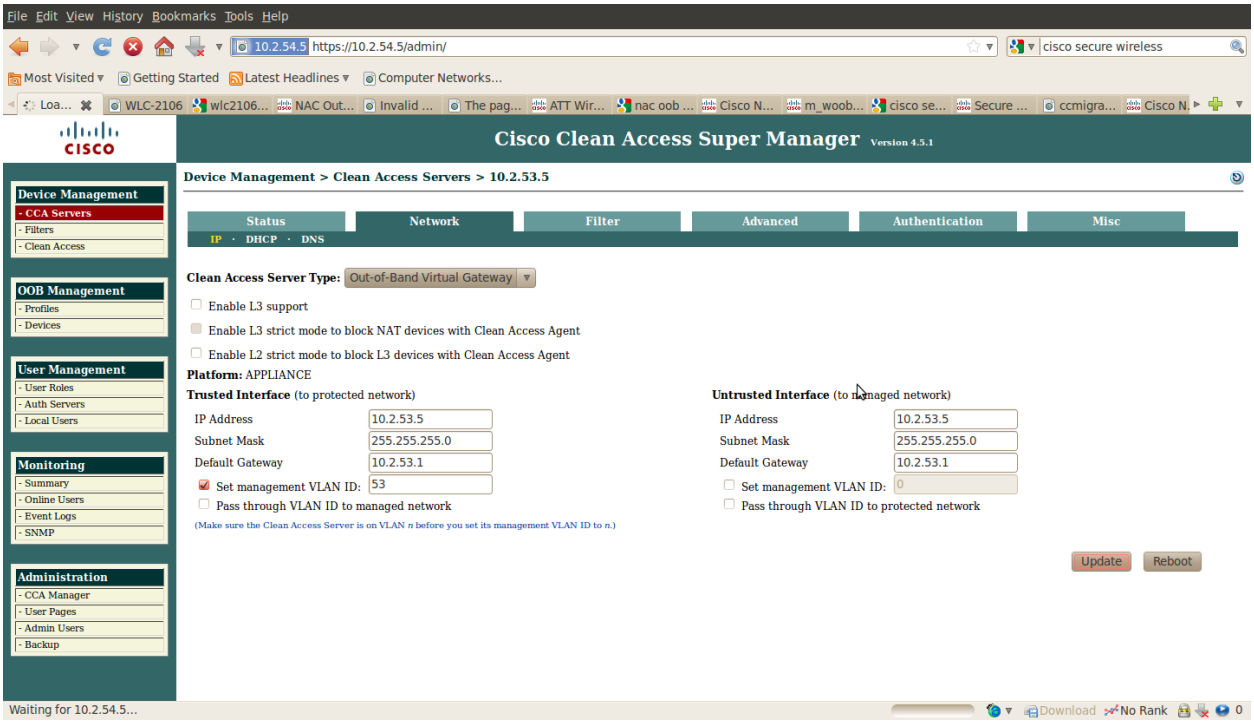

File Edit View History Bookmarks Tools Help
https://10.2.54.5/admin/
cisco secure wireless
Most Visited
Getting Started
Latest Headlines
Computer Networks...
Cisco Clean Access Super Manager Version 4.5.1
Device Management
- CCA Servers
- Filters
- Clean Access
OOB Management
- Profiles
- Devices
User Management
- User Roles
- Auth Servers
- Local Users
Monitoring
- Summary
- Online Users
- Event Logs
- SNMP
Administration
- CCA Manager
- User Pages
- Admin Users
- Backup
Require use of Clean Access Agent (for Windows & Macintosh OSX only)
Clean Access Agent Download Page Message (or URL):
Network Security Notice: This network is protected by the Clean Access Agent, a component of the Cisco Clean Access Suite. The Clean Access Agent ensures that your computer meets the requirements for accessing this network,
Require use of Cisco NAC Web Agent (for Windows 2000/XP/Vista only)
Cisco NAC Web Agent Launch Page Message (or URL):
Network Security Notice: This network is protected by the Cisco NAC Web Agent, a component of the Cisco Clean Access Suite. The Cisco NAC Web Agent ensures that your computer meets the requirements for accessing this network,
Allow restricted network access in case user cannot use Clean Access Agent or Cisco NAC Web Agent
Restricted Access User Role: guest
Restricted Access Button Text: Get Restricted Network Access
Restricted Network Access Message:
Restricted Network Access: If you cannot use the Clean Access Agent or Cisco NAC Web Agent, you can obtain restricted network access temporarily by clicking the button below.
Show Network Policy to Clean Access Agent and Cisco NAC Web Agent users (for Windows only)
Network Policy Link:
Logoff Clean Access Agent users from network on their machine logoff or shutdown after 0 secs (for Windows & In-Band setup)
(Setting the time to zero secs will logout user immediately. Valid range: 0 - 300 secs.)
Refresh Windows domain group policy after login (for Windows only)
Automatically close login success screen after 0 secs
(Setting the time to zero secs will not display the login success screen. Valid range: 0 - 300 secs.)
Automatically close logout success screen after 0 secs (for Windows only)
(Setting the time to zero secs will not display the logout success screen. Valid range: 0 - 300 secs.)
Update
Cancel
Done

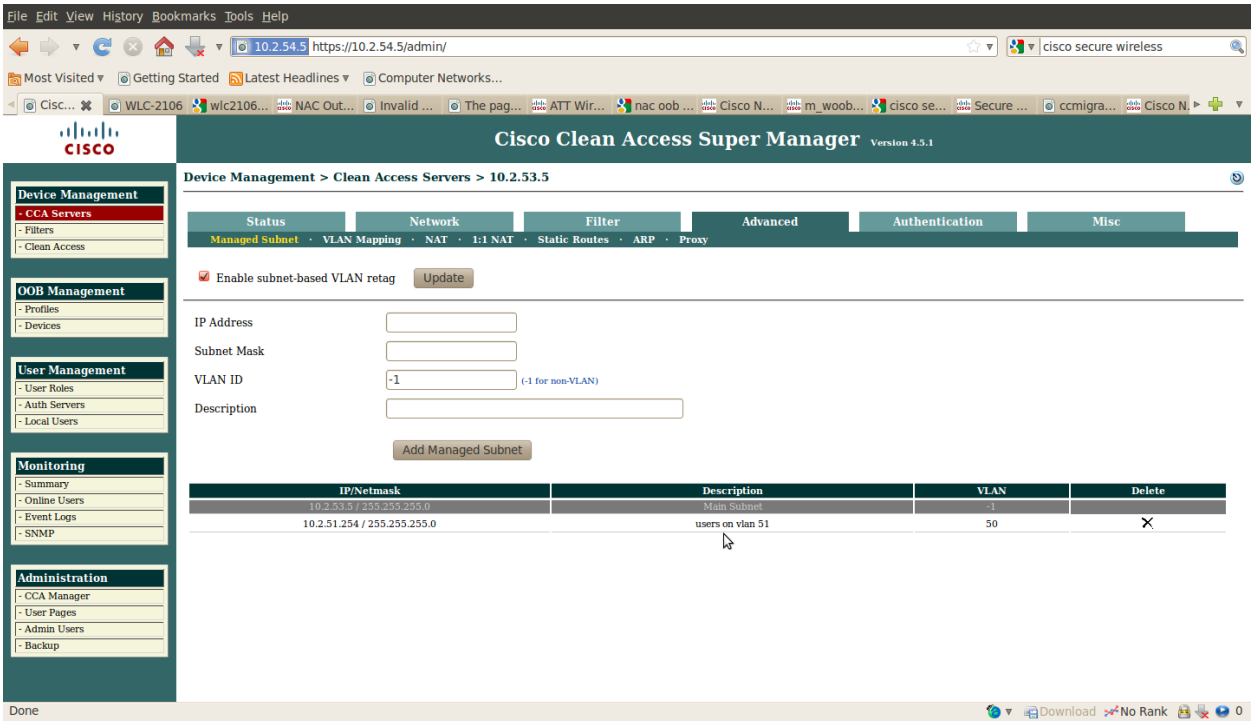

File Edit View History Bookmarks Tools Help
https://10.2.54.5/admin/
cisco secure wireless
Most Visited
Getting Started
Latest Headlines
Computer Networks...
Cisco Clean Access Super Manager Version 4.5.1
OOB Management > Profiles
Device Management
- CCA Servers
- Filters
- Clean Access
OOB Management
- Profiles
- Devices
User Management
- User Roles
- Auth Servers
- Local Users
Monitoring
- Summary
- Online Users
- Event Logs
- SNMP
Administration
- CCA Manager
- User Pages
- Admin Users
- Backup
Group
Device
Port
VLAN
SNMP Receiver
List · New · Edit
(These settings must match the device setup to ensure that the Clean Access Manager can read/write to the device correctly)
Profile Name wlc
Device Model Cisco Wireless LAN Controllers
SNMP Port 161
Description wlc profile
SNMP Read Settings
SNMP Version SNMP V2C
Community String public
SNMP Write Settings
SNMP Version SNMP V2C
Community String private
Update
Reset
Done

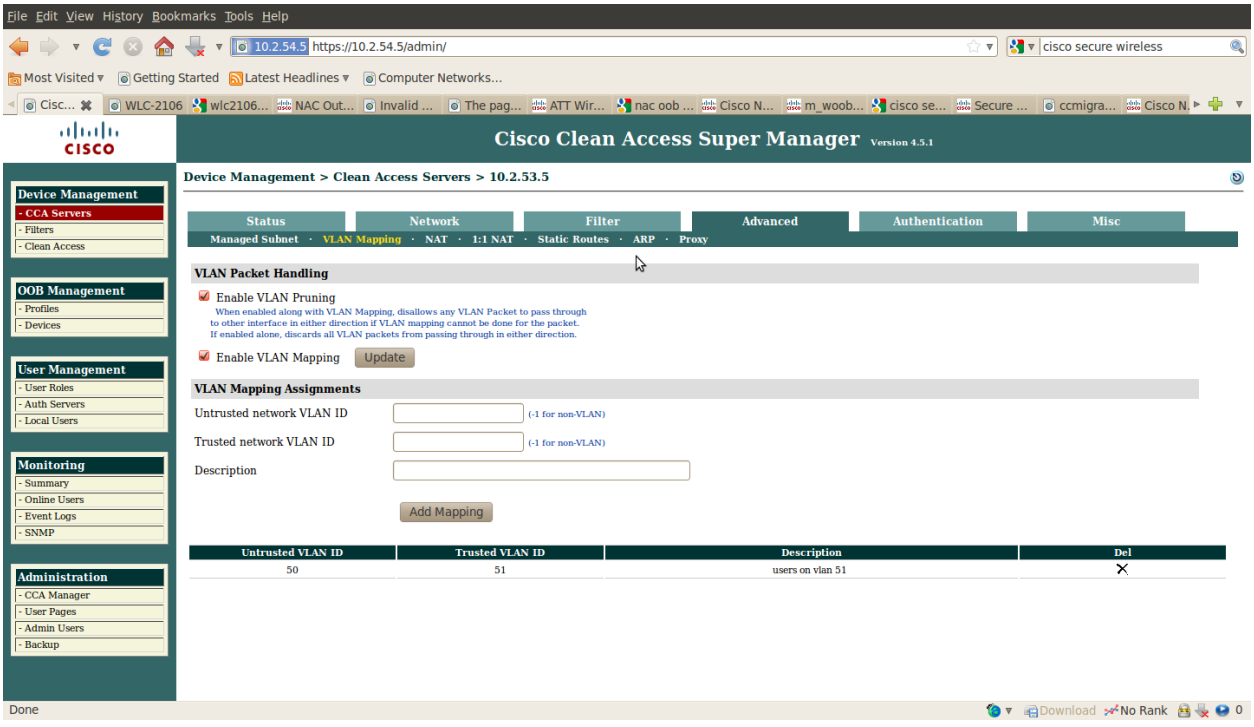

File Edit View History Bookmarks Tools Help
https://10.2.54.5/admin/
cisco secure wireless
Cisco Clean Access Super Manager Version 4.5.1
OOB Management > Profiles
Device Management
- CCA Servers
- Filters
- Clean Access
OOB Management
- Profiles
- Devices
User Management
- User Roles
- Auth Servers
- Local Users
Monitoring
- Summary
- Online Users
- Event Logs
- SNMP
Administration
- CCA Manager
- User Pages
- Admin Users
- Backup
Group
Device
Port
VLAN
SNMP Receiver
SNMP Trap · Advanced Settings
(Configure the SNMP daemon running on the Clean Access Manager. The device setup must match these settings to be able to send traps to the Clean Access Manager)
Trap Port on Clean Access Manager
162
SNMP V1 Settings
Community String
public
SNMP V2c Settings
Community String
nac-cam-rcv
SNMP V3 Settings
Security Method
NoAuthNoPriv
User Name
cam_user
User Auth
User Priv
Update
https://10.2.54.5/admin/switch/profile_trap_edit.jsp?CCA_TOKEN=KeNUyMiPraBrCswDtRsvzTg0aofV5v4l-OPTEXBa2zE.

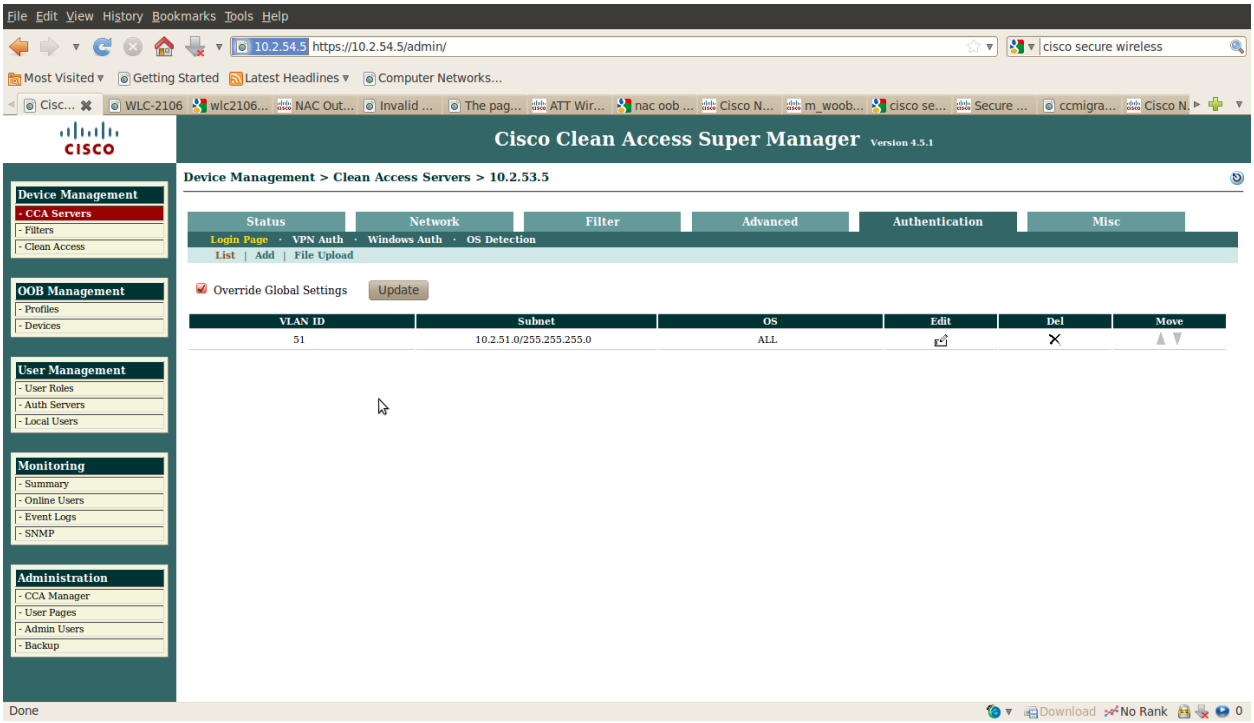

File Edit View History Bookmarks Tools Help
https://10.2.54.5/admin/
cisco secure wireless
Cisco Clean Access Super Manager Version 4.5.1
OOB Management > Devices
Device Management
- CCA Servers
- Filters
- Clean Access
OOB Management
- Profiles
- Devices
User Management
- User Roles
- Auth Servers
- Local Users
Monitoring
- Summary
- Online Users
- Event Logs
- SNMP
Administration
- CCA Manager
- User Pages
- Admin Users
- Backup
Devices
Discovered Clients
Wired Clients · Wireless Clients
(This page shows all the clients discovered from SNMP traps sent by Cisco Wireless LAN Controllers.)
Show clients connected to WLC with IP: ALL
Show client with MAC:
Delete All Clients
Delete Selected
Clients/Page: 25
Clients 1-1 of 1 | First | Previous | Next | Last |
MAC
IP
WLC
SSID
AP MAC
Auth VLAN
Access VLAN
Last Update
00:1D:E0:0D:6A:EF
N/A
10.2.14.10
cisco
00:26:0B:2A:AF:10
50
51
2010-07-22 13:55:36.404
https://10.2.54.5/admin/switch/mgmt_client_wlc.jsp?CCA_TOKEN=KeNUyMiPraBrCswDtRsvzTg0aofV5v4l-OPTEXBa2zE.

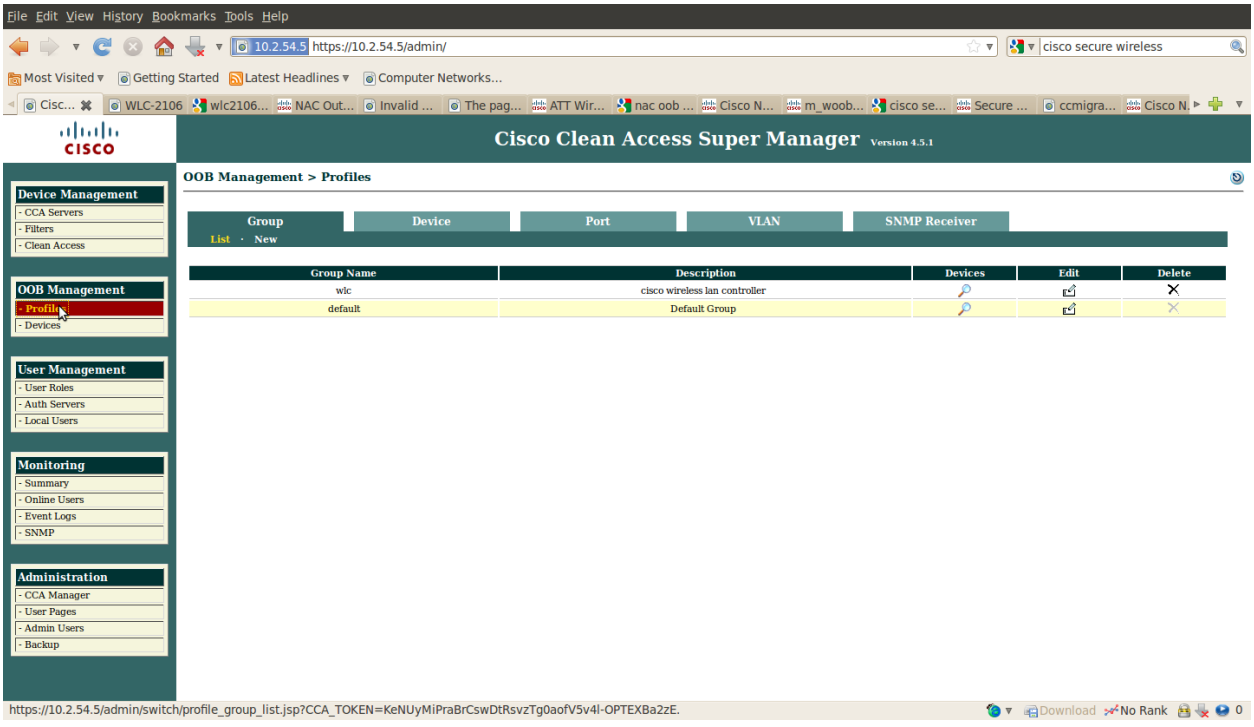

File Edit View History Bookmarks Tools Help
https://10.2.54.5/admin/
cisco secure wireless
Cisco Clean Access Super Manager Version 4.5.1
Device Management > Clean Access Servers > 10.2.53.5
Status
Network
Filter
Advanced
Authentication
Misc
Module
Status
IP Filter
Started
DHCP Forward
Started
Active Directory SSO
Stopped
Windows NetBIOS SSO
Stopped
Device Management
- CCA Servers
- Filters
- Clean Access
OOB Management
- Profiles
- Devices
User Management
- User Roles
- Auth Servers
- Local Users
Monitoring
- Summary
- Online Users
- Event Logs
- SNMP
Administration
- CCA Manager
- User Pages
- Admin Users
- Backup
Done

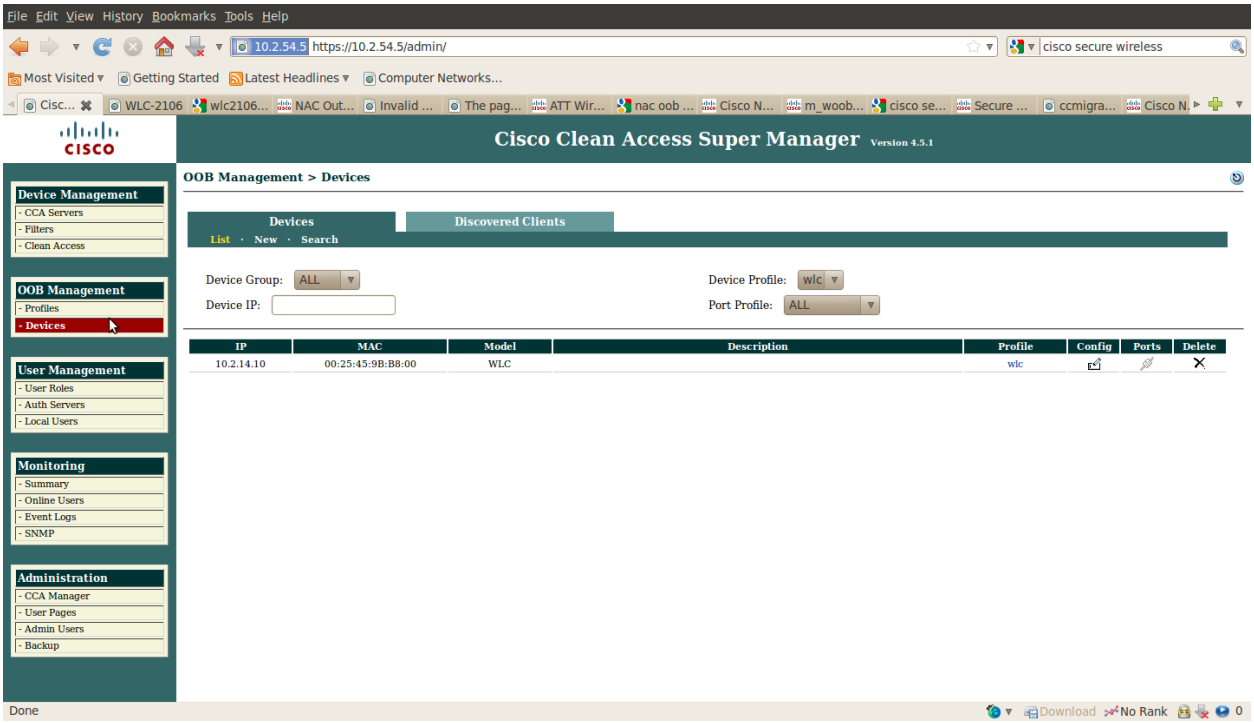

File Edit View History Bookmarks Tools Help
https://10.2.54.5/admin/
cisco secure wireless
Cisco Clean Access Super Manager Version 4.5.1
Device Management > Clean Access Servers > 10.2.53.5
Status
Network
Filter
Advanced
Authentication
Misc
IP · DHCP · DNS
Clean Access Server Type: Out-of-Band Virtual Gateway
Enable L3 support
Enable L3 strict mode to block NAT devices with Clean Access Agent
Enable L2 strict mode to block L3 devices with Clean Access Agent
Platform: APPLIANCE
Trusted Interface (to protected network)
IP Address 10.2.53.5
Subnet Mask 255.255.255.0
Default Gateway 10.2.53.1
Set management VLAN ID: 53
Pass through VLAN ID to managed network
(Make sure the Clean Access Server is on VLAN n before you set its management VLAN ID to n.)
Untrusted Interface (to managed network)
IP Address 10.2.53.5
Subnet Mask 255.255.255.0
Default Gateway 10.2.53.1
Set management VLAN ID: 0
Pass through VLAN ID to protected network
Update
Reboot
Device Management
- CCA Servers
- Filters
- Clean Access
OOB Management
- Profiles
- Devices
User Management
- User Roles
- Auth Servers
- Local Users
Monitoring
- Summary
- Online Users
- Event Logs
- SNMP
Administration
- CCA Manager
- User Pages
- Admin Users
- Backup
Waiting for 10.2.54.5...

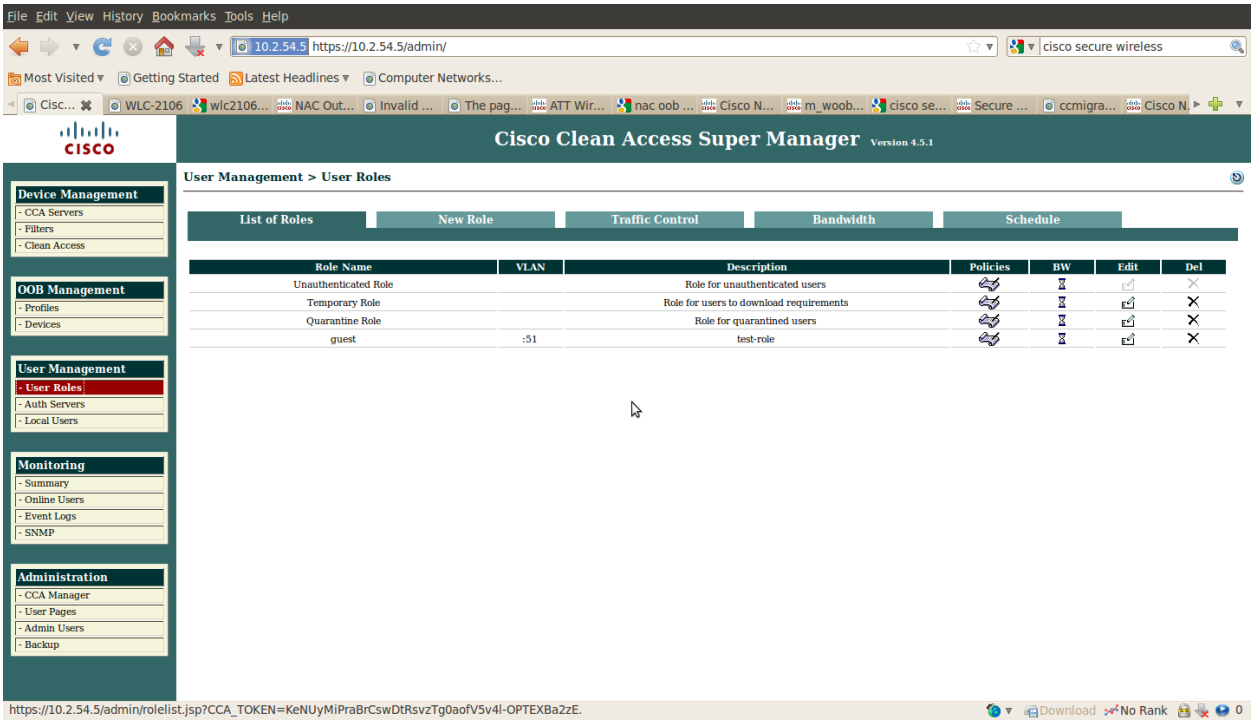

File Edit View History Bookmarks Tools Help
https://10.2.54.5/admin/
cisco secure wireless
Most Visited
Getting Started
Latest Headlines
Computer Networks...
Cisco Clean Access Super Manager Version 4.5.1
Device Management > Clean Access Servers > 10.2.53.5
Device Management
- CCA Servers
- Filters
- Clean Access
OOB Management
- Profiles
- Devices
User Management
- User Roles
- Auth Servers
- Local Users
Monitoring
- Summary
- Online Users
- Event Logs
- SNMP
Administration
- CCA Manager
- User Pages
- Admin Users
- Backup
Status
Network
Filter
Advanced
Authentication
Misc
Managed Subnet · VLAN Mapping · NAT · 1:1 NAT · Static Routes · ARP · Proxy
Enable subnet-based VLAN retag
Update
IP Address
Subnet Mask
VLAN ID
-1
(-1 for non-VLAN)
Description
Add Managed Subnet
IP/Netmask
Description
VLAN
Delete
10.2.53.5 / 255.255.255.0
Main Subnet
-1
10.2.51.254 / 255.255.255.0
users on vlan 51
50
Done


File Edit View History Bookmarks Tools Help
https://10.2.54.5/admin/
cisco secure wireless
Most Visited
Getting Started
Latest Headlines
Computer Networks...
Cisco Clean Access Super Manager Version 4.5.1
Device Management > Clean Access Servers > 10.2.53.5
Device Management
- CCA Servers
- Filters
- Clean Access
OOB Management
- Profiles
- Devices
User Management
- User Roles
- Auth Servers
- Local Users
Monitoring
- Summary
- Online Users
- Event Logs
- SNMP
Administration
- CCA Manager
- User Pages
- Admin Users
- Backup
Status
Network
Filter
Advanced
Authentication
Misc
Managed Subnet · VLAN Mapping · NAT · 1:1 NAT · Static Routes · ARP · Proxy
VLAN Packet Handling
Enable VLAN Pruning
When enabled along with VLAN Mapping, disallows any VLAN Packet to pass through to other interface in either direction if VLAN mapping cannot be done for the packet. If enabled alone, discards all VLAN packets from passing through in either direction.
Enable VLAN Mapping
Update
VLAN Mapping Assignments
Untrusted network VLAN ID
(-1 for non-VLAN)
Trusted network VLAN ID
(-1 for non-VLAN)
Description
Add Mapping
Untrusted VLAN ID
Trusted VLAN ID
Description
Del
50
51
users on vlan 51
Done


File Edit View History Bookmarks Tools Help
https://10.2.54.5/admin/
cisco secure wireless
Most Visited
Getting Started
Latest Headlines
Computer Networks...
Cisco Clean Access Super Manager Version 4.5.1
Device Management > Clean Access Servers > 10.2.53.5
Device Management
- CCA Servers
- Filters
- Clean Access
OOB Management
- Profiles
- Devices
User Management
- User Roles
- Auth Servers
- Local Users
Monitoring
- Summary
- Online Users
- Event Logs
- SNMP
Administration
- CCA Manager
- User Pages
- Admin Users
- Backup
Status
Network
Filter
Advanced
Authentication
Misc
Login Page · VPN Auth · Windows Auth · OS Detection
List | Add | File Upload
Override Global Settings
Update
VLAN ID
Subnet
OS
Edit
Del
Move
51
10.2.51.0/255.255.255.0
ALL
Done
Download
No Rank
0


File Edit View History Bookmarks Tools Help
https://10.2.54.5/admin/
cisco secure wireless
Most Visited
Getting Started
Latest Headlines
Computer Networks...
Cisco Clean Access Super Manager Version 4.5.1
OOB Management > Profiles
Device Management
- CCA Servers
- Filters
- Clean Access
OOB Management
- Profiles
- Devices
User Management
- User Roles
- Auth Servers
- Local Users
Monitoring
- Summary
- Online Users
- Event Logs
- SNMP
Administration
- CCA Manager
- User Pages
- Admin Users
- Backup
Group
Device
Port
VLAN
SNMP Receiver
List · New
Group Name
Description
Devices
Edit
Delete
wic
cisco wireless lan controller
default
Default Group
https://10.2.54.5/admin/switch/profile_group_list.jsp?CCA_TOKEN=KeNUyMiPraBrCswDtRsvzTg0aofV5v4l-OPTEXBa2zE.
Download
No Rank
0


File Edit View History Bookmarks Tools Help
https://10.2.54.5/admin/
cisco secure wireless
Most Visited
Getting Started
Latest Headlines
Computer Networks...
Cisco Clean Access Super Manager Version 4.5.1
OOB Management > Devices
Devices
Discovered Clients
List · New · Search
Device Group: ALL
Device IP:
Device Profile: wlc
Port Profile: ALL
IP MAC Model Description Profile Config Ports Delete
10.2.14.10 00:25:45:9B:B8:00 WLC wlc
Device Management
- CCA Servers
- Filters
- Clean Access
OOB Management
- Profiles
- Devices
User Management
- User Roles
- Auth Servers
- Local Users
Monitoring
- Summary
- Online Users
- Event Logs
- SNMP
Administration
- CCA Manager
- User Pages
- Admin Users
- Backup
Done


File Edit View History Bookmarks Tools Help
https://10.2.54.5/admin/
cisco secure wireless
Most Visited
Getting Started
Latest Headlines
Computer Networks...
Cisco Clean Access Super Manager Version 4.5.1
User Management > User Roles
List of Roles
New Role
Traffic Control
Bandwidth
Schedule
Role Name VLAN Description Policies BW Edit Del
Unauthenticated Role Role for unauthenticated users
Temporary Role Role for users to download requirements
Quarantine Role Role for quarantined users
guest :51 test-role
Device Management
- CCA Servers
- Filters
- Clean Access
OOB Management
- Profiles
- Devices
User Management
- User Roles
- Auth Servers
- Local Users
Monitoring
- Summary
- Online Users
- Event Logs
- SNMP
Administration
- CCA Manager
- User Pages
- Admin Users
- Backup
https://10.2.54.5/admin/rolelist.jsp?CCA_TOKEN=KeNUyMiPraBrCswDtRsvzTg0aofV5v4l-OPTEXBa2zE.