



WiNG Express User Guide

For Version 5.9

Published: June 2017

Extreme Networks, Inc.
Phone / +1 408.579.2800
Toll-free / +1 888.257.3000

www.extremenetworks.com

© 2017 Extreme Networks, Inc. All rights reserved.

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries. All other names are the property of their respective owners. All other registered trademarks, trademarks, and service marks are property of their respective owners. For additional information on Extreme Networks trademarks, see www.extremenetworks.com/company/legal/trademarks.

P/N 9035125-01

Copyright © 2017 Extreme Networks, Inc. All rights reserved.

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see:

www.extremenetworks.com/company/legal/trademarks

Software Licensing

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at:

www.extremenetworks.com/support/policies/software-licensing

Support

For product support, phone the Global Technical Assistance Center (GTAC) at 1-800-998-2408

(toll-free in U.S. and Canada) or +1-408-579-2826. For the support phone number in other countries, visit: <http://www.extremenetworks.com/support/contact/>

For product documentation online, visit: <https://www.extremenetworks.com/documentation/>

Table of Contents

Introduction to WiNG Express	7
Basic WiNG Express Access Point Configuration	11
Dashboard.....	19
Dashboard.....	19
Monitor	21
Radios.....	21
Details.....	22
WLANs.....	23
Details.....	25
Clients	26
Details.....	27
Application Visibilty	29
Application	29
Category	31
Configuration	33
Basic	33
WiNG Assist	33
Startup Assist.....	33
Service Assist	35
Basic Settings.....	38
LAN.....	40
WAN.....	42
Wireless.....	44
Security.....	54
Firewall	54
WIPS	56
Application Visibility	58
Schedule Policy	61

Services.....	62
DHCP	62
RADIUS.....	65
Management.....	67
Access Points	70
Loading the Enterprise User Interface	72
Basic Access Point Settings	75
Event History.....	78
Event History	78

Preface

Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short [online feedback form](#). You can also email us directly at InternallInfoDev@extremenetworks.com.

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

- **GTAC (Global Technical Assistance Center) for Immediate Support**
 - Phone: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact
 - Email: support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- **GTAC Knowledge** — Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- **The Hub** — A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- **Support Portal** — Manage cases, downloads, service contracts, product licensing, and training and certifications.

Extreme Networks Publications

General

Product documentation is available at: <http://documentation.extremenetworks.com>. Release notes are available at: www.extremenetworks.com/support/release-notes

Open Source Declarations

Some software files have been licensed under certain open source licenses. More information is available at: www.extremenetworks.com/support/policies/software-licensing

Introduction to WiNG Express

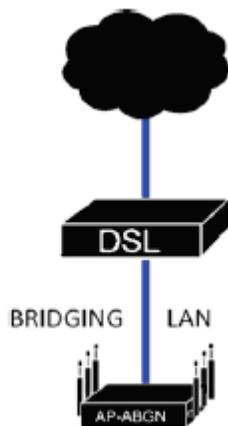
WiNG Express Access Points are specifically designed to meet the wireless deployment and radio coverage needs of small and mid-size businesses without compromising WLAN Enterprise class feature set and functionality.

WiNG Express is a simplified version of the existing operating system currently shipping with the WiNG family of controllers, service platforms and Access Points. WiNG Express Access Points utilize an easy-to-use, easy-to-understand graphic user interface that simplifies end-to-end WLAN management. WiNG Express enables the creation of a fully network-aware WLAN with the intelligence required to route wireless transmissions as efficiently and securely as possible.

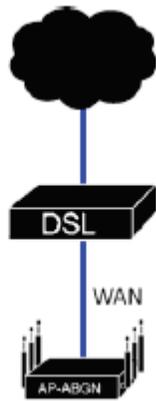
Within a WiNG Express managed network, a single Access Point can manage a network of up to 24 peer model Access Points, eliminating the need for a managing controller resource, thus simplifying initial deployments and their costs. Express Access Points can automatically discover, connect and provision peer model Access Points with a pre-defined network profile in just minutes.

WiNG Express Access Point portfolio consists of two dual radio 802.11ac Access Points (AP7502E and AP7522E) and four 802.11n Access Points (AP6511E, AP6521E, AP6522E and AP6562E).

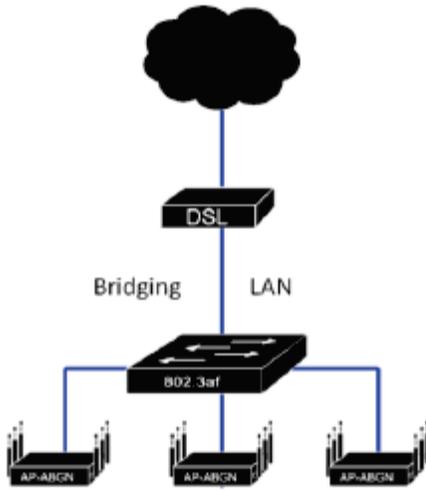
WiNG Express is designed for single-site Access Point deployments not exceeding more than 24 Access Points of the same model. The following network deployments are specifically targeted:



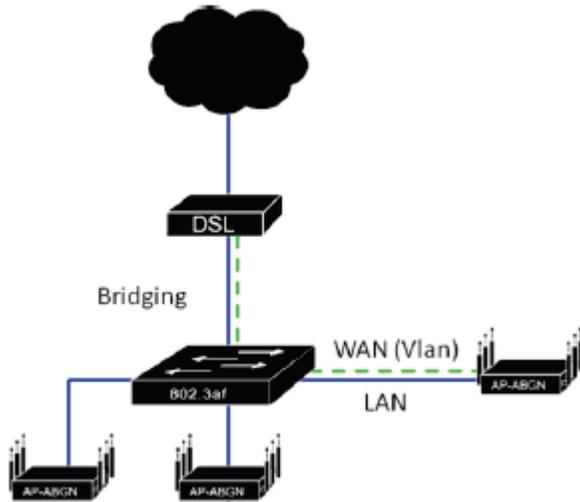
Case 1: Single AP deployment, LAN



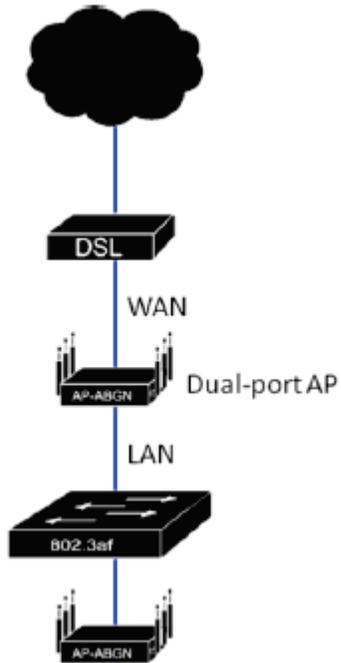
Case 2: Single AP deployment, WAN



Case 3: Multi AP deployment, LAN



Case 4: Multi AP deployment, WAN



Case 5: Multi AP dual-port deployment, WAN

Basic WiNG Express Access Point Configuration

For a WiNG Express SKU Access Point, both the WiNG Express UI and an *Over The Air* (OTA) provisioning configuration are required for a basic setup and network connection.

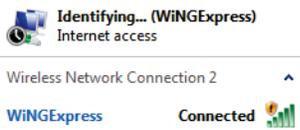
To set a basic configuration and access WiNG Express management functions:

1. Power up the Access Point.

The Access Point can be powered using an appropriately rated power adapter, POE injector or POE switch resource.

2. Connect to the Access Point.

Connect to the WiNG Express SSID. For Windows systems, locate the SSID by selecting the network icon on the bottom right corner of the screen. For MAC systems, locate the SSID by selecting the network icon on the top right corner of the screen.



Open a browser (Chrome, Firefox or Internet Explorer) and enter <https://express.extremenetworks.com/>.

The login screen displays.

3. Enter the default username **admin** in the **Username** field.
4. Enter the default password **admin123** in the **Password** field.
5. Select the **Login** button to load the management interface.

If this is the first time the WiNG Express interface has been accessed, a screen displays prompting for the Access Point's country code.

6. Select the **Country Code** specific to this Access Point's deployment location.

Selecting the correct country is central to legal operation. Each country has its own regulatory restrictions concerning electromagnetic emissions and the maximum RF signal strength that can be transmitted. Select Apply to implement the selected Country Code. SKU's only support certain countries (for example: a US SKU only includes US, Guam, Puerto Rico, American Samoa, US Virgin Islands and Mariana Island).

The Access Point automatically displays a Dashboard where users can assess network health and conduct a diagnostic performance review.

Note

At some point in the Access Point's initial setup, the default password should be changed to enhance the security of the network. Refer to the Configuration > Management screen to change the default password.

- Expand the **Configuration** menu item and select **Basic**.

Configuration -> Basic Settings

Basic Configuration Settings

AP Name: *

Country Name: *

Virtual Controller:

Timezone:

Date & Time: Hour: Mins: AM PM

NTP Server:

Controller Adoption

+ Add Delete	
Host	Level
<input type="text" value="192.168.1.55"/>	<input type="text" value="Local"/>
<input type="button" value="Update"/> <input type="button" value="Cancel"/>	

- Set the following Basic Configuration Settings for this Access Point:

AP Name - Provide an AP Name as this Access Point's WiNG Express network identifier. If setting this Access Point as a Virtual Controller, each Access Point managed by this Virtual Controller lists this Access Point's AP Name as its own. The AP Name is a required parameter.

Country Code - If the Country Code was not set when the Access Point was initially powered on, set the country now to ensure the Access Point's legal operation. The Access Point's wireless capabilities are disabled until the required country code is set.

Virtual Controller - Select this option to define this Access Point as a Virtual Controller capable of managing and provisioning up to 24 Access Points of the same model. If selecting this Access Point as a Virtual Controller, those Access Points managed by this Virtual Controller will list this Access Point's AP Name as its own. Only one Virtual Controller can be designated.

Timezone - Use the drop-down menu to specify the geographic timezone where the Access Point is deployed. Different geographic time zones have daylight savings clock adjustments, so specifying the timezone correctly is important to account for geographic time changes.

Date & Time - Set the date, hour and minute for the Access Point's current system time. Specify whether the current time is in the AM or PM.

NTP Server - Optionally provide the IP address of a NTP server resource. Network Time Protocol (NTP) manages time and/or network clock synchronization within the WiNG Express network. NTP is a client/server implementation. Access Points (NTP clients) periodically synchronize their clock with a master clock (an NTP server). For example, an Access Point resets its clock to 07:04:59 upon reading a time of 07:04:59 from its designated NTP server.

Controller Adoption - To adopt a controller enter the IP address in the Host field and select a Level from the drop-down menu.

9. Select **Apply** to implement the updates.
10. Expand the **Configuration** menu item and select **WAN**.

WAN Settings

Enable:

Port: ge1

Interface: vlan1

DHCP Client Static IP PPPoE Settings

Static IP/Mask: *

Primary DNS:

Secondary DNS:

Default Gateway:

11. Refer to the **WAN Settings** field and set the following:

Enable - Select this option to allow a connection between the Access Point and a larger network or outside world through the WAN port. Disable this option to isolate the WAN connection. No connections to a larger network or Internet are possible. Clients cannot communicate beyond configured subnets. Both the physical Port used to connect to the WAN and the *virtual Interface* (VLAN) are also listed and fixed.

DHCP Client - Select this option to enable DHCP for the Access Point WAN connection. This is useful, if the target network or *Internet Service Provider* (ISP) uses DHCP. DHCP is a protocol that includes mechanisms for IP address allocation and delivery of host-specific configuration parameters from a DHCP server to a host. Some of these parameters are IP address, network mask, and gateway. The WAN and LAN ports should not both be configured as DHCP clients.

Static IP - Select this option to bypass DHCP address allocation resources and manually set the IP address for the Access Point's WAN connection. Manually provide the Access Point's Static IP/Mask and Default Gateway.

PPPoE Settings - Optionally enable *Point-to-Point Protocol over Ethernet* (PPPoE) on the WAN network. If PPPoE is enabled, provide the required Auth Type, Login Name and Login Password. Server Name and Default Gateway are optional settings. PPP is a data-link protocol for dialup connections allowing an Access Point to use a broadband modem (DSL, cable modem, etc.) for access to high-speed data and broadband networks. Most DSL providers support (or deploy) the PPPoE protocol. PPPoE uses standard encryption, authentication, and compression as specified by the PPPoE protocol. PPPoE enables the Access Point to establish a point-to-point connection to an ISP over an existing Ethernet interface.

Static IP / Mask - Specify an IP address for the WAN connection if using static address assignment for the WAN port. An IP address uses a series of four numbers expressed in dot notation, for example, 190.188.12.1. Additionally, specify a Mask for the Access Point’s WAN connection. This number is available from the ISP for a DSL or cable-modem connection, or from an administrator if the Access Point connects to a larger network.

Primary/Secondary DNS/Default Gateway - If using a static IP or DHCP, enter the Primary and Secondary DNS server resource’s numerical IP address and Default Gateway.

Note
 Create a VLAN if segmenting traffic between the Access Point’s WAN and LAN. Complete steps 13 and 14 to define the required VLAN. Otherwise, proceed to step 15.

12. Select **Apply** to implement the updates.
13. Expand the **Configuration** menu item and select **Access Points**. Each **AP Name** displays as a link that can be selected to update the configuration of that specific Access Point. Select a target AP Name link from amongst those displayed in the Access Points screen.

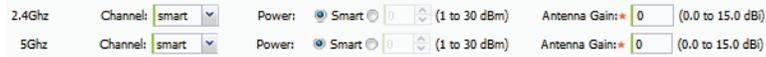
NAT Interface Settings

Number of Interfaces: 1				
Interface (1-4094)	Description	IP Address	NAT Enable	Edit
VLAN1		192.168.13.21/24	✘	✎

Refer to the **LAN IP Interface Settings** field, and add a VLAN and Static IP as required for enabling DHCP (within the Configuration > Services screen) for client IP address requests and ensuring routable traffic.

14. Select **Apply** to commit the updates to the selected Access Point’s configuration.
15. Expand the **Configuration** menu item and select **Wireless**.
 Use the Wireless screen to define radio and WLAN settings. Default radio settings remain as is for the Access Point’s basic setup.

In respect to the **Radio Settings**, the professional installer should be aware of the following:



Note

The above example includes a field for setting the antenna gain. This setting is only available for external antenna model Access Points.

The **Channels** available are channels for which the product is approved in its selected country. The professional installer must ensure the product is set to operate under conditions, and on channels, approved by country regulations.

Selecting **Smart** as the Power setting automatically configures radio power to not exceed the maximum power allowed by the defined country. For static power settings, the professional installer must ensure the configured power levels are compliant with local and regional regulations. The county selected automatically limits the maximum output power that can be set.

For external antenna model Access Points, configure the **Antenna Gain** based on the antenna used in the deployment. The set gain value should include the antenna gain, along with any additional components, such as extension cables used between the Access Point and the antenna.

In respect to the **Wireless LAN** settings, WiNG Express Access Points ship with a default WLAN (WINGExpress). However, this WLAN does not provide adequate authentication to protect from unauthorized user access. An additional WLAN configuration should be created and validated before deleting the default WLAN.

Wireless LAN

+ Add		Delete		Row Count: 1			
	Name	Enable	SSID	VLAN	Authentication Type	2.4GHz	5GHz
<input type="checkbox"/>	WINGExpress	<input checked="" type="checkbox"/>	WINGExpress	2100	captive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

16. To create a new WLAN, select **+ Add** from the upper, left-hand side of the **Wireless LAN** field.

Wireless LAN

Name: *

Enable:

SSID: * Client-To-Client Communication

Security: Open
 Secure-PSK
 Secure-802.1x
 Guest

Band: 2.4 GHz 5 GHz

VLAN: * (1 - 4094)

Description:

17. Set the following configuration attributes for the new WLAN:

Name - Provide a unique name for the WLAN as its network identifier. This is a required setting.

Enable - Select this setting to enable this WLAN within the Access Point managed network and provide some measure of data protection not available in the default WLAN.

SSID - Specify the WLAN's SSID. The WLAN SSID is case sensitive and alphanumeric. This SSID length should not exceed 32 characters. This is a required setting. Select **Client-To-Client Communication** to enable client interoperability within this WLAN. The default is disabled, meaning clients are not allowed to exchange packets with other clients. It does not necessarily prevent clients on other WLANs from sending packets to this WLAN, but if this setting is disabled on the other WLAN, clients are not permitted to interoperate at all.

Security - The screen displays with the **Open** option selected. Naming and saving such a policy (as is) would provide no security and might only make sense in a network wherein no sensitive data is either transmitted or received. This default setting is not recommended.

If selecting **Secure-PSK**, select an encryption type of WEP-64, WEP-128, TKIPCCMP and enter an encryption key. Define whether the key is entered in ASCII or HEX characters. Detailed security and encryption information is available in the **Configuration > Wireless** section of the documentation.

If selecting **Secure-802.1x**, provide an IP address (or hostname) and a shared secret (password) used to access an external RADIUS server resource for validating user requests to the Access Point's WLAN resources.

Selecting **Guest** displays fields for captive portal Web page creation, and is beyond the scope of this basic Access Point configuration.

Band - Select the 2.4 GHz and/or 5 GHz (if supported) radio bands supports by the Access Point and its connected client traffic. If this Access Point is designated as a Virtual Controller AP, both radio bands should be enabled.

VLAN - Use the spinner control to specify a VLAN from 1 - 4,094 for this WLAN. When a client associates with a WLAN, the client is assigned a VLAN by load balance distribution. Do not use VLAN 1 with the WLAN if the WAN port has been enabled.

Description - Optionally enter a WLAN description to further describe the WLAN's deployment objective within the WiNG Express managed network.

18. Select **Apply** to commit the updates to the Access Point's WLAN configuration.

19. Expand the **Configuration** menu item and select **Services**.

Configuration -> Services ?

DHCP **RADIUS**

This configuration will be applied only to the Virtual Controller

DHCP Settings

Enable DHCP Server

+ Add		Delete		Number of DHCP Pools: 1							
	Interface	IP	Default Gate	Primary DNS	Secondary Df	Start IP	End IP	Lease Time (da	Lease Time (hd	Lease Time (mi	
<input type="checkbox"/>	vlan2100	192.168...	192.168...	192.168...		192.168...	192.168...	1	0	0	

20. Select **Enable DHCP Server** to ensure the Access Point can provision IP addresses to requesting clients over the specified interface.

Note

A VLAN must be already configured and available to the DHCP server as a viable interface between the Access Point and requesting client. Refer to the LAN IP Interface Settings field (within the Edit Access Point screen), and add a VLAN.

Select **+ Add** and provide a default gateway, primary DNS server, and a starting and ending IP range of addresses that constitute a pool of addresses available to requesting clients. Additional DHCP options are available and are documented in the **Configuration > Services > DHCP** section.

21. Select **Apply** to commit the updates to the Access Point's DHCP configuration.
22. At this point, you're ready to connect to the network using the security restrictions applied to the newly created WLAN. Ensure the new secure WLAN has been enabled, and check whether a client is able to access the network.

**Note**

Only when the new WLAN configuration is validated as accessible should the existing WiNG Express default WLAN be deleted.

Dashboard

Dashboard

The dashboard enables administrators to review and troubleshoot Access Point managed network operation. Additionally, the dashboard allows an administrator to assess network component health and conduct a diagnostic review of device performance.

To review high-level Access Point dashboard information:

1. Select **Dashboard** in the main menu.



2. Review the following to assess the health of the network:

<p>System Information</p>	<p>Displays the administrator assigned device Name, software Version, Country Name for legal geographic deployment and number of detected Online and Offline Devices. This screen also lists whether this Access Point has been enabled as a Virtual Controller. The Access Point's IP address, MAC address and Current Time and Up Time also display. Virtual Controllers are capable of managing and provisioning either 24 or 64 Access Points of the same model. Only one Virtual Controller can be designated.</p>
<p>Client Segmentation</p>	<p>Displays a set of pie charts segregating WLAN utilization amongst peer Access Points and client types. Use this information to help assess whether client loads exceed the number and type of WLANs currently deployed with managed Access Points.</p>

Network Usage	Displays the network throughput (both in the transmit and receive directions) for the selected Radio or WLAN over the defined trending period of <i>30 minutes, 2 hours</i> or <i>24 hours</i> .
Client Count	Displays total network client count for the selected trending period of <i>30 minutes, 2 hours</i> or <i>24 hours</i> . Clients are partitioned into their current 2.4Ghz and 5Ghz radio bands to help assess whether the client load is adequately supported in each band.

Monitor

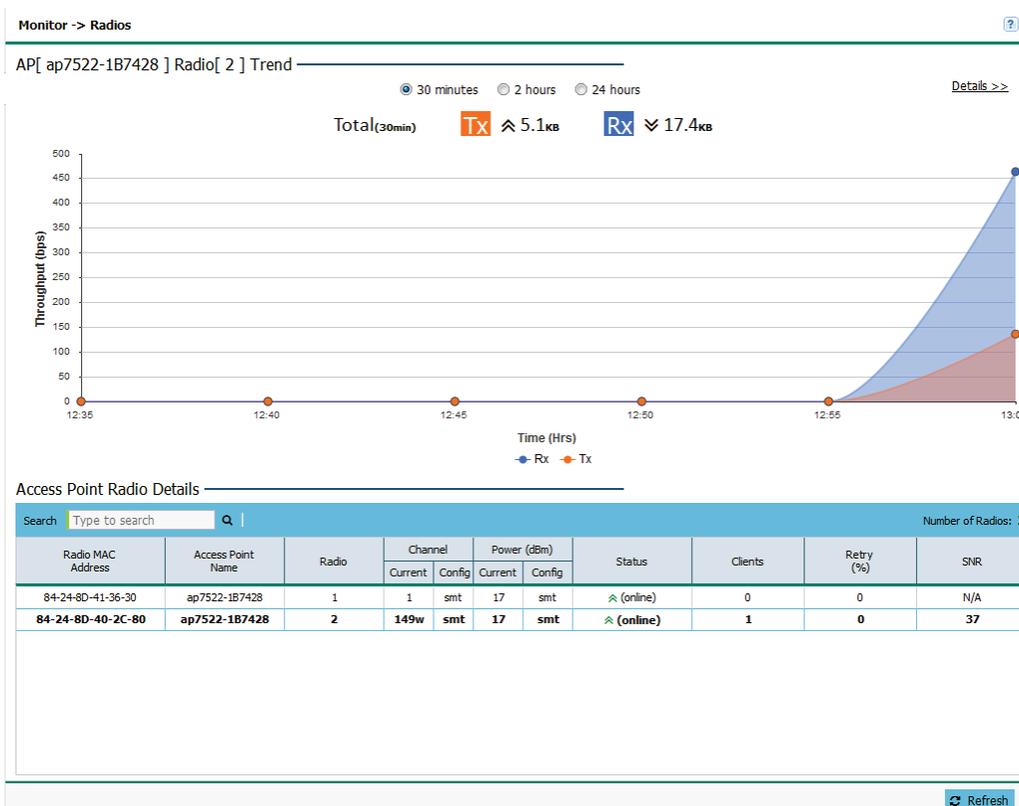
The **Monitor** screens provide detailed, real-time information about the network and RF health for Access Point Radios, WLANs and wireless Clients. Use the information on these screens to track RF traffic, throughput, signal to noise ratio and client health.

Radios

Use the **Radios** screen to assess the quality of the Access Point radio's utilization, power consumption, and client connections.

To monitor managed Access Point radios:

1. Select **Monitor** from the main menu and click on **Radios**.



2. Select a trending interval of **30 minutes**, **2 hours** or **24 hours** from the radio buttons at the top of the page. The graph updates accordingly with the radio's **Throughput**.
3. Review the following **Access Point Radio Details**:

Radio MAC Address	Displays the <i>Media Access Control</i> (MAC) address factory assigned to each radio as its hardware identifier on the network.
Access Point Name	Displays the Access Point's unique administrator assigned name provided upon initial configuration.

Radio	Displays the radio number for each Access Point radio on the network. AP6511 and AP6521 models are single radio models, other models support at least two radios.
Channel: Current / Config	Displays the current channel number each listed Access Point radio is set to transmit and receive on, as well as its configured channel number. The <i>Channels</i> available for configuration are channels for which the product is approved in its selected country. The professional installer must ensure the product is set to operate under conditions, and on channels, approved by country regulations.
Power (dBm): Current / Config	Displays the current power level in dBm for each Access Point radio as well as its configured power level. If <i>Smart</i> is the defined power setting, the radio automatically configures power to not exceed the maximum power allowed by the defined country. For static power settings, the professional installer must ensure the configured power levels are compliant with local and regional regulations. The country selected automatically limits the maximum output power that can be set.
Status	Displays the current operational status for each Access Point. If an Access Point is online, two green up arrows display. If an Access Point is offline, two green down arrows display.
Clients	Displays the number of clients currently associated to each Access Point radio on the network. AP6511 and AP6521 single radio Access Points support 128 clients, the other models support up to 256 client connections.
Retry (%)	Displays the retry percentage for packets sent on each Access Point radio. The retry rate helps assess the overall effectiveness of the RF environment (as displayed as a percentage) and a function of the connection rate in both directions.
SNR	Displays the connected client's <i>signal to noise ratio</i> (SNR). SNR is a measure that compares the level of a desired signal to the level of background noise. It is defined as the ratio of signal power to the noise power. A SNR of 45 or higher indicates excellent RF performance. A SNR of less than 15 indicates poor RF performance. A low SNR could warrant a different Access Point connection to improve performance.

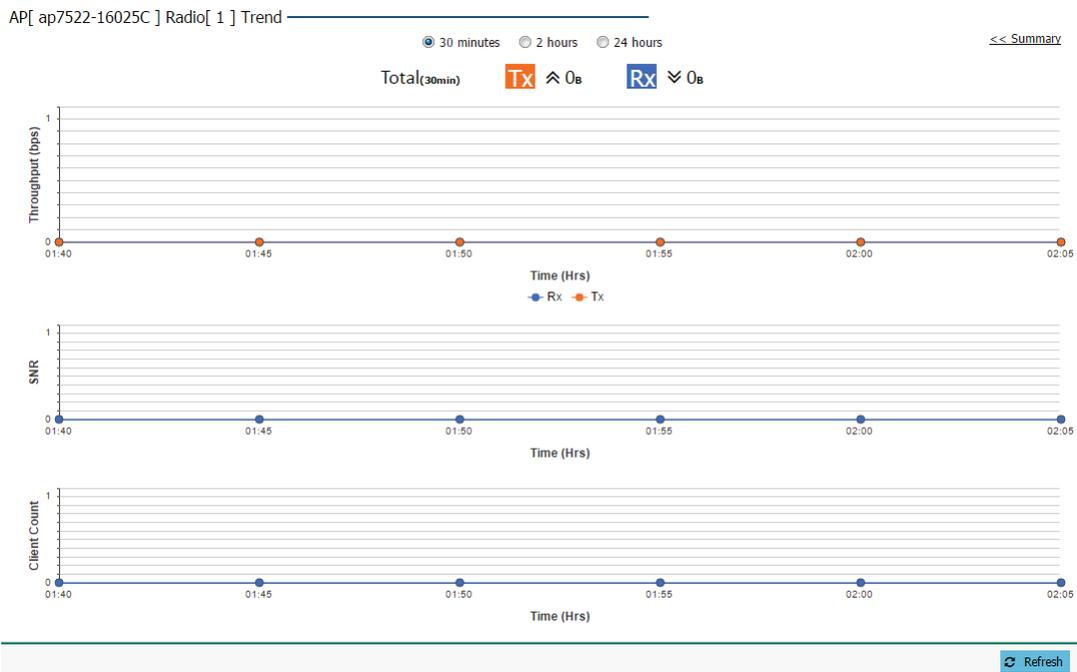
4. Select **Details** to assess individual Access point radio utilization data in greater detail.

Details

Access Point radio data can be analyzed to define periods where the radio's transmit and receive capabilities are jeopardized, or whether noise detected on the network is excessive and warrants administration. Client connections can also be reviewed to determine if the radio has an optimal number of connected client devices in respect to periods when the radio is over/under utilized.

To review Access Point radio details:

1. Select **Monitor** from the main menu and select **Radios**. Select a radio, then **Details**.



2. Select a reporting interval of **30 minutes**, **2 hours** or **24 hours** from the radio buttons at the top of the page. The graph updates accordingly with the radio's **Throughput**, **SNR** and **Client Count**.
3. Review the **Throughput (bps)** table to assess periods of heavy or light transmission and receive utilization over trended periods.

Transmitted packets display in blue, received packets in green.

4. Refer to the **SNR** field to assess periods where the Access Point's radio quality could be compromised due to excessive noise on the network.

Signal to noise ratio (SNR) is an interference measurement to help administrators assess whether an Access Point needs load balancing with the assistance of neighbor radios. Additionally, a low SNR could warrant power compensation to account for poorly performing radios. A SNR of 45 or higher indicates excellent RF performance. A SNR of less than 15 indicates poor RF performance.

5. Use the **Client Count** table to help determine whether the client load should be increased or decreased based on radio under/over utilization (throughput) and the level of interference detected on the managed network.

AP6511 and AP6521 single radio Access Points support 128 clients, other models support up to 256 client connections.

6. To return to the parent radio screen, select << **Summary** in the upper, right-hand, side of the graph.

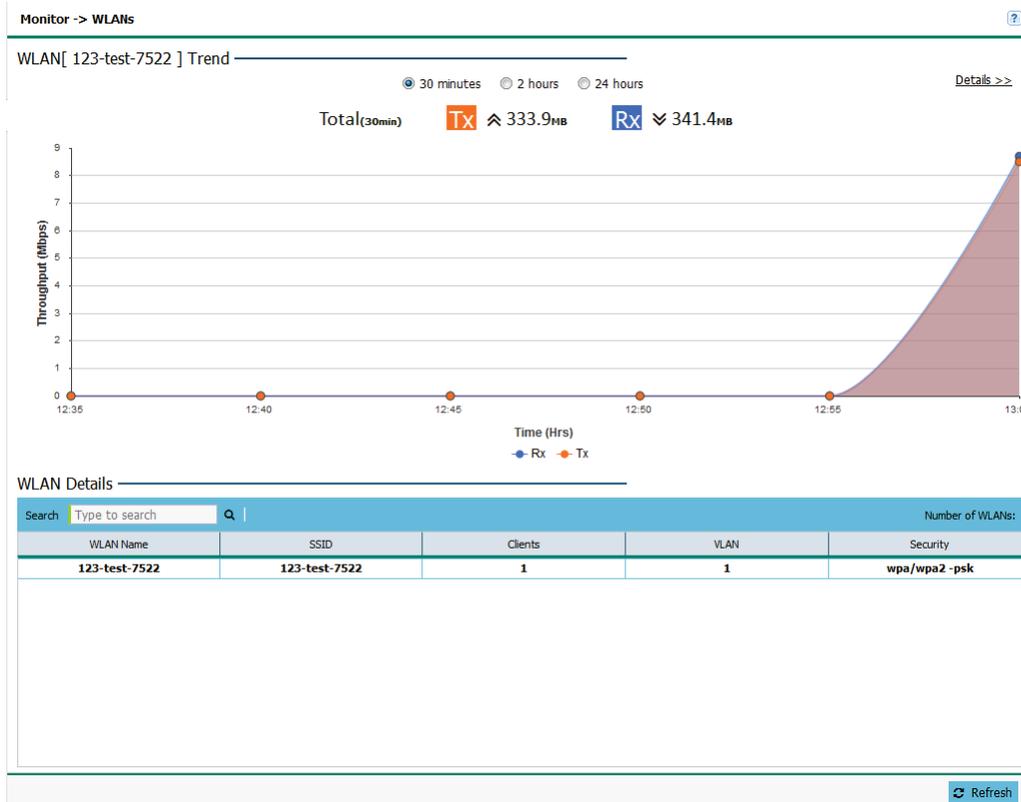
WLANs

A WLAN can be advertised from a single Access Point radio or can span multiple Access Points and radios. WLAN configurations can be defined to only support specific areas of a site. For example a guest access WLAN may only be mapped to a 2.4GHz radio in a lobby or conference room providing limited coverage, while a data WLAN is mapped to all 2.4GHz and 5GHz radios at the branch site providing complete coverage.

Periodically refer to the WLANs screen to monitor an Access Point's WLAN utilization and whether WLAN usage is consistent with an Access Point's deployment objective and the security needs of its connected clients.

To review Access Point's WLAN utilization:

1. Select **Monitor** from the main menu and select **WLANs**.



2. Select a reporting interval of **30 minutes**, **2 hours** or **24 hours** from the radio buttons at the top of the page. The graph updates accordingly with the radio's **Throughput**.
3. Review the following WLAN information to help determine whether the Access Point's WLAN utilization is optimally set for its deployment objective:

WLAN Name	Displays the administrator defined WLAN name for each of the WLANs. Spaces between words are not permitted in the name. The name could be a logical representation of the WLAN's coverage area (engineering, marketing etc.). The name cannot exceed 32 characters.
SSID	Displays the network identifier <i>Services Set Identification</i> (SSID) associated with the WLAN. The maximum number of characters for the SSID is 32.
Clients	Displays the collective number of clients comprising the WLAN's membership, as pooled from each of the Access Points in this listed WLAN.
VLAN	Displays the VLAN ID to which the WLAN is mapped.

Security	<p>Displays the encryption and/or authentication security settings, if any, applied to Access Point traffic. Authentication ensures only known and trusted users or devices access a WLAN's network resources.</p> <p><i>Encryption</i> is central for WLAN security, as it provides data privacy for traffic forwarded over a WLAN. When the 802.11 specification was introduced, <i>Wired Equivalent Privacy</i> (WEP) was the primary encryption mechanism. New device deployments should use either WPA or WPA2 encryption.</p> <p><i>Authentication</i> is enabled per WLAN to verify the identity of both users and devices. Authentication is a challenge and response procedure for validating user credentials such as username, password and secret-key information.</p> <p>A <i>captive portal</i> configuration provides secure authenticated access using a standard Web browser. Captive portals provide authenticated access by capturing and re-directing a wireless user's Web browser session to a captive portal login page where the user must enter valid credentials to access to the network.</p>
-----------------	--

- To review more granular details of a specific WLAN, select it from the table and select the **Details >>** link.

Details

A WLAN's configuration can be periodically reviewed in detail to assess whether its configuration still supports the deployment objectives of those Access Points utilizing it, or if configuration changes are needed to better support network client connections.

To review Access Point information in detail:

- Select **Monitor** from the main menu and click on **WLANs**.



- Select a reporting interval of **30 minutes**, **2 hours** or **24 hours** from the radio buttons at the top of the page. The graph updates accordingly with the radio's **Throughput** and **Client Count**.
- Refer to the following throughput and client data for the selected WLAN:

Throughput	Displays the WLAN's time trended throughput (as impacted by the Access Point's utilizing this WLAN) in both the transmit and receive directions. Use the Throughput table to assess periods of heavy or light transmission and receive utilization over trended periods. Transmitted packets display in blue, received packets in green.
Client Count	Displays the time trended number of clients comprising the WLAN's membership, as pooled from all the Access Points in this WLAN. AP6511 and AP6521 single radio Access Points support 128 clients, other models support up to 256 client connections.

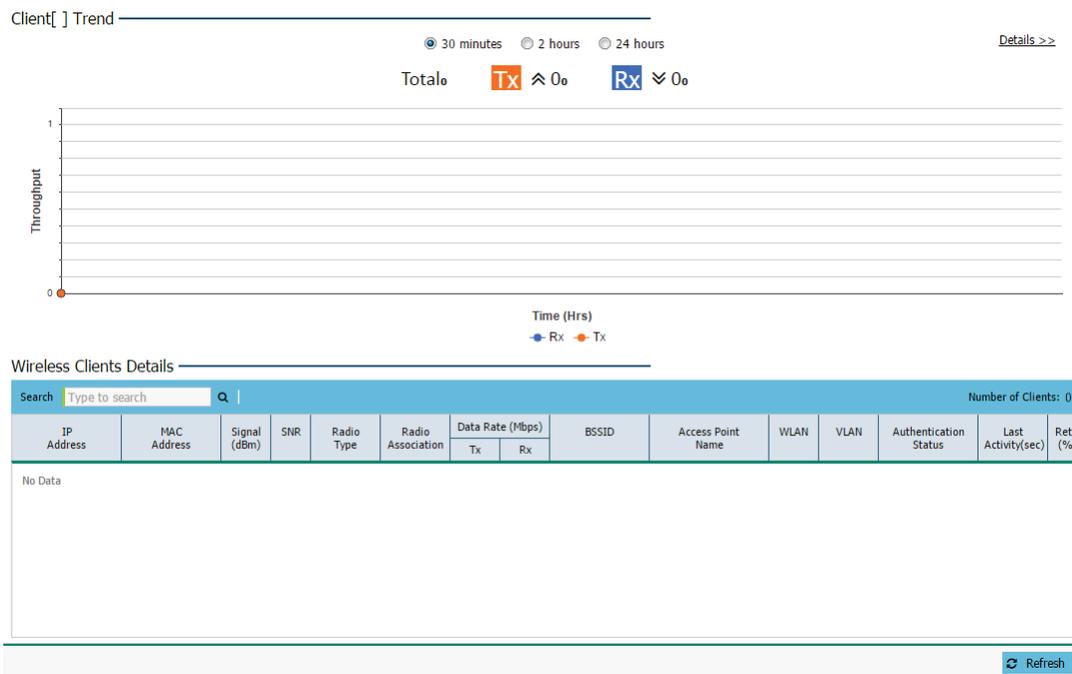
4. To return to the WLAN screen, select << Summary.

Clients

Refer to the **Clients** screen to assess performance on specific wireless client interfaces.

To review an Access Point's wireless interface connection utilization:

1. Select **Monitor** from the main menu and click on **Clients**.



2. Select a reporting interval of **30 minutes**, **2 hours** or **24 hours** from the radio buttons at the top of the page. The graph updates accordingly with the radio's **Throughput**.

3. Review the following information for clients connected to managed Access Point radios:

IP Address	Displays the current IP address the client is using as its network identifier.
MAC Address	Displays the <i>Media Access Control</i> (MAC) address factory assigned to each wireless client as its unique hardware network identifier.
Signal (dBm)	Displays the client radio's current power level in dBm. Use this information to assess whether client performance could be improved by connecting to a different Access Point.

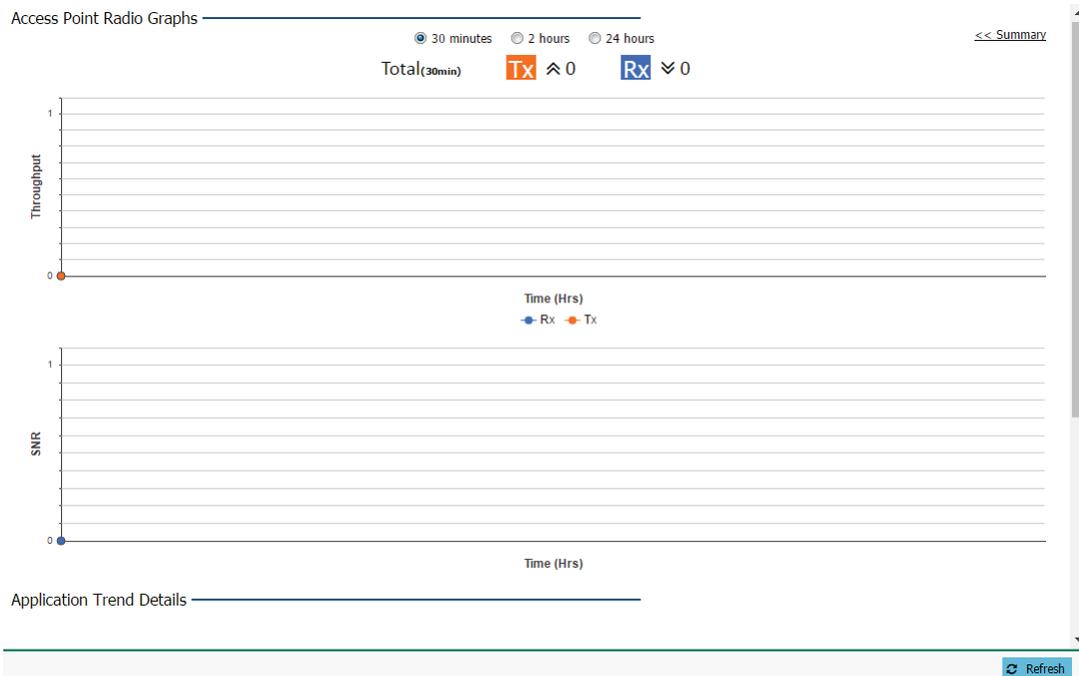
SNR	Displays the connected client's <i>signal to noise ratio</i> (SNR). SNR is a measure that compares the level of a desired signal to the level of background noise. It is defined as the ratio of signal power to the noise power. A SNR of 45 or higher indicates excellent RF performance. A SNR of less than 15 indicates poor RF performance. A low SNR could warrant a different Access Point connection to improve performance.
Radio Type	Lists the 802.11 radio types present in the wireless client. AP7502 and AP7522 models are capable of 802.11ac connections.
Radio Association	Displays the AP radio that each listed client is associated with.
Data Rate (Mbps) Tx / Rx	Displays the listed client radio's transmit and receive data rates (in Mbps). Use this information to assess RF activity versus other client radios in the same radio coverage area.
BSSID	Displays the BSSID of the managed Access Point establishing the client's wireless connection.
Access Point Name	Displays the Access Point's unique administrator assigned name provided upon initial configuration.
WLAN	Displays the WLAN's <i>Services Set Identification</i> (SSID) the wireless client is currently associated with.
VLAN	Displays the VLAN (virtual LAN) number the wireless client is marked to pass traffic on.
Authentication Status	Displays the authentication type in use by the wireless client to secure a connection to its associated WLAN.
Activity Last (sec)	Displays the last detected transmit and receive activity for the listed client within the Access Point radio coverage area.
Retry (%)	Displays the retry percentage for packets sent on each client radio. The retry rate helps assess the overall effectiveness of the RF environment (as displayed as a percentage) and a function of the connect rate in both directions.
Vendor	Displays the device manufacturer for each wireless client connected to the managed network.

Details

Refer to the **Clients** screen to assess performance on specific wireless client interfaces.

To review an Access Point's wired interface connection utilization:

1. Select **Monitor** from the main menu and click on **Clients**.
2. Select **Details** to display the **Client Details** graph.



3. Select a reporting interval of **30 minutes**, **2 hours** or **24 hours** from the radio buttons at the top of the page. The graph updates accordingly with the radio's **Throughput** and **SNR**.
4. Refer to the following throughput and client data for the selected clients:

<p>Throughput</p>	<p>Displays the WLAN's time trended throughput (as impacted by the Access Point's utilizing this WLAN) in both the transmit and receive directions. Use the <i>Throughput</i> table to assess periods of heavy or light transmission and receive utilization over trended periods. Transmitted packets display in blue, received packets in green.</p>
<p>SNR</p>	<p>Refer to the SNR field to assess periods where the client's radio quality could be compromised due to excessive noise on the network.</p> <p>Displays the connected client's <i>signal to noise ratio</i> (SNR). SNR is a measure that compares the level of a desired signal to the level of background noise. It is defined as the ratio of signal power to the noise power. A SNR of 45 or higher indicates excellent RF performance. A SNR of less than 15 indicates poor RF performance. A low SNR could warrant a different Access Point connection to improve performance.</p>

5. Refer to **Application Trend Details** for recurring application category details on the AP.
6. To return to the Clients screen, select **<< Summary**.

Application Visibility

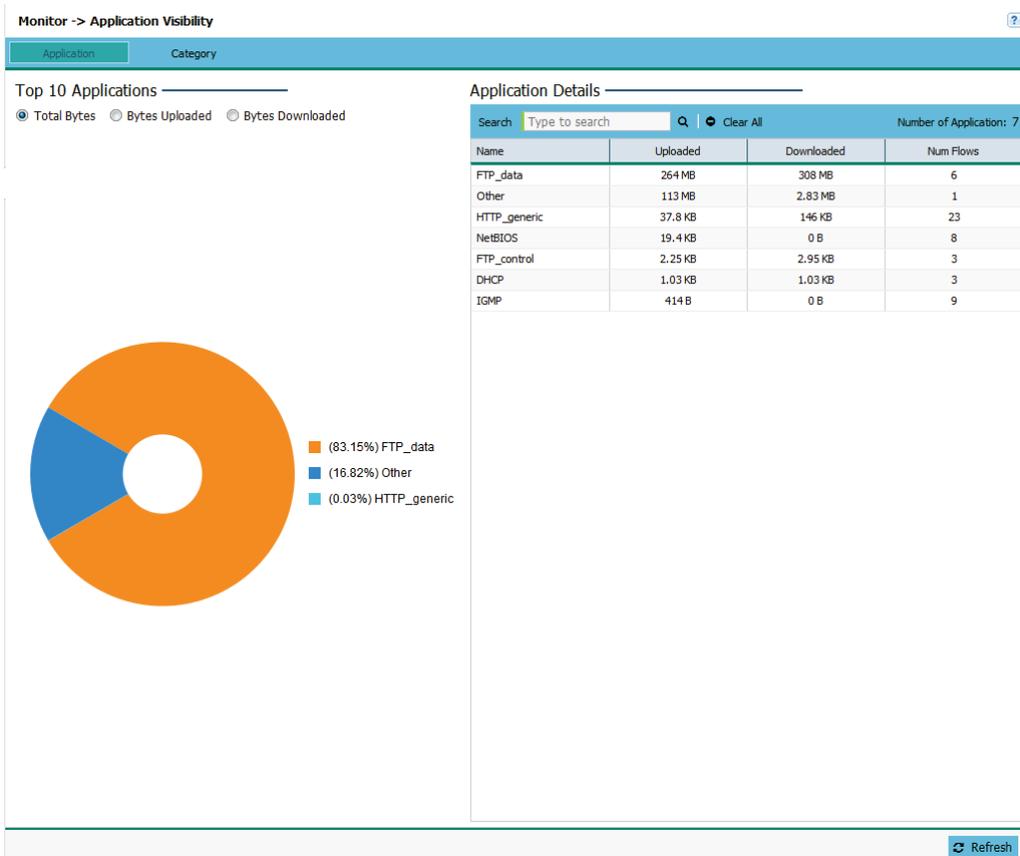
Deep packet inspection (DPI) is an advanced packet filtering technique functioning at the application layer. Use DPI to find, identify, classify, reroute or block packets containing specific data or codes that other packet filtering techniques (examining only packet headers) cannot detect.

Enable DPI to scan data packets passing through the network. The contents of each packet are scanned, occasionally logged and blocked or routed to their destination. Deep packet inspection helps an ISP block the spread of viruses, illegal downloads and prioritize data transmitted by bandwidth-heavy applications (video and VoIP applications) to help prevent network congestion.

Application

To monitor application visibility:

1. Select **Monitor** from the main menu and click on **Application Visibility**.



2. Refer to the **Top 10 Applications** graph to assess the most prolific, and allowed, application data passing through member devices.

Total Bytes	Displays the top ten utilized applications in respect to total data bytes passing through the managed network. These are only the administrator allowed applications approved for proliferation within the network.
--------------------	---

Bytes Uploaded	Displays the top ten applications in respect to total data bytes uploaded through the managed network. If this application data is not aligned with application utilization expectations, consider allowing or denying additional applications and categories or adjusting their precedence (priority).
Bytes Downloaded	Displays the top ten applications in respect to total data bytes downloaded from the managed network. If this application data is not aligned with application utilization expectations, consider allowing or denying additional applications and categories or adjusting their precedence (priority).

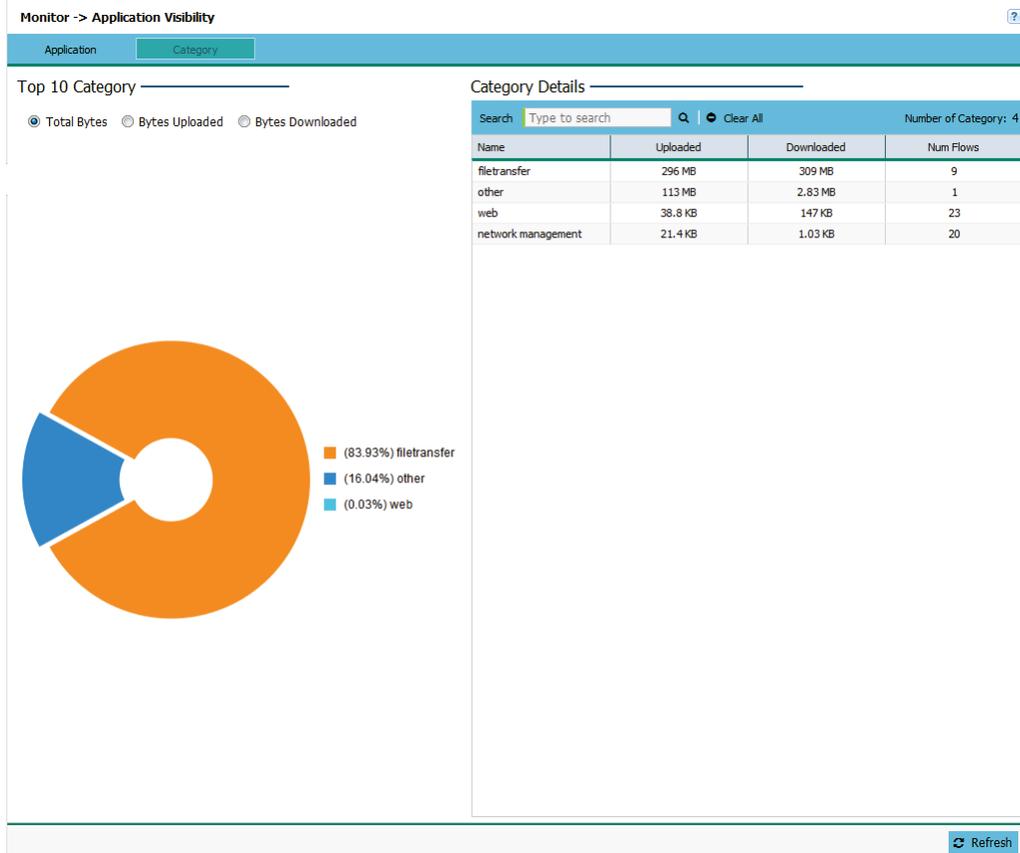
3. Refer to the **Application Details** table to assess specific application data utilization:

Name	Lists the allowed application name whose data (bytes) is passing through the managed network.
Uploaded	Displays the amount of uploaded application data (in bytes) passing the through the managed network.
Downloaded	Displays the amount of downloaded application data (in bytes) passing the through the managed network.
Num Flows	Lists the total number of application data flows passing through the network for each listed application. An application flow can consist of packets in a specific connection or media stream. Application packets with the same source address/port and destination address/port are considered one flow.
Clear All	Select this option to clear the application data counters and begin a new assessment.

Category

To monitor application category information:

1. Select **Monitor** from the main menu and click on **Application Visibility**.



2. Refer to the **Top 10 Category** graph to assess the most prolific, and allowed, application data categories.

Total Bytes	Displays the top ten application categories in respect to total data bytes passing through the managed network. These are only the administrator allowed application categories approved for proliferation within the network.
Bytes Uploaded	Displays the top ten application categories in respect to total data bytes uploaded through the managed network. If this category data is not aligned with application utilization expectations, consider allowing or denying additional categories or adjusting their precedence (priority).
Bytes Downloaded	Displays the top ten application categories in respect to total data bytes downloaded from the managed network. If this category data is not aligned with application utilization expectations, consider allowing or denying additional categories and categories or adjusting their precedence (priority).

3. Refer to the **Category Details** table to assess specific application category data utilization:

Name	Lists the allowed category whose application data (in bytes) is passing through the network.
-------------	--

Uploaded	Displays the number of uploaded application category data (in bytes) passing the through the network.
Downloaded	Displays the number of downloaded application category data (in bytes) passing the through the network.
Num Flows	Lists the total number of application category data flows passing through devices. A category flow can consist of packets in a specific connection or media stream. Packets with the same source address/port and destination address/port are considered one flow.
Clear All	Select this option to clear the application category data counters and begin a new assessment.

Configuration

The Configuration screens contain the settings needed to configure basic device information and wired and wireless network settings, security, DHCP, access management and Access Point settings.

Basic

WiNG Assist

Use WiNG Assist to define an AP7522, AP7532, AP7562 or AP7622 model Access Point's basic configuration with a minimum required number of steps. Two separate configuration options are available, **Startup Assist** and **Service Assist**, depending on your network's routing and captive portal (hotspot) requirements.

Creating a Service Assist configuration requires a wireless LAN configuration be defined first using Startup Assist before WAN and LAN updates can be defined using Service Assist. If logging in using a factory default configuration, Startup Assist automatically displays. Otherwise, both Startup Assist and Service Assist can be launched at any time from the upper-left of the **Basic Configuration** screen.

Startup Assist

Start up Assist

Start up assist provides the basic setup information required to get one wireless LAN operational. Optionally, you may enable the guest portal. For Detailed configuration, Please access the appropriate page

Virtual Controller:

Country Name: * India-in

Timezone: Asia/Calcutta

Date & Time: 03/15/2016 Hour: 12 Mins: 31 AM PM

WLAN Settings

WLAN 1 Name: wlan1

Authentication: Open PSK

Key (If PSK):* Show Ascii Hex

WLAN 2 Name: wlan2

Authentication: Open PSK

Key (If PSK):* Show Ascii Hex

Use **Startup Assist** to deploy an Access Point wireless LAN in an existing network with a router and DHCP services.

Note

Startup Assist configuration updates overwrite existing settings. To delete or update Startup Assist configuration settings, either rerun Startup Assist or navigate to where those parameters appear in the user interface and update them accordingly.

To provide the Access Point a basic configuration using the minimum number of configuration steps:

1. Power the Access Point using an appropriate power adapter, PoE injector, or PoE switch.
2. Connect to the Access Point.
 - a) If deploying an Express Access Point, connect to the “ExpressXXYY” SSID.
 - b) If deploying an Enterprise Access Point, the default IP address is located on the backside of the Access Point.
3. Enter the default username **admin**.
4. Enter the default password **admin123**.

If logging in using a factory default configuration, **Startup Assist** automatically displays. Otherwise, it can be initiated at any time from the upper-left of the Basic Configuration screen.

Note

Startup Assist automatically sets the radio transmit power and enables Auto Channel selection. The Access Point’s name is automatically assigned based on the Access Point type plus the last three octets of the device’s hardcoded MAC address. WLAN 1 and WLAN 2 both use VLAN ID 1 by default. To adjust any of these parameters, edit the appropriate configuration screen directly.

5. Set the following Startup Assist parameters:

Virtual Controller - Select this option to define the Access Point as a Virtual Controller capable of managing and provisioning up to 24 Access Points of the same model (AP6511, AP6521, AP6522 or AP7502) or 64 Access Points of the same model (AP7522, AP7532, AP7562 or 7622). If defining this Access Point as a Virtual Controller, those Access Points managed by this Virtual Controller will list this Access Point’s AP Name as its own. Only one Virtual Controller can be designated.

Country Name - Set the country specific to this Access Point’s deployment location. Selecting the correct country is central to legal operation. Each country has its own regulatory restrictions concerning electromagnetic emissions and the maximum RF signal strength that can be transmitted.

Timezone - Use the drop-down menu to specify the geographic timezone where the Access Point is deployed. Different geographic time zones have daylight savings clock adjustments, so specifying the timezone correctly is important to account for geographic time changes.

Date & Time -Set the date, hour and minute for the Access Point’s current system time. Specify whether the current time is in the AM or PM.

WLAN 1 Name - Provide a unique name for this WLAN as its network identifier. This is a required setting. The WLAN name assigned is used for the network identifying SSID and is assigned to both of the Access Point's radios.

Authentication - Select PSK to apply a 64 character maximum passphrase. The authenticating device must use the same PSK algorithm during authentication. Selecting Show displays the key in exposed plain text (not recommended).

Selecting **Open** is not a recommended authentication scheme, as it would provide the Access Point's WLAN no security via credential exchange and would only make sense in a network where no sensitive data is either transmitted or received.

Key (If PSK) - If using PSK, enter a WPA2 Key to password protect the WLAN. Define whether the key is entered in ASCII or HEX (hexadecimal string) characters. Selecting *Show* to expose the key is not recommended.

WLAN 2 (optional) - If a second WLAN is required enter the *WLAN 2 Name*, *Authentication* and *Key* in the associated fields. WLAN 2 is an optional setting.

6. Select **Apply** to save and commit the Startup Assist changes to the Access Point's configuration. Select **Discard** to revert to the last saved configuration.

The Virtual Controller, Country Name, Timezone and Date & Time portions of the Basic Settings screen update with the settings applied and saved in Startup Assist screen. WLAN updated made in Startup Assist are displayed in Wireless screen, not the Basic Configuration screen.

Service Assist

Service Assist

Service assist will configure routing, NAT and DHCP using common configuration assumptions. For detailed configuration please access the appropriate page.

WAN IP Type: DHCP Static IP

WLAN/LAN DHCP server: Yes No

Guest Portal: Yes No

Affected WLAN:*

i For Virtual Controller, Please allow VLAN 2200 on GE1 of the AP and on your switch's GE as well.

Apply
Discard

Use Service Assist to deploy a new Access Point functioning as a router and a DHCP server. This is a common deployment scenario when utilizing a wireless hotspot.

Note

Service Assist configuration updates overwrite existing WAN and LAN settings. To delete or update Service Assist configuration settings, either rerun Service Assist or navigate to where those parameters appear in the WAN and LAN user interface screens and update them accordingly.

1. To set an Access Point's Service Assist configuration, begin with Startup Assist and create at least one wireless LAN.
2. Power the Access Point using an appropriate power adapter, PoE injector, or PoE switch.
3. Connect to the Access Point.
 - If deploying an Express Access Point, connect to the "ExpressXXYY" SSID.
 - If deploying an Enterprise Access Point, the default IP address is located on the backside of the Access Point.
4. Enter the default username **admin**.
5. Enter the default password **admin123**.

If logging in using a factory default configuration, Startup Assist automatically displays.

6. Create a **Startup Assist** configuration with at least one complete wireless LAN defined, then return to the next step in this section.
7. Select the **Service Assist** button from the upper, left-hand, side of the Basic Configuration screen.

Note

Service Assist automatically assigns a VLAN ID of 2300 for the WAN's VLAN.

8. Set the following Service Assist parameters:

WAN IP Type – Select DHCP to enable the Access Point to obtain its IP address and network configuration from a DHCP server running on the upstream network. For example, many *Internet Service Providers* (ISP) use DHCP to provide network addresses. Select Static IP to bypass DHCP address allocation and manually set the IP address for the Access Point's WAN connection.

Note

If utilizing DHCP for the Access Point's WAN, primary DNS is provided by the DHCP client on VLAN 2300.

WLAN/LAN DHCP Server – Select this option to enable the Access Point's on-board DHCP server and NAT firewall. By default, the DHCP server is the 192.168.200.x network. To adjust DHCP server options, edit the DHCP server configuration screen directly.

Guest Portal – Select Yes to enable a wireless LAN to operate as an open guest network with a captive portal. When enabled, the company name is added to the default portal page. No authentication is enabled however. Guests see a portal page entitled "High Speed Internet offered by <Company Name>."

Affected WLAN - Select the wireless LAN that you wish to operate as a guest portal. To make advanced configuration changes to the default captive portal, directly edit the captive portal configuration screen.

9. Select **Apply** to save and commit the Service Assist changes to the Access Point's configuration. Select **Discard** to revert to the last saved configuration.

When **Service Assist** settings are applied, the WAN and LAN pages of the user interface update with their new values. The settings applied in the Service Assist page do not update any of the values in the Basic Configuration screen.

Refer to the **Basic** screen to set many of the basic parameters required to get the Access Point up and running with little additional configuration.

Basic Settings

To configure an Access Point's basic settings:

1. Select **Configuration Settings** from the main menu, then select **Basic**.

The **Basic Configuration Settings** screen also displays the first time a user connects to the user interface on an unconfigured Access Point.

2. Configure the following **Basic Configuration Settings**:

AP Name	Provide an AP Name used as this Access Point's administrative network identifier. If setting this Access Point as a Virtual Controller, each Access Point managed by this Virtual Controller lists this Access Point's AP Name as its own. The AP Name is a required parameter.
Country Name	If the Country Name was not set when the Access Point was initially powered on, set the country now to ensure the Access Point's legal operation. The Access Point's wireless capabilities are disabled until the required country name is set.
Virtual Controller	Select this option to define the Access Point as a Virtual Controller capable of managing and provisioning up to 24 Access Points of the same model (AP6511, AP6521, AP6522 or AP7502) or 64 Access Points of the same model (AP7522, AP7532, 7562 or 7622). If selecting this Access Point as a Virtual Controller, those Access Points managed by this Virtual Controller lists this Access Point's AP Name as its own. Only one Virtual Controller can be designated.

Timezone	Use the drop-down menu to specify the geographic timezone where the Access Point is deployed. Different geographic time zones have daylight savings clock adjustments, so specifying the timezone correctly is important to account for geographic time changes.
Date & Time	Set the date, hour and minute for the Access Point's current system time. Specify whether the current time is in the AM or PM.
NTP Server	Optionally provide the IP address of a NTP server resource. <i>Network Time Protocol</i> (NTP) manages time and/or network clock synchronization within the network. NTP is a client/server implementation. Access Points (NTP clients) periodically synchronize their clock with a master clock (an NTP server). For example, an Access Point resets its clock to 07:04:59 upon reading a time of 07:04:59 from its designated NTP server.
Adoption MTU	Specify the <i>Maximum Transmission Unit</i> (MTU) used by the Access Point. The MTU is the largest physical packet size in bytes a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent. Select <i>Local</i> to optimize the MTU for local network traffic. Select <i>VPN</i> to optimize MTU for transmission over a <i>Virtual Private Network</i> (VPN). Select <i>Custom</i> to specify a specific MTU value in bits between 900 and 1500.
Adoption Mode	Specify the adoption mode for Access Points. Select <i>Controller</i> to allow adoption of supported Access Points by this device. Select <i>Cloud</i> to allow to allow adoption of devices using the cloud. Select <i>Auto</i> to let the device select its Adoption Mode.

Note

Changing the Country Name resets the Access Point's radio(s). During the reset there is no communication with the Access Point through its wireless interfaces. When the reset is complete, communication with the Access Point is restored.

3. In the **Controller Adoption** settings enter a controller **Host** and **Level** using **+Add**. Remove existing controller entries using **Delete**.

Note

A maximum of two controllers may be added using the GUI. Additional controllers may be added using the command line interface.

- When all required settings are configured, click **Apply** to save the changes to the **Basic Configuration Settings**.

LAN

Refer to the **LAN** screen to set the virtual controller's wired interfaces.

To configure an Access Point's wired interface settings:

- Select **Configuration** settings from the main menu then select **LAN**.

LAN Port Settings

Number of Interfaces: 1				
Port	Enable	Allowed VLAN (1-5,6,9)	Untagged VLAN (1-4094)	Edit
ge1	✓		1	✎

IP Settings

Go to Access Points page to add interfaces with static IP addresses

Number of IP Interfaces: 1				
Interface	Description	DHCP Client	Edit	
VLAN1		✓	✎	

Apply Discard

The **LAN** page is divided into **LAN Port Settings** and **IP Settings** fields.

Note

Changes made to an Access Point's Configuration are pushed (provisioned) to Access Points of the same model.

2. Configure the following **LAN Port Settings** for each LAN port:

Port	<p>Displays the physical interface (GE1, FE1, etc.) for each Access Point wired connection on the network. Supported Access Point models have unique physical interface connections. Supported interfaces include:</p> <p><i>AP6511</i> - FE1, FE2, FE3, FE4, UP1/POE</p> <p><i>AP6521</i> - GE1/POE (LAN)</p> <p><i>AP6522</i> - GE1/POE (LAN)</p> <p><i>AP6562</i> - GE1/POE (LAN)</p> <p><i>AP7502</i> - GE1, FE1, FE2, FE3</p> <p><i>AP7522</i> - GE1/POE (LAN)</p> <p><i>AP7532</i> - GE1/POE (LAN)</p> <p><i>AP7562</i> - GE1/POE (LAN)</p> <p><i>AP7622</i> - GE1/POE (LAN)</p>
Enable	Select <i>Enable</i> to allow traffic on the selected wired interface. To disable wired traffic on a specific Access Point interface, uncheck the box.
Allowed VLAN	Displays allowed VLANs for traffic routing on each Access Point's wired port.
Untagged VLAN	Displays the VLAN(s) untagged traffic is transmitted and received on.
Edit	Select <i>Edit</i> to make changes to the selected interface.

3. Configure the following **IP Settings** for each VLAN interface:

Note

VLAN interfaces may also be added, edited or deleted on the Configuration > Access Points screen in the IP Settings tab.

Interface	Displays the LAN connection's numeric VLAN interface where LAN traffic has been segregated.
Description	Optionally provide a description for each VLAN interface.
DHCP Client	Select DHCP to provision IP Address and Mask information using a DHCP Server. DHCP is a protocol that includes mechanisms for IP address allocation and delivery of host-specific configuration parameters from a DHCP server to a host. Some of these parameters are IP address, network mask, and gateway. To manually configure network addresses, uncheck the DHCP check box and enter an IP Address and subnet mask.
Edit	Select <i>Edit</i> to make changes to the selected interface.

Add	Select to <i>Add</i> create a new VLAN interface.
Delete	To delete VLAN interfaces select the VLAN(s) and click <i>Delete</i> .

WAN

Refer to the **WAN** screen to set specific Access Point wide area network interfaces.

To configure an Access Point's WAN interface settings:

1. Select **Configuration** settings from the main menu then select **WAN**.

Configuration -> WAN ?

WAN Settings

Enable:

Port: ge1

Interface: vlan1

DHCP Client
 Static IP
 PPPoE Settings

Static IP/Mask:

Primary DNS:

Secondary DNS:

Default Gateway:

NAT Interface Settings

Number of Interfaces: 2				
Interface (1-4094)	Description	IP Address	NAT Enable	Edit
VLAN1	WAN Interface	1.1.1.85/24	✘	✎
VLAN200		192.168.22.1/24	✔	✎

2. Configure the following **WAN Settings**:

Enable	Select this option to allow a connection between the Access Point and a larger network or outside world through the WAN port. Disable this option to isolate the WAN connection. No connections to a larger network or Internet are possible. Clients cannot communicate beyond configured subnets. Both the physical Port used to connect to the WAN and the <i>Virtual Local Area Network</i> (VLAN) interface are fixed.
Port	Select the physical port connected to the WAN interface. The available port list varies based on device model.
Interface	Displays the WAN connection's numeric VLAN interface where WAN traffic has been segregated.

DHCP Client	Select this option to enable DHCP for the Access Point WAN connection. This is useful, if the target network or <i>Internet Service Provider</i> (ISP) uses DHCP. DHCP is a protocol that includes mechanisms for IP address allocation and delivery of host-specific configuration parameters from a DHCP server to a host. Some of these parameters are IP address, network mask, and gateway. The WAN and LAN ports should not both be configured as DHCP clients.
Static IP / Mask	Select this option to bypass DHCP address allocation resources and manually set the IP address for the Access Point's WAN connection. Manually provide the Access Point's Static IP/Mask and Default Gateway.
PPPoE Settings	Optionally enable <i>Point-to-Point Protocol over Ethernet</i> (PPPoE) on the WAN network. If PPPoE is enabled, provide the <i>Login Name</i> , <i>Login Password</i> , <i>Server Name</i> , <i>Default Gateway</i> , <i>Primary DNS</i> and <i>Secondary DNS</i> IP addresses. PPP is a data-link protocol for dialup connections. PPPoE allows an Access Point to use a broadband modem (DSL, cable modem, etc.) for access to high-speed data and broadband networks. Most DSL providers support (or deploy) the PPPoE protocol. PPPoE uses standard encryption, authentication, and compression methods as specified by the PPPoE protocol. PPPoE enables Access Points to establish a point-to-point connection to an ISP over an existing Ethernet interface.
Login Name	When enabling PPPoE, provide the login name provided by your ISP.
Login Password	When enabling PPPoE, provide the password associated to the login name provided by your ISP.
Server Name	When enabling PPPoE, provide a server name if required by your ISP.
Static IP / Mask	Select this option to bypass DHCP address allocation resources and manually set the IP Address for the Access Point's WAN connection. Manually provide the Access Point's Static IP/Mask and Default Gateway.
Primary DNS	When using a static IP, enter an IP Address for the main DNS server resource for the Access Point's WAN interface.
Secondary DNS	When using a static IP, enter an IP Address for the backup (secondary) Domain Name Server providing DNS services for the Access Point's WAN interface.
Default Gateway	When using a static IP, enter the IP Address of the network's default gateway. A default gateway provides an entry/exit point for the network as it commonly connects an internal network to an external network.

3. The NAT Interface Settings section displays the following:

Interface	Display's the NAT interface's numeric VLAN interface (1-4094) where traffic has been segregated.
Description	Displays the description configured each NAT entry configured in the <i>Configuration > Access Points</i> edit screen.
IP Address	Displays the IP Address for each configured NAT interface.

NAT Enable	Displays if <i>Network Address Translation</i> (NAT) is enabled on the selected interface. NAT converts an IP address in one network to a different IP address or set of IP addresses in another network. The Access Point's router maps its local (Inside) network addresses to WAN (Outside) IP addresses and translates the WAN IP addresses on incoming packets to local IP addresses. NAT is useful because it allows the authentication of incoming and outgoing requests, and minimizes the number of WAN IP addresses needed when a range of local IP addresses is mapped to each WAN IP address.
------------	---

Wireless

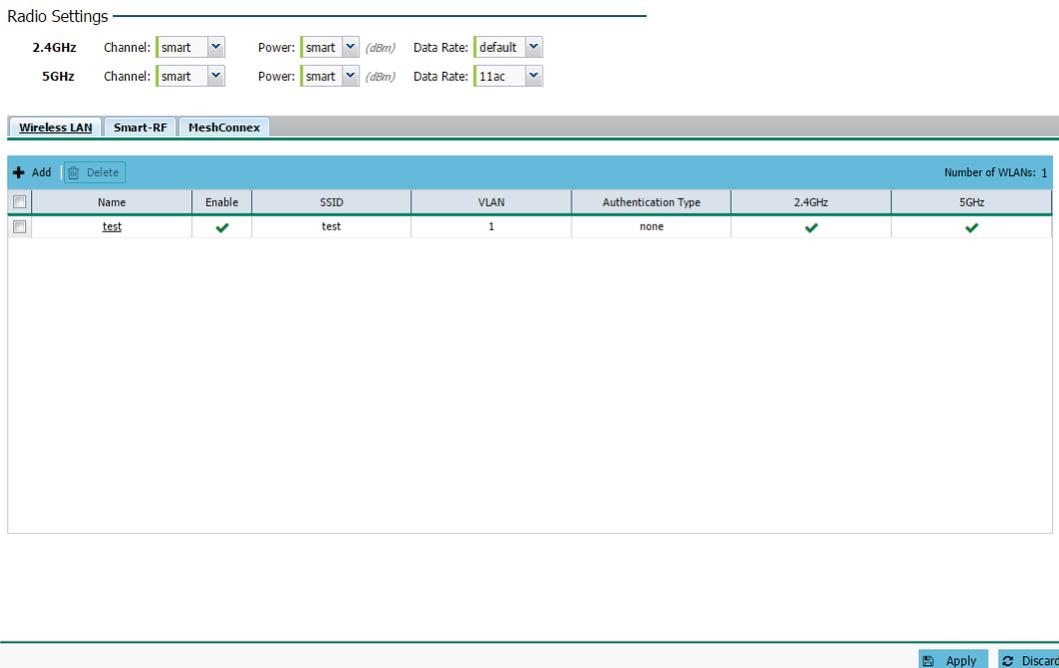
A *Wireless Local Area Network* (WLAN) is a data-communications system and wireless local area network that flexibly extends the functionalities of a wired LAN. A WLAN links two or more devices using spread-spectrum or OFDM modulation based technology. A WLAN does not require lining up devices for line-of-sight transmission, and are thus, desirable for wireless networking. Roaming users can be handed off from one wireless controller connected Access Point to another, like a cellular phone system. WLANs can therefore be configured around the needs of specific user groups, even when they are not in physical proximity.

WLANs are mapped to radios on each connected Access Point. A WLAN can be advertised from a single Access Point radio or can span multiple Access Points and radios. WLAN configurations can be defined to only provide service to specific areas. For example a guest access WLAN may only be mapped to a 2.4GHz radio in a lobby or conference room providing limited coverage, while a data WLAN is mapped to all 2.4GHz and 5GHz radios at the branch site providing complete coverage.

Periodically refer to the **Wireless** screen to monitor an Access Point's WLAN utilization and whether WLAN usage is consistent with an Access Point's deployment objective and the security needs of its connected clients.

To configure WLAN properties to be complimentary with Access Point deployment objectives and client support needs:

1. Select **Configuration** settings from the main menu then select **Wireless**.



The **Wireless** screen is partitioned into **Radio Settings**, **Wireless LAN**, **Smart RF** and **MeshConnex** fields.

Note

Changes made to an Access Point's Configuration are pushed (provisioned) to Access Points of the same model.

2. Configure the following **Radio Settings** for the 2.4Ghz and 5Ghz radios:

Channel	Use the drop-down menu to select a channel for the 2.4Ghz or 5Ghz radio. To enable automatic channel selection based on RF conditions, select <i>Smart</i> from the drop-down menu. The channels available for configuration are channels for which the product is approved in its selected country. The professional installer must ensure the product is set to operate under conditions, and on channels, approved by country regulations.
Power	Specify a radio power for the 2.4Ghz or 5Ghz radio or select <i>Smart</i> to let the Access Point manage the power settings based on network conditions. Selecting <i>Smart</i> as the Power setting automatically configures radio power to not exceed the maximum power allowed by the defined country. For static power settings, the professional installer must ensure the configured power levels are compliant with local and regional regulations. The county selected automatically limits the maximum output power that can be set.
Data Rate	Use the drop-down menu to specify the data transmission rate for probe response transmissions. Options are specific to each device model and radio type but may include, <i>default</i> , <i>11bgn(802.11b/g/n)</i> , <i>11gn(802.11g/n)</i> , <i>11n(802.11n)</i> , <i>11an(802.11a/n)</i> , <i>11anac(802.11a/n/ac)</i> and <i>11nac(802.11n/ac)</i> .

3. Select **+Add** to add a new WLAN. To edit an existing WLAN, select the name of that WLAN. To remove an existing WLAN highlight it and select **Delete**.

The **Wireless LAN** edit screen displays.

4. Specify the following for each managed WLAN:

Name	Add or edit a name for the WLAN. This name is used throughout the user interface as a network identifier.
Enable	Displays a green check mark if the WLAN (and all its unique configuration attributes) is enabled for Access Point utilization, and a red X if the WLAN is disabled.
SSID	Specify the WLAN's network identifier SSID. The WLAN SSID is case sensitive and alphanumeric. SSID length should not exceed 32 characters.
Hide	Select this option to disable broadcast of the SSID used by this WLAN.
Client-To-Client Communications	Select this option to enable client message exchanges within this WLAN. The default is enabled, meaning clients are allowed to exchange packets with other clients. It does not necessarily prevent clients on other WLANs from sending packets to this WLAN, but as long as this setting also disabled on that WLAN, clients are not permitted to interoperate.
Band	Select 2.4Ghz or 5Ghz (or both) to specify radio band support for an Access Point's requesting clients on this WLAN.
VLAN	Use the spinner control to specify a VLAN from 1 - 4,094 for this WLAN. When a client associates with a WLAN, the client is assigned a VLAN by load balance distribution. Do not use VLAN 1 with the WLAN if the WAN port has been enabled.
Description	Optionally, enter descriptive text to help differentiate this WLAN from others with similar configurations.
Security	<p>Displays the WLAN Authentication type. Authentication is enabled per WLAN to verify the identity of both users and devices. Authentication is a challenge and response procedure for validating user credentials such as username, password and sometimes secret-key information.</p> <p>The screen displays with the <i>Open</i> option selected. Naming and saving such a policy (as is) would provide no security and might only make sense in a network wherein no sensitive data is either transmitted or received. This default setting is not recommended.</p> <p>If selecting <i>Secure-PSK</i>, select an encryption type for the WLAN. Define whether the key is entered in ASCII or HEX characters. Selecting Show to expose the key is not recommended.</p>

<p>Encryption (Secure-PSK only)</p>	<p>When Secure-PSK security is selected, use the drop-down menu to select an encryption type. Available encryption types include:</p> <p><i>WEP-64 - Wired Equivalent Privacy (WEP)</i> is a security protocol specified in the Wi-Fi standard. WEP is designed to provide a WLAN with a level of security and privacy comparable to that of a wired LAN. WEP can be used with open, shared, MAC and 802.1X EAP authentications. WEP is optimal for WLANs supporting legacy deployments when also used with 802.1X EAP authentication to provide user and device authentication and dynamic WEP key derivation and periodic key rotation. 802.1X provides authentication for devices and also reduces the risk of a single WEP key being deciphered. If 802.1X support is not available on the legacy device, MAC authentication should be enabled to provide device level authentication. WEP 64 uses a 40-bit key concatenated with a 24-bit <i>initialization vector (IV)</i> to form the RC4 traffic key. WEP 64 is a less robust encryption scheme than WEP 128 (containing a shorter WEP algorithm for a hacker to potentially duplicate), but networks that require more security are at risk from a WEP flaw. WEP is only recommended when clients are incapable of using more robust forms of security. The existing 802.11 standard alone offers administrators no effective method to update keys.</p> <p><i>WEP-128</i> - WEP 128 uses a 104-bit key which is concatenated with a 24-bit <i>initialization vector (IV)</i> to form the RC4 traffic key. WEP may be all a small-business user needs for the simple encryption of wireless data. However, networks that require more security are at risk from a WEP flaw. WEP is only recommended if there are client devices incapable of using higher forms of security. The existing 802.11 standard alone offers administrators no effective method to update keys. WEP 128 provides a more robust encryption algorithm than WEP 64 by requiring a longer key length and pass key. Thus, making it harder to hack through the replication of WEP keys.</p> <p><i>TKIP-CCMP</i> - CCMP is a security standard used by the <i>Advanced Encryption Standard (AES)</i>. AES serves the same function TKIP does for WPA-TKIP. CCMP computes a <i>Message Integrity Check (MIC)</i> using the proven <i>Cipher Block Chaining (CBC)</i> technique. Changing just one bit in a message produces a totally different result. The encryption method is <i>Temporal Key Integrity Protocol (TKIP)</i>. TKIP addresses WEP's weaknesses with a re-keying mechanism, a per-packet mixing function, a message integrity check and an extended initialization vector. However, TKIP also has vulnerabilities.</p>
<p>Encryption (Secure-PSK only)</p>	<p><i>WPA2-CCMP</i> - WPA2 is a 802.11i standard that provides even stronger wireless security than <i>Wi-Fi Protected Access (WPA)</i> and WEP. CCMP is the security standard used by the <i>Advanced Encryption Standard (AES)</i>. AES serves the same function TKIP does for WPA-TKIP. CCMP computes a <i>Message Integrity Check (MIC)</i> using the proven <i>Cipher Block Chaining (CBC)</i> technique. Changing just one bit in a message produces a totally different result. WPA2/CCMP is based on the concept of a <i>Robust Security Network (RSN)</i>, which defines a hierarchy of keys with a limited lifetime (similar to TKIP). Like TKIP, the keys the administrator provides derive other keys. Messages are encrypted using a 128-bit secret key and a 128-bit block of data. The end result is an encryption scheme as secure as any a controller, service platform or Access Point provides for its connected clients.</p>

<p>Key (Secure-PSK only)</p>	<p>When Secure-PSK security is selected, enter an encryption key. For WEP-64 and WEP-128 enter a 4 to 32 character Pass Key and click the <i>Generate</i> button. The pass key can be any alphanumeric string. Controllers, service platforms, Access Points and their connected clients use the algorithm to convert an ASCII string to the same hexadecimal number. Clients without adapters need to use WEP keys manually configured as hexadecimal numbers. For TKIP-CCMP and WPA2-CCMP enter either an alphanumeric string of 8 to 63 ASCII characters or 64 HEX characters as the primary string both transmitting and receiving authenticators must share. The alphanumeric string allows character spaces. The string is converted to a numeric value. This passphrase saves the administrator from entering the 256-bit key each time keys are generated.</p>
<p>RADIUS VLAN Assignment (Secure-802.1x and Guest only)</p>	<p>Select this option to enable the RADIUS server to assign a VLAN, post authentication. Once a captive portal user is authenticated, the user is assigned the VLAN configured in this field.</p>
<p>Bypass Captive Portal Detection</p>	<p>Refer to the Bypass field to enable or disable Bypass Captive Portal Detection capabilities. If enabled, captive portal detection requests are bypassed. This feature is disabled by default.</p>
<p>RADIUS (only Secure-802.1x)</p>	<p>Configure the RADIUS server to use for authentication. Select from</p> <p><i>Local</i> - Select this option to use the onboard RADIUS server.</p> <p><i>Controller</i> - Select this option to use the RADIUS server on the adopting controller.</p> <p><i>External</i> - Select this option to configure an external RADIUS server. Provide the primary server's IP address or hostname and the secret shared with the server. Optionally provide the secondary server's IP address or hostname and the secret password shared with the server.</p>
<p>Only Internet Access</p>	<p>Select this option to prevent client devices from accessing resources on the VLAN. This option restricts the clients to locations on the Internet only.</p>
<p>Use DHCP/NAT on APs</p>	<p>Select this option to use DHCP information provided by the Access Points. When selected, provide a DNS server IP for name resolutions. When selected, the Client-To-Client Communication option is not available and the VLAN is defaulted to VLAN 2200.</p>
<p>Bypass Captive Portal Detection</p>	<p>Select this option to enable social media authentication. A requesting client's user credentials require authentication through social media credential exchange and validation.</p>

<p>Access Type</p>	<p>Select the authentication scheme applied to clients requesting captive portal guest access to the WiNG network. Within the WiNG UI there's 6 options. The WiNG CLI uses 5 options. User interface options include:</p> <p><i>No authentication required</i> - Requesting clients are redirected to the captive portal Welcome page without authentication.</p> <p><i>RADIUS Authentication</i> - A requesting client's user credentials require authentication before access to the captive portal is permitted. This is the default setting.</p> <p><i>Registration</i> - A requesting client's user credentials require authentication through social media credential exchange and validation.</p> <p><i>Email Access</i> - Clients use E-mail username and passwords for authenticating their captive portal session. Optionally set whether E-mail access requests are RADIUS validated.</p> <p><i>Mobile Access</i> - Mobile clients use their device's access permissions for authenticating their captive portal session. Optionally set whether mobile access requests are RADIUS validated.</p> <p><i>Other Access</i> - Requesting guest clients use a different means of captive portal session access (aside from E-mail or mobile device permissions). Optionally set whether these other access requests are RADIUS validated.</p>
<p>Lookup Information</p>	<p>When <i>Other Access</i> is selected as the access type, provide a 1-32 character lookup information string used as a customized authentication mechanism.</p>
<p>Registration Type</p>	<p>Set the self-registration type for this selected WLAN. Options include <i>Device</i>, <i>User</i> and <i>Device-OTP</i>.</p> <p>When guest users are authenticating (registering) using their User ID (Email Address/Mobile Number/ Member ID) and received pass code, the WLAN authentication type should be MAC-Authentication and the WLAN registration type should be set as device-OTP.</p> <p>When captive portal device registration is through social media, the WLAN registration type should be set as device registration, and the captive portal needs to be configured for guest user social authentication.</p>
<p>Radius Group</p>	<p>Use this field to provide a name for the default RADIUS group to which each authenticated guest user will become a member of.</p>
<p>Session Timeout (Guest Only)</p>	<p>Configure the session timeout value for Guest User access. This is the time after which the guest user is forced to re-authenticate.</p>

5. In the **WLAN Rate Limit** section configure the following settings:

<p>Enable (Per-Client)</p>	<p>Select this option to enable WLAN Rate limiting. Rate limiting reduces the maximum rate sent or received from the wireless network (and WLAN) per wireless client. It prevents any single user from overwhelming the wireless network. It can also provide differential service for service providers. Once enabled, configure the value in the per-client field.</p>
-----------------------------------	--

Per-Client	If per-client WLAN rate limiting is enabled, use the spinner controls to configure the per-client data rate limit between 50 - 1,000,000 kbps. The client's maximum data speed is limited the configured rate.
Enable (Aggregate WLAN)	Select this option to enable WLAN Rate limiting for the WLAN as a whole. Once enabled configure the value in the aggregate field.
Aggregate (WLAN)	If aggregate WLAN rate limiting is enabled, use the spinner controls to configure the WLAN aggregate data rate limit between 50 -1,000,000 kbps. The collective data rate for all clients on the WLAN is limited to the configured rate.

6. Configure the following **Other Settings**:

Client Roam Assist	Select this option to enable client roam assist. By monitoring a client's packets and the received signal strength indicator (RSSI) of a given client, decisions can be made on the optimal Access Point to which the client needs to roam. Then forcefully direct the client to the optimal Access Point.
Voice VLAN	Select this option to enable a dedicated voice VLAN for the WLAN. If enabled voice traffic will be tagged with with this VLAN.

7. Select the **Smart-RF** tab to review and configure power and channel settings.

Radio Settings

2.4GHz Channel: smart Power: smart (dBm) Data Rate: default
 5GHz Channel: smart Power: smart (dBm) Data Rate: 11ac

Wireless LAN **Smart-RF** MeshConnex

Power Settings

2.4 GHz Min: 4 Max: 17 (1-20) dBm
 5 GHz Min: 4 Max: 17 (1-20) dBm

Allowed Channel List

2.4 GHz Channel: Select Channel All
 5 GHz Channel: Select Channel All

Channel Width: Select Filter DFS

Scanning Configurations

2.4 GHz 5 GHz
 Client Aware Scanning 1 1
 Voice Aware Scanning (dynamic) (dynamic)

Smart RF is not applicable for AP7502

Apply Discard

8. Configure the following **Smart-RF** settings for the WLAN:

Power Settings 2.4 GHz / 5 GHz	Specify the minimum and maximum power levels, between 1 and 20 dBm, for both the 2.4 GHz and the 5 GHz radios. These are value restrictions applied to Smart RF power compensations for poorly performing or failed radios.
---------------------------------------	---

Filter DFS	Select this option to filter channels used for DFS scanning for RADAR. When enabled, the unit continuously monitors the spectrum, searching for signals with a specific pattern indicating radar activity. Upon detecting radar, the unit immediately stops transmitting on this channel and starts looking for another radar-free channel.
Allowed Channel List	Selecting this option enables a dynamic update of the channel list utilized on the 2.4 GHz and 5 GHz radios. To add an allowed channel, select it from the drop-down menu and click the green + sign. To remove a channel, select it from the list and click the red trashcan. To add all channels to the allowed list, select All then select the green + sign.
Channel Width 2.4 GHz / 5 GHz	<p>Use the drop-down menu to specify the channel width in Smart RF scans. Specify the channel width for both 2.4 GHz and 5 GHz traffic if applicable.</p> <p><i>Default-Scan</i> - Each channel's width is fixed and defaulted to either 40MHz-Upper (Ch 1), 40MHz-Lower (Ch 6 and CH 11) or 80MHz (CH 36, CH 40, CH 44 and CH 48).</p> <p><i>Custom-Scan</i> - When custom channels are selected for RSSI scans, each selected channel can have its own width defined. Numerous channels have their width fixed at 20MHz, 802.11a radios support 20 and 40 MHz channel widths.</p> <p><i>Channel-Lock</i> - If a specific channel is selected and locked for an RSSI scan, there's no ability to refine the width between adjacent channels, as only one channel is locked.</p>
Client Aware Scanning 2.4 GHz / 5 GHz	Select this option to enable client aware scanning on the channel specified. Enable for both 2.4 GHz and 5 GHz traffic if applicable.

9. Select the **MeshConnex** tab to view and configure mesh wireless settings. A mesh point is an AP that establishes an all-wireless path to the mesh portal. Mesh APs locate and associate with their nearest neighbor, which provides the best path to the mesh portal.

Radio Settings

2.4GHz Channel: Power: (dBm) Data Rate:

5GHz Channel: Power: (dBm) Data Rate:

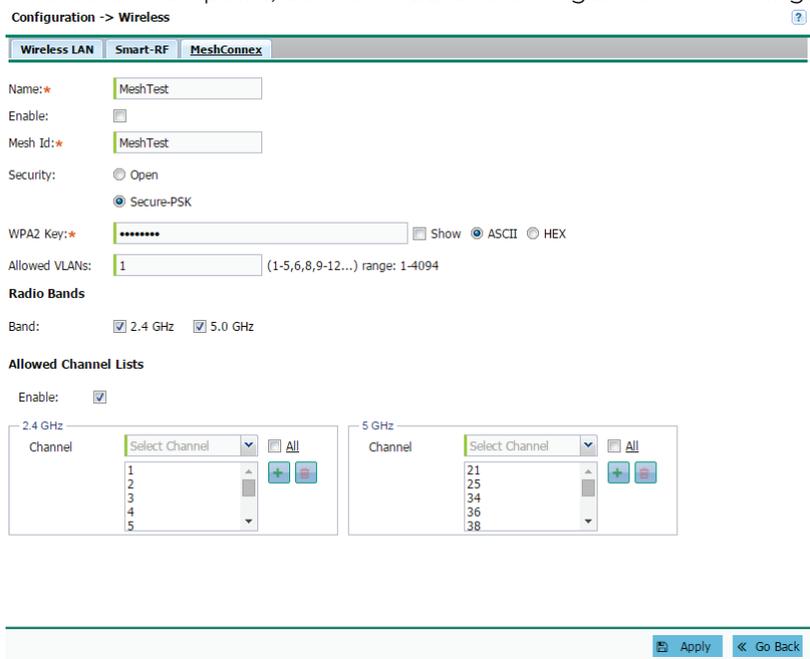
Wireless LAN | Smart-RF | **MeshConnex**

+ Add Number of Mesh Policies: 0

<input type="checkbox"/>	Name	Enable	Mesh ID	Control VLAN	Allowed VLANs	Security Mode
No Data						

Name	Displays the names of configured mesh points (mesh dedicated Access Points).
Enable	Specifies the status of each configured mesh point, either <i>Enabled</i> or <i>Disabled</i> .
Mesh ID	Displays the IDs (mesh identifiers) assigned to mesh points.
Control VLAN	Displays the VLAN (virtual interface ID) for the control VLAN on each of the configured mesh points.
Allowed VLANs	Displays the list of VLANs allowed on each of the configured mesh points.
Security Mode	Displays the security for each of the configured mesh points. The field will display <i>None</i> for no security or <i>PSK</i> for pre-shared key authentication.

To add a mesh point, select **+Add** and configure the following:



Name	Specify a name for the new mesh point. The name should be descriptive to easily differentiate it from other mesh points. This field is mandatory.
Enable	Toggles the status of a mesh point on or off. To enable a mesh point, select this option.
Mesh ID	Specify a numeric mesh identifier for this mesh point. This field is optional.
Security	<p>Displays the Security type.</p> <p>The screen displays with the <i>Open</i> option selected. Naming and saving such a policy (as is) would provide no security and might only make sense in a network wherein no sensitive data is either transmitted or received. This default setting is not recommended.</p> <p>If selecting <i>Secure-PSK</i>, select an encryption type for the WLAN. Define whether the key is entered in ASCII or HEX characters. Selecting Show to expose the key is not recommended.</p>
Allowed VLANs	Specify the VLANs allowed to pass traffic on the mesh point. Separate all VLANs with a comma. To specify a range of allowed VLANs separate the starting VLAN and the ending VLAN with a hyphen.
Radio Bands	Select to enable 2.4 GHz and 5.0 GHz radio bands for the mesh point. Unselecting a radio band will disable it for the mesh point.

Allowed Channel List	Selecting this option enables a mesh point channel list dynamic update on the 2.4 GHz and 5 GHz radios. To add an allowed channel, select it from the drop-down menu and click the green + sign. To remove a channel, select it from the list and click the red trashcan icon. To add all channels to the allowed list, select All then select the green + sign.
-----------------------------	--

Security

When protecting wireless traffic to and from a managed Access Point, an administrator should not lose sight of the security solution in its entirety, since the chain is as weak as its weakest link. The system provides seamless data protection and user validation to protect and secure data at each vulnerable point in the Access Point managed network. Access Points support a Layer 2 wired/wireless firewall and *Wireless Intrusion Protection System* (WIPS) capabilities, while additionally strengthened with a premium multi-vendor overlay security solution from Air Defense with 24x7 dedicated protection. This security is offered at the most granular level, with role, location and device categorization based network access control available to users based on identity as well as the security posture of the client device.

Firewall

A *firewall* is a mechanism enforcing network access control, and is considered a first line of defense in protecting proprietary information within the Access Point managed network. The means by which this is accomplished varies, but in principle, a firewall can be thought of as mechanisms both *blocking* and *permitting* data traffic within the network. Firewalls implement uniquely defined access control policies, so if you don't have an idea of what kind of access to allow or deny, a firewall is of little value, and in fact could provide a false sense of network security.

With supported Access Points, firewalls are configured to protect against unauthenticated logins from outside the network. This helps prevent hackers from accessing an Access Point's managed wireless clients. Well designed firewalls block traffic from outside the network, but permit authorized users to communicate freely with outside the network. All messages entering or leaving an Access Point pass through the firewall, which examines each message and blocks those not meeting the security criteria (rules) defined.

Firewall rules define the traffic permitted or denied within the network. Rules are processed by a firewall supported device from first to last. When a rule matches the network traffic a controller or service platform is processing, the firewall uses that rule's action to determine whether traffic is allowed or denied.

Rules comprise conditions and actions. A condition describes a traffic stream of packets. Define constraints on the source and destination device, the service (for example, protocols and ports), and the incoming interface. An action describes what should occur to packets matching the conditions set. For example, if the packet stream meets all conditions, traffic is permitted, authenticated and sent to the destination device.

To configure **Firewall** rules:

1. Select **Configuration** from the main menu. Select **Security**, then **Firewall**.

Configuration -> Security ?

Firewall | Wireless IPS | Application Visibility (AVC) | Scheduler

Enable Firewall:

WLAN ACL Rules

Precedence	Enabled	Action	Source IP	Destination IP	Protocol	Direction	Interface	Edit
1	<input checked="" type="checkbox"/>	<input type="radio"/>	2.2.2.0/24	Any	0(p)	out	123-cap	<input type="checkbox"/>
2	<input checked="" type="checkbox"/>	<input type="radio"/>	3.3.3.0/24	Any	0(p)	out	123	<input type="checkbox"/>

Wireless Client Association ACL Rules

Precedence	Action	Start MAC	End MAC	Interface	Edit
1	<input type="radio"/>	00-00-00-00-00-00	12-12-12-12-12-12	123-cap,123	<input type="checkbox"/>

Apply Discard

The firewall screen is divided into **WLAN ACL Rules** and **Wireless Client Association ACL Rules** fields.

Note

Changes made to an Access Point's configuration are pushed (provisioned) to Access Points of the same model.

2. Select **Enable Firewall** to allow firewall functionality. This is enabled by default.
3. Set the following **WLAN ACL Rules**:

Precedence	Specify or modify a precedence for this IP policy between 1-1000. Rules with lower precedence are always applied to packets first. If modifying a precedence to apply a higher integer, it moves down the table to reflect its lower priority.
Enabled	Select a firewall rule's <i>Enable</i> or <i>Disable</i> icon to determine this rule's inclusion with the IP firewall policy.
Action	Every IP firewall rule is made up of matching criteria rules. The action defines what to do with a packet if it matches the specified criteria. The following actions are supported: <i>Deny</i> - Instructs the firewall to stop a packet from its destination. <i>Permit</i> - Instructs the firewall to allow a packet to proceed to its destination.
Source IP	Determine whether filtered packet source for this IP firewall rule require any classification (any), are designated as a set of configurations consisting of protocol and port mappings (an alias), set as a numeric IP address (host) or defined as network IP and mask.

Destination IP	Determine whether filtered packet destinations for this IP firewall rule do not require any classification (any), are designated as a set of configurations consisting of protocol and port mappings (an alias), are set as a numeric IP address (host) or defined as network IP and mask. Selecting alias requires a destination network group alias be available or created.
Protocol	Define the access protocols impacted by the WLAN's ACL rule configuration.
Direction	Specify the direction for ACL rule.
Interface	Specify the interface for the WLAN ACL rule to affect.

4. Set the following **Wireless Client Association ACL Rules**:

Precedence	Specify or modify a precedence for this IP policy between 1-1000. Rules with lower precedence are always applied to packets first. If modifying a precedence to apply a higher integer, it will move down the table to reflect its lower priority.
Action	Every IP firewall rule is made up of matching criteria rules. The action defines what to do with the packet if it matches the specified criteria. The following actions are supported: <i>Deny</i> - Instructs the firewall to stop a packet from its destination. <i>Permit</i> - Instructs the firewall to allow a packet to proceed to its destination.
Start MAC	Specify the source MAC address or network group configuration used as basic matching criteria for this ACL rule. The source MAC ensures only an authenticated endpoint is allowed to send traffic.
End MAC	Specify the destination MAC address or network group configuration used as basic matching criteria for this ACL rule. The end MAC represents the destination MAC address of the packet examined for matching purposes and potential device exclusion.
Interface	Use the drop-down menu to specify the interface configurations impacted by the ACL's rule configuration.

WIPS

Access Points can utilize the *Wireless Intrusion Protection Systems* (WIPS) to provide continuous protection against wireless threats and act as an additional layer of security complementing wireless VPNs and encryption and authentication policies. WIPS is supported through dedicated sensor devices designed to actively detect and locate unauthorized Access Points. Upon detection, they use mitigation techniques to block the devices by manual termination or air lock down.

Unauthorized APs are untrusted Access Points connected to a LAN accepting client associations. They can be deployed for illegal wireless access to a corporate network, implanted with malicious intent by an attacker, or could just be misconfigured Access Points that do not adhere to corporate policies. An attacker can install an unauthorized AP with the same ESSID as the authorized WLAN, causing a nearby client to associate to it. The unauthorized AP can then steal user credentials from the client, launch a *man-in-the middle* attack or assume control of wireless clients to launch denial-of-service attacks.

Access Points support unauthorized AP detection, location and containment natively. A WIPS server can alternatively be deployed (in conjunction with the Access Point) as a dedicated solution within a separate enclosure. A WIPS deployment provides the following Enterprise class security management features and functionality:

Threat Detection - Threat detection is central to a wireless security solution. Threat detection must be robust enough to correctly detect threats and swiftly help protect the Access Point managed wireless network.

Rogue Detection and Segregation - A WIPS supported Access Point distinguishes itself by both identifying and categorizing nearby Access Points. WIPS identifies threatening versus non-threatening Access Points by segregating Access Points attached to the network (unauthorized APs) from those not attached to the network (neighboring Access Points). The correct classification of potential threats is critical for administrators to act promptly against rogues and not invest in a manual search of neighboring Access Points to isolate the few attached to the network.

To configure **Wireless IPS** on a managed Access Point:

1. Select **Configuration** from the main menu. Select **Security**, then **Wireless IPS**.

Configuration -> Security ?

Firewall **Wireless IPS** Application Visibility (AVC) Scheduler

Rogue AP Detection

Enable Rogue AP Detection Off-Channel Scan

Search Number of Unsanctioned APs: 303

	Unsanctioned AP MAC	Channel	SSID	RSSI	Reporter AP Name
	84-24-8D-46-35-60	52	tenantsix	-77	ap7522-1B7428
	B4-C7-99-BC-37-70	6	Alpha-Phone	-39	ap7522-1B7428
	84-24-8D-B2-8D-20	149	tenantfour	-79	ap7522-1B7428
	B4-C7-99-95-C0-20	40	vlan157-adsp	-62	ap7522-1B7428
	84-24-8D-96-D1-70	149	Tenattwo	-65	ap7522-1B7428
	5C-0E-88-D9-F2-90	36	Pick-n-Pack	-74	ap7522-1B7428
	74-67-F7-08-E5-F0	149	tenantbrine	-84	ap7522-1B7428
	FC-0A-81-88-1F-70	1	vx9_sanity_site1	-42	ap7522-1B7428
	84-24-8D-42-3E-10	36	tenateight	-77	ap7522-1B7428
	B4-C7-99-68-49-80	1	site-3-wlan-24	-56	ap7522-1B7428
	B4-C7-99-68-62-80	149	site-3-wlan-24	-53	ap7522-1B7428
	84-24-8D-96-C9-F0	149	tenantthree	-70	ap7522-1B7428
	84-24-8D-4A-B8-40	149	tenantsix	-76	ap7522-1B7428
	FC-0A-81-08-60-50	36	EU-CPU-captive	-73	ap7522-1B7428
	84-24-8D-41-F7-B0	36	tenantsix	-75	ap7522-1B7428
	74-67-F7-3C-1C-70	149	TxBF	-48	ap7522-1B7428
	84-24-8D-B1-31-60	149	tenantfour	-78	ap7522-1B7428
	00-23-68-94-E5-30	149		-45	ap7522-1B7428
	74-67-F7-12-C5-C0	1	noc1-site10-ap8432	-61	ap7522-1B7428
	84-24-8D-99-51-90	36	Alpha-Phone	-76	ap7522-1B7428
	B4-C7-99-E5-87-40	149	site-3-wlan-23	-56	ap7522-1B7428
	84-24-8D-68-5B-20	153	your-ssid	-72	ap7522-1B7428
	84-24-8D-98-FD-C0	1	AVC14	-61	ap7522-1B7428
	FC-0A-81-96-0D-60	6	vx9_sanity_site1	-37	ap7522-1B7428
	74-67-F7-08-C2-E0	52	site-2-wlan-17	-53	ap7522-1B7428
	84-24-8D-96-45-A0	1	Tenattwo	-85	ap7522-1B7428
	FC-0A-81-B8-94-30	1	oob_ssid_ap7502	-65	ap7522-1B7428
	74-67-F7-08-94-F0	149	tenantfour	-69	ap7522-1B7428
	5C-0E-88-7F-07-D0	36		-25	ap7522-1B7428
	84-24-8D-45-F1-30	1	site_1	-43	ap7522-1B7428

2. Select **Enable Rogue AP Detection** to allow the detection of unauthorized (unsanctioned) devices from this WIPS policy.
3. Select **Off-Channel Scan** to scan across all channels using this Access Point's radio. Channel scans use Access Point resources and can be time consuming, so only enable when sure radio bandwidth can be dedicated to the channel scan and does not negatively impact client support.

Note

Changes made to an Access Point's configuration are pushed (provisioned) to Access Points of the same model.

4. Review the following **Wireless IPS** event information:

Unsanctioned AP MAC	Displays the hardware encoded MAC address of each listed Access Point. The MAC address is set at the factory and cannot be modified via the management software.
Channel	Displays the channel where the unsanctioned AP was detected.
Is Rogue	Displays whether the detected device has been classified as a rogue device whose detection threatens the interoperation of authorized connected devices.
SSID	Displays the <i>Service Set ID</i> (SSID) of the network to which the detected Access Point belongs.
RSSI	Displays the <i>Received Signal Strength Indicator</i> (RSSI) of the detected Access Point. Use this variable to help determine whether an additional device connection would improve network coverage or add noise.
Reporter AP Name	Displays the hardware encoded <i>Media Access Control</i> (MAC) address of the Access Point reporting the listed WIPS event.

Application Visibility

Note

Application Visibility is available on the following platforms: AP7602, AP7622.

Deep packet inspection (DPI) is an advanced packet filtering technique functioning at the application layer. Use DPI to find, identify, classify, reroute or block packets containing specific data or codes that other packet filtering techniques (examining only packet headers) cannot detect.

Enable DPI to scan data packets passing through the WiNG managed network. The contents of each packet are scanned, occasionally logged and blocked or routed to their destination. Deep packet inspection helps an ISP block the spread of viruses, illegal downloads and prioritize data transmitted by bandwidth-heavy applications (video and VoIP applications) to help prevent network congestion.

To configure **Application Visibility** on a managed Access Point:

1. Select **Configuration** from the main menu. Select **Security**, then **Application Visibility**.

Configuration -> Security ?

Firewall Wireless IPS **Application Visibility (AVC)** Scheduler

Enable Dpi:

WLAN Application Rules Number of Rules: 2

Precedence	Action	Category	Application	Schedule Policy	Mark Type	Mark Value	Ingress Rate	Egress Rate	Wlan	Edit
1	deny	social networking	-	-	-	-	-	-	123-cap	
2	deny	gaming	-	-	-	-	-	-	123	

Wlan Application Schedule Rules Number of Schedule: 2

Days	Start Time	End Time	Wlan	Edit
weekdays	01:00	01:01	123-cap	
weekends	01:00	01:01	123	

The **Application Visibility (AVC)** screen is divided into **WLAN Application Rules** and **WLAN Application Schedule Rules**.

2. Select **Enable DPI** to find, identify, classify, reroute or block packets containing specific data or codes that other packet filtering techniques cannot detect.
3. Create new **WLAN Application Rules** by selecting **+ Add Rule** and configuring the following fields:

Precedence	Set the priority (from 1 - 256) for the application policy rule. The lower the value, the higher the priority assigned to this rule's enforcement action and the category and application assigned. A precedence also helps resolve conflicting rules for applications and categories.
Action	Set the action executed on the selected application category and application. The default setting is Allow.
Category	Select the category for which the application rule applies. Selecting All auto-selects All within the Application table.
Application	Select All from the Application table to list all application category statistics, or specify a particular category name to display its statistics only. An application policy defines the rules or actions executed on recognized HTTP (Facebook), Enterprise (Webex) and peer-to-peer (gaming) applications or application-categories.
Schedule Policy	Select a schedule policy from the drop-down menu. If a schedule policy does not exist, create one in the Scheduler section. Schedule policies strategically enforce application filter policy rules for specific intervals. This provides stricter, time and schedule based, access or restriction to specific applications and their parent categories.

Mark Type	<i>Mark</i> actions mark packets for a recognized application and category with DSCP/8021p values used for QoS.
Mark Value	Displays the DSCP/8021p application or category value associated with each WLAN application rule.
Ingress Rate	Specify an ingress (incoming traffic) rate for the rate-limiter for this application rule.
Egress Rate	Specify an egress (outgoing traffic) rate for the rate-limiter for this application rule.
WLAN	Specify the WLAN to apply the application rules.

4. To delete an existing rule, select that rule from the table and select **Delete Rule**.
5. Create new **WLAN Application Schedule Rules** by selecting **+ Add Schedule** and configure the following fields:

Days	Specify the number of days the application rule should be applied.
Start Time	Specify a starting date and time for the application rule to start.
End Time	Specify an end date and time for the application rule to stop.
WLAN	Specify the WLAN which to apply the application rules to.

6. To delete an existing schedule, select that rule from the table and select **Delete Schedule**.

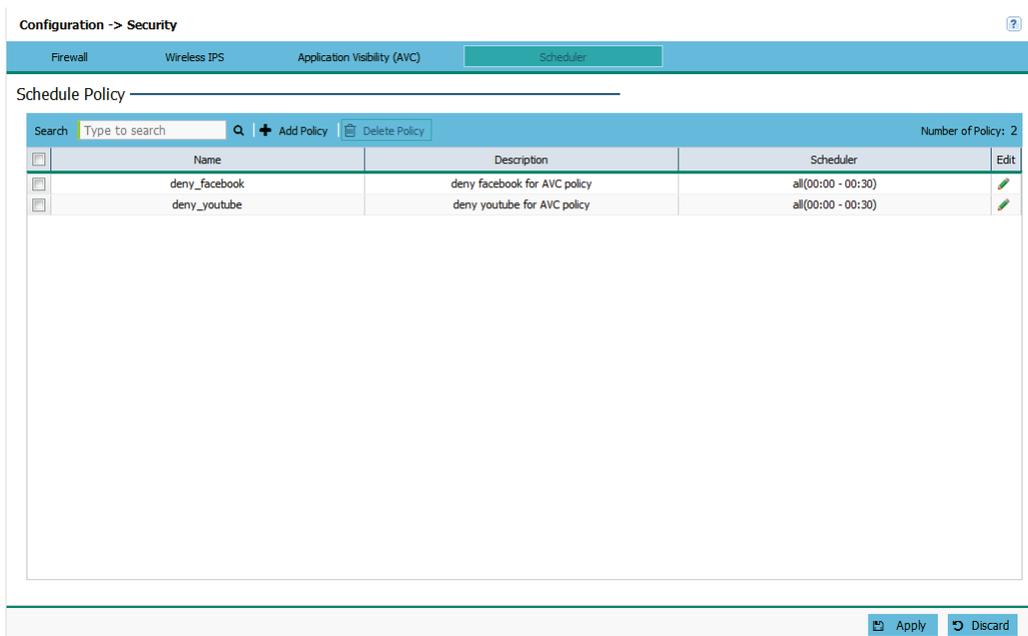
Schedule Policy

Note
 Schedule Policy is available on the following platforms: AP7602 & AP7622.

Define schedule policies to strategically enforce application filter policy rules for specific intervals. This provides stricter, time and schedule based, access or restriction to specific applications and their parent categories.

To configure a **Schedule Policy** for a managed Access Point:

1. Select **Configuration** from the main menu. Select **Security**, then **Schedule Policy**.



2. Set the following schedule parameters:

Name	Provide a name for the new schedule policy. Enter a 32-character maximum <i>Name</i> relevant to its specific permissions objective.
Description	Provide this schedule policy an 80-character maximum Description to differentiate it from other policies with similar time rule configurations.
Scheduler	Create one or more schedule rules by selecting <i>+ Add</i> and specify the <i>Days</i> of the week as well as <i>Start</i> and <i>End Times</i> .

3. Create a new **Schedule Policy** by selecting **+ Add Policy** and configure the following:

Name	Provide a name for the new schedule policy.
Description	Optionally, provide a description for the schedule policy.
Schedule Rules	Create one or more schedule rules by selecting <i>+ Add</i> and specify the <i>Days</i> of the week as well as <i>Start</i> and <i>End Times</i> .

- To delete an existing schedule select that rule from the table and select **Delete Policy**.

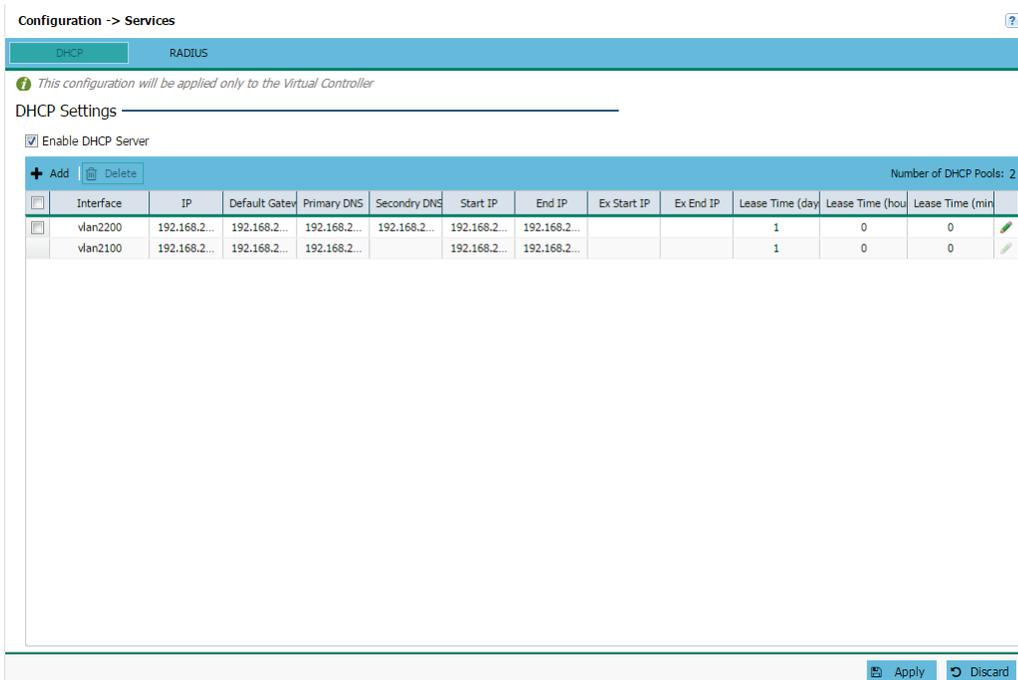
Services

DHCP

DHCP is a protocol that includes mechanisms for IP address allocation and delivery of host-specific configuration parameters from a DHCP server to a host. Some of these parameters are IP address, network mask, and gateway. The WAN and LAN ports should not both be configured for DHCP support.

To configure DHCP **Services**:

- Select **Configuration** from the main menu. Select **Services**.



The DHCP Settings screen displays.

2. Select **Enable DHCP Server** to assign IP addresses to requesting wireless clients. Enabling DHCP allows the Access Point’s onboard DHCP server resource to provide IP and DNS information to requesting clients on the LAN interface.
3. If the DHCP server is enabled, configure the following settings:

Interface	<p>Use the drop-down menu to select an interface for the DHCP server. Supported Access Points have the following interfaces:</p> <p><i>AP6511</i> - FE1, FE2, FE3, FE4, UP1</p> <p><i>AP6521</i> - GE1/POE (LAN)</p> <p><i>AP6522</i> - GE1/POE (LAN)</p> <p><i>AP6562</i> - GE1/POE (LAN)</p> <p><i>AP7502</i> - GE1, FE1, FE2, FE3</p> <p><i>AP7522</i> - GE1/POE (LAN)</p> <p><i>AP7532</i> - GE1/POE (LAN)</p> <p><i>AP7562</i> - GE1/POE (LAN)</p> <p><i>AP7602</i> - GE1/POE (LAN)</p> <p><i>AP7622</i> - GE1/POE (LAN)</p>
------------------	---

IP	Specify the IP mask for each entry in the DHCP server. Applying a subnet mask to an IP address separates the address into a host address and an extended network address. Subnets can improve network security and performance by organizing hosts into logical groups.
Default Gateway	Enter the IP address of the network's default gateway. A default gateway provides an entry/exit point for the network as it commonly connects an internal network to an external network.
Primary DNS	Enter an IP Address for the main DNS server resource for the Access Point's WAN interface.
Secondary DNS	Enter an IP Address for the backup (secondary) Domain Name Server providing DNS services for the Access Point's WAN interface.
Start IP	Enter the starting IP Address for each DHCP address pool range configured. Ensure the range is large enough to meet the needs of requesting clients.
End IP	Enter the ending IP Address for each DHCP address pool range configured. Ensure the range is large enough to meet the needs of requesting clients.
Lease Time (days)	The lease time displays in days if it has been defined for a listed network pool. DHCP leases provide addresses for defined times to requesting clients. If a client does not use the leased address for the defined time, that IP address can be re-assigned to another requesting DHCP client.
Lease Time (hours)	The lease time displays in days if it has been defined for a listed network pool. DHCP leases provide addresses for defined times to requesting clients. If a client does not use the leased address for the defined time, that IP address can be re-assigned to another requesting DHCP client.
Lease Time (minutes)	The lease time displays in days if it has been defined for a listed network pool. DHCP leases provide addresses for defined times to requesting clients. If a client does not use the leased address for the defined time, that IP address can be re-assigned to another requesting DHCP client.

Note

To add a VLAN that is accessible in a DHCP pool the VLAN with a static IP address must be added on the Configuration > Access Points screen in the IP Settings tab.

RADIUS

The Access Point's local RADIUS server allows the configuration of user groups with common user policies. User group names and associated users are stored in the Access Point's local database. The user ID in the received access request is mapped to the associated wireless group for authentication.

To view RADIUS configurations:

1. Select **Configuration** tab from the main menu.
2. Select the **Services** tab from the **Configuration** menu.
The upper pane of the user interface displays the **DHCP** and **RADIUS** options.
3. Select **RADIUS**.

4. Select **Enable Radius Server** to activate the internal RADIUS server.
5. Select **Start Radius Server** to start the RADIUS service on the AP.
6. Review the following RADIUS group configuration information. To create a new RADIUS group click **+ Add**. To remove an existing group or groups, select them from the table and click **Delete**.

RADIUS Group	Displays the group name or identifier assigned to each listed group when it was created. The name cannot exceed 32 characters or be modified as part of the group edit process.
Guest User Group	Select to enable RADIUS access to the guest user group with the settings outlined in this section.
VLAN	Displays the VLAN ID used by the group. The VLAN ID is representative of the shared SSID each group member (user) employs to interoperate within the network (once authenticated by the local RADIUS server).

WLAN SSID	Displays the <i>Service Set ID</i> (SSID) of the Access Point's network. Access Point's network. Select All to add all SSIDs to the table. To add individual SSIDs, select them from the drop-down menu and select the green + sign. To remove SSIDs from the table, select one or more SSID and select the red delete icon.
Rate limit from air	Specify the maximum data rate in kbps between 100 and 1,000,000 for traffic originating on the wireless network.
Rate limit to air	Specify the maximum data rate in kbps between 100 and 1,000,000 for traffic destined for the wireless network.
Inactivity Timeout	Specify a time limit, in seconds, before the guest user group is automatically timed out. If the user or group times out they must reauthenticate with the RADIUS server.

7. Review the following RADIUS schedule information and modify as needed:

Access by time	To enable restricted guest access to the RADIUS server by time of day, select this option and then specify a Start Time and End Time in the fields below.
Start Time	When Access by Time is enabled, specify the start time users within each listed group can access local RADIUS resources.
End Time	When Access by Time is enabled, specify the end time users within each listed group lose access to the local RADIUS resources.
Access by Day of Week	To enable specific weekday guest access to the RADIUS server, select this option and select each of the days to enable access.

8. When adding or editing a RADIUS user, verify and configure the following:

User ID	Displays the name or identifier assigned to each user when created. The name cannot exceed 32 characters or be modified as part of the edit process.
Guest User	Select to enable RADIUS access using the guest user group with this user.
Group	Use the pull-down menu to select which group to associate with the RADIUS user.
Email ID	Specify an E-mail address for the RADIUS user. This can be a local E-mail address or a fully qualified E-mail address.
Telephone	Specify the telephone number associated with the RADIUS user. This is an optional field.
Start Date / Start Time	Specify a start date and time when this RADIUS user is activated.
Expiry Date / Expiry Time	Specify an end date and time when this RADIUS user is deactivated.
Access Duration	Specify how long the RADIUS user is active by selecting an access duration. To allow the use of the Expiry Date and Expiry Time fields select the Til Expiry option. Specify a duration in Days:Hours:Minutes format. The RADIUS user is deactivated once the set duration has expired.

Management

Access Points have mechanisms to allow/deny access for separate interfaces and protocols (HTTP, HTTPS, Telnet, SSH or SNMP). Management access can be enabled/disabled as required for unique policies. This access functionality is not meant to function as an ACL (in routers or other firewalls), where administrators specify and customize specific IPs to access specific interfaces. It is rather a means of disabling unused interfaces to reduce network vulnerabilities.

To enhance security, administrators can apply various restrictions as needed to:

- Restrict SNMP and Web UI access to specific hosts or subnets
- Disable un-used and insecure interfaces as required within managed access profiles. Disabling un-used management services can dramatically reduce an attack footprint and free resources on managed devices
- Provide authentication for management users
- Apply access restrictions and permissions to management users

Management restrictions should be applied to meet specific policies or industry requirements requiring only certain devices or users be granted access to critical Access Point resources. Management restrictions can also be applied to reduce the Access Point's attack footprint when guest services are deployed.

To configure the Access Point's management settings:

1. Select **Configuration** settings from the main menu then select **Management**.

The screenshot displays the Management configuration interface, which is divided into several sections:

- Administrator:** Shows the current username as 'admin' and a 'Change User Password' button.
- Access:** A list of protocols with checkboxes: HTTP (unchecked), HTTPS (checked), Telnet (checked), and SSHv2 (checked).
- Syslog Server:** Includes a 'Logging' checkbox (checked), a 'Logging Level' dropdown menu set to 'Warning', and a 'Server IP' input field.
- SNMP Settings:**
 - Enable checkboxes for SNMPv1 (unchecked), SNMPv2 (unchecked), and SNMPv3 (checked).
 - SNMP v1/v2 Community String:** Read-only Access is 'public' and Read/Write Access is 'private'.
 - SNMP v3 Users:** A table with columns for Username, Password, Authentication, and Encryption.

Username	Password	Show	Authentication	Encryption
snmpmanager	*****	<input type="checkbox"/>	MD5	DES
snmpoperator	*****	<input type="checkbox"/>	MD5	DES
snmptrap	*****	<input type="checkbox"/>	MD5	DES
- SNMP Traps:** Includes a 'Trap Generation' checkbox (unchecked) and a table with columns for IP Address, Port, and Version. The table currently contains 'No Data'.

At the bottom right of the configuration area, there are 'Apply' and 'Discard' buttons.

The **Management** screen is partitioned into **Administrator**, **Access**, **Syslog Server**, **SNMP Settings** and **SNMP Traps** fields.

Note

Changes made to an Access Point's configuration are pushed (provisioned) to Access Points of the

same model.

2. In the **Administrator** section, select **Change User Password** to change the default administrator login password to something more proprietary and secure.
3. Set the following **Access** settings:

HTTP	Select the checkbox to enable HTTP device access. HTTP provides limited authentication and no encryption.
HTTPS	Select the checkbox to enable HTTPS device access. HTTPS (<i>Hypertext Transfer Protocol Secure</i>) is more secure than HTTP. HTTPS provides both authentication and data encryption as opposed to just authentication (as is the case with HTTP).
Telnet	Select the checkbox to enable Telnet device access. Telnet provides a command line interface to a remote host over TCP. Telnet provides no encryption, but does provide a measure of authentication. Telnet access is disabled by default.
SSHv2	Select the checkbox to enable SSH device access. SSH (<i>Secure Shell</i>) version 2, like Telnet, provides a command line interface to a remote host. SSH transmissions are encrypted and authenticated, increasing the security of transmission. SSH access is disabled by default.

4. In the **Syslog Server** section configure the following settings:

Logging	Select this option to log system events to a log file or a syslog server. Selecting this option enables the rest of the parameters required to define the Access Point's logging configuration. This option is disabled by default.
Logging Level	Event severity coincides with the syslog level defined for the Access Point. Assign a numeric identifier to log events based on criticality. Severity levels include: <i>0 - Emergency, 1 - Alert, 2 - Critical, 3 - Errors, 4 - Warning, 5 - Notice, 6 - Info and 7 - Debug.</i> The default logging level is 4.
Server IP	Enter the IP addresses where logged system events can be sent on behalf of the event generating Access Point.

5. Set the following **SNMP Settings**:

Enable SNMPv1	SNMP v1 exposes a device's management data so it can be managed remotely. Device data is exposed as variables accessed and modified as text strings, with version 1 being the original (rudimentary) implementation. SNMPv1 is disabled by default.
Enable SNMPv2	SNMPv2 provides device management using a hierarchical set of variables. SNMPv2 uses Get, GetNext, and Set operations for data management. SNMPv2 is enabled by default.
Enable SNMPv3	SNMPv3 adds security and remote configuration capabilities to previous versions. The SNMPv3 architecture introduces the <i>user-based security model</i> (USM) for message security and the <i>view-based access control model</i> (VACM) for access control. The architecture supports the concurrent use of different security, access control and message processing techniques. SNMPv3 is enabled by default.

SNMP v1/v2 Community String	Set the access permission for each community string used to retrieve or modify information. Available options include: <i>Read Only</i> - Allows a remote device to retrieve information. <i>Read-Write</i> - Allows a remote device to modify settings.
SNMPv3 Users: User Name	Use the drop-down menu to define a user name of <i>snmpmanager</i> , <i>snmpoperator</i> or <i>snmptrap</i> .
SNMPv3 Users: Password	Provide the user's password in the field provided. Select <i>Show</i> to display the actual character string used in the password. Leaving the check box unselected protects the password and displays each character as <i>"*"</i> .
SNMPv3 Users: Authentication	Select the user authentication type used with the listed SNMPv3 user. The selected authentication scheme ensures only trusted users can utilize Access Point network resources.
SNMPv3 Users: Encryption	Select the encryption scheme used with the listed SNMPv3 user. The selected encryption scheme ensures only trusted devices can utilize Access Point network resources.

6. In the **SNMP Traps** section select **+ Add** for each entry configure the following:

Trap Generation	Select the <i>Trap Generation</i> checkbox to enable trap generation using the trap receiver configuration defined. This feature is disabled by default.
IP Address	Sets the IP address of an external server resource dedicated to receive SNMP traps on behalf of the Access Point.
Port	Set the virtual port of the server resource dedicated to receiving SNMP traps. The default port is port 162.
Version	Sets the SNMP version to send SNMP traps. SNMPv2c is the default.

7. To remove a trap, highlight it in the table and select **Delete**.

Access Points

Use the Access Points screen to assess the configuration and network health of managed Access Points. Individual Access Points can be selected and their configurations customized as required to better support the deployment objective of the network.

To review **Access Points**:

1. Select **Access Points** from the main menu.

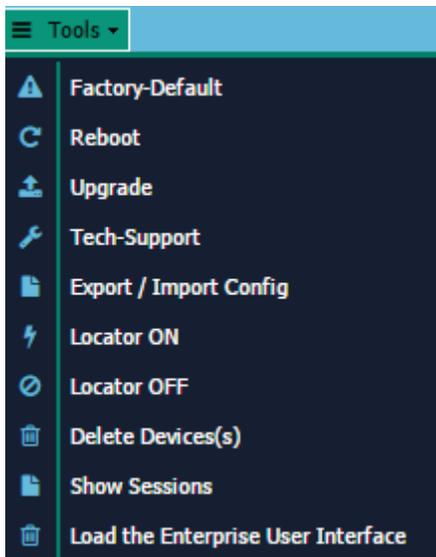
AP Name	AP Status	IP Address	2.4 GHz		5 GHz		Firmware
			Channel	Power (dbm)	Channel	Power (dbm)	
ap6522-52DD64	⬆️ (online)	1.1.1.85	6(smt)	4(smt)	60w(smt)	9(smt)	5.8.3.0-033M

2. The **Managed Access Points** section displays the following:

AP Name	Displays the administrator assigned Access Point name. Names can be revised using the Edit menu.
AP Status	Displays the active state of each listed Access Point. If an Access Point is online, two green up arrows are displayed. If an Access Point is offline two green down arrows display.
IP Address	Displays the current IP Address assigned to each Access Point as its network identifier. IPv6 formatted IP addresses are not supported, and the IP address is in an IPv4 format.
2.4GHz Channel	Displays the current radio channel number set for the 2.4 GHz radio on each Access Point. AP6511 and AP6521 Access Points are single radio models, the other supported Access Points are dual radio models.
2.4 GHz Power	Displays the 2.4 GHz radio's current power level in dBm. If using a dual radio model Access Point, each radio should be configured with a unique transmit power in respect to its intended client support function.
5 GHz Channel	Displays the current radio channel number for the 5 GHz radio, if applicable, on each managed Access Point. AP6511 and AP6521 Access Points are single radio models, and will not display channel information for a second radio.

5 GHz Power	Displays the 5 GHz radio's current power level in dBm. If using a dual radio model Access Point, each radio should be configured with a unique transmit power in respect to its intended client support function.
Firmware	Displays the full firmware version number on each listed Access Point. Periodically compare the Access Point's firmware version against the latest version available on the Support site to help ensure the Access Point is deployed with the most recent firmware, providing the most recent feature set.

- To access advanced Access Point options, select an AP or multiple APs from the **Managed Access Points** section and select the **Tools** pull-down menu.



The following tools are available:

Factory-Default	Selecting <i>Factory-Default</i> displays a prompt confirming whether to reset the device to factory defaults. Selecting <i>Yes</i> resets the device to factory default settings and will reboot the device. Choosing this option will erase all information and settings stored on the device. Selecting <i>No</i> cancels the reset and returns to the Access Point screen.
Reboot	Selecting <i>Reboot</i> displays a prompt confirming the device reboot. Selecting <i>Yes</i> reboots the device, and the user interface is unavailable until the device has rebooted. You will be required to log in to the user interface once the device has finished rebooting. Selecting <i>No</i> cancels the reboot and returns you to the Access Point screen.
Upgrade	<p>Selecting <i>Upgrade</i> displays the Device Upgrade page. If <i>Basic</i> is selected, enter the URL for the upgrade firmware in the following format:</p> <p><i>URL Syntax:</i> <code>ftp://<hostname IP>[:port]/path/file</code> <code>ftp://<user>:<passwd>@<hostname IP>[:port]/path/file</code></p> <p>If <i>Advanced</i> is selected, configure the Protocol, Port, Hostname or IP Address, Username, Password and directory path to for the firmware file. Firmware upgrades are supported via the FTP, TFTP and HTTP protocols.</p>

<p>Tech-Support</p>	<p>Selecting Tech-Support displays the Copy Tech Support screen where system information and logs can be transferred to technical support by configuring the Protocol, Port, Hostname or IP Address, Username, Password and directory path to for the tech support server. The transfer of this information is supported via the FTP, TFTP and HTTP protocols. The tech support filename is auto generated by the device based on the device MAC address, passing file name in path results in failure.</p>
<p>Export / Import Config</p>	<p>Selecting Export / Import Config displays a screen where configuration files can be imported or exported from the device. When <i>Local</i> is selected the start-up system configuration file is displayed as plain text in a window. To import a new configuration, erase the contents of the configuration window and paste the contents of a new configuration file into the window. When all changes are complete, click the import button to import the new configuration file onto the device. To export a configuration file using the Local option, simply copy the contents of the configuration window and paste it into a text file on your local system. Configuration files can also be imported from or exported to remote systems. Select <i>Remote</i> and specify the Protocol, Port, Hostname or IP Address, Username, Password and directory path to for the remote server. The transfer of this information is supported via the FTP, TFTP and HTTP protocols.</p>
<p>Locator ON</p>	<p>Select <i>Locator ON</i> to flash the Access Point's LEDs to differentiate this Access Point from others in the same deployment area.</p>
<p>Locator OFF</p>	<p>Select <i>Locator OFF</i> to stop the Access Point's LEDs from flashing.</p>
<p>Delete Devices</p>	<p>Use this option to delete offline APs from the managed system. The Access Point must first be offline before it may be deleted.</p>
<p>Show Sessions</p>	<p>Select Show Sessions to display a list of all active logged on sessions.</p>
<p>Load The Enterprise User Interface</p>	<p>Select Load the Enterprise User Interface to enable the advanced Enterprise user interface on supported APs. This requires an Access Point reboot.</p> <p>Configuration changes are populated within the Enterprise user interface. For example, if the Controller IP address is set using this user interface, the same configuration is retained on the Enterprise user interface. Reverting back from the Enterprise user interface to this user interface requires the Access Point to be reset to a full factory default. This is not a trivial operation. Using the Enterprise user interface is recommended only if already familiar with it.</p>

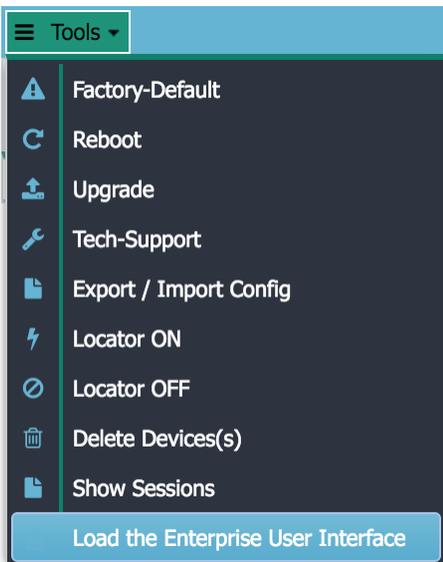
Loading the Enterprise User Interface

Note

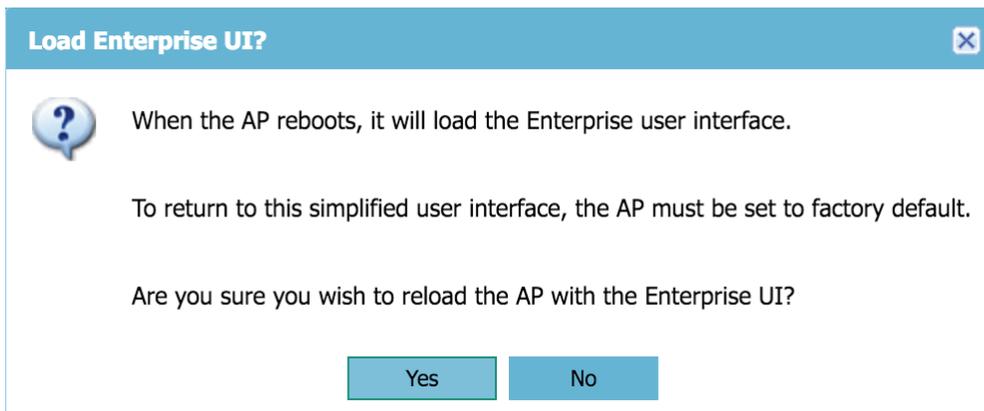
Loading the Enterprise user interface is only supported on AP7522, AP7532 and AP7562 model Access Points.

To load the Enterprise user interface on a supported Access Point:

1. Select **Access Points** from the **Configuration** section of the main menu.
2. Select an Access Point from the table and select **Tools**.



3. Select **Load the Enterprise User Interface** from the **Tools** menu. A warning dialog appears.



Note

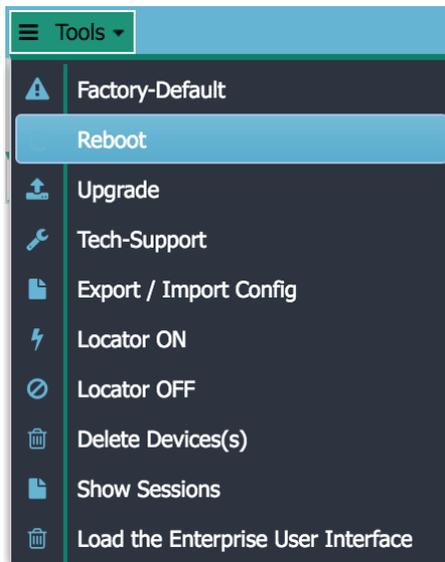
Once the enterprise user interface is activated, the Access Point must be reset to factory defaults to load the simplified user interface again. Once this is done none of the configuration made in the Enterprise user interface is retained.

4. To proceed loading the enterprise user interface, select **Yes**. The Access Point loads the Enterprise user interface at next reboot.

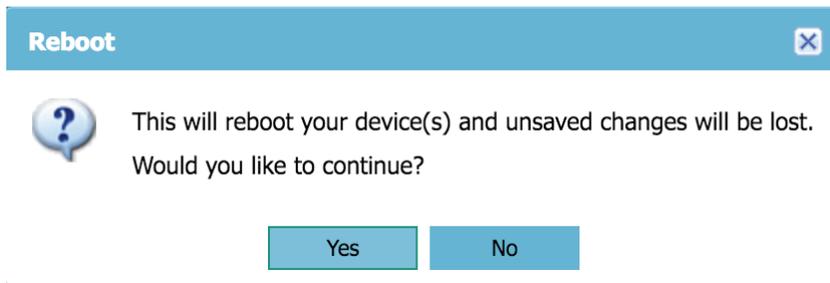
Note

Configuration changes made in the simplified user interface carry over to the Enterprise user interface after the Enterprise user interface is loaded.

5. To reboot the Access Point, select it from the table and select **Tools**.



6. Select **Reboot** from the **Tools** menu. A warning dialog appears.



7. Select **Yes** to reboot the device using the enterprise user interface.

Basic Access Point Settings

- To edit an Access Point's settings, click on the **AP Name** of the Access Point you wish to edit.

Edit -> ap7532-1777B4 ?

Basic Settings

Name:

Location : default

Version : 5.8.2.0-020D

Model : AP-7532-67030-WR

Up Time : 0 days, 07 hours 18 minutes

MAC Address: 84-24-8D-17-77-B4

Default Gateway:

Wireless Settings

2.4GHz Channel: Power: (dBm) Data Rate:

5GHz Channel: Power: (dBm) Data Rate:

Radius Server Settings

Enable Radius Server:

IP Settings | DNS Servers | Route

[Detail >>](#)

Add		Delete		Number of Interfaces: 1	
<input type="checkbox"/>	Interface (1-4094)	Description	IP Address	Edit	
<input type="checkbox"/>	VLAN1	WAN Interface	192.168.1.1/24		

- Refer to the following device information in **Basic Settings**:

AP Name	Displays the unique name assigned to the Access Point. This name can be changed on this screen or the <i>Configuration > Basic</i> screen.
Location	Displays the location name configured on the <i>Configuration > Basic</i> screen.
Version	Displays the active firmware version currently running on the Access Point.
Model	Displays the device model number for the Access Point.
Up Time	Displays the amount of time in days, hours and minutes since the last time the device rebooted. Use this information to determine whether a newer firmware version is available potentially providing an enhanced feature set.
MAC Address	Displays the hardware encoded MAC address of the Access Point. The MAC address is set at the factory and cannot be modified via the management software.

Default Gateway	Displays the default gateway information for the Access Point. A default gateway provides an entry/exit point for the network as it commonly connects an internal network to an external network. To override the default gateway address, specify a new IP address.
------------------------	--

3. Configure the following options for **Wireless Settings**:

2.4 GHz Channel / Power	Use the drop-down menu to select a channel for the 2.4GHz radio. Set the transmit power of the selected Access Point radio. If using a dual radio model Access Point, each radio should be configured with a unique transmit power in respect to its intended client support function. Select the Smart option to let Smart RF determine the transmit power. A setting of 0 defines the radio as using Smart RF to determine its output power. 0 dBm, Smart RF, is the default value.
5 GHz Channel / Power	If applicable, use the drop-down menu to select a channel for the Access Point's 5GHz radio. All model Access Points support a second radio, with the exception of single radio model AP6511 and AP6521 Access Points. If using a dual radio model Access Point, each radio should be configured with a unique transmit power in respect to its intended client support function. Select the Smart option to let Smart RF determine the transmit power. A setting of 0 defines the radio as using Smart RF to determine its output power. 0 dBm, Smart RF, is the default value.

4. Select **Enable RADIUS Server** to enable the onboard RADIUS server. RADIUS settings can be configured on the RADIUS Screen.
5. Optionally, from the **IP Settings** tab **Add**, **Edit** or **Delete** LAN Settings for the Access Point. When adding and editing settings specify the following:

Interface	Use the drop-down menu to select an Access Point interface to connect to the network. Keep unused interfaces disabled to reduce network vulnerabilities.
Description	Enter a description for each interface to distinguish it from other devices with similar attributes.
IP Address	Enter or edit the IP Address associated with each interface. Click the edit icon next to the corresponding interface to edit the IP Address.
Edit	Select <i>Edit</i> to make changes to the selected interface.
Add	Select to <i>Add</i> create a new VLAN interface.
Delete	To delete VLAN interfaces select the VLAN(s) and click <i>Delete</i> .

Note

VLAN interfaces may also be added, edited or deleted on the Configuration > LAN screen.

6. Selecting **Detail** will display the details screen which displays the **Default Gateway** and **DNS** server information in addition to the VLAN information. VLANs cannot be added, edited or deleted in the details screen.
7. Optionally, from the **DNS Servers** tab, override DNS server settings for the Access Point. When adding and editing DNS servers settings specify the following:

IP Address	Enter or edit the IP Address associated with each interface. Click the edit icon next to the corresponding interface to edit the IP Address.
-------------------	--

- Optionally, from the **Route** tab, **Add**, **Edit** or **Delete** LAN settings for the Access Point. When adding and editing settings specify the following:

Network Address	Specify the destination IP address and mask in the A.B.C.D/M format.
Gateway	Optionally specify the default gateway IP address and mask, in A.B.C.D/M format, used to communicate with the main router. A default gateway provides an entry/exit point for the network as it commonly connects an internal network to an external network.

- When all required settings are configured, click **Apply** to save the changes to the Access Point configuration.
- To return to the Access Points screen click **<< Go Back**.

Event History

Event History

The **Event History** displays historical events for managed Access Points. Events can be filtered in the search field.

To review the event history:

1. Select **Event History** from the main menu.

Event History ?

Events

Timestamp	Module	Message	Severity	Source	Hostname
Sun Jan 03 16:49:53 2016	SYSTEM	Logged out user 'admin' with privilege 'superuser' from '169.254.2.90(web)'	info	84-24-8D-16-02-5C	ap7522-16025C
Sun Jan 03 16:28:10 2016	SYSTEM	UI user 'admin' from: '169.254.2.90' authentication failed	error	84-24-8D-16-02-5C	ap7522-16025C
Sun Jan 03 16:27:54 2016	SYSTEM	System Cold start. System came up at Jan 03 16:27:54 2016	info	84-24-8D-16-02-5C	ap7522-16025C
Sun Jan 03 16:26:20 2016	DIAG	LED state message RADIO_2_52G_NOT_CONFIG from module DOT11	info	84-24-8D-16-02-5C	ap7522-16025C
Sun Jan 03 16:26:20 2016	RADIO	Radio 'ap7522-16025C:R2' changing state from 'Initializing' to 'Off(no wlan/meshpoints mapped)'	notice	84-24-8D-16-02-5C	ap7522-16025C
Sun Jan 03 16:26:20 2016	DIAG	LED state message RADIO_2_52G_LED_ON from module DOT11	info	84-24-8D-16-02-5C	ap7522-16025C
Sun Jan 03 16:26:20 2016	RADIO	Radio 'ap7522-16025C:R2' changing state from 'Off' to 'Initializing'	notice	84-24-8D-16-02-5C	ap7522-16025C
Sun Jan 03 16:26:19 2016	NSM	Interface ge1 is up	warn...	84-24-8D-16-02-5C	ap7522-16025C
Sun Jan 03 16:26:19 2016	DIAG	LED state message RADIO_1_24G_NOT_CONFIG from module DOT11	info	84-24-8D-16-02-5C	ap7522-16025C
Sun Jan 03 16:26:19 2016	RADIO	Radio 'ap7522-16025C:R1' changing state from 'Initializing' to 'Off(no wlan/meshpoints mapped)'	notice	84-24-8D-16-02-5C	ap7522-16025C
Sun Jan 03 16:26:19 2016	DIAG	LED state message RADIO_1_24G_LED_ON from module DOT11	info	84-24-8D-16-02-5C	ap7522-16025C
Sun Jan 03 16:26:19 2016	RADIO	Radio 'ap7522-16025C:R1' changing state from 'Off' to 'Initializing'	notice	84-24-8D-16-02-5C	ap7522-16025C
Sun Jan 03 16:26:19 2016	DIAG	LED state message RADIO_2_52G_NOT_CONFIG from module DOT11	info	84-24-8D-16-02-5C	ap7522-16025C
Sun Jan 03 16:26:19 2016	RADIO	Radio 'ap7522-16025C:R2' changing state from 'Initializing' to 'Off(no wlan/meshpoints mapped)'	notice	84-24-8D-16-02-5C	ap7522-16025C

2. Review the following event data to determine the severity of specific events and the devices reporting them:

Timestamp	Displays the timestamp (time zone specific) when the displayed event message was generated. Use this information to help assess whether the listed timestamp coincides with any known issue impacting the network.
------------------	--

Module	Displays the Access Point module (resource) detecting, reporting and tracking the event. Events detected by other modules are not tracked.
Message	Displays error or status messages for each event listed. Use the message text as an additional means of assessing an event's potential impact to the managed Access Point.
Severity	Displays the severity of the event as defined for tracking from the Configuration screen. Severity options include: <i>All Severities</i> – All events are displayed irrespective of their severity <i>Critical</i> – Only critical events are displayed <i>Error</i> – Only errors and above are displayed <i>Warning</i> – Only warnings and above are displayed <i>Informational</i> – Only informational and above events are displayed
Source	Displays the hardware encoded MAC address of the source device tracked by the selected module.
Hostname	Displays the administrator assigned name of the source device tracked by the listed module.

3. Use the **Search** field as necessary to refine event history to specific criteria.
4. Select **Clear All** clear the event counters and begin a new event log collection.
5. Select **Refresh** to manually update the event history logs. If you have selected **Stop** select refresh to re-enable automatic updating
6. Select **Stop** to stop automatic updating of the event history logs.