Cyberoam WLAN Implementation Guide

Version 10

Document version 10.01.0416 - 1.0-29/10/2010

IMPORTANT NOTICE

Elitecore 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. Elitecore assumes no responsibility for any errors that may appear in this document. Elitecore reserves the right, without notice to make changes in product design or specifications. Information is subject to change without notice.

USER'S LICENSE

The Appliance described in this document is furnished under the terms of Elitecore's End User license agreement. Please read these terms and conditions carefully before using the Appliance. By using this Appliance, you agree to be bound by the terms and conditions of this license. If you do not agree with the terms of this license, promptly return the unused Appliance and manual (with proof of payment) to the place of purchase for a full refund.

LIMITED WARRANTY

Software: Elitecore warrants for a period of ninety (90) days from the date of shipment from Elitecore: (1) the media on which the Software is furnished will be free of defects in materials and workmanship under normal use; and (2) the Software substantially conforms to its published specifications except for the foregoing, the software is provided AS IS. This limited warranty extends only to the customer as the original licenses. Customers exclusive remedy and the entire liability of Elitecore and its suppliers under this warranty will be, at Elitecore or its service center's option, repair, replacement, or refund of the software if reported (or, upon, request, returned) to the party supplying the software to the customer. In no event does Elitecore warrant that the Software is error free, or that the customer will be able to operate the software without problems or interruptions. Elitecore hereby declares that the anti virus and anti spam modules are powered by Kaspersky Labs and Commtouch respectively and the performance thereof is under warranty provided by Kaspersky Labs and by Commtouch. It is specified that Kaspersky Lab does not warrant that the Software identifies all known viruses, nor that the Software will not occasionally erroneously report a virus in a title not infected by that virus.

Hardware: Elitecore warrants that the Hardware portion of the Elitecore Products excluding power supplies, fans and electrical components will be free from material defects in workmanship and materials for a period of One (1) year. Elitecore's sole obligation shall be to repair or replace the defective Hardware at no charge to the original owner. The replacement Hardware need not be new or of an identical make, model or part; Elitecore may, in its discretion, replace the defective Hardware (or any part thereof) with any reconditioned product that Elitecore reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware.

DISCLAIMER OF WARRANTY

Except as specified in this warranty, all expressed or implied conditions, representations, and warranties including, without limitation, any implied warranty or merchantability, fitness for a particular purpose, non-infringement or arising from a course of dealing, usage, or trade practice, and hereby excluded to the extent allowed by applicable law.

In no event will Elitecore or its supplier be liable for any lost revenue, profit, or data, or for special, indirect, consequential, incidental, or punitive damages however caused and regardless of the theory of liability arising out of the use of or inability to use the product even if Elitecore or its suppliers have been advised of the possibility of such damages. In no event shall Elitecore's or its supplier's liability to the customer, whether in contract, tort (including negligence) or otherwise, exceed the price paid by the customer. The foregoing limitations shall apply even if the above stated warranty fails of its essential purpose.
In no event shall Elitecore or its supplier be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual, even if Elitecore or its suppliers have been advised of the possibility of such damages.

RESTRICTED RIGHTS

CORPORATE HEADQUARTERS

Elitecore Technologies Ltd.
904 Silicon Tower,
Off. C.G. Road,
Ahmedabad – 380015, INDIA
Phone: +91-79-26405600
Fax: +91-79-26407640
Web site: www.elitecore.com , 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
eLitecore Technologies Ltd.
904, Silicon Tower
Off C.G. Road
Ahmedabad 380015
Gujarat, India.
Phone: +91-79-66065606
Fax: +91-79-26407640
Web site: www.elitecore.com

Cyberoam contact:
Technical support (Corporate Office): +91-79-26400707
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

This feature is applicable to CR15wi 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.

The Cyberoam CR15wi 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, CR15wi delivers comprehensive protection to small, remote and branch office users from threats like malware, virus, spam, phishing, and pharming attacks.

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.

CR15wi models, by default include one wireless interface called WLAN1.

Limitations

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

CR15wi supports 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
- WPA-Enterprise, WPA2-Enterprise

Note

This feature will be available only with Wi-Fi Appliances – Cyberoam CR15wi.

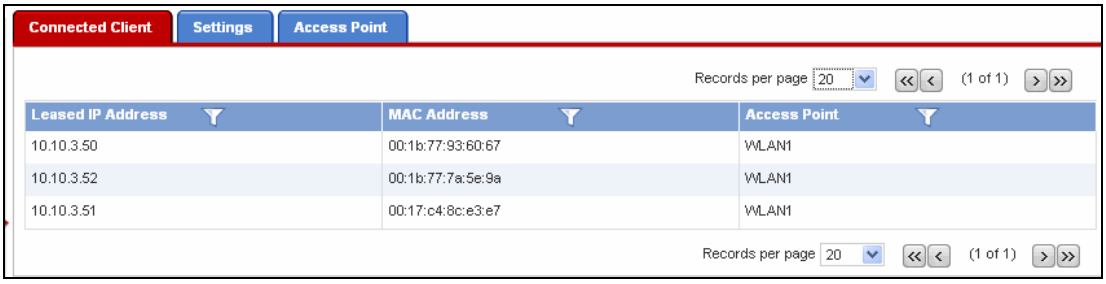
Connected Client

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



Screen – View Connection Status

Screen Elements	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	All the MAC addresses that exactly match the MAC address specified in the criteria. For example, if the search string is 10:15:18:A1:BC:22, all the addresses exactly matching the string will be displayed.
starts with	All the MAC addresses that starts with the specified search criteria. 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.
contains	All the MAC addresses that contain the string specified in the criteria. For example, if the search string is BC, all the MAC addresses like 10:15:18:A1:BC:22, containing the string are displayed.

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.

Screen – Search Access Point

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

Table – Search Access Point screen elements

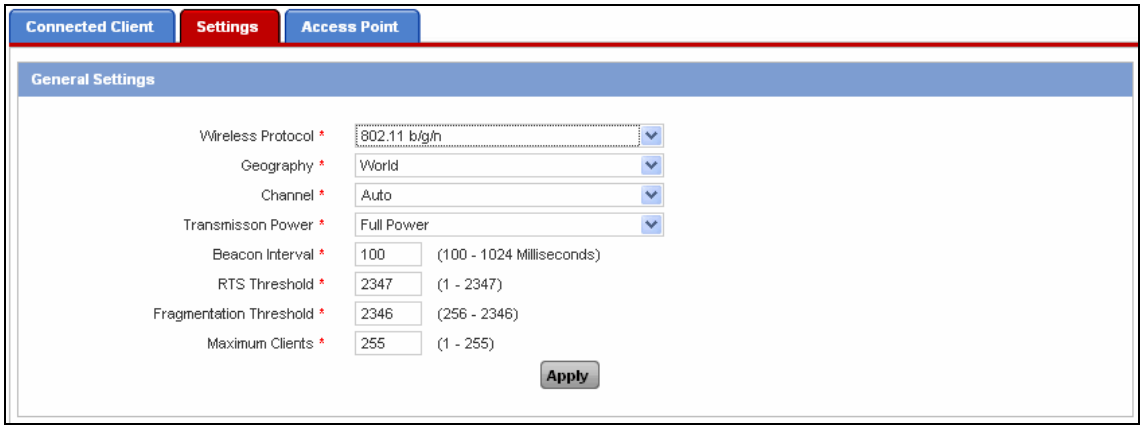
Settings

The page allows general configuration of Wireless LAN connection.

By default, CR15wi includes 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 Elements	Description
Wireless Protocol	Select the Wireless Protocol to be used. • 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. Default - 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 to a small area, select minimum. . **Available Options**: • Full Power • Half

	• Quarter • Eighth • Minimum Default value is - Full Power. Full power sends the strongest signal to the WLAN.
Beacon Interval	Specify the time interval between two beacon packets to be sent. **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. **Range**: 100 – 1024 milliseconds **Default value**: 100 milliseconds
RTS Threshold	Specify the threshold time before the RTS frames are sent. 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. If network throughput is slow or a large number of frame retransmissions are occurring, decrease the RTS threshold to enable RTS clearing. **Range**: 1 – 2347 **Default value**: 2346
Fragmentation Threshold	It is the maximum size of a data packet before it is broken into smaller packets, reducing the chance of packet collisions. CR15wi will allow specified number of bytes of fragmented data in the network. If the packet size is larger than the threshold, packets will be fragmented before transmission. **Range**: 256 – 2346 **Default value**: 2346
Maximum Clients	Specify the maximum number of clients that are allowed to connect across all the access points simultaneously. **Range**: 1 – 255 **Default value**: 255

Table – WLAN General Settings screen elements

Access Point

CR15wi 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 Cyberoam is deployed in Bridge mode.

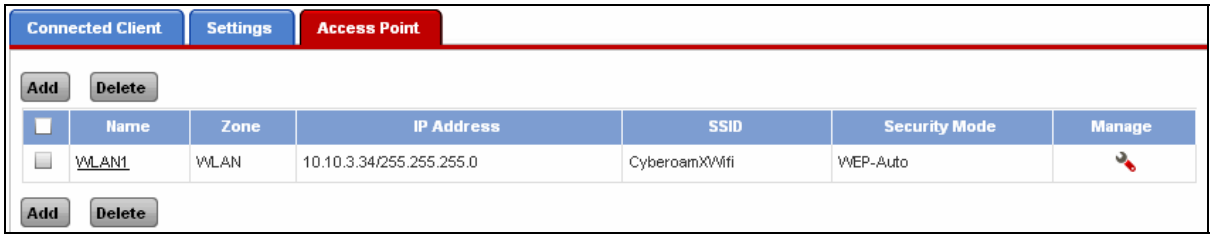
To manage access points, go to **Network → Wireless LAN → Access Point**. You can:

- 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



Screen – Manage Access Point

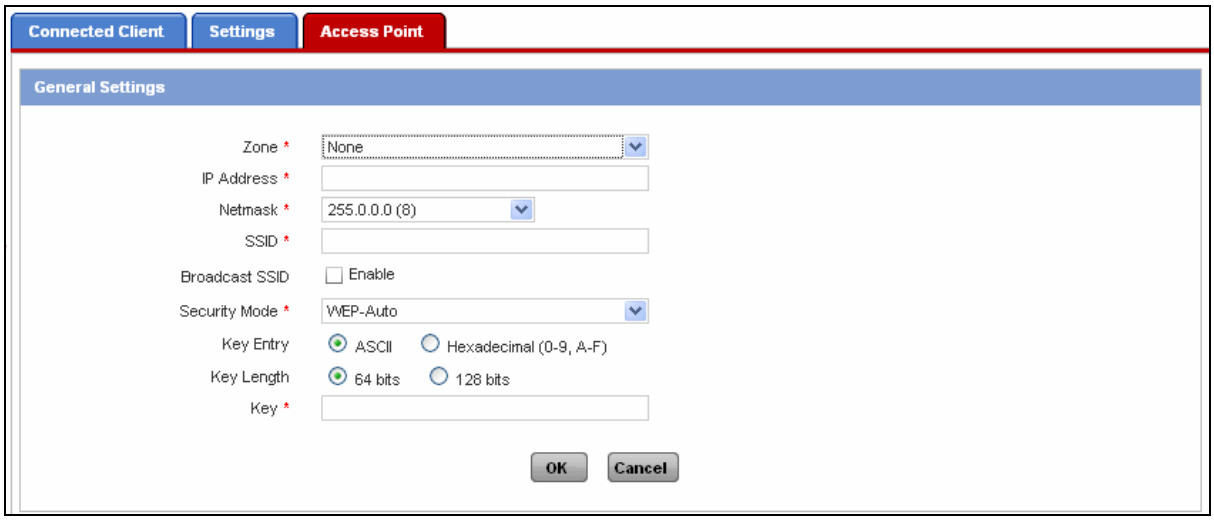
Screen Elements	Description
Add Button	Add a new Access Point.
Name	Name of the Access Point.
Zone	Zone of Access point. Access point can be the member of LAN zone only.
IP Address	IP Address and netmask for the access point. If Cyberoam is deployed as Bridge, IP address will not be displayed.
SSID	Unique 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	Security Mode selected. **Available Options**: • WEP-Open • WEP-Shared • WEP-Auto • WPA –PSK • WPA2-PSK • WPA-WPA2-PSK-Auto
Edit Icon	Edit the Access Point details
Delete Button	Delete the Access Point.

Table – Manage Access Point screen elements

Add Access Point

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.



Screen – Add Access Point

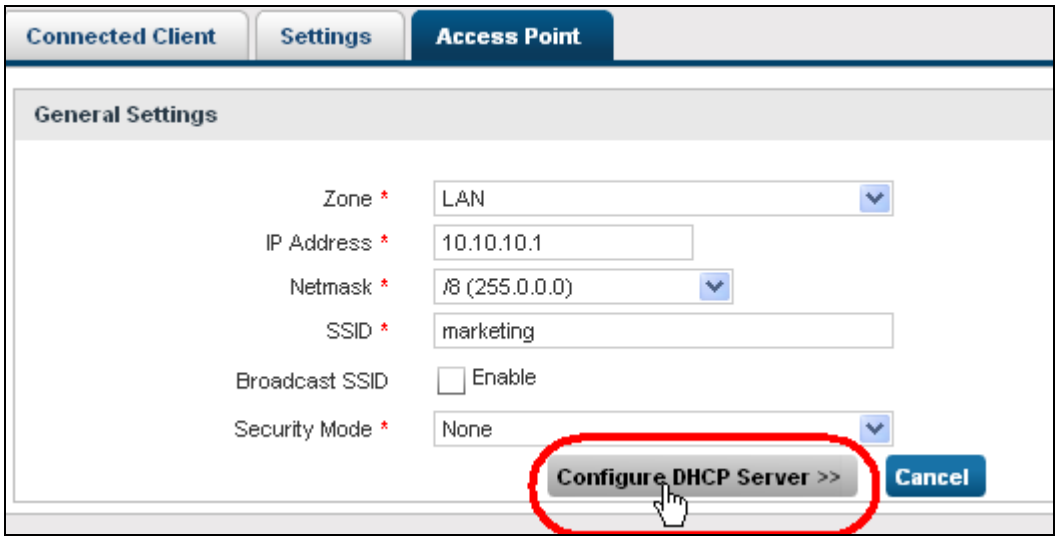
Screen Elements	Description
Zone	Select Zone for the Access Point. Access Point can be the member of LAN zone only.
IP Address	Specify IP Address for the Access Point.
Netmask	Specify subnet mask. In case of multiple Access points, each access point should be configured with unique subnet mask.
SSID	Specify Service Set Identifier (SSID). The access point is identified by its SSID. Users who want to use the wireless network must configure their computers with this SSID.
Broadcast SSID	Enable to broadcast the SSID.

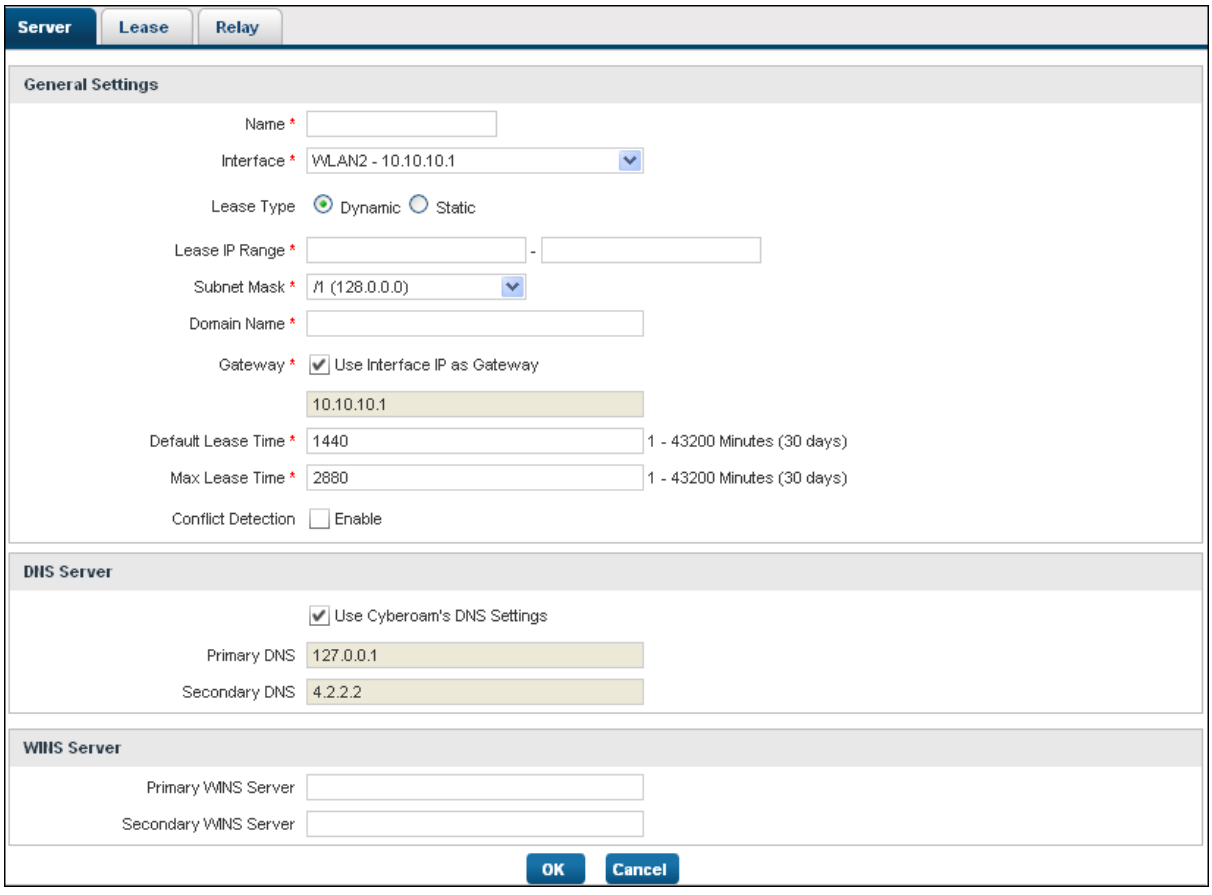
	Broadcasting the SSID enables clients to connect to your wireless network without knowing the SSID. For security purpose, do not broadcast the SSID as there will be less chances of an unwanted user connecting to your wireless network. If you choose not to broadcast the SSID, you need to forward SSID to your users so that they can configure their wireless devices.
Security Mode	Select the security mode for encrypting the wireless traffic. **Available Options**: • WEP-Open • WEP-Shared • WEP-Auto • WPA –PSK • WPA2-PSK • WPA-WPA2-PSK-Auto • WPA-Enterprise • WPA2-Enterprise WPA mode is better for security than WEP mode.
For WEP-Open, WEP-Shared and WEP-Auto only	
Key Entry	Select Key entry mode **Available Options**: ASCII or Hexadecimal
Key Length	Select the length of security key. A longer key length ensures better security. **Available Options**: 64 bit or 128 bit
Key	Specify security key for authentication.
For WPA –PSK, WPA2-PSK and WPA-WPA2-PSK-Auto only	
Encryption	Select the Encryption type **Available Options**: • TKIP – Temporal Key Integrity Protocol. It is a protocol for enforcing key integrity on a per-packet basis. • AES – Advanced Encryption Standard • Auto
Pass Phrase	Specify the phase to be used as password Range: 8 – 63 characters
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**: • TKIP – Temporal Key Integrity Protocol. It is a protocol for enforcing key integrity on a per-packet basis. • AES – Advanced Encryption Standard • Auto
Server IP and 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	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

The moment Access point is added successfully, you will be prompted to DHCP Server for the access point. Click Configure DHCP Server. You will be re-directed to DHCP Configuration page.





Screen Elements	Description

Name	Unique name for the DHCP server
Interface	Interface acting as an Access point
Lease Type	Select Lease Type. **Available Options**: • **Dynamic** - Specify range of IP address from which DHCP server must assign to the clients and subnet mask for the IP address range. It is also possible to configure multiple IP range for a same interface. • **Static** - If you always want to assign specific IP addresses to some or all clients, you can define static MAC address to IP address mappings. For defining, MAC-IP mapping, you should know the MAC address of the client's network card. The MAC address is usually specified in a hexadecimal digits separated by colons (e.g., 00:08:76:16:BC:21). Specify host name, MAC and IP address. Click Add icon  to add more than one MAC-IP mapping pair and Remove icon  to delete MAC-IP mapping pair.
Subnet Mask	Select subnet mask for the server.
Domain Name	Specify domain name that the DHCP server will assign to the DHCP Clients.
Gateway	Specify IP address for default Gateway or click "Use Interface IP as Gateway"
Default Lease Time	Specify default lease time and maximum lease time. Input range - 1 to 43200 seconds (30 days). Default - 1440 minutes
Max Lease Time	Specify maximum lease time. DHCP client must ask the DHCP server for new settings after the specified maximum lease time. Input range - 1 to 43200 seconds (30 days). Default - 2880 minutes
Conflict Detection	Enable IP conflict detection to check the IP before leasing i.e. if enabled the already leased IP will not be leased again. Can be configured only if lease type is "Dynamic"
DNS Server	Click "Use Cyberoam's DNS settings" to use Cyberoam DNS or Specify IP address of Primary and Secondary DNS servers
WINS Server	Specify IP address of Primary and Secondary WINS servers