



Cyberoam WLAN Implementation Guide

Version 10

Document Version 10.04.5.0007 - 30/11/2013

Important Notice

Cyberoam Technologies Pvt. Ltd. has supplied this Information believing it to be accurate and reliable at the time of printing, but is presented without warranty of any kind, expressed or implied. Users must take full responsibility for their application of any products. Cyberoam Technologies Pvt. Ltd. assumes no responsibility for any errors that may appear in this document. Cyberoam Technologies Pvt. Ltd. reserves the right, without notice to make changes in product design or specifications. Information is subject to change without notice.

USER'S LICENSE

Use of this product and document is subject to acceptance of the terms and conditions of Cyberoam End User License Agreement (EULA) and Warranty Policy for Cyberoam UTM Appliances.

You will find the copy of the EULA at <http://www.cyberoam.com/documents/EULA.html> and the Warranty Policy for Cyberoam UTM Appliances at <http://kb.cyberoam.com>.

RESTRICTED RIGHTS

Copyright 1999 - 2013 Cyberoam Technologies Pvt. Ltd. All rights reserved. Cyberoam, Cyberoam logo are trademark of Cyberoam Technologies Pvt. Ltd.

Corporate Headquarters

Cyberoam Technologies Pvt. Ltd.
901, Silicon Tower, Off. C.G. Road,
Ahmedabad – 380006, INDIA
Phone: +91-79-66065606
Fax: +91-79-26407640
Web site: www.cyberoam.com

Technical Support

You may direct all questions, comments, or requests concerning the software you purchased, your registration status, or similar issues to Customer care/service department at the following address:

Corporate Office
Cyberoam Technologies Pvt. Ltd.
901, Silicon Tower
Off C.G. Road
Ahmedabad 380006
Gujarat, India.
Phone: +91-79-66065606
Fax: +91-79-26407640
Web site: www.cyberoam.com

Cyberoam contact:
Technical support (Corporate Office): +91-79-66065777
Email: support@cyberoam.com
Web site: www.cyberoam.com

Visit www.cyberoam.com for the regional and latest contact information.

Typographic Conventions

Material in this manual is presented in text, screen displays, or command-line notation.

Item	Convention	Example
Server		Machine where Cyberoam Software - Server component is installed
Client		Machine where Cyberoam Software - Client component is installed
User		The end user
Username		Username uniquely identifies the user of the system
Part titles	Bold and shaded font typefaces	Report
Topic titles	Shaded font typefaces	Introduction
Subtitles	Bold & Black typefaces	Notation conventions
Navigation link	Bold typeface	System → Administration → Appliance Access it means, to open the required page click on System then on Administration and finally click Appliance Access
Name of a particular parameter / field / command button text	Lowercase italic type	Enter policy name, replace policy name with the specific name of a policy Or Click Name to select where Name denotes command button text which is to be clicked
Cross references	Hyperlink in different color	refer to Customizing User database Clicking on the link will open the particular topic
Notes & points to remember	Bold typeface between the black borders	Note
Prerequisites	Bold typefaces between the black borders	Prerequisite Prerequisite details

Contents

Overview	6
Connected Client	7
View Connection Status	7
Settings.....	10
WLAN General Settings.....	10
Access Point	12
View the list of Access Points	12
Access Point Parameters	13
Rogue Access Point.....	15
Discover Access Points	16
Mark Access Point as Rogue.....	18

Overview

Note

This section is applicable to Wi-Fi models only.

Wireless Local Area Network (WLAN) is used to associate devices through wireless distribution method and connection to the internet is provided through an access point.

Wi-Fi appliances support three wireless protocols called IEEE 802.11n, 802.11b and 802.11g, and send data via radio transmissions. By functioning as an Access point, secure wireless gateway and firewall, it provides real-time network protection and high-speed wireless connectivity.

Apart from the access point for wireless LAN, by integrating with firewall, Wi-Fi delivers comprehensive protection to small, remote and branch office users from threats like malware, virus, spam, phishing, and pharming attacks.

Note

All the screen shots in the Cyberoam User Guides have been taken from NG series of appliances. The feature and functionalities however remains unchanged across all Cyberoam appliances.

As WLAN interface is a member of LAN zone:

- All the services enabled for the LAN zone from the Appliance Access page are automatically applicable on WLAN1 and other access points too.
- All the firewall rules applied on LAN zone will be applied on WLAN access points too.

Wi-Fi models, by default include one wireless interface called WLAN1.

Limitations

1. Only one access point can be configured when appliance is deployed in Bridge mode
2. Alias and VLAN sub-interfaces are not supported for access point interfaces.

Wi-Fi appliances support the following wireless network standards:

- 802.11n (5 GHz Band)
- 802.11b (2.4-GHz Band)
- 802.11g (2.4-GHz Band)
- WEP64 and WEP128 Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA), WPA2 and WPA2 Auto using pre-shared keys
- [Connected Client](#)
- [Settings](#)
- [Access Point](#)

Connected Client

The page displays all the connected Wireless LAN clients. You can filter connected clients by searching for IP Address, MAC Address or by access points

To view and manage connected WLAN clients, go to **Network → Wireless LAN → Connected Client**. You can:

- [View](#)
- [Search](#)

View Connection Status


Records Per Page 20 (1 of 1)		
Leased IP Address	MAC Address	Access Point
10.10.3.62	68:09:27:39:28:a1	WLAN1
-	a0:88:b4:d6:27:f0	WLAN1
10.10.3.58	18:87:96:5c:c3:29	WLAN1
10.10.3.51	e0:b9:ba:3b:96:0c	WLAN1
10.10.3.56	08:11:96:0d:f1:c4	WLAN1
Records Per Page 20 (1 of 1)		

Screen – View Connection Status

Screen Element	Description
Leased IP Address	IP Address leased for Wireless connection.
MAC Address	MAC Address of the device
Access Point	Wireless Access Point from which the connection is established

Table – View Connection Status screen elements

Search Clients


IP Address – Click the Search icon  in the Leased IP Address column to search specific address. A pop-up window is displayed that has filter criteria for search. Address can be searched on the following criteria: is equal to, starts with, contains. Click OK to get the search results and Clear button to clear the results.

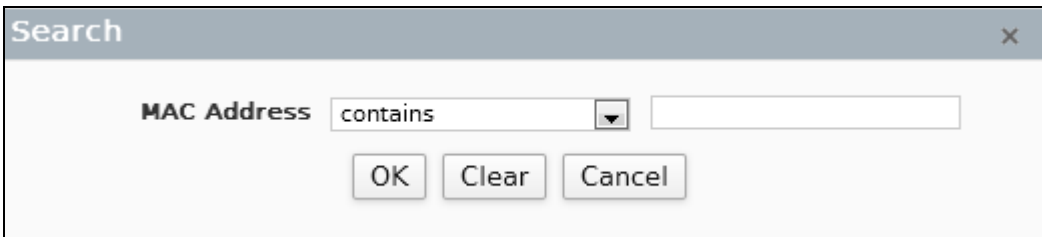


Screen – Search Leased IP Address

Search Criteria	Search Results
is equal to	All the IP addresses that exactly match the IP Address specified in the criteria. For example, if the search string is 192.168.1.1, all the addresses exactly matching the string will be displayed.
starts with	All the IP Addresses that starts with the specified criteria. For example, if the search string is 10, all the addresses like 10.1.1.1, starting with the number 10 will be displayed.
contains	All the addresses that are in the IP range specified in the search string. For example, if the search string is 1.1.1.2-1.1.1.10, all the IP Addresses like 1.1.1.5 or 1.1.1.8 falling in this range will be displayed.

Table – Search Leased IP Address screen elements

MAC Address – Click the Search icon  in the MAC Address column to search specific address. A pop-up window is displayed that has filter criteria for search. Address can be searched on the following criteria: is equal to, starts with, contains. Click OK to get the search results and Clear button to clear the results.




Screen – Search MAC Address

Search Criteria	Search Results
-----------------	----------------

is equal to	<p>All the MAC Addresses that exactly match the MAC Address specified in the criteria.</p> <p>For example, if the search string is 10:15:18:A1:BC:22, all the addresses exactly matching the string will be displayed.</p>
starts with	<p>All the MAC Addresses that starts with the specified search criteria.</p> <p>For example, if the search string is 10, all the addresses like 10:15:18:A1:BC:22, starting with the number 10 will be displayed.</p>
contains	<p>All the MAC Addresses that contain the string specified in the criteria.</p> <p>For example, if the search string is BC, all the MAC Addresses like 10:15:18:A1:BC:22, containing the string are displayed.</p>

Table – Search MAC Address screen elements

Access Point – Click the Search icon  in the Access Point column to search for clients with access point. Access Point can be searched on the following criteria: is, is not, contains and does not contain. A pop-up window is displayed that has filter conditions for search. Click OK to get the search results and Clear button to clear the results.

Search Criteria	Search Results
is	<p>All the Access Points that exactly match with the string specified in the criteria.</p> <p>For example, if the search string is Test, only Access Point with the name exactly matching “Test” are displayed.</p>
is not	<p>All the Access Points that do not match with the string specified in the criteria.</p> <p>For example, if the search string is Test, all Access Point except with the name exactly matching “Test” are displayed.</p>
contains	<p>All the Access Points that contain the string specified in the criteria.</p> <p>For example, if the search string is Test, all the Access Points containing the string “Test” are displayed.</p>
does not contain	<p>All the Access Points that do not contain the string specified in the criteria.</p> <p>For example, if the search string is Test, all the Access Points not containing the string “Test” are displayed.</p>

Table – Search Access Point screen elements

Settings

The page allows general configuration of Wireless LAN connection.

By default, Wi-Fi appliances include one wireless interface, called WLAN1 and additional seven interfaces can be added. All wireless interfaces use the same wireless parameters and hence there is no need to configure different settings for each interface.

WLAN General Settings

To configure WLAN connection, go to **Network → Wireless LAN → Settings**.

Screen – WLAN General Settings

Screen Element	Description
Wireless Protocol	Select the Wireless Protocol to be used. <ul style="list-style-type: none"> • 802.11b/g/n • 802.11g/n • 802.11b/g • 802.11n • 802.11g • 802.11b
Geography	Select your country or location. This determines which channels will be available for your network
Channel	Select a channel for your wireless network. Available channel options are based on the Geographical location you selected. By default the Channel is selected automatically –(Auto).
Transmission Power	Select power level of the radio signal transmission, higher the number, larger the area CR15wi will broadcast. For example, if you want signal to go from building-to-building, select Full Power and if you want to keep the wireless signal

	<p>to a small area, select minimum.</p> <p>.</p> <p>Available Options:</p> <ul style="list-style-type: none"> • Full Power • Half • Quarter • Eighth • Minimum <p>By default the transmission power value is Full Power. Full power sends the strongest signal to the WLAN.</p>
Beacon Interval	<p>Specify the time interval between two beacon packets to be sent.</p> <p>Beacon Packets - Access Points broadcast Beacons to synchronize wireless networks. For faster connectivity, select lower time interval. However, lower time interval will increase the number of beacons sent. While this will make it quicker to find and connect to the wireless network, it requires more overhead, slowing the throughput.</p> <p>By default the beacon interval is 100 milliseconds Beacon Interval range: 100 – 1024 milliseconds.</p>
RTS Threshold	<p>Specify the threshold time before the RTS frames are sent.</p> <p>The RTS threshold is the maximum size, in bytes, of a packet that the CR15wi will accept without sending RTS/CTS packets to the sending wireless device.</p> <p>If network throughput is slow or a large number of frame retransmissions are occurring, decrease the RTS threshold to enable RTS clearing.</p> <p>By default the RTS threshold value is 2347. RTS Threshold range: 1 – 2347</p>
Fragmentation Threshold	<p>It is the maximum size of a data packet before it is broken into smaller packets, reducing the chance of packet collisions. Appliance will allow specified number of bytes of fragmented data in the network.</p> <p>If the packet size is larger than the threshold, packets will be fragmented before transmission.</p> <p>By default the fragmentation threshold value is 2346. Fragmentation Threshold range: 256 – 2346</p>
Maximum Clients	<p>Specify the maximum number of clients that are allowed to connect across all the access points simultaneously.</p> <p>By default the maximum number of clients allowed is 255. Maximum Clients allowed range: 1 – 255</p>

Table – WLAN General Settings screen elements




Access Point

Wi-Fi models, by default include one wireless interface called WLAN1 and support up to seven additional wireless interfaces to be configured as Access Points. All the configured access points use the same wireless parameters.

Limitations

- Only one access point can be configured when appliance is deployed in Bridge mode.




To manage access points, go to **Network → Wireless LAN → Access Point**. You can:

- [Add](#)
- [View](#)
- [Edit](#) – Click the Edit icon  in the Manage column against the access point to be modified. Edit Access Point page is displayed which has the same parameters as the Add Access Point page.
- [Delete](#) – Click the Delete icon  in the Manage column against an Access Point to be deleted. A dialog box is displayed asking you to confirm the deletion. Click OK to delete the Access point. To delete multiple Access points, select them  and click the Delete button.

Note

Default Access Point cannot be deleted.

View the list of Access Points

<div>Add Delete</div>						
<input type="checkbox"/>	Name	Zone	IP Address	SSID	Security Mode	Manage
<input type="checkbox"/>	<u>WLAN1</u>	LAN	10.10.3.34/255.255.255.0	CyberoamXWifi	WPA-WPA2-PSK-Auto	
<input type="checkbox"/>	<u>WLAN2</u>	LAN	10.101.101.1/255.255.255.0	cyberoam- 1	WEP-Auto	 
<div>Add Delete</div>						


Screen – Manage Access Point

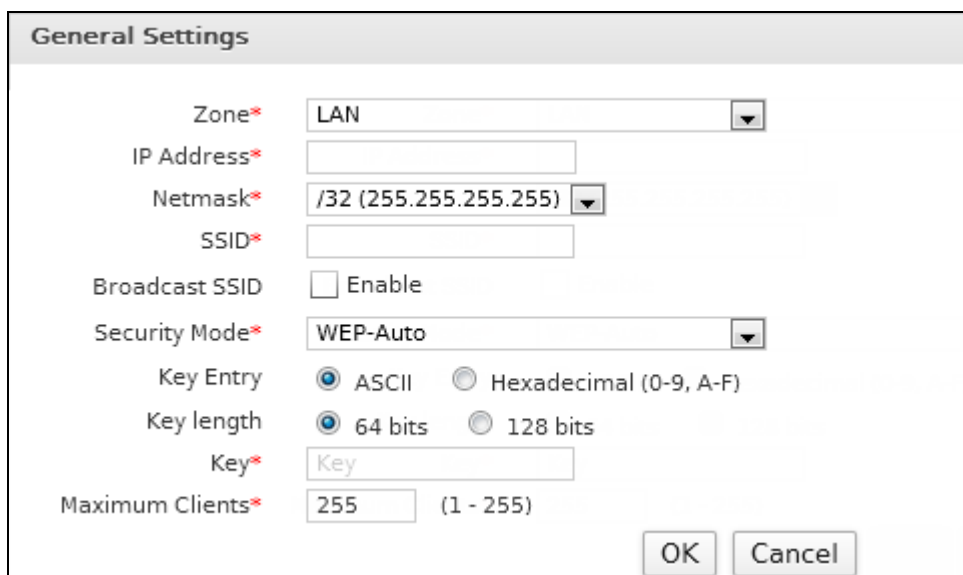
Screen Element	Description
Add Button	Add a new Access Point.
Name	Name of the Access Point.
Zone	Zone of Access point. Access point can be the member of LAN zone only.
IP Address	IP Address and netmask for the access point. If appliance is deployed as Bridge, IP Address will not be displayed.
SSID	Unique Service Set Identifier (SSID) for broadcast. The access point is identified by its SSID. The access point sends broadcast messages advertising its SSID for the

	receiver to acknowledge and use the Internet through that access point.
Security Mode	<p>Security Mode selected.</p> <p>Available Options:</p> <ul style="list-style-type: none"> • None • WEP-Open • WEP-Shared • WEP-Auto • WPA –PSK • WPA2-PSK • WPA-WPA2-PSK-Auto • WPA-Enterprise • WPA2-Enterprise
Edit Icon	Edit the Access Point details.
Delete Button	Delete the Access Point.

Table – Manage Access Point screen elements

Access Point Parameters

To add or edit access points, go to **Network → Wireless LAN → Access Point**. Click Add Button to add a new access point. To update the details, click on the access point or Edit icon  in the Manage column against the access point you want to modify.



General Settings

Zone* LAN

IP Address*

Netmask* /32 (255.255.255.255)

SSID*

Broadcast SSID ☐ Enable

Security Mode* WEP-Auto

Key Entry ☒ ASCII ☐ Hexadecimal (0-9, A-F)

Key length ☒ 64 bits ☐ 128 bits

Key* Key

Maximum Clients* 255 (1 - 255)

OK Cancel

Screen – Add Access Point

Screen Element	Description
Zone	<p>Select Zone for the Access Point.</p> <p>Access Point can be the member of LAN zone only.</p>
IP Address	Specify IP Address for the Access Point.
Netmask	Specify subnet mask.

SSID	<p>Specify Service Set Identifier (SSID).</p> <p>The access point is identified by its SSID. Users who want to use the wireless network must configure their computers with this SSID.</p>
Broadcast SSID	<p>Enable to broadcast the SSID.</p> <p>Broadcasting the SSID enables clients to connect to your wireless network without knowing the SSID. For security purpose, do not broadcast the SSID as there will be less chances of an unwanted user connecting to your wireless network. If you choose not to broadcast the SSID, you need to forward SSID to your users so that they can configure their wireless devices.</p>
Security Mode	<p>Select the security mode for encrypting the wireless traffic.</p> <p>Available Options:</p> <ul style="list-style-type: none"> • WEP-Open • WEP-Shared • WEP-Auto • WPA –PSK • WPA2-PSK • WPA-WPA2-PSK-Auto <p>WPA mode is better for security than WEP mode.</p>
For WEP-Open, WEP-Shared and WEP-Auto only	
Key Entry	<p>Select Key entry mode</p> <p>Available Options:</p> <ul style="list-style-type: none"> • ASCII • Hexadecimal
Key Length	<p>Select the length of security key. A longer key length ensures better security.</p> <p>Available Options:</p> <ul style="list-style-type: none"> • 64 bit • 28 bit
Key	Specify security key for authentication.
For WPA –PSK, WPA2-PSK and WPA-WPA2-PSK-Auto only	
Encryption	<p>Select the Encryption type.</p> <p>Available Options:</p> <ul style="list-style-type: none"> • TKIP – Temporal Key Integrity Protocol • AES – Advanced Encryption Standard • Auto
Pass Phrase	<p>Specify the phase to be used as password</p> <p>Pass Phrase range: 8 – 63 characters</p>
Group Key update	Enable the 'Group Key Update' checkbox to generate new security key after the configured timeout interval.
Timeout Interval	Specify the timeout interval for generating security key.

For WPA–Enterprise and WPA2-enterprise	
Encryption	Select the Encryption type. Available Options: <ul style="list-style-type: none"> • TKIP – Temporal Key Integrity Protocol • AES – Advanced Encryption Standard • Auto
Server IP & port	IP Address and Port number of the primary RADIUS server.
Shared Secret	Password with which primary RADIUS server can be accessed.
Backup Server IP and Port	IP Address and Port number of the backup RADIUS server.
Shared Secret	Password with which backup RADIUS server can be accessed.

Table – Add Access Point screen elements

Note

Once the Access Point is added, you can configure Access Point as a DHCP Server.

Rogue Access Point

A Rogue Access Point (AP) is any Wi-Fi access point connected to your network without authorization. It can be a setup used by an attacker for the purpose of sniffing wireless network traffic i.e. to conduct a man-in-the-middle attack. It allows anyone with a Wi-Fi-equipped device to connect to your corporate network, leaving your IT assets wide open for the casual snooper or criminal hacker.

Appliance can alleviate this by recognizing rogue access points potentially attempting to gain access to your network.

Click "**Schedule system- trigger scan**" to enable a schedule for Rogue AP Scan. You can select from the pre-defined schedules or create a [custom schedule](#).

General Settings	
<input type="checkbox"/> Schedule system-triggered scan at	<div> Schedule ▼ <i>i</i> </div> <div>Apply</div>

Screen – General Settings

Screen – Add Schedule

To discover rogue access points and authorize access points, go to **Network → Wireless LAN → Rogue AP scan**. You can:

- [Scan for nearby access points](#)
- [Authorize AP](#)
- [Mark AP as Rogue](#)

Discover Access Points

To increase the security capabilities and identify the unauthorized APs, Wireless appliances provides scanning capability by which nearby APs can be discovered and administrator can take countermeasures against the most common types of illicit wireless activity.

Go to **Network → Wireless LAN → Rogue AP scan** to manually scan or schedule scanning for the automatic discovery of APs. To schedule the scanning, enable schedule based scanning and select the schedule. To manually scan, click “Scan Now”.

If you are scanning for the first time, after enabling Wireless LAN, all the discovered APs will be listed in Unrecognized Access Points table. Scanning result is displayed in the form of 3 tables:



Unrecognized Access Points

Scan Results

Rogue AP scan was last carried out at 2013-02-01 16:02:38 Hours

Scan Now

Unrecognized Access Points

Channel	BSSID	SSID	Signal Strength	Security Mode	Wireless Mode	Action
1	00:06:5a:c6:2a:71	Colubris Network	39	WEP	11b/g	 

Screen – Unrecognized Access Points

Unrecognized Access Points table lists all the discovered nearby APs and displays following information:

Channel - The radio channel used by the access point.



BSSID - The MAC Address of the radio interface of the detected access point.

SSID - The radio SSID of the access point.



Signal Strength - The strength of the detected radio signal

Security Mode - Mode for encrypting the wireless traffic

Wireless Mode – Wireless protocol

Action – Click the icon  to mark the AP as authorized AP and move in the Authorized AP table.
Click the icon  to mark the AP as Rogue AP and move to the Rogue AP table.

Rogue Access Points

Rogue Access Points						
Channel	BSSID	SSID	Signal Strength	Security Mode	Wireless Mode	Action
11	00:06:5a:c6:2a:71	Colubris Network	24	WPA/AES	11b/g	 

Screen – Rogue Access Points

Rogue Access Points table lists all the APs marked as “Rogue” and displays following information:

Channel - The radio channel used by the access point.

BSSID - The MAC Address of the radio interface of the detected access point.


SSID - The radio SSID of the access point.

Signal Strength - The strength of the detected radio signal



Security Mode - Mode for encrypting the wireless traffic

Wireless Mode – Wireless protocol

Action – Click the icon  to mark the AP as authorized AP and move in the Authorized AP table.

Click the icon  to mark the AP as unrecognized AP and move to the Unrecognized AP table.

Authorized Access Points

Authorized Access Points						
Channel	BSSID	SSID	Signal Strength	Security Mode	Wireless Mode	Action
1	00:06:5a:c6:2a:71	Colubris Network	60	WPAPSK/TKIPAES	11b/g/n	 

Screen – Authorized Access Points

Authorized Access Points table lists all the APs marked as “Rogue” and displays following information:

Channel - The radio channel used by the access point.



BSSID - The MAC Address of the radio interface of the detected access point.

SSID - The radio SSID of the access point.


Signal Strength - The strength of the detected radio signal

Security Mode - Mode for encrypting the wireless traffic


Wireless Mode – Wireless protocol

Action – Click the icon  to mark the AP as unrecognized AP and move to the Unrecognized AP table. Click the icon  to mark the AP as Rogue AP and move to the Rogue AP table.

Authorize Access Points

All the discovered Access Points detected are regarded as unrecognized until they are identified as authorized for operation. To authorize an access point, click the icon  against the AP to be marked as authorized in the Unrecognized AP table.

Mark Access Point as Rogue

All the discovered Access Points detected are regarded as unrecognized until they are identified as authorized or rogue for operation. To mark an access point as rogue, click the icon  against the AP to be marked as rogue in the Unrecognized AP table.