



WiNG Express Manager 5.8.2



User Guide



Zebra and the Zebra head graphic are registered trademarks of ZIH Corp. The Symbol logo is a registered trademark of Symbol Technologies, Inc., a Zebra Technologies company.
© 2015 Symbol Technologies, Inc.

Contents

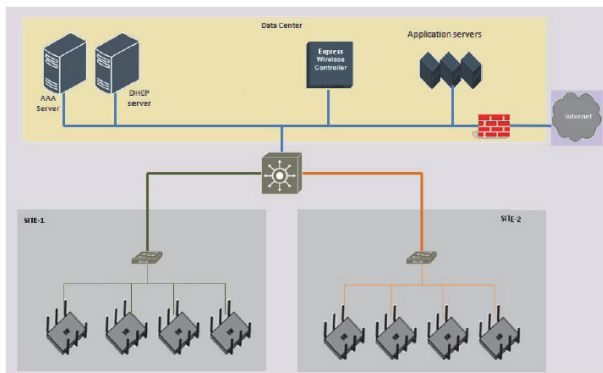
WiNG Express Manager	5
Dashboard	7
System Dashboard.....	8
Site Dashboard.....	9
Heat Map	10
Monitor	11
Monitor AP Radios (System)	11
Radio Details (System).....	13
Monitor AP Radios (Site)	14
Radio Details (Site).....	16
Monitor WLANs (System)	17
WLAN Details (System)	20
Monitor WLANs (Site).....	21
WLAN Details (Site)	24
Monitor Clients (System).....	25
Clients Details (System)	27
Monitor Clients (Site).....	29
Clients Details (Site)	30
Application Visibility (System)	31
Application	31
Category	33
Application Visibility (Site)	34
Application.....	34
Category	36
Guest Access (System).....	37
Statistics (System)	37
Social (System)	40
Reports (System)	41
Notification (System)	42
Database (System)	44
Guest Access (Site).....	46
Statistics (Site).....	46
Social (Site)	48
Reports (Site)	49
Notification (Site)	51
Database (Site).....	52
Configuration.....	55
Configuration (System).....	55
Basic Configuration (System)	55
Sites Details (System)	59
Multi-Site Auto Provisioning (System)	60
LAN Configuration (System)	62
Wireless Configuration (System).....	64
Security Firewall Configuration (System).....	74
Security Certificate Configuration (System)	78
Security Application Visibility (System)	80
RADIUS Configuration (System).....	81
Basic Management Configuration (System)	84
Guest Management Configuration (System)	86
Device Configuration (System)	89
Configuration (Site).....	93
Basic Configuration (Site)	93
LAN Configuration (Site)	95
Wireless Configuration (Site).....	96
Security Firewall Configuration (Site).....	108
Security WIPS Configuration (Site)	112

DHCP Configuration (Site)	114
RADIUS Configuration (Site)	115
Device Configuration (Site)	118
Troubleshoot	123
Event History.....	123
Tools	124
CUSTOMER-SUPPORT.....	127

WING EXPRESS MANAGER

Zebra provides a highly scalable centrally managed controller and virtual controller based Wireless LAN solution for customers deploying 802.11ac Wireless LAN services in a small business environment, such as single site to multi-site deployments that scale up to 1024 Access Points. In a typical deployment, a Zebra Access Point acts as a virtual controller that supports a number of Access Points deployed in a private network across a site. Express Wireless controllers are installed at the data center and the Access Points are deployed across the campus. The configuration and management is performed by the Zebra Express wireless controllers or the virtual controllers.

In a typical WiNG Express deployment, the wireless user traffic is bridged locally by the Access Point towards the destination. The local forwarding mode eliminates the latency of routing the traffic through the wireless controller and unnecessary overload on the wireless controller.



You can utilize Express APs for most deployments, with two wireless controllers working in high availability mode. Zebra offers various wireless controllers and Access Point models to suit the needs of various enterprise requirements. The number of Access Points supported depends on the controller model and Access Point. Each Access Point can provide full QoS (Quality of Service), security and mobility by itself, without tunneling the traffic through the wireless controller.

DASHBOARD

WiNG Express Manager is offered in both hardware and virtual appliance solutions to meet your deployment needs.

If your 25 Access Points are spread over multiple locations, or if your business requires more than 25 Access Points in one or more location, WiNG Express Manager can easily scale up to 1,024 Access Points in all of your sites.

In This Chapter

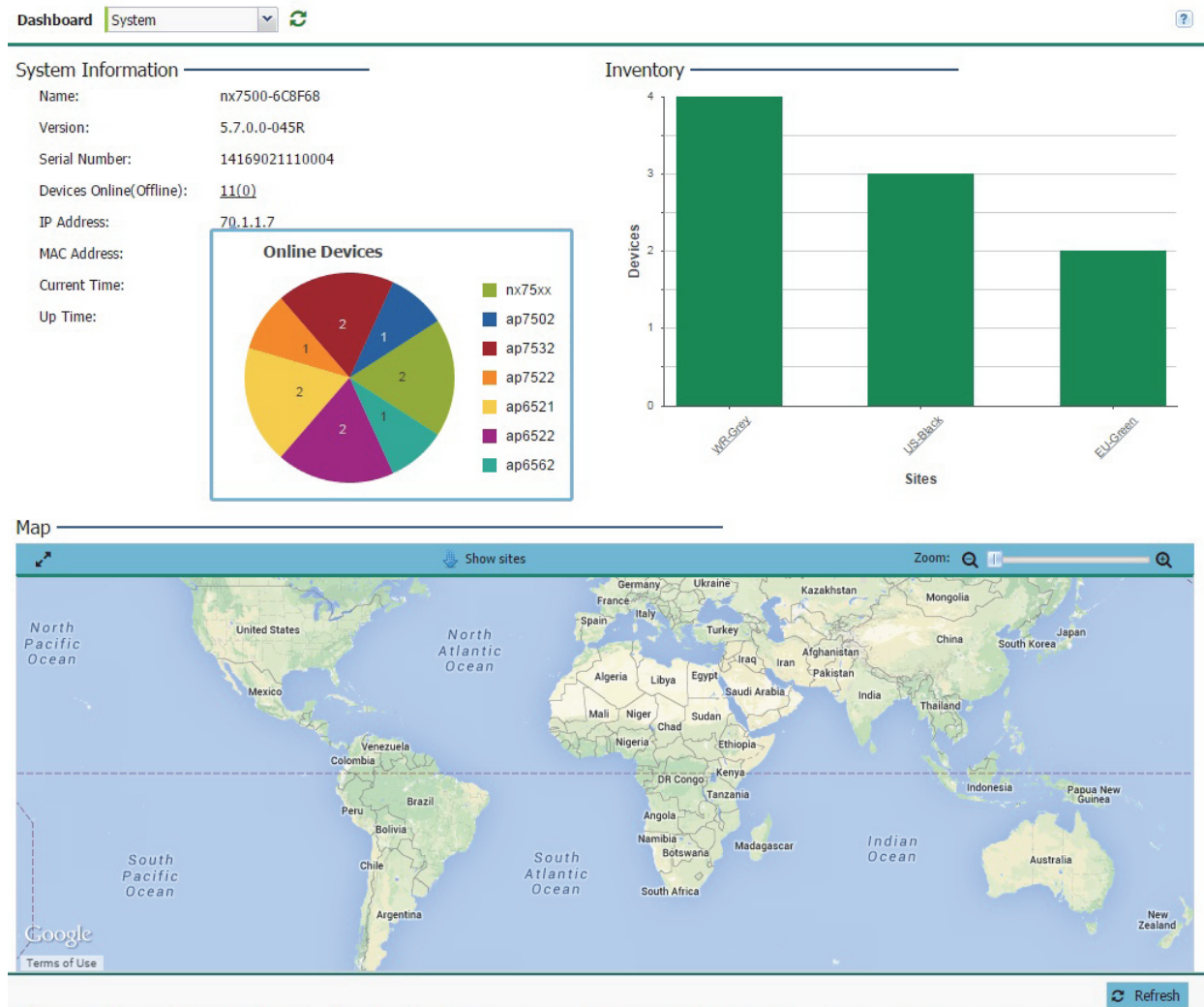
System Dashboard.....	8
Site Dashboard.....	9

System Dashboard

The dashboard enables administrators to review and troubleshoot the network, assess network component health and conduct a diagnostic review of device performance.

To review high-level WiNG Express Manager dashboard information:

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



- 2 Review the following to assess the health of the WiNG Express managed network:

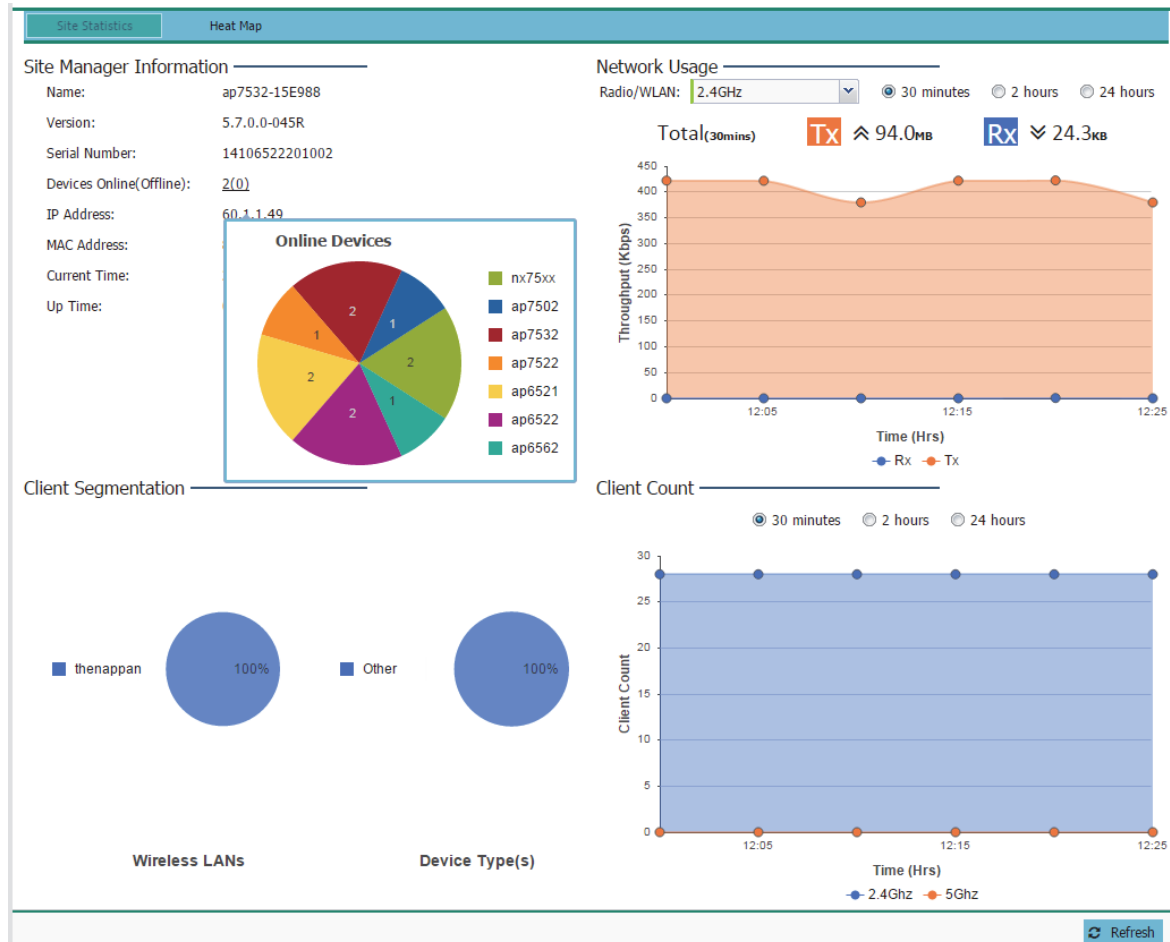
System Information	Displays the administrator assigned device <i>Name</i> , <i>Version</i> , <i>Serial Number</i> , the number of Online and Offline devices, the designated <i>IP</i> and <i>Device MAC</i> addresses, <i>Current Time</i> and <i>Up Time</i> listing when the Express Manager was last offline.
Inventory	Displays a graph showing device utilization amongst managed devices. Use this information to assess the device load of APs currently being deployed in WiNG Express Manager network.
Map View	Displays a map view showing the site locations for all configured sites. Use the Zoom controls to change the magnification of the map and click and drag to move the map's position.

Site Dashboard

The dashboard enables administrators to review and troubleshoot 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 WiNG Express Manager dashboard information:

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



- 2 Review the following to assess the health of the WiNG Express Manager network:

<p>Site Information</p>	<p>Displays the administrator assigned device <i>Name</i>, <i>Version</i>, <i>Serial Number</i>, the number of Online and Offline devices, and a designated <i>IP</i> and <i>Device MAC</i> addresses, <i>Current Time</i> and <i>Up Time</i> listing when the WiNG Express Manager was last offline.</p>
<p>Network Usage</p>	<p>Displays the network throughput (both in the transmit and receive directions) for the selected device or system over the defined trending period of <i>30 minutes</i>, <i>2 hours</i> or <i>24 hours</i>.</p>
<p>Client Segmentation</p>	<p>Displays a set of pie charts segregating the WLAN utilization amongst peer device types. Use this information to assess whether client loads exceed the number and type of WLANs currently deployed with WiNG Express managed Access Points.</p>

Network Client Count	Displays the total client count for the network over the selected time of <i>30 minutes, 2 hours or 24 hours</i> . Clients are partitioned into their current 2.4Ghz and 5Ghz radio bands to assess whether the client load is adequately supported in each band.
-----------------------------	---

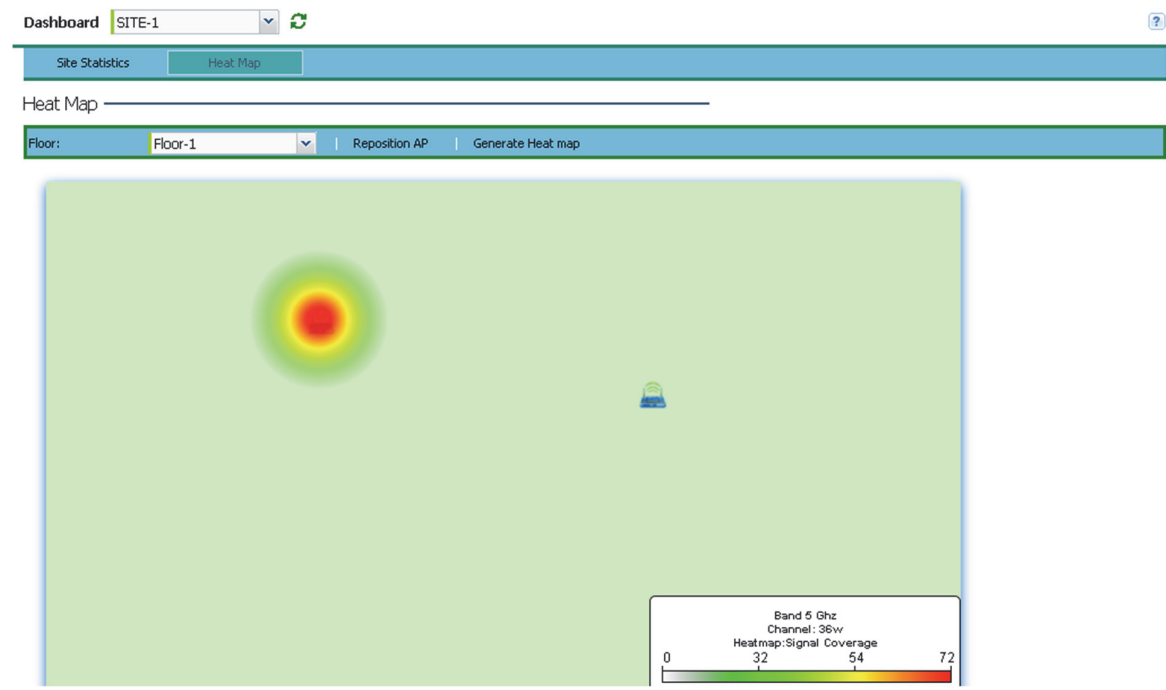
- 3 Select **Heat Map** for detailed signal and coverage information for the active site.

Heat Map

The dashboard enables administrators to review and troubleshoot 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 WiNG Express Manager dashboard information:

- 1 Select **Dashboard** in the main menu.
- 2 Select **Heat Map**.



- 3 Select a **Floor** from the drop-down menu.
- 4 When all devices are positioned correctly on the floor plan select **Generate Heat map**. The heat map for each AP displays the signal coverage corresponding to the key at the bottom right of the screen.

MONITOR

The ongoing system and site level log tracks and maintains a complete WLAN event history, providing valuable trending information and details to address a specific incident and prevent its re-occurrence. Inspect aggregated analytics at the system level, or drill-down to site-specific details for more granularity.

In This Chapter

Monitor AP Radios (System)	11
Monitor AP Radios (Site).....	14
Monitor WLANs (System).....	17
Monitor WLANs (Site).....	21
Monitor Clients (System).....	25
Monitor Clients (Site).....	29
Application Visibility (System)	31
Application Visibility (Site)	34
Guest Access (System).....	37
Guest Access (Site).....	46

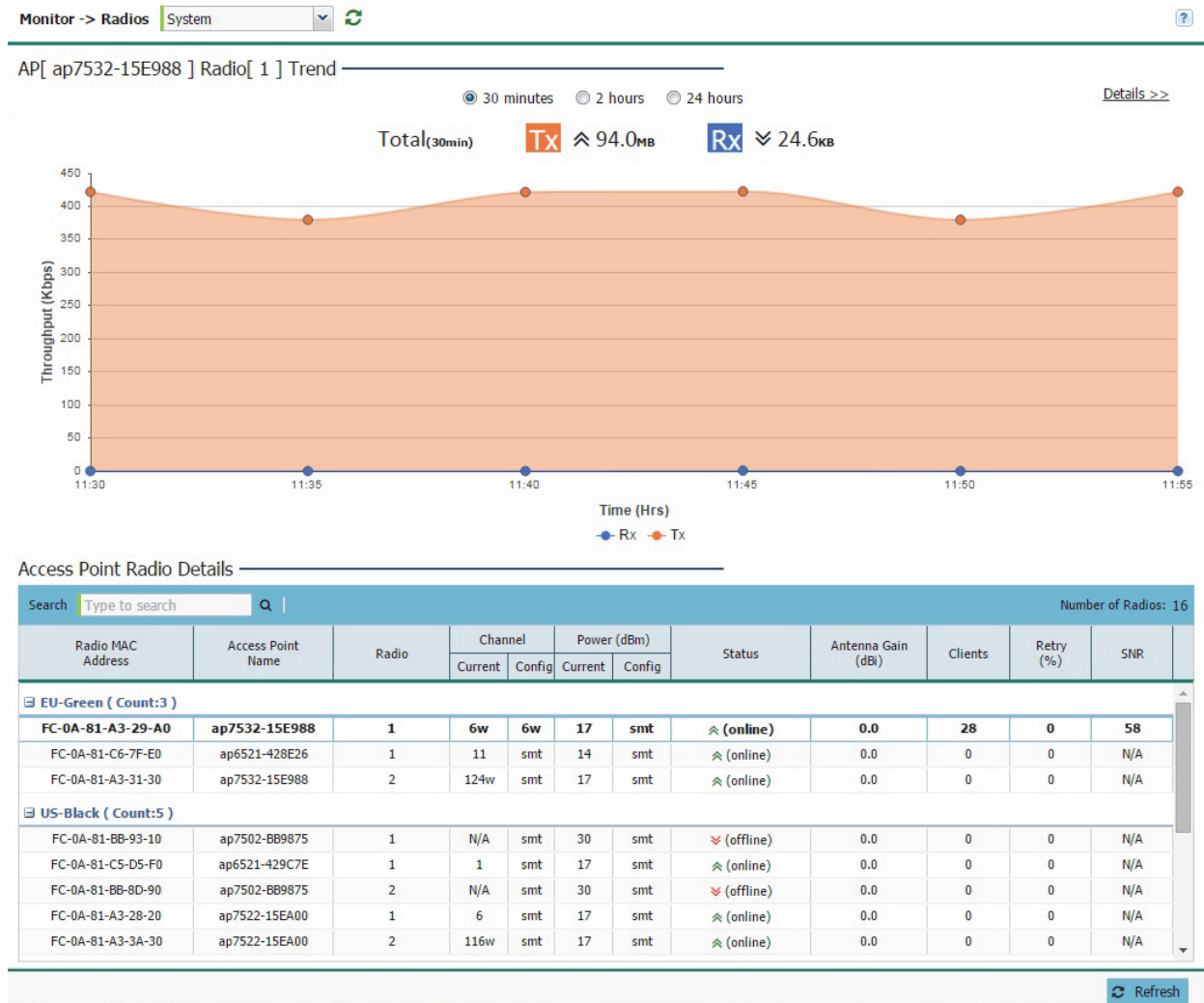
Monitor AP Radios (System)

Use the Radios screen to assess radio utilization, power consumption and client connection quality.

To monitor WiNG Express Manager connected Access Point radios:

- 1 Select **Monitor** from the main menu and select **Radios**.

- Select an 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 utilization, power and signal strength.



- 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 WiNG Express Manager connection.
Radio	Displays the radio number for each Access Point radio on the network. AP6511 and AP6521 models are single radio models, all other models support at least two radios.
Channel: Current / Config	Displays the current channel number each listed Access Point radio is assigned to transmit and receive. 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 (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 status for each Access Point. If an Access Point is up, two green up arrows display. If an Access Point is down, two green down arrows display.
Clients	Displays the number of clients currently associated to each Access Point radio. AP6511 and AP6521 single radio Access Points support 128 clients, other dual-radio models support 128 clients per radio, up to a total of 256 client connections.
Retry (%)	Displays the retry percentage for packets transmitted 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 high 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.

Radio Details (System)

Use the **Radio Details** screen to review information about the quality of the WiNG Express Manager connected radio utilization, power consumption, and client connections.

To monitor WiNG Express Manager connected Access Point radios:

- 1 Select **Monitor** from the main menu and click on **Radios**.
- 2 Select an 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 utilization, power and signal strength.

3 Select **Details**.



4 Use the detailed graphs to analyze trends or anomalies in the **Throughput**, **SNR** (Signal to Noise Ratio), and **Client Count** over the specified time period.

5 Select << **Summary** to return to the main radio screen.

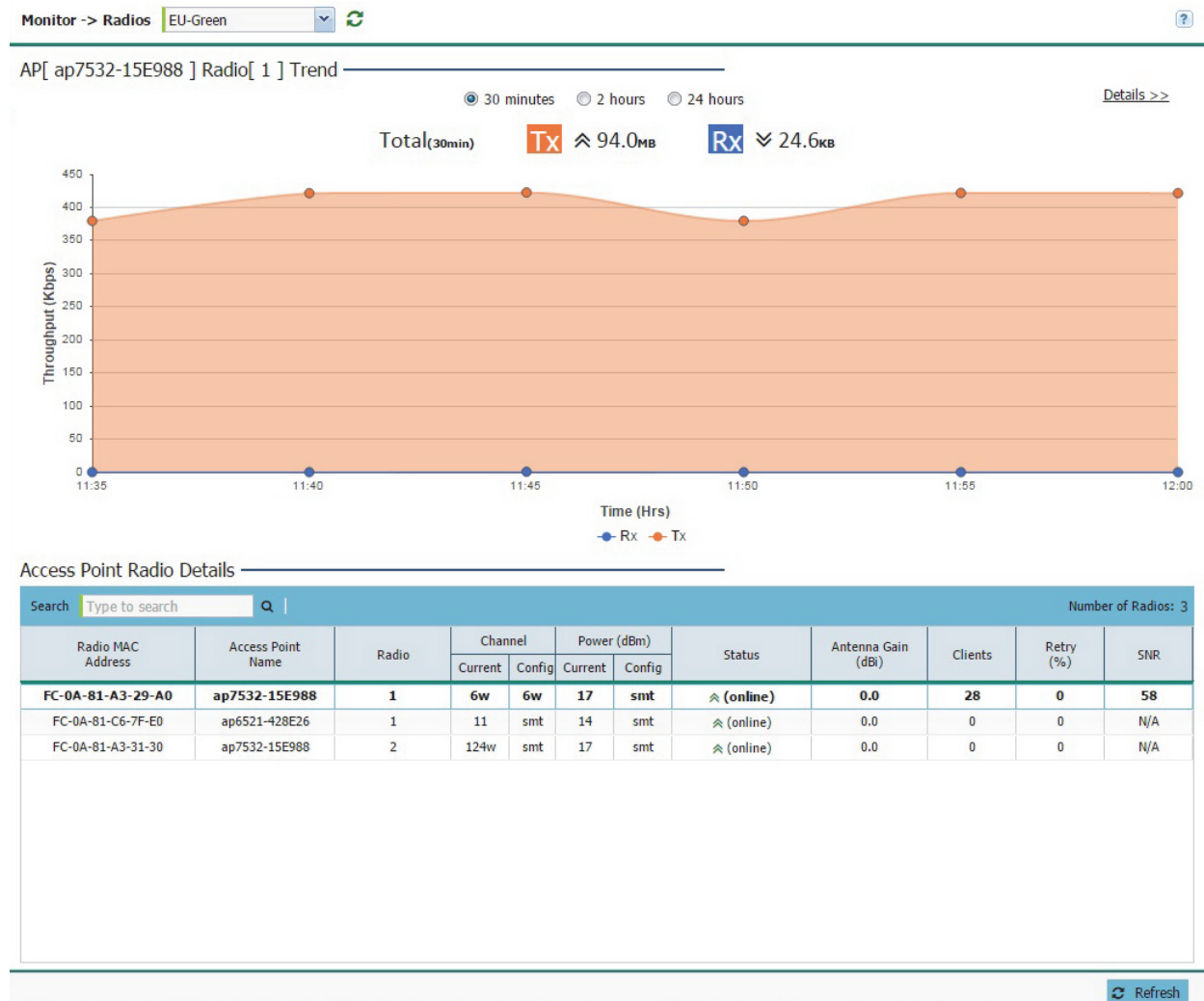
Monitor AP Radios (Site)

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

To monitor WiNG Express Manager connected Access Point radios:

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

- 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 utilization, power and signal strength.



- 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 by the WiNG Express Manager.
Radio	Displays the radio number for each Access Point radio on the network. AP6511 and AP6521 models are single radio models, remaining models support at least two radios.
Channel: Current / Config	Displays the current channel number each listed Access Point radio uses to transmit and receive. Available Channels 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 an Access Point radio's current power level in dBm and 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 status for each Access Point. If an Access Point is up (operational), two green up arrows display. If an Access Point is down (offline), two green down arrows display.
Clients	Displays the number of clients currently associated to each Access Point radio. AP6511 and AP6521 single radio Access Points support 128 clients. Remaining dual-radio models support up to 256 client connections.
Retry (%)	Displays the retry percentage for packets sent on each Access Point radio. Use the retry rate to assess the overall effectiveness of the RF environment (as displayed as a percentage).
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 high 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.

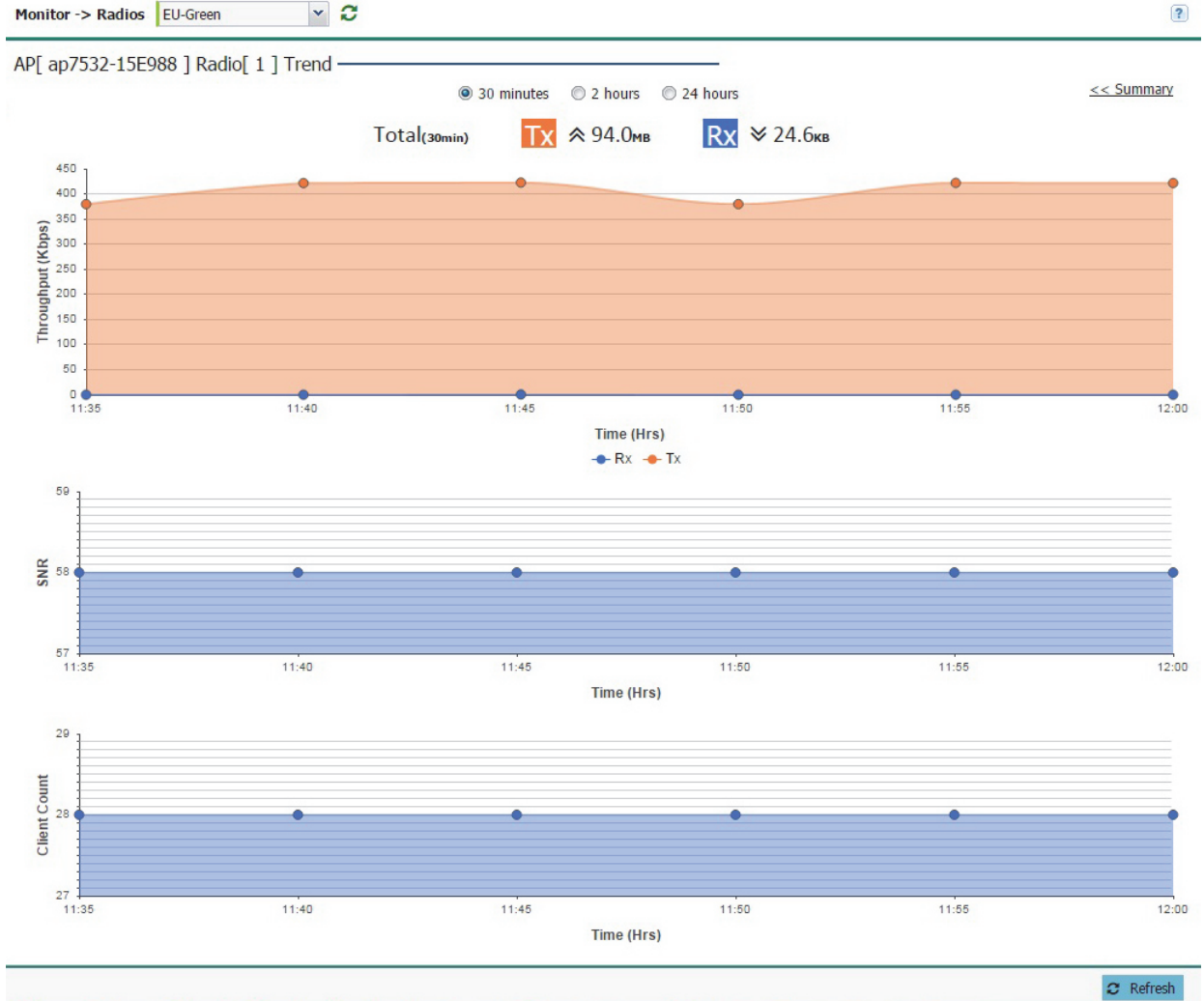
Radio Details (Site)

Use the **Radio Details** screen to assess WiNG Express Manager connected radio utilization, power consumption, and client connections.

To monitor WiNG Express Manager connected Access Point radios:

- 1 Select **Monitor** from the main menu and click on **Radios**.
- 2 Select time 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 utilization, power and signal strength.

3 Select **Details**.



- 4 Use the detailed graphs to analyze trends or anomalies in the **Throughput**, **SNR** (Signal to Noise Ratio), and **Client Count** over the specified time period.
- 5 Select **<< Summary** to return to the main radio screen.

Monitor WLANs (System)

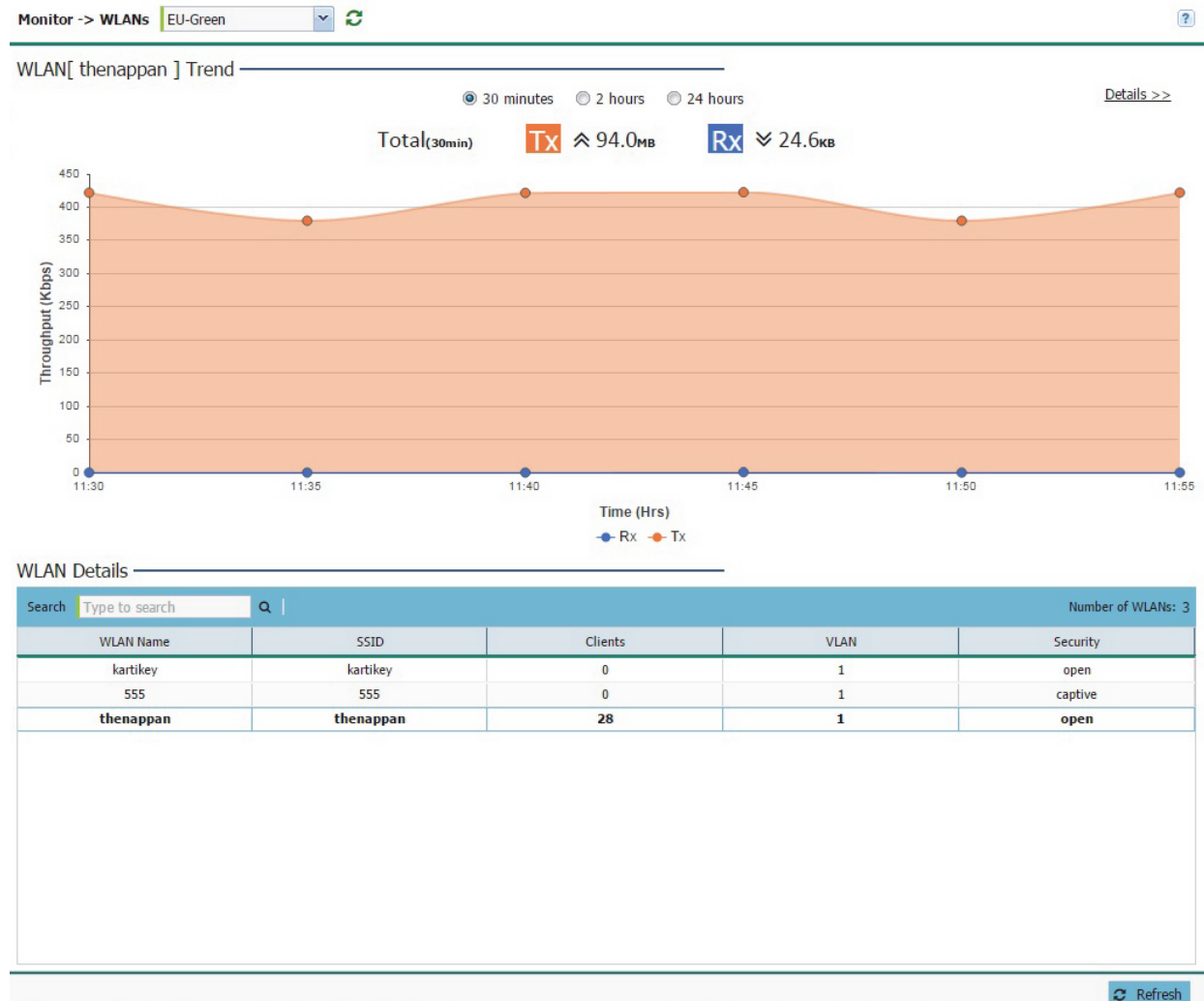
A WLAN can be advertised from a single Access Point radio or can span multiple Access Points. WLAN configurations can be defined to only support specific areas of a site. For example, a guest access WLAN could only be mapped to a 2.4GHz radio in a lobby or conference room providing limited coverage, 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 WiNG Express Manager Access Point utilization:

- 1 Select **Monitor** from the main menu and select **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, noise ratio and client counts.



- Review the following WLAN information to help determine whether the Access Point's WLAN utilization is optimally set for its WiNG Express Manager deployment objective:

WLAN Name	Displays the administrator defined WLAN name for each of the WiNG Express 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 <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 using 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 member traffic either with peer Access Points or client connections. Authentication ensures only known and trusted users or devices can 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>WEP-64 - Wired Equivalent Privacy</i> (WEP) is a security protocol specified in the IEEE <i>Wireless Fidelity</i> (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 802.1 X 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</i> (IV) 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</i> (IV) 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>Security (Continued)</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><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 are used to 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><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>
--	---

- 4 To review more granular details of a specific WLAN, select it from the table and select the [Details >>](#) link.

WLAN Details (System)

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 to specific areas of a site. For example a guest access WLAN could 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 WiNG Express Manager Access Point 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, noise ratio and client counts.

3 Select **Details**.



- 4 Use the detailed graphs to analyze trends or anomalies in the **Throughput** and **Client Count** over the specified period of time.
- 5 Select **<< Summary** to return to the main WLAN screen.

Monitor WLANs (Site)

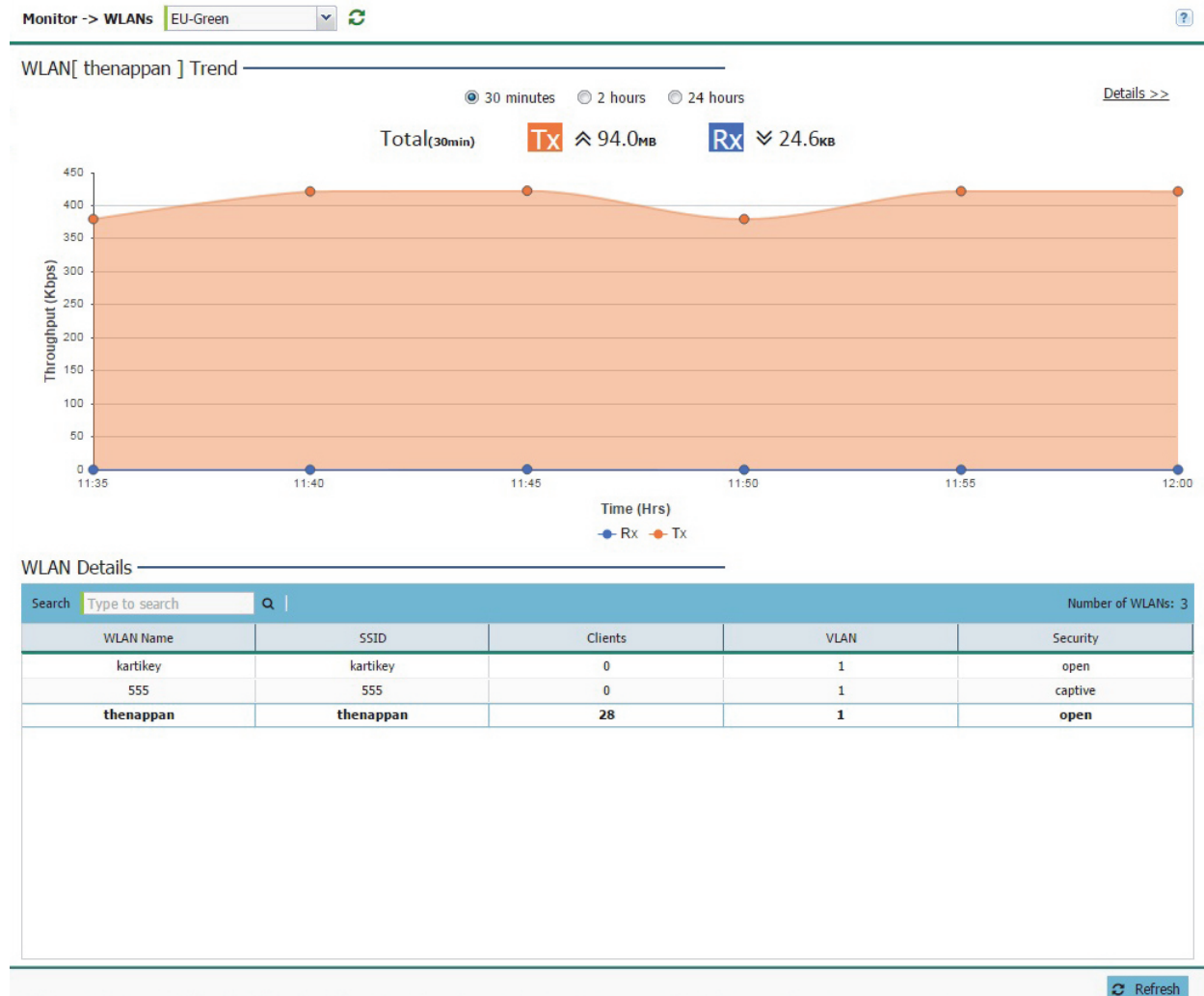
A WLAN can be advertised from a single Access Point or span multiple Access Points. WLAN configurations can be defined to only provide to specific areas of a site. For example, a guest access WLAN may only be mapped to a 2.4GHz radio in a lobby or conference room providing limited coverage, while a data 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 WiNG Express Manager Access Point utilization:

- 1 Select **Monitor** from the main menu and select **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, noise ratio and client counts.



- Review the following WLAN information to help determine whether the Access Point's WLAN utilization is optimally set for its WiNG Express Manager deployment objective:

WLAN Name	Displays the administrator defined WLAN name for each WLAN. 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 <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 using 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 member traffic either with peer Access Points or client connections. Authentication ensures only known and trusted users or devices can 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>WEP-64 - Wired Equivalent Privacy</i> (WEP) is a security protocol specified in the IEEE <i>Wireless Fidelity</i> (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 802.1 X 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</i> (IV) 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</i> (IV) 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>Security (Continued)</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><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 are used to 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><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>
--	---

- 4 To review more granular details of a specific WLAN, select it from the table and select the [Details >>](#) link.

WLAN Details (Site)

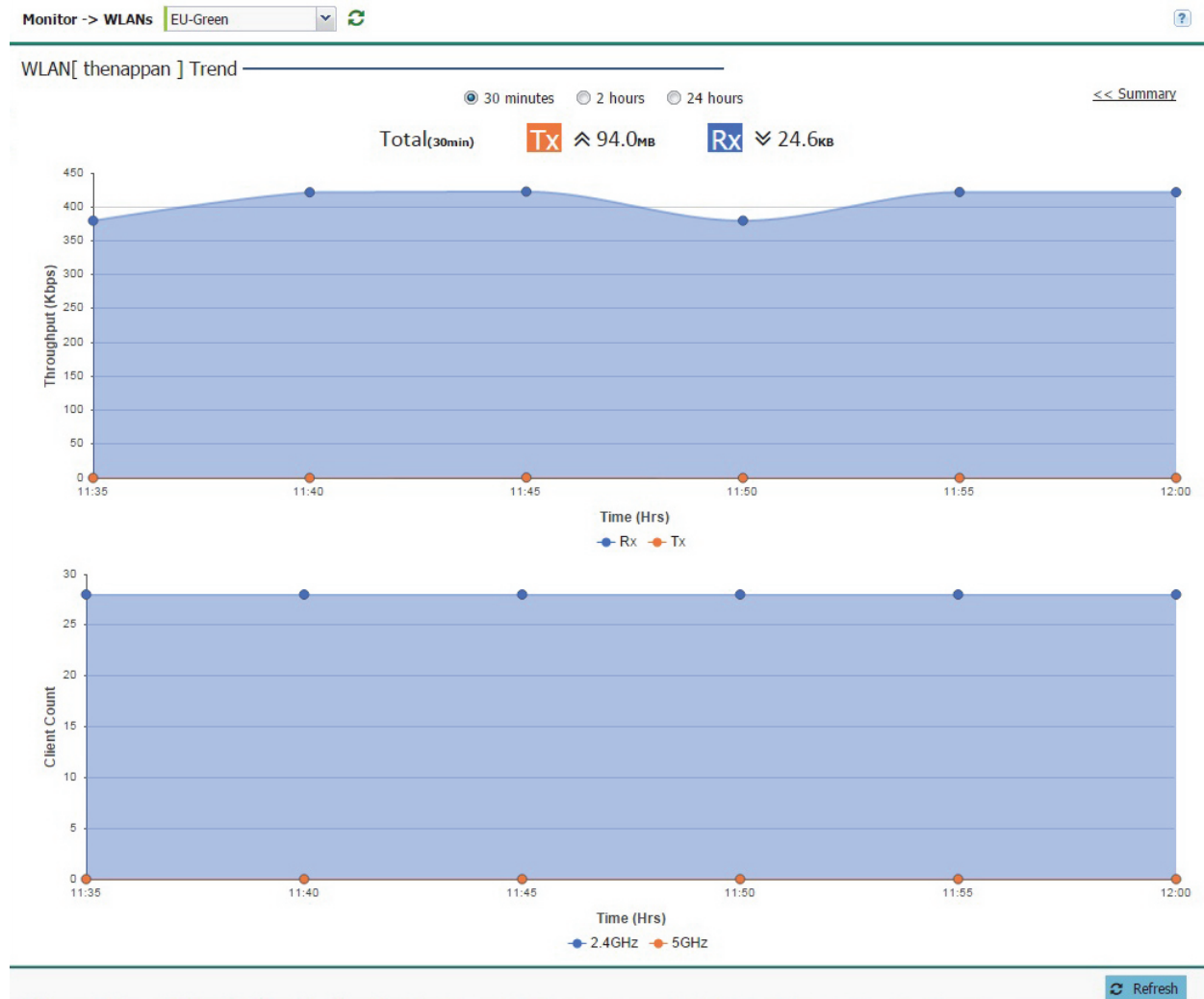
A WLAN can be advertised from a single Access Point radio or can span multiple Access Points. WLAN configurations can be defined to only provide to specific areas of a site. For example a guest access WLAN could only be mapped to a 2.4GHz radio in a lobby or conference room providing limited coverage, 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 WiNG Express Manager Access Point 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, noise ratio and client counts.

3 Select **Details**.



- 4 Use the detailed graphs to analyze trends or anomalies in the **Throughput** and **Client Count** over the specified time period.
- 5 Select **<< Summary** to return to the main WLAN screen.

Monitor Clients (System)

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

To review an Access Point's wireless interface connection:

- 1 Select **Monitor** from the main menu.

2 Select Clients.

Monitor -> Clients System ↻ ?

Client[60.1.1.15] Trend 30 minutes 2 hours 24 hours [Details >>](#)

Total(30min) **Tx** ≈ 3.4MB **Rx** ≈ 0B

Wireless Clients Details

Search Number of Clients: 28

IP Address	MAC Address	Signal (dBm)	SNR	Channel	Radio Type	Radio Association	Data Rate (Mbps)		BSSID	Access Point Name	WLAN	VLAN	Authenticatio Status
							Tx	Rx					
EU-Green (Count:28)													
60.1.1.15	00-31-DD-01-00-1B	-34	58	6	11bgn	1	130	0	FC-0A-81-A3-29-A0	ap7532-15E988	the...	1	none
60.1.1.38	00-31-DD-01-00-05	-34	58	6	11bgn	1	130	1	FC-0A-81-A3-29-A0	ap7532-15E988	then...	1	none
60.1.1.37	00-31-DD-01-00-09	-34	58	6	11bgn	1	130	10	FC-0A-81-A3-29-A0	ap7532-15E988	then...	1	none
60.1.1.35	00-31-DD-01-00-08	-34	58	6	11bgn	1	130	0	FC-0A-81-A3-29-A0	ap7532-15E988	then...	1	none
60.1.1.18	00-31-DD-01-00-18	-34	58	6	11bgn	1	130	0	FC-0A-81-A3-29-A0	ap7532-15E988	then...	1	none
60.1.1.34	00-31-DD-01-00-0A	-34	58	6	11bgn	1	130	1	FC-0A-81-A3-29-A0	ap7532-15E988	then...	1	none

↻ Refresh

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, noise ratio and client counts.

3 Review the following client information for WiNG Express Manager connected 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 WiNG Express Manager connected 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 high 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, AP7522 and AP7532 models are capable of 802.11ac connections.
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 managed client radios in the same radio coverage area.
BSSID	Displays the BSSID of the WiNG Express Manager connected Access Point establishing the client's wireless connection.
Access Point Name	Displays the Access Point's unique administrator assigned name provided upon initial WiNG Express management.
WLAN	Displays the SSID of the Wireless LAN, if any, which the wireless client is currently associated with.
VLAN	Displays the VLAN number the wireless client is marked to pass traffic on.
Authentication Status	Displays the authentication type used by the wireless client to connect 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 manufacturer of each listed client as a means of assessing its support capabilities with the WiNG Express managed network.

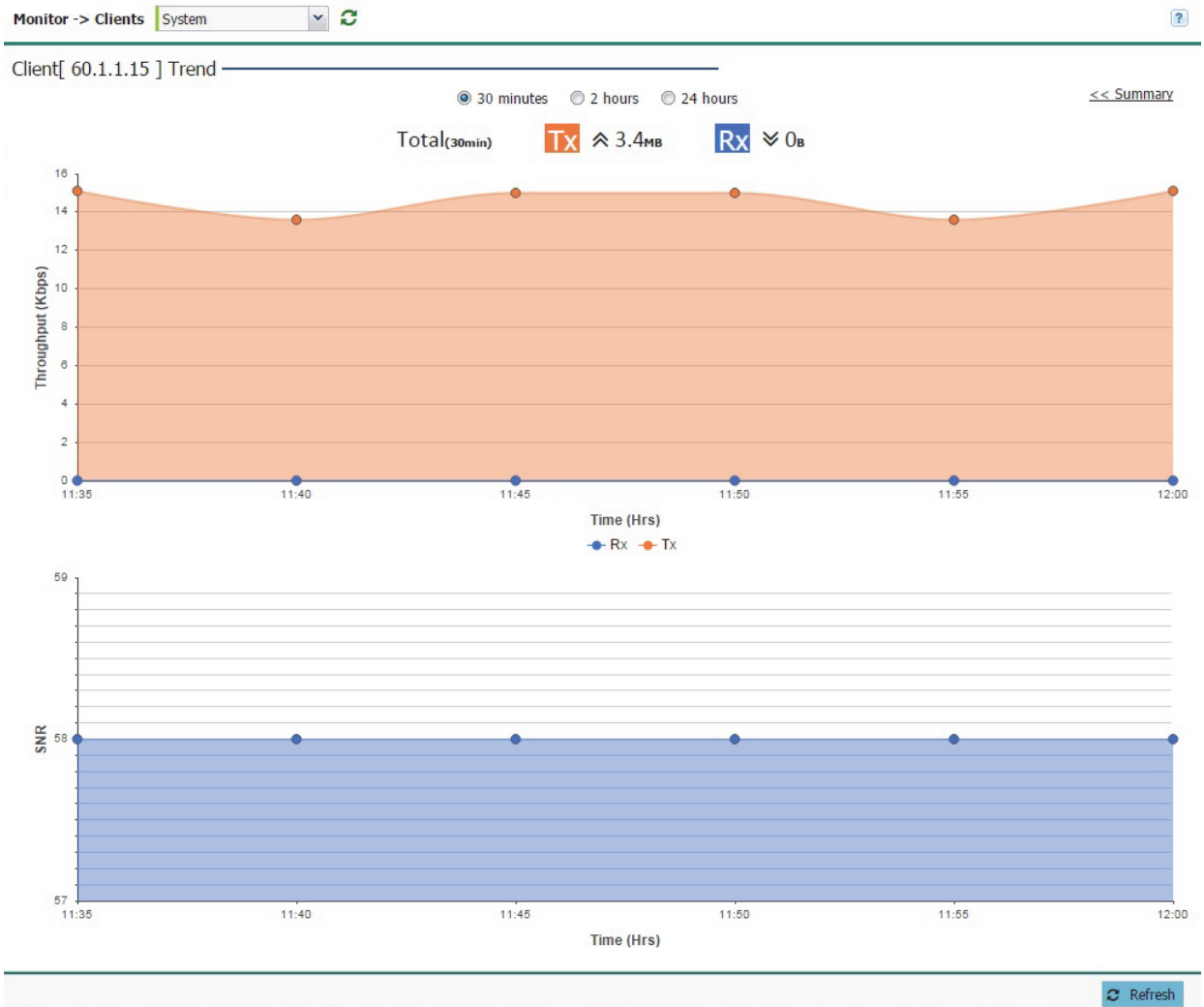
Clients Details (System)

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

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

- 1 Select **Monitor** from the main menu.
- 2 Select **Clients**.

3 Select **Details**.



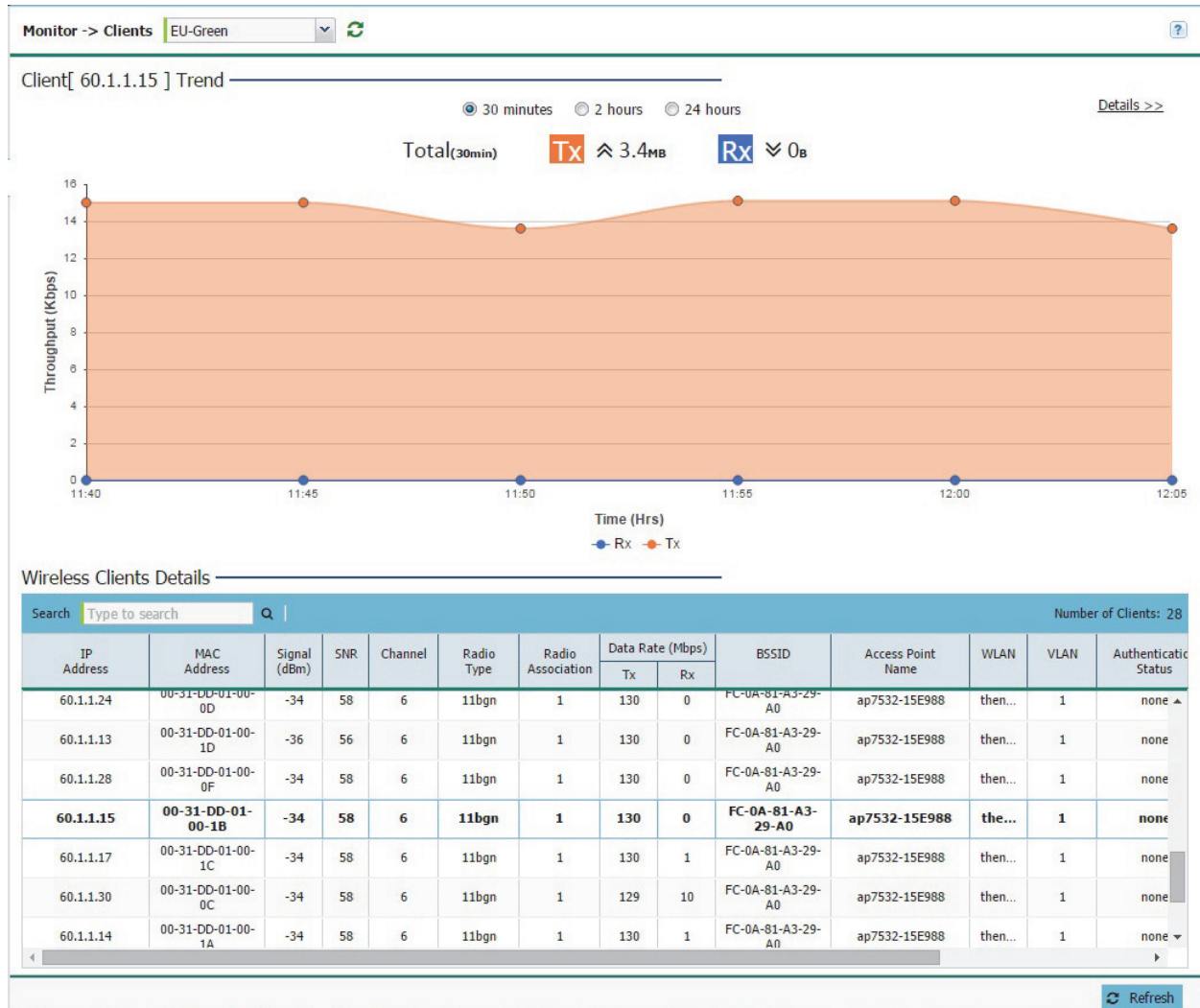
- 4 Use the detailed graphs to analyze trends or anomalies in the **Throughput** and **SNR** (Signal to Noise Ratio) and **Top 10 Applications Trends** over the specified period of time.
- 5 Select **<< Summary** to return to the main clients screen.

Monitor Clients (Site)

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

To review a client'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, noise ratio and client counts.
- 3 Review the following for clients connected to WiNG Express Manager connected Access Points:

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 WiNG Express Manager connected Access Point if available.

SNR	Displays the connected client's <i>signal to noise ratio</i> (SNR). SNR is a measure comparing 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, AP7522 and AP7532 models are capable of 802.11ac connections.
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 managed client radios in the same radio coverage area.
BSSID	Displays the BSSID of the Access Point establishing the client's wireless connection.
Access Point Name	Displays the Access Point's unique administrator assigned name provided upon initial WiNG Express Manager connection.
WLAN	Displays the SSID of the Wireless LAN, if any, which the wireless client is currently utilizing.
VLAN	Displays the VLAN number the wireless client is marked to pass traffic on.
Authentication Status	Displays the authentication type used by the wireless client to connect to its associated WLAN.
Activity Last (sec)	Displays the last detected transmit and receive activity for the listed client within the WiNG Express Manager radio coverage area.
Retry (%)	Displays the retry percentage for packets sent on each client radio. Use the retry rate to assess the overall effectiveness of the RF environment (as displayed as a percentage).
Vendor	Displays the manufacturer of each listed client as a means of assessing its support capabilities within the WiNG Express managed network.

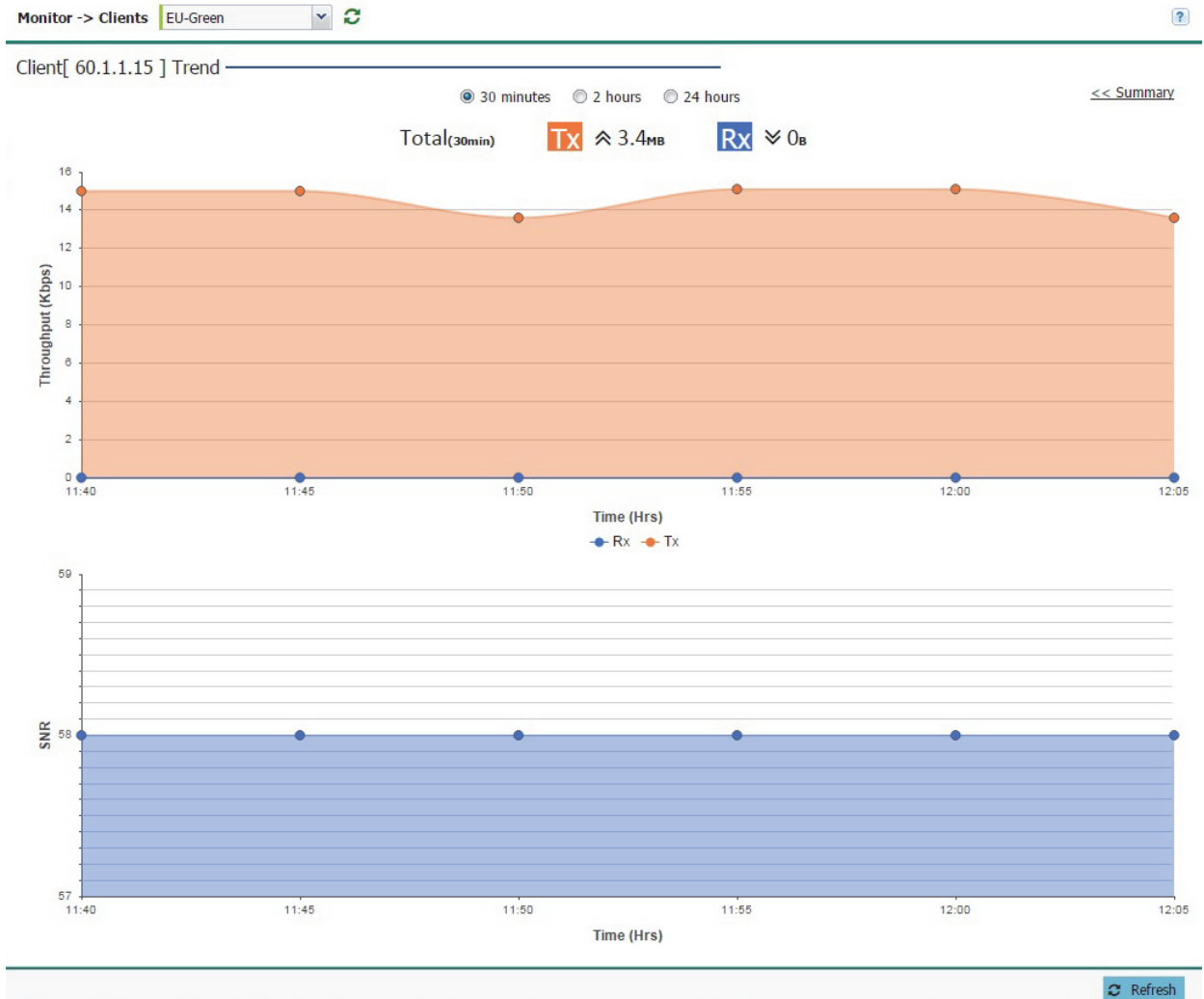
Clients Details (Site)

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

To review a client's wireless interface connection utilization:

- 1 Select **Monitor** from the main menu.
- 2 Select **Clients**.

3 Select **Details**.



- Use the detailed graphs to analyze trends or anomalies in the **Throughput** and **SNR** (Signal to Noise Ratio) over the specified period of time as specified at the top of the screen.
- Select **<< Summary** to return to the main clients screen.

Application Visibility (System)

Controllers and service platforms can inspect every byte of each application header packet allowed to pass their managed radio devices. When an application is recognized and classified by the application recognition engine, administrator defined actions can be applied to that specific application.

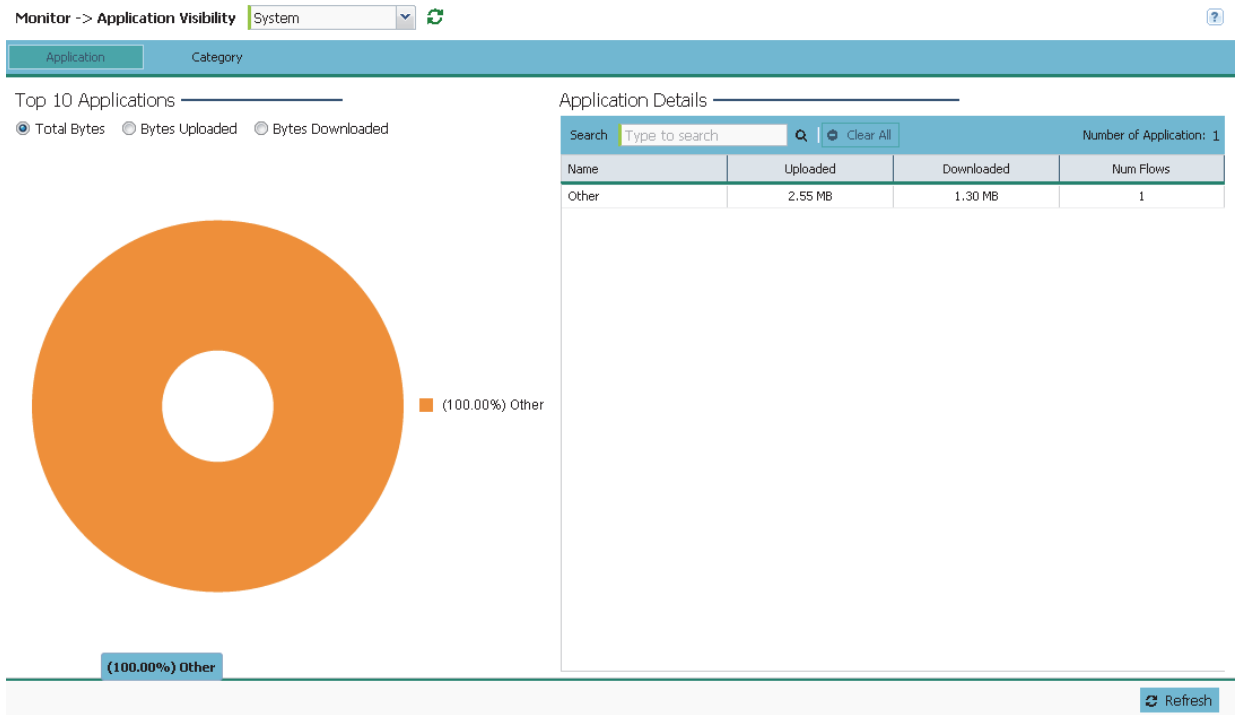
Note: **Application Visibility** is available on the following platforms: AP7522, AP7522E, AP7532.

Application

To monitor system application utilization statistics:

- Select the Monitor menu from the Web UI.

- 2 Select a **Application Visibility**.
 - 3 Select **System** from the drop-down menu.
- The **Application** tab displays by default.



Note: **Application Visibility** is available on the following platforms: AP7522, AP7522E, AP7532.

- 4 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 Express Manager 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 Express Manager 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 Express Manager 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).

- 5 Refer to the **Application Details** table to assess specific application data utilization:

Name	Lists the allowed application name whose data (bytes) are passing through the Express Manager network.
Uploaded	Displays the number of uploaded application data (in bytes) passing through the Express Manager network.

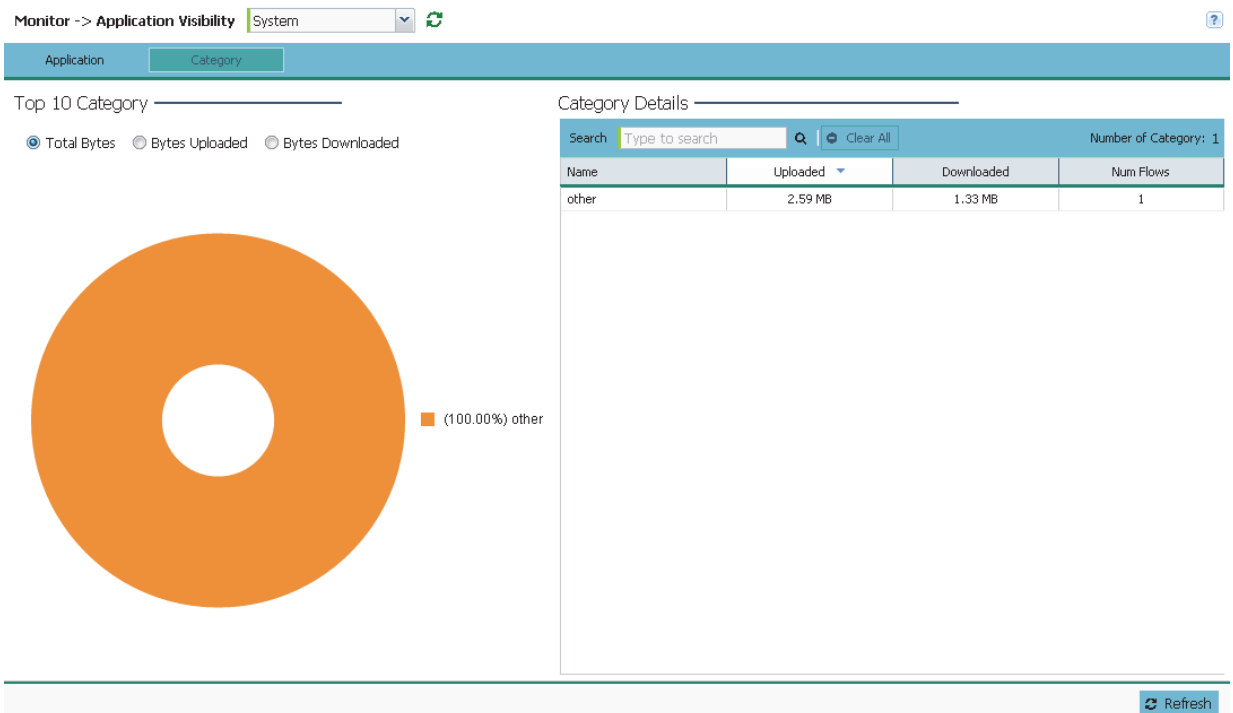
Downloaded	Displays the number of downloaded application data (in bytes) passing the through the Express Manager network.
Num Flows	Lists the total number of application data flows passing through the Express Manager for each listed application. An application flow can consist of packets in a specific 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 assessment data counters and begin a new assessment.

Category

Each application can be classified into a group (a category) representing a high level classifier group to which the application belongs.

To monitor system application category statistics:

- 1 Select the Monitor menu from the Web UI.
- 2 Select a **Application Visibility**.
- 3 Select **System** from the drop-down menu.
The **Application** tab displays by default.
- 4 Select the **Category** tab from the top menu.



Note: **Application Visibility** is available on the following platforms: AP7522, AP7522E, AP7532.

- 5 Refer to the **Top 10 Category** graph to assess the most prolific, and allowed, application data categories utilized by the Express Manager.

Total Bytes	Displays the top ten application categories in respect to total data bytes passing through the Express Manager network. These are only the administrator allowed application categories approved for proliferation within the Express Manager network.
Bytes Uploaded	Displays the top ten application categories in respect to total data bytes uploaded through the Express Manager 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 Express Manager 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).

- 6 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 Express Manager network.
Uploaded	Displays the number of uploaded application category data (in bytes) passing the through the Express Manager network.
Downloaded	Displays the number of downloaded application category data (in bytes) passing the through the Express Manager network.
Num Flows	Lists the total number of application category data flows passing through Express Manager connected 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 assessment data counters and begin a new assessment.

Application Visibility (Site)

Controllers and service platforms can inspect every byte of each application header packet allowed to pass their managed radio devices. When an application is recognized and classified by the application recognition engine, administrator defined actions can be applied to that specific application.

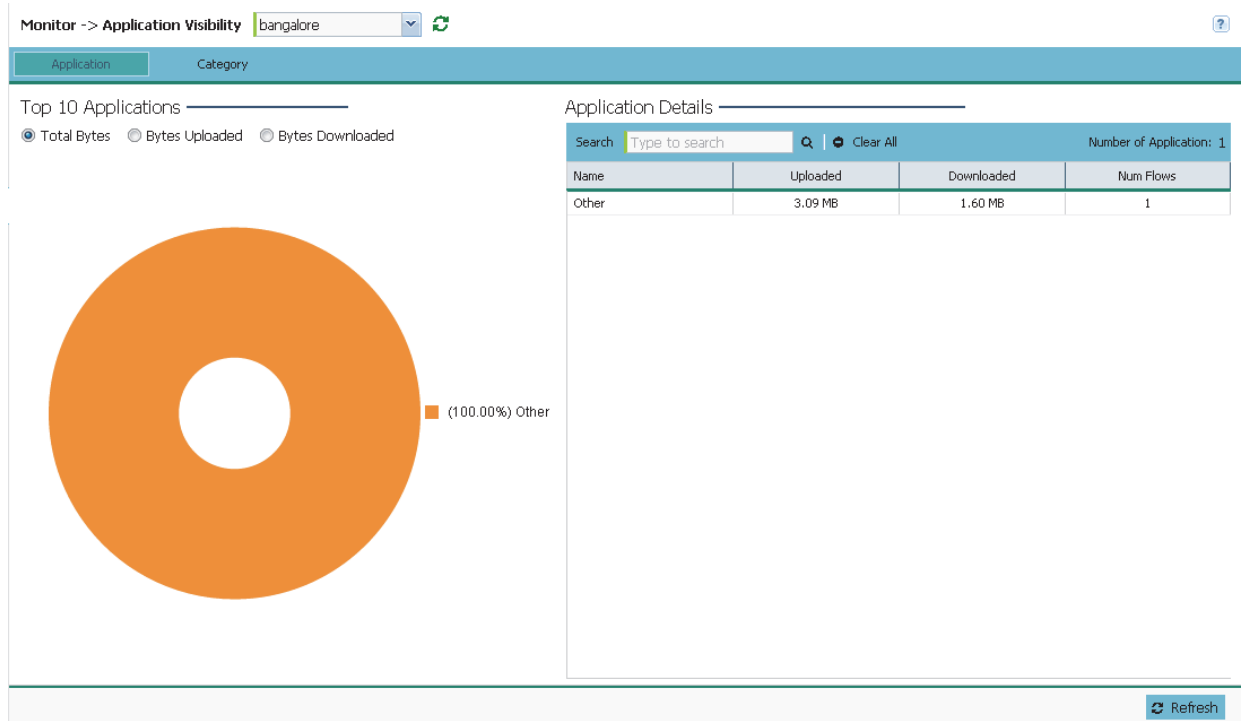
Note: **Application Visibility** is available on the following platforms: AP7522, AP7522E, AP7532.

Application

To monitor site application utilization statistics:

- 1 Select the Monitor menu from the Web UI.
- 2 Select a **Application Visibility**.
- 3 Select a site from the drop-down menu.

The **Application** tab displays by default.



Note: **Application Visibility** is available on the following platforms: AP7522, AP7522E, AP7532.

- 4 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 Express Manager 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 Express Manager 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 Express Manager 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).

- 5 Refer to the **Application Details** table to assess specific application data utilization:

Name	Lists the allowed application name whose data (bytes) are passing through the Express Manager network.
Uploaded	Displays the number of uploaded application data (in bytes) passing the through the Express Manager network.

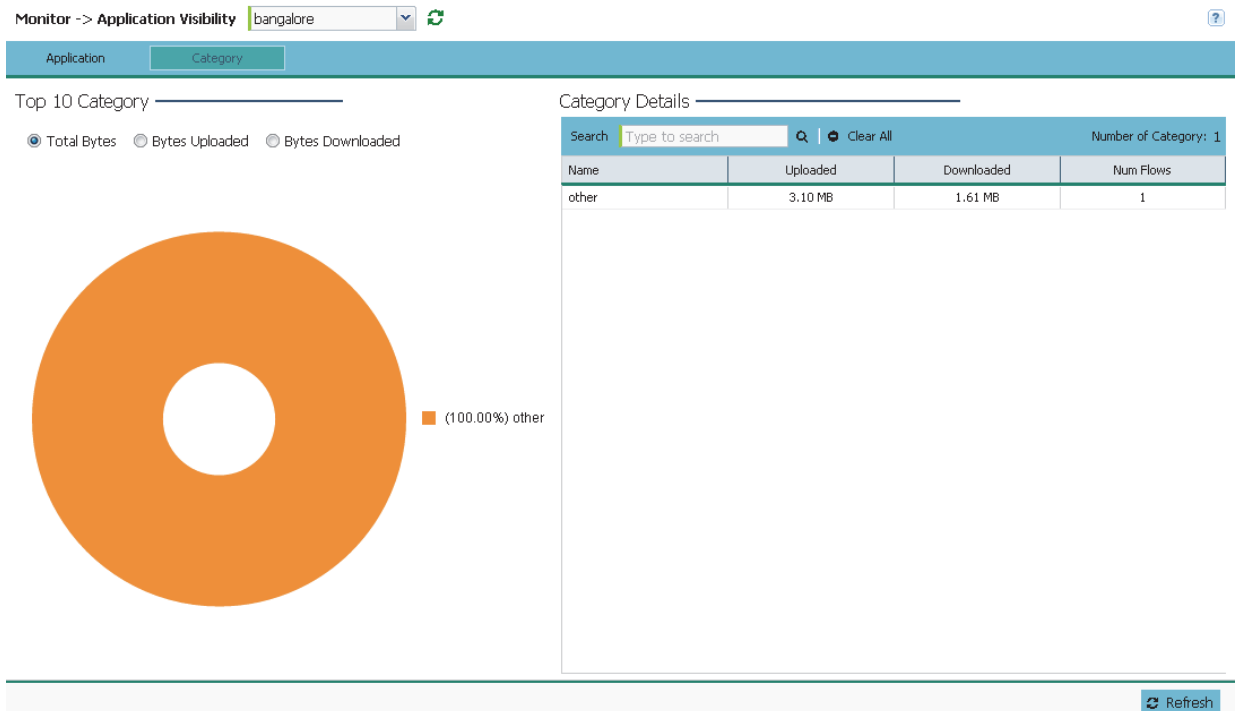
Downloaded	Displays the number of downloaded application data (in bytes) passing the through the Express Manager network.
Num Flows	Lists the total number of application data flows passing through the Express Manager for each listed application. An application flow can consist of packets in a specific 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 assessment data counters and begin a new assessment.

Category

Each application can be classified into a group (a category) representing a high level classifier group to which the application belongs.

To monitor system application category statistics:

- 1 Select the Monitor menu from the Web UI.
- 2 Select an **Application Visibility**.
- 3 Select a site from the drop-down menu.
The **Application** tab displays by default.
- 4 Select the **Category** tab from the top menu.



Note: **Application Visibility** is available on the following platforms: AP7522, AP7522E, AP7532.

- 5 Refer to the **Top 10 Category** graph to assess the most prolific, and allowed, application data categories utilized by the Express Manager.

Total Bytes	Displays the top ten application categories in respect to total data bytes passing through the Express Manager network. These are only the administrator allowed application categories approved for proliferation within the Express Manager network.
Bytes Uploaded	Displays the top ten application categories in respect to total data bytes uploaded through the Express Manager 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 Express Manager 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).

- 6 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 Express Manager network.
Uploaded	Displays the number of uploaded application category data (in bytes) passing the through the Express Manager network.
Downloaded	Displays the number of downloaded application category data (in bytes) passing the through the Express Manager network.
Num Flows	Lists the total number of application category data flows passing through Express Manager 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 assessment data counters and begin a new assessment.

Guest Access (System)

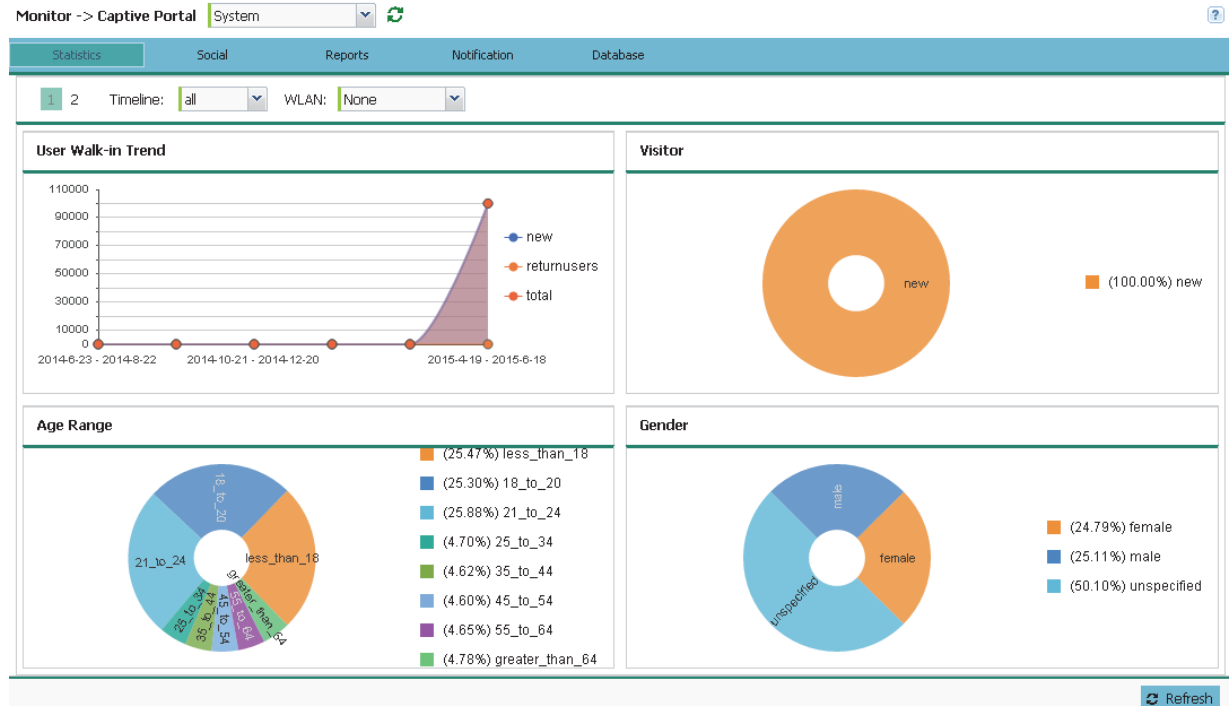
Statistics (System)

The Statistics screen displays information on the Express Manager guest client network. It includes browser utilization, new versus returning user trends, client user age, client operating system, device type proliferation and gender trending.

To monitor **Guest Access Statistics**:

- 1 Select the **Monitor** menu from the Web UI.
- 2 Select **Guest Access**.
- 3 Select **System** from the drop-down menu.

The **Statistics** tab displays by default.



The **Statistics** screen is divided into two screens (1 and 2 as selectable from the top, left-hand, corner).

- 4 Refer to the top of the screen to configure how the following trending periods and user filters are set for guest access statistics and reporting:

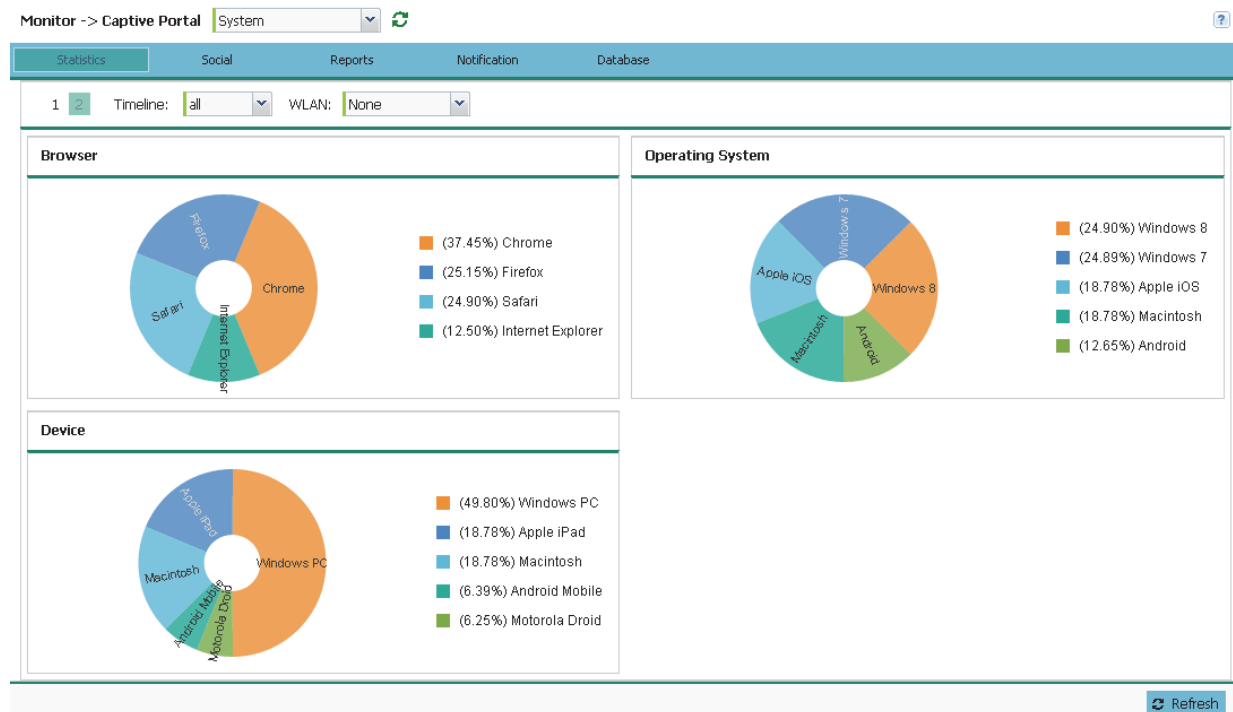
Timeline	Use the drop-down menu to specify whether statistics are gathered for <i>1-Day, 1-Month, 1-Week, 2-Hours, 30-Mins or 5-Hours</i> . Timelines support the latest time period from present. For example, specifying <i>30-Mins</i> displays statistics for the most recent 30 minutes trended.
WLAN	Use the drop down menu to filter guest access statistics to a specific WLAN.

- 5 Refer to the following to assess guest client walk-in trends, age, visitor status and gender to assess whether guest client utilization is in line with guest access deployment objectives:

User Walk-in Trend	Walk-in trending enables an administrator to filter new guest access clients versus return guest clients out of the total reported for the trending period and selected WLAN. New guest users (blue), return guests (red) or total guests can either be collectively displayed or individually displayed by selecting one, two or all three of the options.
Age Range	Displays guest user age differentiation in pie-chart format. Age ranges are uniquely color coded as Less Than 18, 18 to 20, 21 to 24, 25 to 34, 35 to 44, 45 to 54, 55 to 64 and Greater Than 64. Each age group detected within the trending period displays uniquely in its own color for easy differentiation. Each age range also displays numerically. Periodically assess whether the age ranges meet expectations for guest client access within the Express Manager guest network.

Visitor	Displays return guest clients versus new guest clients in pie-chart format. Both new and returning clients display uniquely in their own color for easy differentiation. Periodically assess whether the number of returning guest clients is line with the guest network’s deployment objectives in respect to the RF Domain(s) and WLAN(s) selected for trending.
Gender	Lists the total number of application data flows passing through the controller or service platform 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.

6 To view the second statistics screen, select **2** from the top left.



7 Refer to the following to review the guest client browser, operating system, and devices to determine whether guest client utilization is in line with guest access deployment objectives:

Browser	Displays guest user browser utilization in pie-chart format. Each client browser type (Chrome, Firefox, Safari and Internet Explorer) detected within the defined trending period displays uniquely in its own color for easy differentiation. The number of guest clients utilizing each browser also displays numerically.
Operating System	Displays guest client operating system utilization in pie-chart format. Each client operating system type (Android, Windows 7, Windows 8, Apple iOS and Macintosh) displays uniquely in its own color for easy differentiation. The number of guest clients utilizing each operating system also displays numerically.

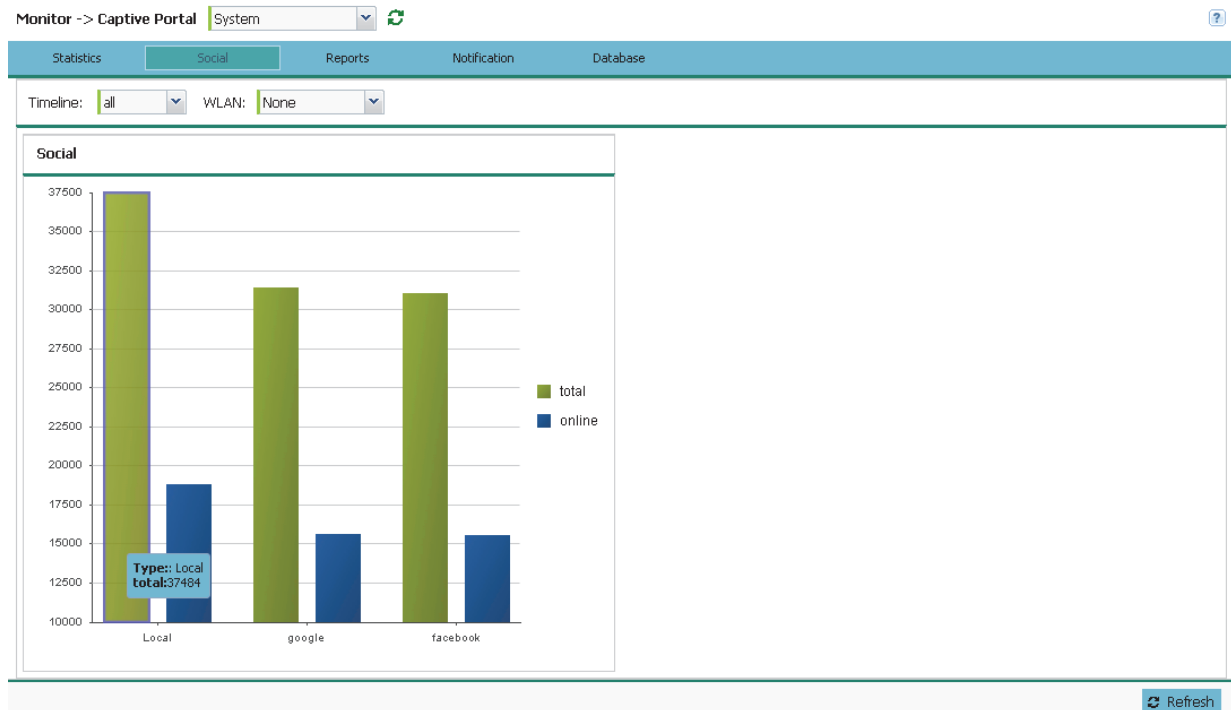
<p>Device</p>	<p>Displays guest client device type utilization in pie-chart format. Each client device type (Windows PC, Macintosh, Apple iPad, Android Mobile and Motorola Droid) displays uniquely in its own color for easy differentiation. The number of each device type detected also displays numerically to help assess their proliferation with WiNG managed guest network.</p>
----------------------	---

Social (System)

Device registration using social media login credentials requires user validation through the guest user's social media account. The guest user authenticates with an administrator configured social media server like Facebook or Google. Upon successful authentication, the guest user's social media profile data (collected from the social media server) is registered on the device.

To view guest access social media utilization for guest clients:

- 1 Select the **Monitor** menu from the Web UI.
- 2 Select **Guest Access**.
- 3 Select **System** from the drop-down menu.
The **Statistics** tab displays by default.
- 4 Select **Social** from the menu bar.



- 5 Refer to the top of the screen to configure how the following trending periods and user filters are set for guest access and social media trending:

<p>Timeline</p>	<p>Use the drop-down menu to specify whether social media statistics are gathered for 1-Day, 1-Month, 1-Week, 2-Hours, 30-Mins or 5-Hours. Timelines support the latest time period from present. For example, specifying 30-Mins displays statistics for the most recent 30 minutes trended.</p>
------------------------	---

WLAN	Use the drop down menu to filter guest access social media statistics to a specific WLAN.
-------------	---



- 6 The data displays in bar graph format, with the total number of social media authenticating clients listed in green, and those currently online displayed in orange for both Google and Facebook authenticating clients. Refer to the **Local** graph to assess those clients requiring captive portal authentication as a fallback mechanism for guest registration through social media authentication.
- 7 Periodically select **Refresh** to update the statistics counters to their latest values.

Reports (System)

Report queries can be filtered and run to obtain information on targeted guest clients within the guest network.

To generate customized guest client reports:

- 1 Select the **Monitor** menu from the Web UI.
- 2 Select **Guest Access**.
- 3 Select **System** from the drop-down menu.
The **Statistics** tab displays by default.
- 4 Select **Reports** from the menu bar.

Monitor -> Captive Portal System  

Statistics Social **Reports** Notification Database

Field: mac Value: Details

Client Details _____

- 5 Select the **Field** drop-down menu at the top, left-hand, side of the screen to define whether the guest client's report data is fetched based on its **MAC**, **Name**, **Mobile**, **Email**, **Member** or **Time**. Once provided, enter an appropriate search string in the **Value** field to generate a report for the target guest client. When completed with the report's search strings, select **Details**.
- 6 Refer to the **Client Details** table to review the following report output:

 Refresh

MAC	Displays the factory encoded hardware MAC address assigned to this guest client at the factory by the manufacturer. This is the guest client's hardware identifier added to the guest user database. If the guest client requests access later, this MAC address is validated against the guest user database, and the client is allowed access to the Express Manager guest network.
Name	Lists the name used for guest access authentication and pass code generation.
Email	Lists the E-mail address used for guest access authentication and the receipt of the required passcode.
Mobile	Lists the guest client's registered mobile number used for guest access authentication requests and the receipt of the required passcode.
Source	Lists the source (Facebook, Google) whose username and password were used as the clients's social media authenticator.

Notification (System)

For each registered guest user, a passcode is sent by E-mail, SMS or both. A guest management policy defines E-mail host and SMS gateway commands, along with credentials required for sending a passcode to guest client via E-mail and SMS. Users can configure up to 32 different guest management policies. Each policy enables the user to configure the SMS gateway, SMS message body, E-mail SMTP server, E-mail subject contents and E-mail message body. There can be only one guest management policy active per device at any one time.

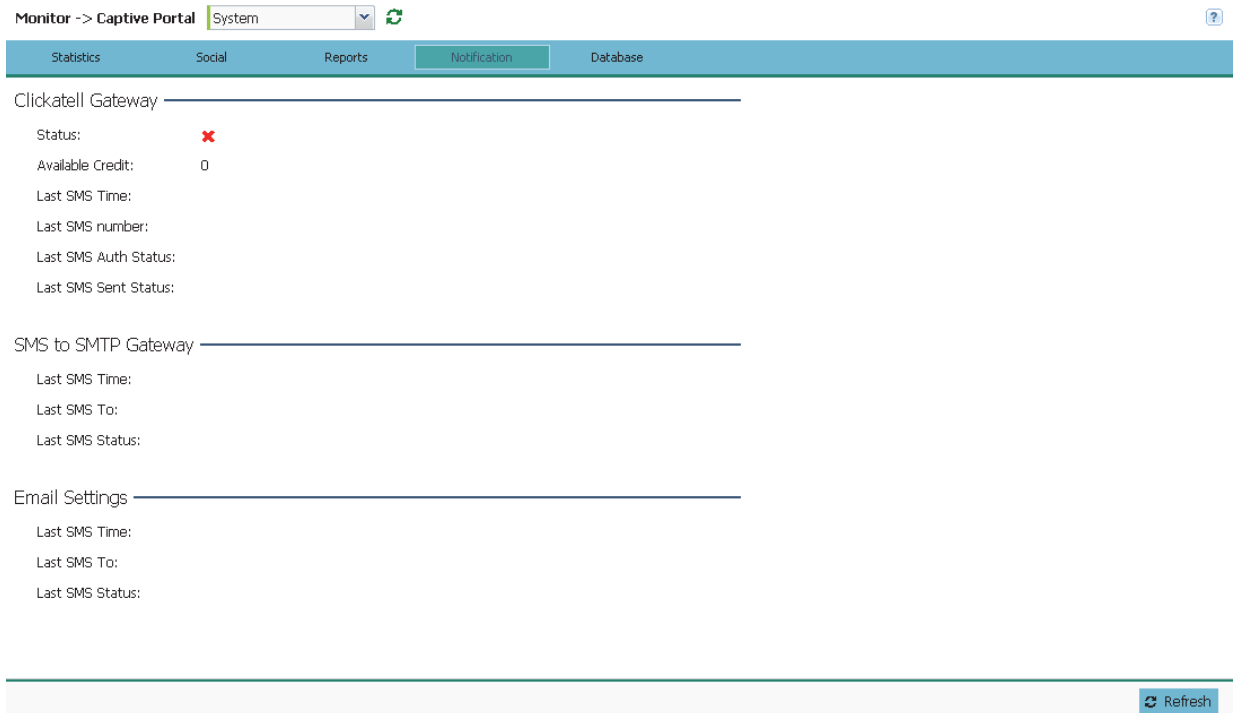
The *short message service* (SMS) is the text messaging service component of phone, E-mail and mobile systems. SMS uses standardized communications protocols to allow fixed or mobile phone devices to exchange text messages.

To review guest client notification statistics:

- 1 Select the **Monitor** menu from the Web UI.
- 2 Select **Guest Access**.
- 3 Select **System** from the drop-down menu.

The **Statistics** tab displays by default.

4 Select **Notification** from the menu bar.



5 Review the following **Clickatell Gateway** information. By default, clickatell is the host SMS gateway server resource for guest access.

Status	Displays an icon as a visual indicator of the gateway status. Green defines the gateway as available. Red indicates the gateway is down and unavailable.
Available Credit	Lists amount of voice access utilization credit available in minutes.
Last SMS Time	Lists the timestamp appended to the sent time of the clickatell SMS gateway message.
Last SMS Number	Lists the numeric status code returned in response to a SMS gateway server guest access request.
Last SMS Auth Status	Lists the SMS authentication credential and validation message exchange status for the listed clickatell gateway session ID.
Last SMS Sent Status	Lists the associated status strings returned in response to a SMS gateway server guest access request.

6 Review the following **SMS to SMTP Gateway** information.

Last SMS Time	Lists the timestamp appended to the sent time of the SMS to SMTP gateway message.
Last SMS To	Lists the recipient of the most recent SMS to SMTP server credential E-mail exchange containing the required passcode for the registered guest.
Last SMS Status	Lists the associated status strings returned in response to a SMS gateway server guest access request.

7 Review the following **Email Gateway** information.

Last SMS Time	Displays the time of the most recent E-mailed passcode to a guest access requesting client. Guest users can register with their E-mail credentials as the primary means of authentication.
Last SMS To	Lists the recipient of this session's server E-mail credential exchange containing the required passcode for the authenticating guest client.
Last SMS Status	Lists the completion status of the most recent server E-mail credential exchange containing the required passcode for the authenticating guest client.

Database (System)

Refer to the Database screen to periodically import or export guest access information to and from a WiNG Express managed device. Archiving guest access utilization data is a good way to assess periods of high and low utilization and better plan for client guest access consumption of controller or Access Point network resources.

To administrate the guest access database:

- 1 Select the **Monitor** menu from the Web UI.
- 2 Select **Guest Access**.
- 3 Select **System** from the drop-down menu.
The **Statistics** tab displays by default.
- 4 Select **Database** from the menu bar.

Monitor -> Captive Portal System

Statistics Social Reports Notification Database

Export Import Delete

Timeline: [Dropdown]

WLAN: [None] [Dropdown]

Format: [JSON] [Dropdown]

URL: * [Text Input] [Advanced]

[Export]

[Refresh]

- 5 Select **Export** to archive guest access data (in JSON or CSV format) to a designated remote location, or Import to upload guest access utilization data back to the WiNG Express managed controller, service platform or Access Point.
- 6 If conducting an **Export** operation, provide the following to refine the data exported:

Timeline	Use the drop-down menu to specify whether guest access statistics are exported for the previous 1-Day, 1-Month, 1-Week, 2-Hours, 30-Mins or 5-Hours. Timelines support the latest time period from present. For example, specifying 30-Mins exports statistics trended over the most recent 30 minutes.
WLAN	Use the drop down menu to filter guest access social media statistics to a specific WLAN.
Format	Define whether the guest access data is exported in JSON or CSV format. JavaScript Object Notation (JSON) is an open standard format using text to export data objects consisting of attribute value pairs. A comma-separated values (CSV) file stores tabular data in plain text. Plain text means the file is interpreted a sequence of characters, so it's human readable with a standard text editor. Each line of the file is a data record. Each record consists of one or more fields, separated by commas.

- 7 When exporting or importing guest access data (regardless of format), provide the following URL data to accurately configure the remote host.

Format	Select the data transfer protocol used for exporting or importing guest access data. Options include <i>FTP</i> and <i>TFTP</i> .
Port	Use the spinner control to set the virtual port for the for the export or import operation.
Host	Provide a textual hostname or numeric IP address of the server used for guest access data transfer operations. Hostnames cannot include an underscore character. Select IPv4 Address to use an IPv4 formatted address as the host. Select IPv6 Address to use an IPv6 formatted address as the host. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.
Username	If using FTP or SFTP as the data transfer protocol, enter the username required by the remote FTP or SFTP server resource.
Password	If using FTP or SFTP as the data transfer protocol, enter the password required by the remote FTP or SFTP server resource.
Path/File	Specify the path to the server resource where guest access data is either exported or imported. Enter the complete relative path to the file on the server. If electing to use SFTP as the file transfer protocol, its recommended the path/file be set using the <i>command line interface</i> (CLI).

- 8 When the **URL** data is accurately entered, select the **Export** or **Import** button respectively to initiate the operation.
- 9 Optionally select **Delete** to purge either all or part of the guest user database.
- 10 Select **All** to remove the contents of the entire database. Select **Any** to invoke a drop-down menu where Mac, Name, Mobile, Email or a WLAN can be selected to refine the database removal to just a selected entity. Enter the name of the MAC address, user, mobile number or WLAN you wish to remove from the database, then select **Delete**.

Guest Access (Site)

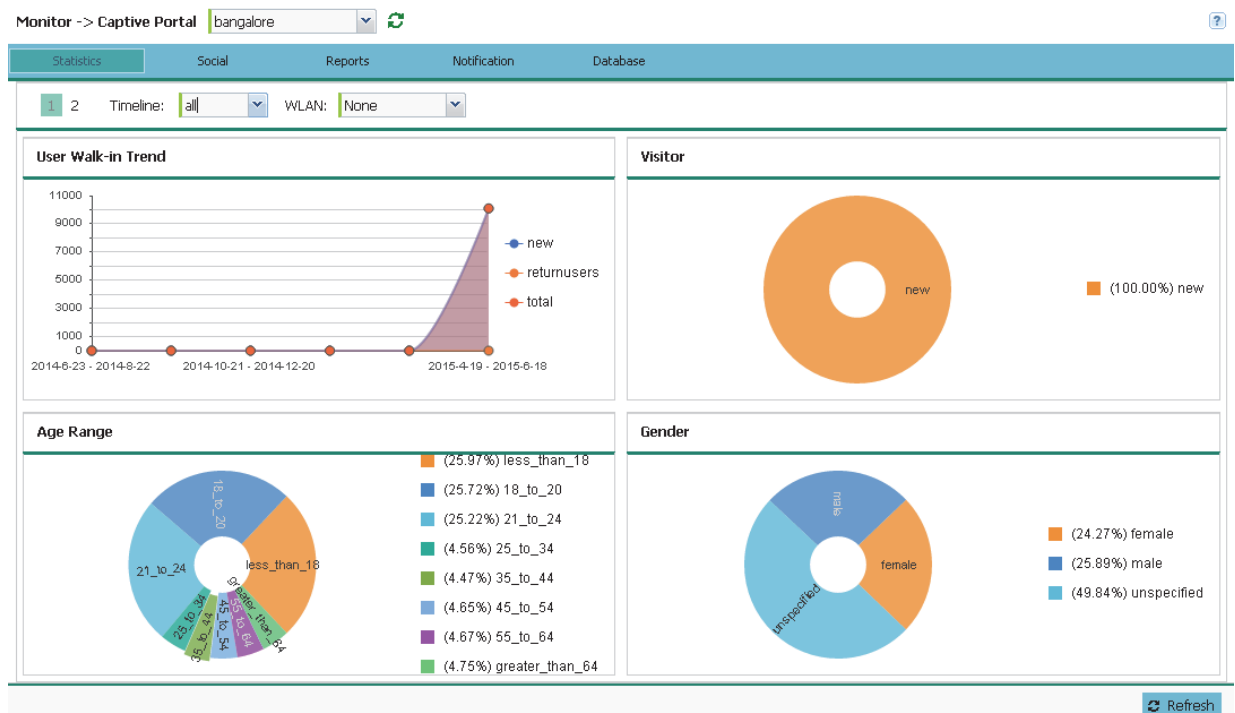
Statistics (Site)

The Statistics screen displays information on the Express Manager guest client network. It includes browser utilization, new versus returning user trends, client user age, client operating system, device type proliferation and gender trending.

To monitor **Guest Access Statistics**:

- 1 Select the **Monitor** menu from the Web UI.
- 2 Select **Guest Access**.
- 3 Select a site from the drop-down menu.

The **Statistics** tab displays by default.



The Statistics screen is divided into two screens, displays by default.

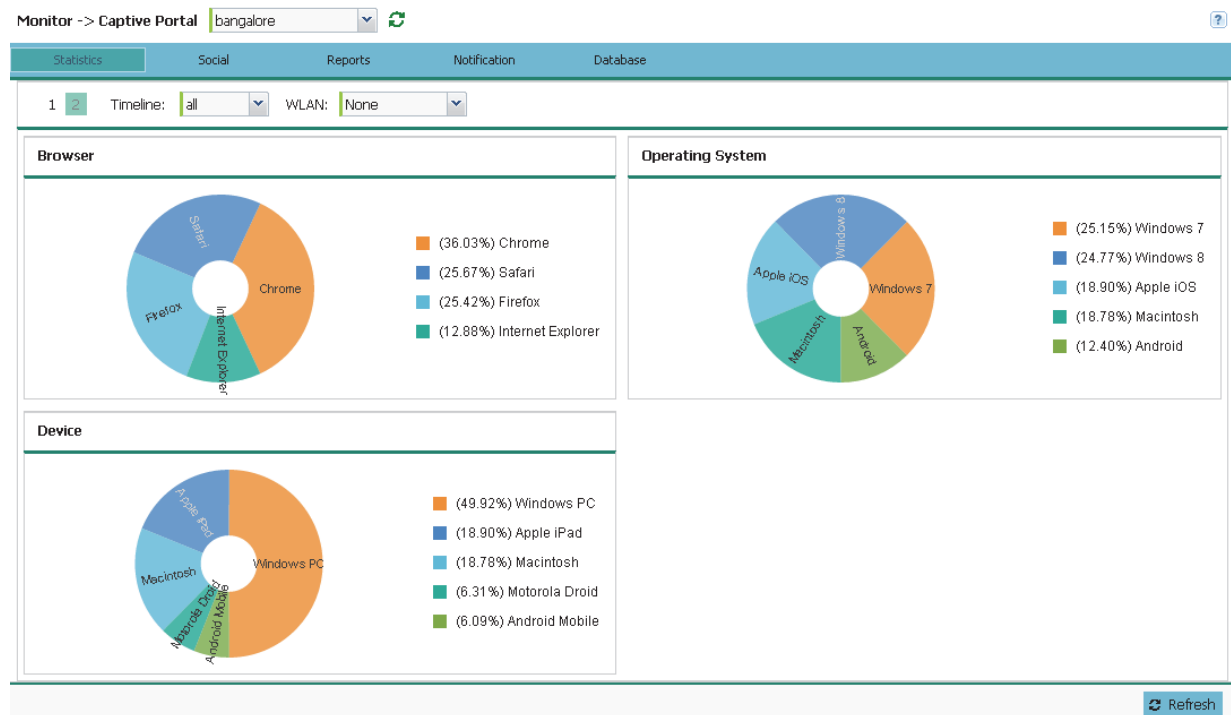
- 4 Refer to the top of the screen to configure how the following trending periods and user filters are set for guest access statistics trending and reporting:

Timeline	Use the drop-down menu to specify whether statistics are gathered for 1-Day, 1-Month, 1-Week, 2-Hours, 30-Mins or 5-Hours. Timelines support the latest time period from present. For example, specifying 30-Mins displays statistics for the most recent 30 minutes trended.
WLAN	Use the drop down menu to filter guest access statistics to a specific WLAN.

- 5 Refer to the following to assess guest client walk-in trends, age, visitor status and gender to assess whether guest client utilization is in line with guest access deployment objectives:

User Walk-in Trend	Walk-in trending enables an administrator to filter new guest access clients versus return guest clients out of the total reported for the trending period and selected WLAN. New guest users (blue), return guests (red) or total guests can either be collectively displayed or individually displayed by selecting one, two or all three of the options.
Age Range	Displays guest user age differentiation in pie-chart format. Age ranges are uniquely color coded as Less Than 18, 18 to 20, 21 to 24, 25 to 34, 35 to 44, 45 to 54, 55 to 64 and Greater Than 64. Each age group detected within the trending period displays uniquely in its own color for easy differentiation. Each age range also displays numerically. Periodically assess whether the age ranges meet expectations for guest client access within the guest network.
Visitor	Displays return guest clients versus new guest clients in pie-chart format. Both new and returning clients display uniquely in their own color for easy differentiation. Periodically assess whether the number of returning guest clients is line with the guest network's deployment objectives in respect to the RF Domain(s) and WLAN(s) selected for trending.
Gender	Lists the total number of application data flows passing through the Express Manager 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.

6 To view the second statistics screen select **2** from the upper left.



7 Refer to the following to review guest client browser, operating system, and devices to determine whether guest client utilization is in line with guest access deployment objectives:

Browser	Displays guest user browser utilization in pie-chart format. Each client browser type (Chrome, Firefox, Safari and Internet Explorer) detected within the defined trending period displays uniquely in its own color for easy differentiation. The number of guest clients utilizing each browser also displays numerically.
Operating System	Displays guest client operating system utilization in pie-chart format. Each client operating system type (Android, Windows 7, Windows 8, Apple iOS and Macintosh) displays uniquely in its own color for easy differentiation. The number of guest clients utilizing each operating system also displays numerically.
Device	Displays guest client device type utilization in pie-chart format. Each client device type (Windows PC, Macintosh, Apple iPad, Android Mobile and Motorola Droid) displays uniquely in its own color for easy differentiation. The number of each device type detected also displays numerically to help assess their proliferation with Express Manager guest network.

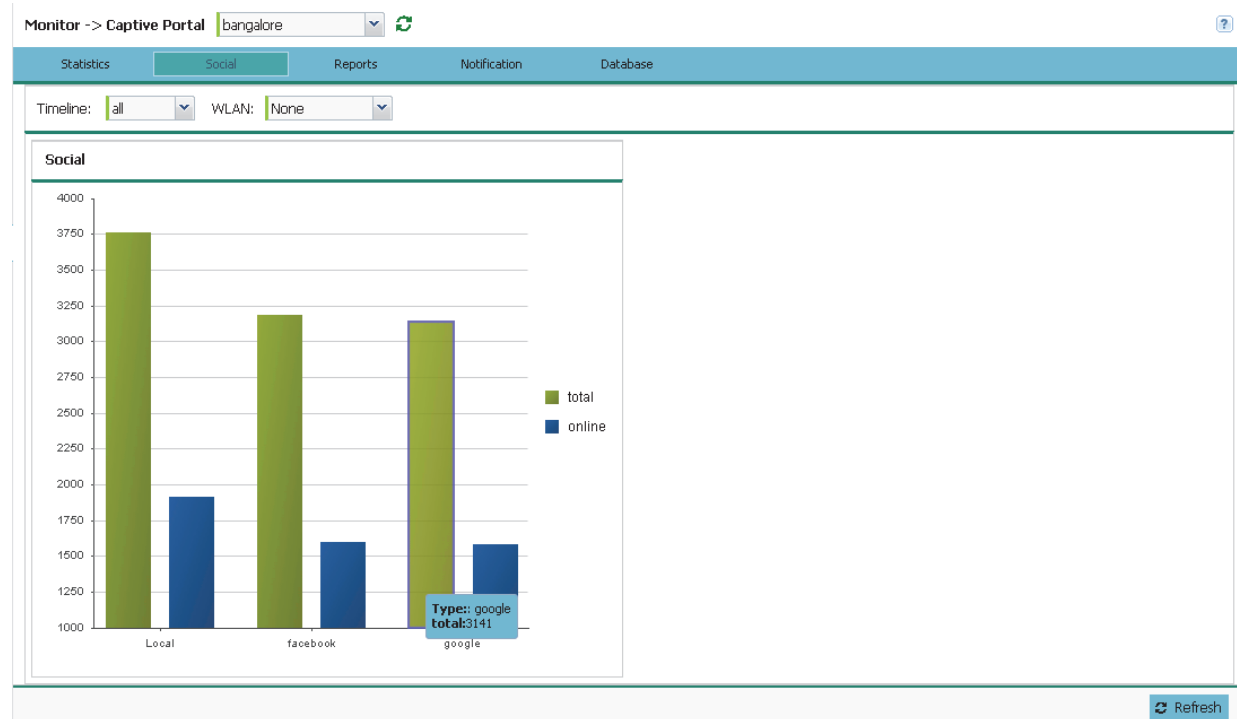
Social (Site)

Device registration using social media login credentials requires user validation through the guest user's social media account. The guest user authenticates with an administrator configured social media server like Facebook or Google. Upon successful authentication, the guest user's social media profile data (collected from the social media server) is registered on the device.

To view guest access social media utilization for guest clients:

- 1 Select the **Monitor** menu from the Web UI.
 - 2 Select **Guest Access**.
 - 3 Select a site from the drop-down menu.
- The **Statistics** tab displays by default.

4 Select **Social** from the menu bar.



5 Refer to the top of the screen to configure how the following trending periods and user filters are set for guest access social media trending:

Timeline	Use the drop-down menu to specify whether social media statistics are gathered for 1-Day, 1-Month, 1-Week, 2-Hours, 30-Mins or 5-Hours. Timelines support the latest time period from present. For example, specifying 30-Mins displays statistics for the most recent 30 minutes trended.
WLAN	Use the drop down menu to filter guest access social media statistics to a specific WLAN.

- The data displays in bar graph format, with the total number of social media authenticating clients listed in green, and those currently online displayed in orange for both Google and Facebook authenticating clients. Refer to the **Local** graph to assess those clients requiring captive portal authentication as a fallback mechanism for guest registration through social media authentication.
- Periodically select **Refresh** to update the statistics counters to their latest values.

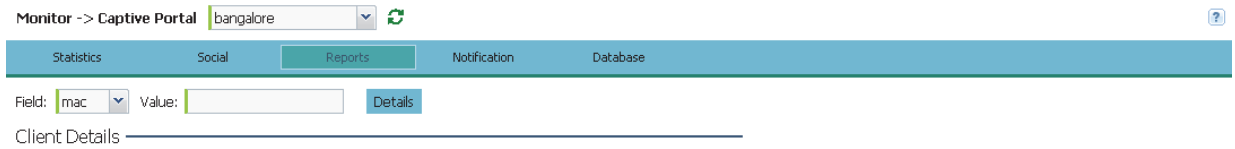
Reports (Site)

Report queries can be filtered and run to obtain information on targeted guest clients within the guest network.

To generate customized guest client reports:

- Select the **Monitor** menu from the Web UI.
- Select **Guest Access**.
- Select a site from the drop-down menu.
The **Statistics** tab displays by default.

- 4 Select **Reports** from the menu bar.



- 5 Select the **Field** drop-down menu at the top, left-hand, side of the screen to define whether the guest client's report data is fetched based on its **MAC**, **Name**, **Mobile**, **Email**, **Member** or **Time**. Once provided, enter an appropriate search string in the **Value** field to generate a report for the target guest client. When completed with the report's search strings, select **Details**.
- 6 Refer to the **Client Details** table to review the following report output:

MAC	Displays the factory encoded hardware MAC address assigned to this guest client by the manufacturer. This is the guest client's hardware identifier added to the guest user database. If the guest client requests access later, this MAC address is validated against the guest user database, and the client is allowed access to the Express Manager guest network.
Name	Lists the name used for guest access authentication and pass code generation.
Email	Lists the E-mail address used for guest access authentication and the receipt of the required passcode.
Mobile	Lists the guest client's registered mobile number used for guest access authentication requests and the receipt of the required passcode.
Source	Lists the source (Facebook, Google) whose username and password were used as the client's social media authenticator.

Notification (Site)

For each registered guest user, a passcode is sent by E-mail, SMS or both. A guest management policy defines E-mail host and SMS gateway commands, along with credentials required for sending a passcode to guest client via E-mail and SMS. Users can configure up to 32 different guest management policies. Each policy enables the user to configure the SMS gateway, SMS message body, E-mail SMTP server, E-mail subject contents and E-mail message body. There can be only one guest management policy active per device at any one time.

The *short message service* (SMS) is the text messaging service component of phone, E-mail and mobile systems. SMS uses standardized communications protocols to allow fixed or mobile phone devices to exchange text messages.

SMS is similar to MAC address based self registration, but in addition a captive portal sends a SMS message to the user on the mobile phone number provided at registration containing an access code. The user then inputs the access code on the user screen. The captive portal verifies the code, returns the *Welcome* page and provides access. This allows the administrator to verify the phone number provided and can be traced back to a specific individual should the need arise.

To review guest client notification statistics:

- 1 Select the **Monitor** menu from the Web UI.
- 2 Select **Guest Access**.
- 3 Select a site from the drop-down menu.
The **Statistics** tab displays by default.
- 4 Select **Notification** from the menu bar.

Monitor -> Captive Portal

Statistics Social Reports **Notification** Database

Clickatell Gateway

Status: x

Available Credit: 0

Last SMS Time:

Last SMS number:

Last SMS Auth Status:

Last SMS Sent Status:

SMS to SMTP Gateway

Last SMS Time:

Last SMS To:

Last SMS Status:

Email Settings

Last SMS Time:

Last SMS To:

Last SMS Status:

Refresh

- 5 Review the following **Clickatell Gateway** information. By default, clickatell is the host SMS gateway server resource for guest access.

Status	Displays an icon as a visual indicator of the gateway status. Green defines the gateway as available. Red indicates the gateway is down and unavailable.
---------------	--

Available Credit	Lists amount of voice access utilization credit available in minutes.
Last SMS Time	Lists the timestamp appended to the sent time of the clickatell SMS gateway message.
Last SMS Number	Lists the numeric status code returned in response to a SMS gateway server guest access request.
Last SMS Auth Status	Lists the SMS authentication credential and validation message exchange status for the listed clickatell gateway session ID.
Last SMS Sent Status	Lists the associated status strings returned in response to a SMS gateway server guest access request.

- 6 Review the following **SMS to SMTP Gateway** information.

Last SMS Time	Lists a timestamp appended to the sent time of the SMS to SMTP gateway message.
Last SMS To	Lists the recipient of the most recent SMS to SMTP server credential E-mail exchange containing the required passcode for the registered guest.
Last SMS Status	Lists the associated status strings returned in response to a SMS gateway server guest access request.

- 7 Review the following **Email Gateway** information.

Last SMS Time	Displays the time of the most recent E-mailed passcode to a guest access requesting client. Guest users can register with their E-mail credentials as the primary means of authentication.
Last SMS To	Lists the recipient of this session's server E-mail credential exchange containing the required passcode for the authenticating guest client.
Last SMS Status	Lists the completion status of the most recent server E-mail credential exchange containing the required passcode for the authenticating guest client.

Database (Site)

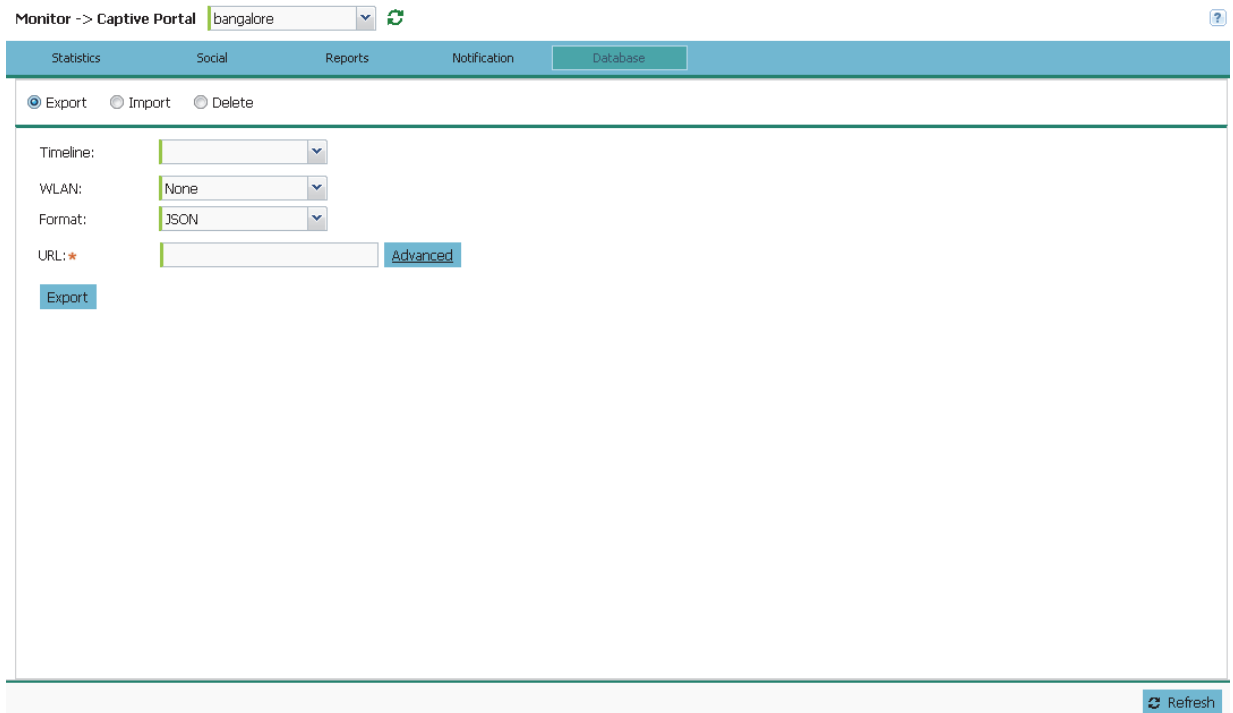
Refer to the **Database** screen to periodically import or export guest access information to and from an Express Manager device. Archiving guest access utilization data is a good way to assess periods of high and low utilization and better plan for client guest access consumption of controller or Access Point network resources.

To administrate the guest access database:

- 1 Select the **Monitor** menu from the Web UI.
- 2 Select **Guest Access**.
- 3 Select a site from the drop-down menu.

The **Statistics** tab displays by default.

4 Select **Database** from the menu bar.



5 Select **Export** to archive guest access data (in JSON or CSV format) to a designated remote location, or **Import** to upload guest access utilization data back to the Express Manager.

6 If conducting an **Export** operation, provide the following to refine the data exported:

Timeline	Use the drop-down menu to specify whether guest access statistics are exported for the previous 1-Day, 1-Month, 1-Week, 2-Hours, 30-Mins or 5-Hours. Timelines support the latest time period from present. For example, specifying 30-Mins exports statistics trended over the most recent 30 minutes.
WLAN	Use the drop down menu to filter guest access social media statistics to a specific WLAN.
Format	Define whether the guest access data is exported in JSON or CSV format. <i>JavaScript Object Notation</i> (JSON) is an open standard format using text to export data objects consisting of attribute value pairs. A <i>comma-separated values</i> (CSV) file stores tabular data in plain text. Plain text means the file is interpreted a sequence of characters, so that it is human readable with a standard text editor. Each line of the file is a data record. Each record consists of one or more fields, separated by commas.

7 When exporting or importing guest access data (regardless of format), provide the following URL data to accurately configure the remote host.

Format	Select the data transfer protocol used for exporting or importing guest access data. Options include <i>FTP</i> and <i>TFTP</i> .
Port	Use the spinner control to set the virtual port for the for the export or import operation.

Host	<p>Provide a textual hostname or numeric IP address of the server used for guest access data transfer operations. Hostnames cannot include an underscore character.</p> <p>Select IPv4 Address to use an IPv4 formatted address as the host. Select IPv6 Address to use an IPv6 formatted address as the host. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.</p>
Username	<p>If using FTP or SFTP and the data transfer protocol, enter the username required by the remote FTP or SFTP server resource.</p>
Password	<p>If using FTP or SFTP and the data transfer protocol, enter the password required by the remote FTP or SFTP server resource.</p>
Path/File	<p>Specify the path to the server resource where guest access data is either exported or imported. Enter the complete relative path to the file on the server. If electing to use SFTP as the file transfer protocol, its recommended the path/file be set using the <i>command line interface</i> (CLI).</p>

- 8 When the **URL** data is accurately entered, select the **Export** or **Import** button respectively to initiate the operation.
- 9 Optionally select the **Delete** button to purge either all or part of the guest user database.
- 10 Select **All** to remove the contents of the entire database. Select **Any** to invoke a drop-down menu where **MAC**, **Name**, **Mobile**, **Email** or a **WLAN** can be selected to refine the database removal. Enter the name of the MAC address, user, mobile number or WLAN to remove from the database, then select **Delete**.

CONFIGURATION

In This Chapter

Configuration (System).....	55
Configuration (Site)	93

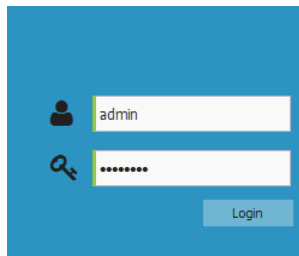
Configuration (System)

Basic Configuration (System)

To provide the basic configuration and access Express Manager functions:

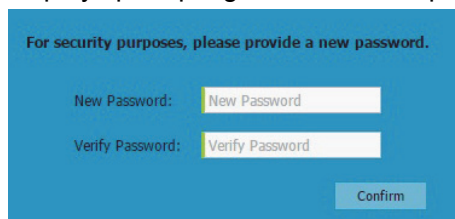
- 1 Power up the device and connect an Ethernet cable to one of the LAN ports.
Open a browser (Chrome, Firefox, Opera, Safari or Internet Explorer) and enter *https://express.zebra.com*.

The login screen displays.



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

If this is the first time the Express Manager interface has been accessed, a screen displays prompting to enter a new password.



- 5 Enter a new password for the admin user.

- 6 The device automatically displays a Dashboard where administrator can assess network health and conduct a diagnostic review of network performance.
- 7 Expand the Configuration menu item and select **Basic**.
- 8 Set the following **Basic Configuration Settings**:

Basic Configuration Settings

System Name: *

Country Name: *

Timezone:

Date & Time: Hour: Mins: AM PM

NTP Server:

Default Gateway:

DNS Servers:

IP Address	Edit
XXX.XXX.XXX.XXX	
XXX.XXX.XXX.XXX	
XXX.XXX.XXX.XXX	

- **System Name** - Provide a System Name used as Express Manager's network identifier. The System Name is a required parameter.
 - **Country Code** - If the Country Code was not set when the device was initially powered on, set the country now to ensure legal operation. The system's wireless capabilities are disabled until the required country code is set.
 - **Timezone** - Use the drop-down menu to specify the geographic timezone where the system 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 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. A controller or service platform (NTP clients) can periodically synchronize their clock with a master clock (an NTP server). For example, a device resets its clock to 07:04:59 upon reading a time of 07:04:59 from its designated NTP server.
 - **Default Gateway** - Optionally specify the default gateway IP address used to communicate with the systems main router.
- 9 The **Firmware** section displays the current and alternate firmware versions queued for the device, the date the most recent firmware was installed and the last upgrade status. In the URL field, enter the complete path to the firmware file for the target device.
 - 10 Optionally select **Advanced** and provide the following information to accurately define the location of the target firmware file:

Protocol	Select the connection protocol used for updating device firmware. Available options include: <i>tftp</i> <i>ftp</i> <i>sftps</i> <i>http</i> <i>cf</i> <i>usb1-4</i>
Port	Use the spinner control or manually enter the value to define the port used for firmware updates. This option is not valid for <i>cf</i> and <i>usb1-4</i> .
IP Address	Enter IP address of the server used to update the firmware. This option is not valid for <i>cf</i> and <i>usb1-4</i> .
Hostname	Provide the hostname of the server used to update the firmware. This option is not valid for <i>cf</i> and <i>usb1-4</i> .
User Name	Define the user name used to access either a <i>FTP</i> or <i>SFTP</i> server.
Password	Specify the password for the user account to access a <i>FTP</i> or a <i>SFTP</i> server.
Path / File	Specify the path to the firmware file. Enter the complete relative path to the file on the server.

- 11 The **Licenses** section displays the number of AP Licenses(number of APs available for adoption under the restrictions of the license). This number applies to dependent mode adaptive APs only, not independent mode APs.

Licenses _____

AAP Licenses	1024
License-in-use	7

AAP License: b2334afc7eeb427ebf094€

- 12 Refer to the following **Cluster** configuration information for the Express Manager network:

Cluster _____

State: running

State	Displays a status indicating whether the cluster is up and running or disabled.
Mode	A cluster member can be in either an <i>Active</i> or <i>Standby</i> mode. All active members can adopt Access Point radios. Standby members only adopt Access Points when an active member has failed, or sees an Access Point not adopted. The default cluster mode is Active.
Name	Define a name for the cluster unique to its configuration. The name cannot exceed 64 characters.
Master Priority	Set a priority from 1 - 255, with the higher value being given higher priority. This configuration is the device's priority to become cluster master. In a cluster environment, one member is elected as cluster master. This configuration is the device's priority to become cluster master. The default value is 128.
Member VLAN	Optionally enable a member VLAN, then use the spinner control to designate the VLAN where cluster members are reachable. Specify a VLAN from 1 - 4094.
Member IP	Specify the IP addresses of the VLAN's cluster members using the IP Address table.
Join Cluster	Click the <i>Join Cluster</i> button to add the device to the cluster configured in the fields above.

13 To configure **Static Routes** click the **+ Add** button and specify IP addresses and network masks in the **Network Address** column. Then provide the **Gateway** used to route traffic.

14 Click **Apply** to save the basic system configuration settings.

Sites Details (System)

Site creation from the system level can be as simple as choosing the default template configuration or cloning the desired configuration from an existing site. Specific system level configuration settings are pushed out globally and automatically applied to all Access Points in all sites or to a specific site, dramatically simplifying the time, effort and cost of network-wide configuration.

To view a site configuration:

- 1 From the main tree, expand the Configuration menu item and select **Sites**.

Configuration -> Sites System ?

Sites Auto Provisioning Policy >>

Add Site Delete		Number of Sites: 5		
<input type="checkbox"/>	Site Name ^	Online/Offline AP(s)	Client(s)	Edit
<input type="checkbox"/>	SITE-1	2/0		
<input type="checkbox"/>	SITE-2	3/0		
<input type="checkbox"/>	SITE-3	1/0		
<input type="checkbox"/>	SITE-4	1/0		
<input type="checkbox"/>	SITE-5	2/0		

Apply Discard

- 2 The **Sites Details** section displays the following information:

Site Name	Displays the user defined site name for each configured site.
Online / Offline APs	Displays two numbers. The first is the number of Access Points online and connected to each configured site. The second is the number of Access Points currently disconnected or offline.
Clients	Displays the number of clients currently connected to Access Point radios within each configured site.

Multi-Site Auto Provisioning (System)

The Express Manager’s auto-provisioning feature allows a multi-site WLAN network without any pre-staging. Policies can be defined for each site to match parameters such as CDP/LLDP string, AP MAC and IP address to place APs in a specific site and apply an appropriate configuration. As a result, the time required to deploy the WLAN infrastructure is significantly reduced.

The system level dashboard contains a map view of all the sites with inventory details for immediate visualization of the entire network. The site-level dashboard displays the status of the Access Points their radios, client devices connected to the Access Points, how available capacity. A drop-down allows you to view information for your preferred time frame for the last 30 minutes, the past two hours or the last 24 hours.

To view site auto provisioning configuration:

- 1 From the main tree, expand the Configuration menu item and select **Sites**.
- 2 Select **Auto Provisioning Policy**.

Configuration -> Sites System

Auto Provisioning Policy Rules << Sites

Added/Modified Rules will be effective after device(s)/controller(s) reboot

+ Add Delete							Number of Rules: 6
<input type="checkbox"/>	Precedence	Operation	Match Type	Match Type value	Site Name		
<input type="checkbox"/>	1		model-number	AP-7532E-67040-WR	SITE-1		
<input type="checkbox"/>	2		model-number	AP-6522E-66030-WR	SITE-2		
<input type="checkbox"/>	3		mac	B4-C7-99-57-F0-C8	SITE-3		
<input type="checkbox"/>	4		mac	B4-C7-99-49-12-F4	SITE-4		
<input type="checkbox"/>	5		model-number	AP-6521E-60020-WR	SITE-5		
<input type="checkbox"/>	6		mac	11-22-33-44-55-66	N/A		

Apply Discard

- 3 The **Auto Provisioning** section displays the following:

Precedence	Define the precedence (sequence) adoption policy rules are applied. Rules with the lowest precedence receive the highest priority. This value is set (from 1 - 1000) when adding a new Auto Provisioning Policy rule configuration.
-------------------	---

Operation	<p>Define the operation taken upon receiving an adoption request from an Access Point. The following operations are available:</p> <p><i>Allow</i> – Allows the normal provisioning of connected Access Points upon request.</p> <p><i>Deny</i> – Denies (prohibits) the provisioning of connected Access Point upon request.</p> <p><i>Redirect</i> – When selected, an Access Point seeks a steering controller (upon adoption request), and forwards the network credentials of a designated controller resource that initiates the provisioning process.</p> <p><i>Upgrade</i> – Conducts the provisioning of requesting Access Points from this controller resource.</p>
Match Type	<p>Set the matching criteria used in the policy. This is like a filter and further refines Access Points capable of adoption. The Match Type can be one of the following:</p> <p><i>MAC Address</i> – The filter type is a MAC Address of the selected Access Point model.</p> <p><i>IP Address</i> – The filter type is the IP address of the selected Access Point model.</p> <p><i>VLAN</i> – The filter type is a VLAN.</p> <p><i>Serial Number</i> – The filter type is the serial number of the selected Access Point model.</p> <p><i>Model Number</i> – The filter type is the Access Point model number.</p> <p><i>DHCP Option</i> – The filter type is the DHCP option value of the selected Access Point model.</p>
Match Type value	<p>Displays the match type value based on the match type specified. The match type value displays the output for the selected match type of <i>MAC Address, IP Address, VLAN, Serial Number, Model Number and DHCP Option</i>.</p>
Site Name	<p>Displays the name of the site associated with each rule.</p>

LAN Configuration (System)

Refer to the **LAN** screen to configure WiNG Express Manager wired interfaces. For most sites the default configuration should work just fine. You can create VLAN interfaces here and assign IP address using DHCP. You can also configure a separate VLAN here for Guest access and enable NAT to the Internet.

To configure wired interface settings:

- 1 Select **Configuration** settings from the main menu then select **LAN**.
- 2 Configure the following **LAN Port Settings** for each LAN port:

Configuration -> LAN System

LAN Port Settings

Number of Interfaces: 14				
Port	Enable	Allowed VLAN (1-5,6,9)	Untagged VLAN (1-4094)	Edit
ge3	✓		1	
ge2	✓		1	
ge1	✓		1	
ge7	✓		1	
ge6	✓		1	
ge5	✓		1	
ge4	✓		1	
xge4	✓		1	
ge9	✓		1	
ge8	✓		1	
xge1	✓		1	
xge2	✓		1	
xge3	✓		1	
ge10	✓		1	

Port	Displays the physical interface (GE1, FE1, etc.) for each wired connection on the network. Supported models each have unique physical interface connections.
Enable	Select <i>Enable</i> to allow traffic on the selected wired interface. To disable wired traffic on a specific interface, uncheck the option.
Allowed VLAN	Displays the VLAN(s) that traffic is allowed on as a virtual interface for each wired port.
Untagged VLAN	Displays the VLAN(s) that 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:

IP Settings

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

The screenshot shows a web interface for managing VLAN interfaces. At the top, there are two buttons: '+ Add Vlan' and 'Delete Vlan'. To the right, it says 'Number of IP Interfaces: 0'. Below this is a table with the following columns: 'Interface', 'Description', 'DHCP Client', and 'Edit'. The table is currently empty, and the text 'No Data' is displayed in the main area.

Interface	Displays the VLAN information for each VLAN interface utilized by the wired port connection.
Description	Optionally provide a description for each VLAN interface.
DHCP	Select DHCP to configure IP Address and Mask information using a DHCP Server. To manually configure the network address, 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.

Wireless Configuration (System)

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 to another. WLANs can therefore be configured around the needs of specific user groups, even when they are not in physical proximity. WLAN configurations can be defined to only provide service to 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.

Wireless LANs are defined individually within a WiNG Express System or Sites. Access Points assigned to the Site using an auto provisioning policy broadcast the WLAN SSID configured at the sites or the WLANs configured at the system level. Each WLAN consists of configuration parameters which define the basic operating parameters for the WLAN as well as authentication, encryption, QoS and firewall options. Changes made to a WLANs configuration are automatically inherited by all Access Points utilizing the WLAN. No WLANs are pre-defined by default in WiNG Express Manager. Wireless LANs can be assigned to a single or both the radios.

To configure WLAN properties to be complimentary with 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** and **Wireless LAN** fields.
- 2 Configure the following **Radio Settings** for the 2.4Ghz and 5Ghz radios on the WiNG Express managed Access Point:

Channel	Use the drop-down menu to select a channel for the 2.4Ghz or 5Ghz radio. Point. 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 Smart to let the Access Point manage the power settings based on network conditions. Selecting <i>Smart</i> 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 used for the transmission of probe responses. 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 Specify the following information for each Wireless LAN:

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 SSID. The WLAN SSID is case sensitive and alphanumeric. SSID length should not exceed 32 characters.
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.
Authentication Type	<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 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>, enter a WPA2 Key to password protect the WLAN. Define whether the key is entered in ASCII or HEX characters. Selecting Show to expose the key is not recommended.</p> <p>If selecting <i>Secure-802.1x</i>, provide an IP address (or hostname) and a shared secret (password) to access an external RADIUS server resource to validate user requests to the WLAN resources.</p>
2.4 GHz	Displays a green check mark if the radio is enabled for WLAN utilization and client support and a red X if the radio is disabled.
5 GHz	Displays a green check mark if the radio is enabled and a red X if the radio is disabled. AP6511 and AP6521 models do not have a second radio.
Edit	Select <i>Edit</i> to change the settings of the selected WLAN.

4 Specify the following in the **Advanced Smart RF** section:

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.
Disable DFS	Select this option to disable DFS scanning for RADAR.
Channel 2.4 GHz / 5 GHz	Use the drop-down menu to select channels available for use in Smart RF scanning. Add them to the list using the + and remove them using the trashcan. Specify the channels for both 2.4 GHz and 5 GHz traffic if applicable.
Channel Width 2.4 GHz / 5 GHz	Use the drop-down menu to specify the channel width in Smart RF scanning. Specify the channel width for both 2.4 GHz and 5 GHz traffic if applicable.

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.
Voice Aware Scanning 2.4 GHz / 5 GHz	Select this option to enable voice aware scanning for voice traffic during scans. Enable for both 2.4 GHz and 5 GHz traffic if applicable.

Editing Wireless Configuration (System)

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 provided service to 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 **Wireless** screen to monitor WLAN utilization and whether WLAN usage is consistent with deployment objectives and the security needs of its connected clients.

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

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

2 Select a WLAN and click on its name to edit.

The screenshot shows the configuration page for a WLAN named 'thenappan'. The 'Enable' checkbox is checked. The SSID is 'zebra'. Security is set to 'Secure-PSK'. Both 2.4 GHz and 5 GHz bands are selected. The VLAN is set to 1. Encryption is set to WEP-64. The WLAN Rate-Limit section shows Per-Client and Aggregate(WLAN) both set to 5000 kbps. Other Settings include Client Roam Assist and Voice VLAN, both of which are unchecked.

3 Configure the following settings for the WLAN:

Name	Add or edit a name for the WLAN. This name is used throughout the Express Manager user interface as its 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 SSID. The WLAN SSID is case sensitive and alphanumeric. SSID length should not exceed 32 characters.
Client-To-Client Communications	Select this option to enable client to client communication 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.

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 secret-key.</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>If selecting <i>Secure-802.1x</i>, provide an IP address (or hostname) and a shared secret (password) used to access an external RADIUS server resource designated to validate user requests to the Access Point's WLAN resources.</p> <p>Selecting <i>Guest</i> displays fields for captive portal Web page creation.</p>
Band	<p>Select a band, <i>2.4Ghz</i> or <i>5Ghz</i> (if supported), to enable specific client radio support on the WLAN.</p>
VLAN	<p>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.</p>
Description	<p>Optionally, enter descriptive text which can be used by administrators to help identify each WLAN.</p>

<p>Encryption (Secure-PSK only)</p>	<p>When <i>Secure-PSK</i> 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 IEEE <i>Wireless Fidelity (Wi-Fi)</i> 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 Message Integrity Check (MIC) 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><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 are used to 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>
--	--

Key (Secure-PSK only)	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.
RADIUS VLAN Assignment (Secure-802.1x and Guest only)	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.
Bypass Captive Portal Detection	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.
RADIUS (only Secure-802.1x)	Configure the RADIUS server to use for authentication. Select from <i>Local</i> - Select this option to use the onboard RADIUS server. <i>Controller</i> - Select this option to use the RADIUS server on the adopting controller. <i>External</i> - Select this option to configure details about 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 shared with the server.
Session Timeout (Guest Only)	Configure the session timeout value for Guest User access. This is the time duration after which the guest user is forced to re authenticate.
Only Internet Access	Select this option to prevent client devices from accessing resources on the VLAN. This option restricts the clients to locations on the internet only.
Use DHCP/NAT on APs	Select this option to use DHCP information as 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.
Bypass Captive Portal Detection	Select this option to enable Social Media Authentication to work on hand-held devices. If enabled, a requesting client's guest user Facebook or Google social media profile (collected from the social media server) is registered on the device. Captive portal authentication then becomes a fallback mechanism to enforce guest registration through social authentication.

Access Type	<p>Select the authentication scheme applied to clients requesting captive portal guest access to the 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>
Lookup Information	<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>
RADIUS	<p>Use this field to provide the information required to access the RADIUS server used for authentication. Select <i>Controller</i> to configure the authentication server as the RADIUS server on the controller. Select <i>External</i> to configure an external RADIUS server for authentication.</p>
Registration Type	<p>Use the Registration Type drop-down menu to set the self-registration type for tis selected WLAN. Options include <i>Device</i>, <i>User</i> and <i>Device-OTP</i>.</p> <p>When captive portal guest users are authenticating using their User ID (Email Address/Mobile Number/ Member ID) and the received pass code in order to complete the registration process. The WLAN authentication type should be MAC-Authentication and the WLAN registration type should be configured 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>
Radius Group	<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>
Expiry Time	<p>Use this field to set the time (from 1 - 43,800 hours) before registration addresses expire and must be re-entered.</p>

Agreement Refresh Time	Set the <i>Agreement Refresh Time</i> as the amount of time (from 0 - 144,000 minutes) before the agreement page is displayed if the user has not been logged during the specified period.
Connection Mode	Use this option to select between HTTP and HTTPS as the connection mode when a client device accesses the Captive Portal server.
Social Media Auth	<p>If <i>Google</i> selected, the requesting client's guest user Google social media profile (collected from the social media server) is registered on the device. Captive portal authentication then becomes a fallback mechanism to enforce guest registration through social authentication. Use the text box to provide the unique client ID received from Google for providing this service.</p> <p>If <i>Facebook</i> selected, the requesting client's guest user Facebook social media profile (collected from the social media server) is registered on the device. Captive portal authentication then becomes a fallback mechanism to enforce guest registration through social authentication. Use the text box to provide the unique client ID received from Facebook for providing this service.</p>
Captive Server	Provide the FQDN of the device providing the Captive Portal service.
Logout FQDN	Set the FQDN address to logout of the captive portal session from the client (for example, logout.guest.com).
DNS Whitelist	A DNS whitelist is used in conjunction with a captive portal to provide access services to wireless clients. Use the whitelist to create a set of allowed destination IP addresses within the captive portal. To effectively host hotspot pages on an external Web server, the IP address of the destination Web server(s) should be in the whitelist. Use the + <i>Add</i> button to add a DNS Whitelist entry.

Note: When using registration as the access type, E-mail and mobile are mandatory fields.

- 4 Use the **Web Pages** section to configure the html pages that are displayed to the guest user.

Use the **Terms and Conditions** check box to enforce the user to accept the terms and conditions before accessing the captive portal.

When **Use Default Files** option is selected, the captive portal displays the default pages that are hosted on this device. When **Upload Files** is selected, the user can upload pages to the device and to the captive portal user. When **External** is selected, provide the complete path to an external server that hosts the files displayed to the captive portal user.

Use the tabs to configure the following fields for each page is displayed to the captive portal user.

Organization's Name	Set any organizational specific name or identifier which clients see during login. The <i>Organization Name</i> setting is only available for the Login page.
Title Text	Set the title text displayed on the pages when wireless clients access captive portal pages. The text should be in the form of a page title describing the respective function of each page and should be unique to each function.

Header Text	Provide header text unique to the function of each page.
Login Message	Specify a message containing unique instructions or information for the users who access the Login, Terms and Condition, Welcome, Fail, No Service or Registration pages. In the case of the Terms and Agreement page, the message can be the conditions requiring agreement before captive portal access is permitted.
Footer Text	Provide a footer message displayed on the bottom of each page. The footer text should be any concluding message unique to each page before accessing the next page in the succession of captive portal Web pages.
Signature	Provide the copyright and legal signature associated with the usage of the captive portal and the usage of the organization name provided. The Signature setting is only available for the Login page.
Main Logo	Provide the URL for the main logo image displayed on the screens. Optionally select the Use as banner option to designate the selected main logo as the page's banner as well. The banner option is disabled by default.
Small Logo	Use the Small Logo field to provide the URL for a small logo image displayed on the screens.

Select **Redirect the user to externally hosted Success URL** field to redirect the captive portal user when the login is successful.

- 5 Select the **Reg Page Fields** tab to configure the look and feel of the Registration page. When setting the properties of the Registration screen, refer to the table to define email, country, gender, mobile, zip, street and name filters used as additional authentication criteria. Guest users are redirected to the registration portal on association to the captive portal SSID. Users are displayed an internal (or) externally hosted registration page where the guest user must complete the registration process if not previously registered. These fields are customizable to meet the needs of organizations providing guest access. The captive portal sends a message to the user (on the phone number or Email address provided at registration) containing an access code. The user inputs the access code and the captive portal verifies the code before returning the Welcome page and providing access. This allows the organization to verify the phone number or Email address is correct and can be traced back to a specific individual.
- 6 Configure the following settings in the **WLAN Rate Limit** section:

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

- 7 Configure the following **Other Settings** section configure the following settings:

Client Roam Assist	Select this option to enable client roam assist. By constantly monitoring a client's packets and the <i>received signal strength indicator</i> (RSSI) of a given client by a group of Access Points, a decision 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 is tagged with this VLAN.

Security Firewall Configuration (System)

When protecting wireless traffic to and from a Express Manager connected 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. Express Manager provides seamless data protection and user validation to protect and secure data at each vulnerable point in the 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. Security is provided at the most granular level, with role, location and device categorization based network access control available based on identity as well as client security posture.

A firewall is a mechanism enforcing network access control, and is considered a first line of defense in protecting proprietary information within the 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 Express Manager connected 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 Express Manager is processing, the firewall uses that rule's action to determine whether traffic is allowed or denied.

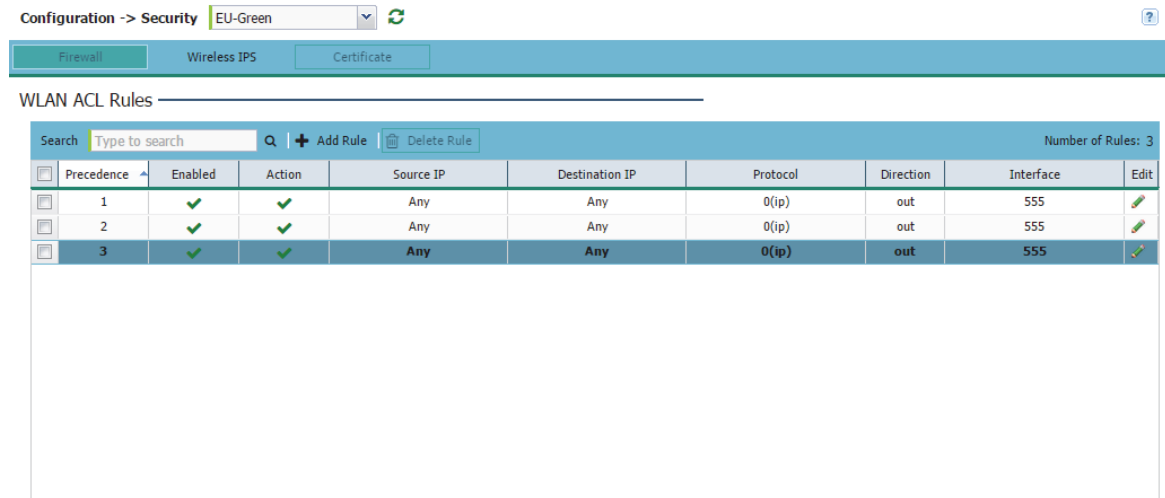
Rules comprise conditions and actions. A condition describes a traffic stream of packets. Define constraints on the source and destination device, the service (for example, protocols and ports), and the incoming interface. An action describes what should occur to packets matching the conditions set. 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**.

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

2 Set the following **WLAN ACL Rules**:



Precedence	Specify or modify a precedence (priority) for this IP policy between 1-5000. 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 stop a packet from reaching its destination. <i>Permit</i> - Instructs the firewall to allow a packet to proceed to its destination.
Source IP	Determine whether the filtered packet source for this IP firewall rule requires any classification (any), is designated as a set of configurations consisting of protocol and port mappings (an alias), is set as a numeric IP address (host) or defined as network IP and mask.
Destination IP	Determine whether the filtered packet destinations for this IP firewall rule requires any classification (any), is designated as a set of configurations consisting of protocol and port mappings (an alias), is 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	Set the access protocols impacted by the WLAN's ACL rule configuration.

Source Port	If using either <i>tcp</i> or <i>udp</i> as the protocol, define whether the source port for incoming ACL rule application is any, equals or an administrator defined range. If not using tcp or udp, this setting displays as N/A. This is the data local origination port designated by the administrator. Selecting equals invokes a spinner control for setting a single numeric port. Selecting range displays spinner controls for <i>Low</i> and <i>High</i> numeric range settings. A source port cannot be a destination port.
Destination Port	If using either <i>tcp</i> or <i>udp</i> as the protocol, define whether the destination port for outgoing IP ACL rule application is any, equals or an administrator defined range. If not using tcp or udp, this setting displays as N/A. This is the data destination port designated by the administrator. Selecting equals invokes a spinner control for setting a single numeric port. Selecting range displays spinner controls for <i>Low</i> and <i>High</i> numeric range settings.
Direction	Specify the direction to determine whether inbound or outbound traffic is filtered.
Interface	Specify the interface for the WLAN ACL rule to affect.

3 Set the following **Wireless Client Association ACL Rules**:

Wireless Client Association ACL Rules

Search <input type="text" value="Type to search"/> <input type="button" value="Q"/> <input type="button" value="+ Add Rule"/> <input type="button" value="Delete Rule"/>					
<input type="checkbox"/>	Precedence	Action	Start MAC	End MAC	
<input type="checkbox"/>	1	✓	00-00-00-00-00-00	FF-FF-FF-FF-FF-FF	
<input type="checkbox"/>	2	✓	00-00-00-00-00-00	FF-FF-FF-FF-FF-FF	
<input type="checkbox"/>	3	✓	00-00-00-00-00-00	FF-FF-FF-FF-FF-FF	

Precedence	Specify or modify a precedence (priority) for this IP policy between 1-5000. 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.
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 reaching its destination. <i>Permit</i> - Instructs the firewall to allow a packet to proceed to its destination.
Source 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.
WLANs	Use the drop-down menu to specify the WiNG Express WLAN configurations impacted by the ACL's rule configuration.

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 the use of 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 lockdown.

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.

Express Manager connected 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. When used within a network and its associated Access Point radios, 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 protect the Access Point.
- ◆ *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 promptly respond to 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 an Access Point:

- 1 Select **Configuration** from the main menu. Select **Security**, then **Wireless IPS**.
- 2 Select **Enable Rogue AP Detection** to allow the detection of unauthorized (unsanctioned) devices this WIPS policy.
- 3 Select **Off-Channel Scan** to scan all channels using this Access Point's radio. Channel scans use Access Point resources and can be time consuming. Only enable when sure the radio can afford bandwidth be dedicated to channel scans and does not negatively impact client support.
- 4 Review the following **Wireless IPS** event information:

Event Name	<p>Displays the rogue AP event type detected by the sensor. Several different event types can occur:</p> <p>An <i>Excessive Action Event</i> is an event where an action is performed repetitively and continuously. DoS attacks come under this category.</p> <p><i>MU Anomaly Events</i> are suspicious client events that can compromise the stability of the network.</p> <p><i>AP Anomaly Events</i> are suspicious frames sent by neighboring APs.</p>
Reporting AP	Displays the hardware encoded <i>Media Access Control</i> (MAC) address of the Access Point reporting the listed WIPS event.
Originating Device	Displays the MAC address of the AP which triggered the reported event. Review this address carefully to validate whether this is a known and approved Access Point or if it's unauthorized and could jeopardize network security.
Detector Radio	Displays the radio number of the detecting Access Point reporting the event. AP6511 and AP6521 model Access Points are single radio models, other supported Access Points are dual radio models.
Time Reported	Displays the date and time stamp for each WIPS event reported.

Security Certificate Configuration (System)

A certificate links identity information with a public key enclosed in the certificate.

A *certificate authority* (CA) is a network authority that issues and manages security credentials and public keys for message encryption. The CA signs all digital certificates it issues with its own private key. The corresponding public key is contained within the certificate and is called a CA certificate. A browser must contain the CA certificate in its Trusted Root Library so it can trust certificates *signed* by the CA's private key.

Depending on the public key infrastructure, the digital certificate includes the owner's public key, the certificate expiration date, the owner's name and other public key owner information.

Each certificate is digitally signed by a *trustpoint*. The trustpoint signing the certificate can be a certificate authority, corporation or individual. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters, and an association with an enrolled identity certificate.

- 1 Select the **Configuration** tab from the Web UI.
- 2 Select **Security** from the Configuration tab.

3 Select **Certificates** from the Device menu.

Configuration -> Security System

Firewall | Wireless IPS | **Certificate**

Manage Certificate | RSA Keys | Create Certificate | Create CSR

All Certificate Details Number of Trustpoints: 1

Trustpoints Name	RSA Key	Valid From
default-trustpoint	default_rsa_key	09/02/2014 12:54:17 UTC

Certificate Details

Subject Name: /CN=NX7500-B4-C7-99-6C-8F-68

Alternate Subject Name:

Issuer Name: /CN=NX7500-B4-C7-99-6C-8F-68

Serial Number: 0635

RSA Key: default_rsa_key

Is Self Signed:

RSA Key Used:

CRL Present:

Is CA:

Validity

Valid From: 09/02/2014 12:54:17 UTC

Valid Until: 08/30/2024 12:54:17 UTC

Certificate Authority (CA) Details

Subject Name:

Alternate Subject Name:

Issuer Name:

[Go Back](#) [Refresh](#)

4 Set the following **Management Security** certificate configurations:

HTTPS Trustpoint	Either use the default-trustpoint or select the <i>Stored</i> radio button to enable a drop-down menu where an existing certificate can be leveraged. To leverage an existing certificate, select the <i>Launch Manager</i> button.
-------------------------	---

5 Set the following **RADIUS Security** certificate configurations:

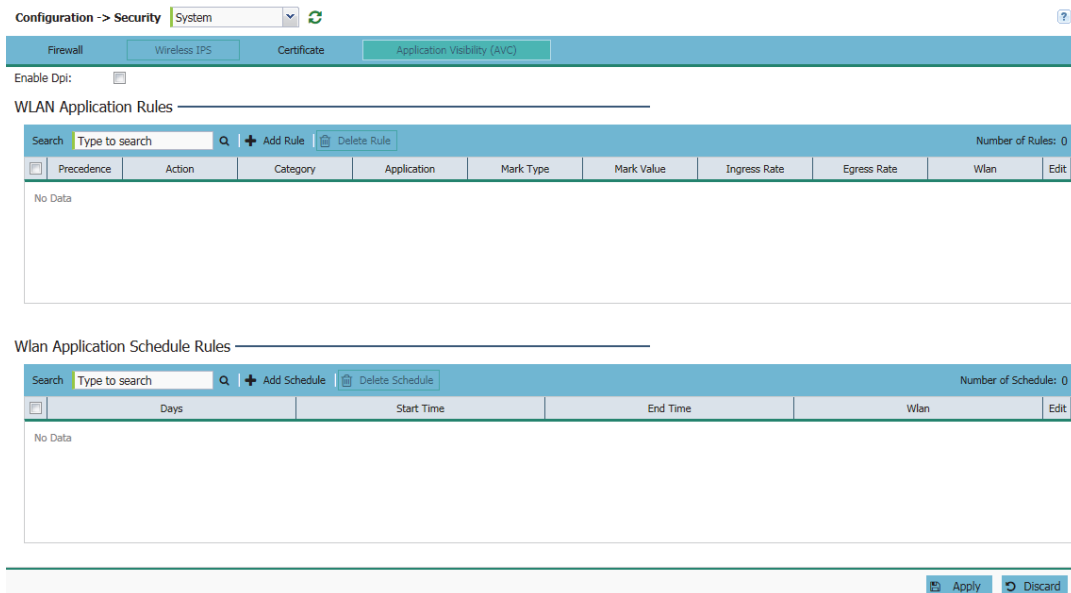
RADIUS Certificate Authority	Either use the default-trustpoint or select the <i>Stored</i> radio button to enable a drop-down menu where an existing certificate can be leveraged. To leverage an existing certificate, select the <i>Launch Manager</i> button.
RADIUS Server Certificate	Either use the default-trustpoint or select the <i>Stored</i> radio button to enable a drop-down menu where an existing certificate/trustpoint can be used. To leverage an existing trustpoint, select the <i>Launch Manager</i> button.

6 Select **OK** to save the changes made to the certificate configurations. Selecting **Reset** reverts to its last saved configuration.

Security Application Visibility (System)

Utilize application visibility to provide deep-packet inspection (application assurance) by inspecting every byte of each application header packet passing through the controller or service platform. When enabled, application data streams are inspected at a granular level to help prevent viruses and spyware from accessing the WiNG Manager network.

- 1 Select the **Configuration** tab from the Web UI.
- 2 Select **Security** from the Configuration tab.
- 3 Select **Application Visibility (AVC)** from the top menu.



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

Note: **Application Visibility** is available on the following platforms: AP7522, AP7522E, AP7532.

- 4 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-selectes 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.
Mark Type	Mark actions mark packets for a recognized application and category with DSCP/8021p values used for QoS.
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 which to apply the application rules.

- 5 To delete an existing rule, select that rule from the table and select **Delete Rule**.
- 6 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.

- 7 To delete and existing schedule select that rule from the table and select **Delete Schedule**.

RADIUS Configuration (System)

The Express Manager's RADIUS server allows the configuration of user groups with common user policies. The RADIUS configuration allows the configuration of user groups with common user policies, such as VLAN and access schedule, and is mapped to WLAN for authentication. User names are created and associated with the user group. Names and associated users are stored in the controller, service platform or 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, left-hand side pane of the UI displays the **RADIUS** option.

The **RADIUS Group** screen displays (by default).

Configuration -> Services System

DHCP **RADIUS**

Enable Radius Server:

Group _____

+ Add		Delete									Number of Groups: 13
<input type="checkbox"/>	Group	VLAN	WLAN SSID	UP Rate-Limit	Down Rate-Limit	Start Time	End Time	Guest			
<input type="checkbox"/>	zzz	1	thenappan	Not Set	Not Set	00:00	23:59	<input checked="" type="checkbox"/>			
<input type="checkbox"/>	333	1	thenappan	Not Set	Not Set	00:00	23:59	<input checked="" type="checkbox"/>			
<input type="checkbox"/>	thenappan	1	thenappan	Not Set	Not Set	00:00	23:59	<input checked="" type="checkbox"/>			
<input type="checkbox"/>	2222	1	thenappan	Not Set	Not Set	00:00	23:59	<input checked="" type="checkbox"/>			
<input type="checkbox"/>	kar	1	kartikey	Not Set	Not Set	00:00	23:59	<input checked="" type="checkbox"/>			

Users _____

+ Add		Delete						Number of Users: 0
<input type="checkbox"/>	Users	Group List	Email	Start Time	End Time	Guest		
<input type="checkbox"/>	zebra	444	ss@yahoo.com		01:01	<input checked="" type="checkbox"/>		

Apply Discard

- 3 Select **Enable Radius Server** to activate the Express Manager's local RADIUS server.
- 4 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 network to which the Access Point belongs.
Rate limit from air	Specify the maximum data rate in kbps between 100 and 1,000,000 for wireless traffic.

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.

- 5 Review the following RADIUS schedule information and modify as needed:

Access by time	To enable guest access to the RADIUS server by time of day, select this option and then specify a <i>Start Time</i> and <i>End Time</i> 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 time users within each listed group lose access to the local RADIUS resources.
Access by Day of Week	To enable guest access to the RADIUS server by specific days of the week, select this option and select each of the days you wish to enable access.

- 6 When adding or editing a RADIUS user, verify and configure the following:

User ID	Displays the name or identifier assigned to each user when it was 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 drop-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 contact telephone number associated with the RADIUS user. This is an optional field.
Start Date / Start Time	Specify a starting 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 Till Expiry option. To specify a duration of time the account is active, set the duration in Days:Hours:Minutes format. The RADIUS user is deactivated once the set duration has passed.

- 7 To add a new group click the **Add** button. To modify the settings of an existing group, select the group and click the **Edit** button. To delete an obsolete group, select the group and click the **Delete** button.

Note: The RADIUS service is not started by default on the AP6511 and AP6521 Access Points. To use RADIUS on these APs, the service must first be started.

Basic Management Configuration (System)

Express Manager devices 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.

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 resources. Management restrictions can also be applied to reduce the device's attack footprint when guest services are deployed.

To configure the device's management settings:

- 1 Select **Configuration** from the main menu then select **Management**.
The **Management** screen is partitioned into Administrator, Access, Syslog Server, SNMP Settings and SNMP Traps fields.
- 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 (Hypertext Transfer Protocol Secure) 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 (Secure Shell) 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 logging configuration. This option is disabled by default.
Logging Level	Event severity coincides with the syslog logging level defined for the Express Manager. 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	SNMPv1 exposes a device's management data so it can be managed remotely. Device data is exposed as variables that can be accessed and modified as text strings, with version 1 being the original (rudimentary) implementation. SNMPv1 is disabled by default.
Enable SNMPv2	Select the checkbox to enable SNMPv2 support. 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	Select the checkbox to enable SNMPv3 support. SNMPv3 adds security and remote configuration capabilities to previous versions. The SNMPv3 architecture introduces the <i>user-based security model (USM)</i> for message security and the <i>view-based access control model (VACM)</i> 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: Access Control	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 snmpmanager, snmpoperator or snmptrap.
SNMPv3 Users: Password	Provide the user's password in the field provided. Select the Show check box to display the actual character string used in the password, while leaving the check box unselected protects the password and displays each character as "*" .
SNMPv3 Users: Authentication	Select the user authentication type used with the listed SNMPv3 user. The selected authentication scheme ensures only trusted users can utilize the Express Manager's 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 the Express Manager's 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**.

Guest Management Configuration (System)

To configure Guest Management rules:

- 1 Select the **Configuration** tab from the Web UI.
- 2 Select **Management** from the Configuration tab.
- 3 Select **Guest** from the top menu.

The screenshot shows the 'Guest Management' configuration page. At the top, there is a breadcrumb 'Configuration -> Management' and a dropdown menu set to 'System'. Below this are two tabs: 'Basic' and 'Guest', with 'Guest' being the active tab. The page is divided into three main sections: 'SMS Settings', 'Email Settings', and 'SMS SMTP Settings'. Each section has an 'Enable' checkbox and various input fields for configuration. At the bottom right, there are 'Apply' and 'Discard' buttons.

The **Guest Management** screen is partitioned into **SMS Settings**, **SMS Settings** and **Email Settings**.

Note: **Guest Management** is available on the following platforms: NX7500E, VX9000E.

4 Enable **SMS Settings** by selecting **Enable** and configure the following fields.

Gateway	Upon receiving the passcode email, the SMS gateway sends the actual notification passcode SMS to the guest user.
Username	Provide a unique 32 character maximum username unique to this SMS guest management configuration. This username requires its own password and must be correctly provided to receive the passcode for registering guest user credentials with SMS.

Password	Define a 63 character maximum password that must be correctly provided with the unique username to receive the passcode for registering guest user credentials with SMS.
App Id	Set a 32 character maximum API Id for the configuration of the clickatell api_id (http/sntp api_id).
User Agent	Specify the user agent for configuring the SMS gateway server and its related credentials for sending the passcode to guests.
Source Number	Set a 32 character maximum source-address from the number associated with clickatell. It can be a large integer or short code.
Message	Create the 1024 character maximum message content for the SMS based request sent to the guest user along with the passcode.

- 5 Enable **SMS SMTP Settings** by selecting **Enable** and configure the following fields.

Gateway	Define a hostname or IPv4 formatted IP address of the SMS gateway server resource used for guest management E-mail traffic, guest user credential validation and passcode reception. Consider providing the host as an alias. An alias enables an administrator to define a configuration item, such as a hostname, as an alias once and use the alias across different configuration items.
Sender	Provide a 100 character maximum sender name for the guest user receiving the passcode required for registering their guest E-mail credentials using SMTP.
Security	Use the drop-down menu to select <i>ssl</i> or <i>starttls</i> as the SMTP server user authentication validation scheme for this particular username and password combination. Optionally select, None to apply to no additional user authentication beyond the required username and password combination. The default value is <i>ssl</i> .
Username	Provide a unique 64 character maximum username unique to this SMTP guest management configuration. This username requires its own password and must be correctly provided to receive the passcode for registering guest user credentials.
Password	Define a 64 character maximum password that must be correctly provided with the unique username to receive the passcode for registering guest user credentials with SMTP.
Recipient Email	Enter a 64 character maximum E-mail address for the recipient of guest management E-mail traffic. The gateway server converts the E-mail into SMS and sends the message to guest users's mobile device.
Subject	Enter a 100 character maximum E-mail subject for the E-mail message sent to the guest user along with the passcode.
Message	Enter a 1024 character maximum E-mail message per the message format required by the gateway server. The sms-over-smtp message format is the required format while sending E-mail to the SMS gateway server.



- 6 Enable **Email Settings** by selecting **Enable** and configure the following fields.

Gateway	Define a hostname or IPv4 formatted IP address of the SMTP server resource used for guest management E-mail traffic, guest user credential validation and passcode reception.
Sender	Provide a 100 character maximum sender name for the guest user receiving the passcode required for registering their guest E-mail credentials.
Security	Use the drop-down menu to select <i>ssl</i> or <i>starttls</i> as the E-mail host server user authentication validation scheme for this particular username and password combination. Optionally select, <i>None</i> to apply to no additional user authentication beyond the required username and password combination.
Username	Provide a unique 100 character maximum username unique to this guest management configuration. This username requires its own password and must be correctly provided to receive the passcode for registering guest E-mail credentials.
Password	Define a 63 character maximum password that must be correctly provided with the unique username to receive the passcode for registering guest E-mail credentials.
Subject	Enter the 100-character maximum E-mail subject for the E-mail message sent to the guest user along with the passcode.
Message	Create the 1024 character maximum message content for the E-mail sent to the guest user along with the passcode.












Device Configuration (System)


Use the Devices tab under the Configuration menu to set site specific information such as Location, Name, Default gateway, VLAN interface and IP address.

- 1 Select **Configuration** from the main menu then select **Devices**.

Configuration -> Devices System  

Managed Devices Tools Show Upgrade Number of Devices: 11

Device Name	Device Status	IP Address	2.4 GHz		5 GHz		Firmware
			Channel	Power (dbm)	Channel	Power (dbm)	
SITE-1 (Count:2)							
<input type="checkbox"/> ap7532-000003	 (online)	60.60.60.10	1(smt)	17(smt)	52w(smt)	4(smt)	5.7.0.0-0368
<input type="checkbox"/> ap7532-805DD0	 (online)	60.60.60.9	1(smt)	17(smt)	36w(smt)	17(smt)	5.7.0.0-0368
SITE-2 (Count:3)							
<input type="checkbox"/> ap6522-5D6780	 (online)	20.20.20.11	11(smt)	17(smt)	44w(smt)	16(smt)	5.7.0.0-0368
<input type="checkbox"/> ap6522-442CF0	 (online)	20.20.20.7	6(smt)	17(smt)	44w(smt)	16(smt)	5.7.0.0-0368
<input type="checkbox"/> ap6522-491394	 (online)	20.20.20.9	1(smt)	17(smt)	149w(smt)	16(smt)	5.7.0.0-0368
SITE-3 (Count:1)							
<input type="checkbox"/> ap6562-57F0C8	 (online)	30.30.30.4	6(smt)	17(smt)	149w(smt)	17(smt)	5.7.0.0-0368
SITE-4 (Count:1)							
<input type="checkbox"/> ap6562-4912F4	 (online)	30.30.30.5	6(smt)	17(smt)	149w(smt)	17(smt)	5.7.0.0-0368
SITE-5 (Count:2)							
<input type="checkbox"/> ap6521-0875EE	 (online)	40.40.40.5	1(smt)	17(smt)	-	-	5.7.0.0-0368
<input type="checkbox"/> ap6521-12C9CD	 (online)	40.40.40.4	1(smt)	17(smt)	-	-	5.7.0.0-0368
System (Count:2)							
<input type="checkbox"/> vx9000-96C278 (active)	 (online)	10.10.10.7	-	-	-	-	5.7.0.0-208656X
<input type="checkbox"/> vx9000-487856 (standby)	 (online)	10.10.10.9	-	-	-	-	5.7.0.0-208656X



- 2 The **Managed Devices** table displays the following information about devices managed at both the system and the site level:

Device Name	Displays the specified device name for each configured device.
Device Status	Displays the online status of each device. If a device is online, it displays two green arrows pointing up. If the device is offline, it displayed two red arrows pointing down.
IP Address	Displays the IPv4 IP Address associated with each configured device.
2.4 GHz Channel	Displays the 2.4 GHz radio channel each configured device is using. If a device is not using a channel or status is unavailable, N/A appears instead of a channel number. If a device is using smart channel selection, (smt) displays after the channel number.
2.4 GHz Power	Displays the configured power level of the 2.4 GHz radio (in dbm) for each configured device. If a device is using smart channel selection, (smt) displays after the power level.
5 GHz Channel	Displays the 5 GHz radio channel that each configured device is using. If a device is not using a channel or status is unavailable, N/A appears instead of a channel number. If a device is using smart channel selection, (smt) displays after the channel number.

5 GHz Power	Displays the configured power level of the 2.4 GHz radio (in dbm) for each configured device. If a device is using smart channel selection, (smt) displays after the power level.
--------------------	---

- 3 The **Tools** menu provides device specific actions that can be performed on one or more device selected from the **Managed Devices** table.



The following actions are available from the Tools drop-down menu:

Factory-Default	Selecting <i>Factory-Default</i> displays a prompt confirming you want to reset the selected device or devices to their factory defaults. Selecting Yes will reset the selected device or devices to factory default settings and will reboot the device. Choosing this option will erase all information and settings stored on the device. Selecting No will cancel the reset and return to the Device screen.
Reboot	Selecting <i>Reboot</i> displays a prompt confirming you want to reboot the device. Selecting Yes will reboot the device and the user interface will be unavailable until the device has rebooted. You will be required to log in to the user interface once the devices has finished rebooting. Selecting No will cancel the reboot and return you to the Devices screen.
Upgrade	Selecting <i>Upgrade</i> opens a dialogue window with firmware upgrade options. Firmware upgrades can be performed on a single selected device, or multiple selected devices of the same device model.
Tech-Support	Selecting <i>Tech-Support</i> 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 the path for the tech support server. Transfer of this information is supported via FTP, TFTP and HTTP protocols. The techsupport filename is auto generated by the device based on the device mac address, passing file name in path results in failure.
Packet Capture	Selecting <i>Packet Capture</i> allows you to capture client packet data based on the packet's address type or port on which received from each selected device or devices. Dropped client packets can also be trended to help assess network and client connectivity health.
IP Route	Selecting <i>IP Route</i> opens a window showing the current IP routes for the selected device or devices.
Export / Import Config	Selecting <i>Export / Import Config</i> displays a screen where configuration files can be imported to or exported from the selected device or devices. When Local is selected the current system configuration file is displayed as plain text in a window. To import a new configuration using this method, 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 and Local is selected, 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. To use this method, select Remote and specify the Protocol, Port, Hostname or IP Address, Username, Password and the path for the remote server. Transfer of this information is supported via FTP, TFTP and HTTP protocols.

Locator ON	Selecting <i>Locator ON</i> flashes the LEDs of the selected device or devices in order to make them easier to find in large deployments.
Locator OFF	Selecting <i>Locator OFF</i> stops flashing the LEDs of the selected device or devices if they have been set to flash using the <i>Locator ON</i> option.
Delete Offline Device(s)	Selecting <i>Delete Offline Device(s)</i> removes any offline devices listed in the Managed Devices table from the network and from the Managed Devices table.

Editing Devices Configuration (System)

- 1 Select **Configuration** from the main menu then select **Devices**.
- 2 Select the **Device Name** to edit the device configuration.

Edit -> ap7532-805DDO [SITE-1]  

Basic Settings

Name: *

Location:

Version: 5.7.0.0-036B

Model: AP-7532E-67040-WR

Up Time: 4 days, 01 hours 41 minutes

MAC Address: FC-0A-81-80-5D-D0

Default Gateway:

Wireless Settings

2.4GHz Channel: Power: (dBm)

5GHz Channel: Power: (dBm)

Radius Server Settings


Enable Radius Server:



IP Settings

DNS Servers

Route

[Detail >>](#)

	Interface (1-4094)	Description	IP Address	NAT	Edit
<input type="checkbox"/>	VLAN60		60.60.60.9/24(DHCP)	✗	

 Apply  Go Back

- 3 The **Basic Settings** section displays the following information for devices managed at the site level:

Name	Enter a name for the device. This name will be used throughout the interface to refer to this device.
Location	Enter a location for the device. This can be a generic name such as First Floor or a specific latitude and longitude.
Version	Displays the software version number currently active on the device.
Model	Displays the device model number and SKU for the selected device.
Uptime	Displays the device uptime in a Days, Hours and Minutes format.

Default Gateway	Specify the IP address of this devices default gateway where all external network traffic is routed through. Entering an IP address here will override the default gateway address.
2.4 GHz Channel	Displays the 2.4 GHz radio channel that each configured device is using. If a device is not using a channel or status is unavailable, <i>N/A</i> appears instead of a channel number. If a device is using smart channel selection, (<i>smt</i>) displays after the channel number.
2.4 GHz Power	Displays the configured power level of the 2.4 GHz radio (in dbm) for each configured device. If a device is using smart channel selection, (<i>smt</i>) displays after the power level.
2.4 GHz Antenna Gain	Set the 2.4 GHz antenna between 0.00 - 15.00 dBm. The Access Point's <i>Power Management Antenna Configuration File</i> (PMACF) automatically configures the Access Point's radio transmit power based on the antenna type, its antenna gain (provided here) and the deployed country's regulatory domain restrictions. Once provided, the Access Point calculates the power range. Antenna gain relates the intensity of an antenna in a given direction to the intensity that would be produced ideally by an antenna that radiates equally in all directions (isotropically), and has no losses. Although the gain of an antenna is directly related to its directivity, its gain is a measure that takes into account the efficiency of the antenna as well as its directional capabilities. Only a professional installer should set the antenna gain. The default value is 0.00.
5 GHz Channel	Displays the 5 GHz radio channel that each configured device is using. If a device is not using a channel or status is unavailable, <i>N/A</i> appears instead of a channel number. If a device is using smart channel selection, (<i>smt</i>) displays after the channel number.
5 GHz Power	Displays the configured power level of the 2.4 GHz radio (in dbm) for each configured device. If a device is using smart channel selection, (<i>smt</i>) displays after the power level.
5 GHz Antenna Gain	Set the 5 GHz antenna between 0.00 - 15.00 dBm. The Access Point's <i>Power Management Antenna Configuration File</i> (PMACF) automatically configures the Access Point's radio transmit power based on the antenna type, its antenna gain (provided here) and the deployed country's regulatory domain restrictions. Once provided, the Access Point calculates the power range. Antenna gain relates the intensity of an antenna in a given direction to the intensity that would be produced ideally by an antenna that radiates equally in all directions (isotropically), and has no losses. Although the gain of an antenna is directly related to its directivity, its gain is a measure that takes into account the efficiency of the antenna as well as its directional capabilities. Only a professional installer should set the antenna gain. The default value is 0.00.
Enable RADIUS Server	Select this option to enable the onboard RADIUS server. RADIUS settings can be configured on the RADIUS screen.

Configuration (Site)

Configurations set at the System level can be modified at the site and device levels. Sites provide the ability to override Wireless LAN SSID names and VLAN assignments for Access Points assigned to the Site.

Basic Configuration (Site)

To configure the basic configuration for the site:

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

Configuration -> Basic Settings EU-Green ?

Basic Configuration Settings

System Name: *

Country Name: *

Timezone:

Date & Time: Hour: Mins: AM PM

NTP Server:

Default Gateway:

DNS Servers:

IP Address	Edit
xxx.xxx.xxx.xxx	<input type="text"/>
xxx.xxx.xxx.xxx	<input type="text"/>
xxx.xxx.xxx.xxx	<input type="text"/>

Floor Plan

Floor: *

Protocol: FTP TFTP HTTP Port: **Basic**

Host: * IP Address Hostname

Username: *

Password: * Show

Path: *

Add Floor Plan

Static Routes

+ Add Number of Routes: 0

Network Address	Gateway	Edit
xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx	<input type="text"/>

- 2 Set the following **Basic Configuration Settings** for this site:

- **System Name** - Provide a name used as the Express Manager's network identifier. This is a required parameter.
- **Country Code** - If the Country Code was not set when the device was initially powered on, set the country now to ensure legal operation. The system's wireless capabilities are disabled until the required country code is set.
- **Timezone** - Use the drop-down menu to specify the geographic timezone where the system is deployed. Not all 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 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. Express Manager connected 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.
 - *Default Gateway* - Optionally specify the default gateway IP address used to communicate with the system's main router.
 - *DNS Server* - Optionally specify the IP Address or addresses of the Domain Name Servers used for the site.
- 3 Specify a **Floor** name and the **URL** of a floor map that displays the site layout. The **Floor Plan** is used to specify the placement of APs and help optimize the RF coverage of a site. To add a floor plan, select **Add Floor Plan** and upload an existing floor plan image.
 - 4 To configure **Static Routes** click the **+ Add** button and specify IP addresses and network masks in the **Network Address** column. Then provide the **Gateway** used to route traffic.
 - 5 Click **Apply** to save the basic system configuration settings.

LAN Configuration (Site)








Refer to the **LAN** screen to set specific Express Manager wired interface configurations. For most sites the default configuration should work fine. But, you can create VLAN interfaces here and assign IP address using DHCP. You can also configure a separate VLAN for guest access and enable NAT to the Internet.

To configure wired interface settings:


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





Configuration -> LAN EU-Green  



LAN Port Settings Number of Interfaces: 7

Port	Enable	Allowed VLAN (1-5,6,9)	Untagged VLAN (1-4094)	Edit
ge2	<input checked="" type="checkbox"/>		1	
ge1	<input checked="" type="checkbox"/>		1	
fe4	<input checked="" type="checkbox"/>		1	
fe2	<input checked="" type="checkbox"/>		1	
fe3	<input checked="" type="checkbox"/>		1	
fe1	<input checked="" type="checkbox"/>		1	
up1	<input checked="" type="checkbox"/>		1	

IP Settings Number of IP Interfaces: 3

 Go to Devices page to add interfaces with static IP addresses

+ Add 		Number of IP Interfaces: 3			
Interface	Description	NAT	DHCP Client	Edit	
VLAN* 2201		<input type="checkbox"/>	<input checked="" type="checkbox"/>		
VLAN2200		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
VLAN1		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		

 Apply  Discard

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

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

Port	Displays the physical interface (GE1, FE1, etc.) for each wired connection on the network. Supported models each have unique physical interface connections.
Enable	Select <i>Enable</i> to allow traffic on the selected wired interface. To disable wired traffic on a specific interface, uncheck the box.
Allowed VLAN	Displays the VLAN(s) traffic is allowed on as a virtual interface for each wired port.
Untagged VLAN	Displays the VLAN(s) untagged traffic will be 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:

Interface	Lists the virtual LAN name (VLAN) used to route traffic.
Description	Optionally provide a description for each VLAN interface.
DHCP	Select DHCP to configure IP Address and mask information using a DHCP Server. To manually configure the network address manually, 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.

Wireless Configuration (Site)

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 Express Manager 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 Express Manager. 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 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 **Wireless** screen to monitor WLAN utilization and assess whether WLAN usage is consistent with a Express Manager's connect Access Point's deployment objectives and the security needs of its connected clients.

To configure WLAN properties a Express Manager's connect Access Point's deployment objectives:

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

The **Wireless** screen is partitioned into **Radio Settings** and **Wireless LAN** fields.

- 2 Configure the following **Radio Settings** for the 2.4Ghz and 5Ghz radios on Express Manager connected Access Points:

Channel	Use the drop-down menu to select a channel for the 2.4Ghz or 5Ghz radio. Point. 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 Smart 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 used for the transmission of probe responses. Options are specific to each device model and radio type but may include, <i>default</i> , <i>11bgn</i> (802.11b/g/n), <i>11gn</i> (802.11g/n), <i>11n</i> (802.11n), <i>11an</i> (802.11a/n), <i>11anac</i> (802.11a/n/ac) and <i>11nac</i> (802.11n/ac).

- 3 In the **Wireless LAN** section specify the following information for each WLAN:

Name	Add or edit a name for the WLAN. This name is used throughout the WiNG Express 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 SSID. The WLAN SSID is case sensitive and alphanumeric. SSID length should not exceed 32 characters.
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.
Hide	Select this option to disable broadcast of the SSID used by this WLAN.
Client-To-Client Communications	Select this option to enable client to client communication 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.

Authentication Type	<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>, enter a WPA2 Key to password protect the WLAN. Define whether the key is entered in ASCII or HEX (hexadecimal string) characters. Selecting <i>Show</i> to expose the key is not recommended.</p> <p>If selecting <i>Secure-802.1x</i>, provide an IP address (or hostname) and a shared secret (password) used to access an external RADIUS server resource designated to validate user requests to WLAN resources.</p> <p>Selecting <i>Guest</i> displays fields for captive portal Web page creation.</p>
2.4 GHz	Displays a green check mark if the radio is enabled for WLAN utilization and client support and a red X if the radio is disabled.
5 GHz	Displays a green check mark if the radio is enabled and a red X if the radio is disabled. AP6511 and AP6521 models do not have a second radio.
Edit	Select <i>Edit</i> to change the settings of the selected WLAN.

4 In the **Advanced Smart RF** section specify the following information:

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.
Disable DFS	Select this to disable DFS scanning for RADAR.
Channel 2.4 GHz / 5 GHz	Use the drop-down menu to select channels available for use in Smart RF scanning. Add them to the list using the + and remove them using the trash can icon. Specify the channels for both 2.4 GHz and 5 GHz traffic if applicable.
Channel Width 2.4 GHz / 5 GHz	Use the drop-down menu to specify the channel width used in Smart RF scanning. Specify the channel width for both 2.4 GHz and 5 GHz traffic if applicable.
Client Aware Scanning 2.4 GHz / 5 GHz	Select this option to enable client aware scanning on the channel specified. Enable this option for both 2.4 GHz and 5 GHz traffic if applicable.
Voice Aware Scanning 2.4 GHz / 5 GHz	Select this option to enable voice aware scanning for voice traffic during scans. Enable this option for both 2.4 GHz and 5 GHz traffic if applicable.

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

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 >>](#)

Interface (1-4094)	Description	IP Address	Edit
VLAN1	WAN Interface	192.168.1.1/24	

Apply | Go Back

- 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 currently active firmware version 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 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. To override the default gateway address specify a new IP address.

- 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 on the Access Point. AP6511E and AP6521E Access Points are single radio version models. 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 AP6511E and AP6521E 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.

- 8 On supported devices select **Enable RADIUS Server** to enable the onboard RADIUS server. RADIUS settings can be configured on the RADIUS Screen.
- 9 Optionally, from the **IP Settings** section **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.
Description	Enter a description for each interface configured to distinguish it from other devices with similar attributes.
IP Address	Enter or edit the IP Address associated with each interface. To edit the IP Address click the edit icon next to the corresponding interface.

- 10 Optionally, from the **DNS Servers** section 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. To edit the IP Address click the edit icon next to the corresponding server entry.
-------------------	---

- 11 Optionally, from the **Route** section **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 the A.B.C.D/M format, used to communicate with the main router.

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

Editing Wireless Configuration (Site)

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 Express Manager 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 provided service to 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 **Wireless** screen to monitor WLAN utilization and whether WLAN usage is consistent with deployment objective and the security needs of its connected clients.

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

- 1 Select **Configuration** from the main menu then select **Wireless**.
- 2 Select a WLAN and click on its name to update its current configuration.
- 3 Configure the following settings for the WLAN:

Name	Add or edit a name for the WLAN. This name is used throughout the WiNG Express 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 SSID. The WLAN SSID is case sensitive and alphanumeric. The 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 to client communication 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 is also disabled on that WLAN, clients are not permitted to interoperate.

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 (hexidecimal string) characters. Selecting <i>Show</i> to expose the key is not recommended.</p> <p>If selecting <i>Secure-802.1x</i>, provide an IP address (or hostname) and a shared secret (password) used to access an external RADIUS server resource designated to validate user requests to the Access Point's WLAN resources.</p> <p>Selecting <i>Guest</i> displays fields for captive portal Web page creation.</p>
Band	<p>Select a band, <i>2.4Ghz or 5Ghz</i> (if supported), to enable operation of that band on the WLAN.</p>
VLAN	<p>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.</p>
Description	<p>Optionally, enter descriptive text which can be used by administrators to help identify each WLAN.</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 are:</p> <p><i>WEP-64 - Wired Equivalent Privacy (WEP)</i> is a security protocol specified in the IEEE <i>Wireless Fidelity (Wi-Fi)</i> 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><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 are used to 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>
--	--

Key (Secure-PSK only)	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.
RADIUS VLAN Assignment (Secure-802.1x and Guest only)	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.
Bypass Captive Portal Detection	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.
RADIUS (only Secure-802.1x)	Configure the RADIUS server to use for authentication. Select from <i>Local</i> - Select this option to use the onboard RADIUS server. <i>Controller</i> - Select this option to use the RADIUS server on the adopting controller. <i>External</i> - Select this option to configure details about 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 shared with the server.
Session Timeout (Guest Only)	Configure the session timeout value for Guest User access. This is the time duration after which the guest user is forced to re authenticate.
Only Internet Access	Select this option to prevent client devices from accessing resources on the VLAN. This option restricts the clients to locations on the internet only.
Use DHCP/NAT on APs	Select this option to use DHCP information as 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.
Bypass Captive Portal Detection	Select this option to enable Social Media Authentication to work on hand-held devices. Using social media, a requesting client's user credentials require authentication through social media credential exchange and validation.

Access Type	<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>
Lookup Information	<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>
RADIUS	<p>Use this field to provide the information required to access the RADIUS server used for authentication. Select <i>Controller</i> to configure the authentication server as the RADIUS server on the controller. Select <i>External</i> to configure an external RADIUS server for authentication.</p>
Registration Type	<p>Use the Registration Type drop-down menu to set the self-registration type for tis selected WLAN. Options include <i>Device</i>, <i>User</i> and <i>Device-OTP</i>.</p> <p>When captive portal guest users are authenticating using their User ID (Email Address/Mobile Number/ Member ID) and the received pass code in order to complete the registration process. The WLAN authentication type should be MAC-Authentication and the WLAN registration type should be configured 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>
Radius Group	<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>

Note: When using registration as the access type, E-mail and mobile are mandatory fields.

- 4 Use the **Web Pages** section to configure the HTML pages displayed to the guest user. Use the **Terms and Conditions** check box to enforce the user to accept the specified terms and conditions before accessing the captive portal.

When **Use Default Files** option is selected, the captive portal displays the default pages that are hosted on this device. When **Upload Files** is selected, the user can upload pages to the device and these files will be displayed to the captive portal user. When **External** is selected, provide the complete path to an external server that hosts the files that will be displayed to the captive portal user.

Use the tabs to configure the following fields for each page displayed to the captive portal user.

Organization's Name	Set any organizational specific name or identifier which clients see during login. The <i>Organization Name</i> setting is only available for the Login page.
Title Text	Set the title text displayed on the pages when wireless clients access captive portal pages. The text should be in the form of a page title describing the respective function of each page and should be unique to each function.
Header Text	Provide header text unique to the function of each page.
Login Message	Specify a message containing unique instructions or information for the users who access the Login, Terms and Condition, Welcome, Fail, No Service or Registration pages. In the case of the Terms and Agreement page, the message can be the conditions requiring agreement before captive portal access is permitted.
Footer Text	Provide a footer message displayed on the bottom of each page. The footer text should be any concluding message unique to each page before accessing the next page in the succession of captive portal Web pages.
Signature	Provide the copyright and legal signature associated with the usage of the captive portal and the usage of the organization name provided. The Signature setting is only available for the Login page.
Main Logo	Use the Main Logo to provide the URL for the main logo image displayed on the screens. Optionally select the Use as banner option to designate the selected main logo as the page's banner as well. The banner option is disabled by default.
Small Logo	Use the Small Logo field to provide the URL for a small logo image displayed on the screens.

Select **Redirect the user to externally hosted Success URL** field to redirect the captive portal user when the login is successful.

- 5 Select the **Reg Page Fields** tab to configure the look and feel of the Registration page.

When setting the properties of the Registration screen, refer to the table to define email, country, gender, mobile, zip, street and name filters used as additional authentication criteria. Guest users are redirected to the registration portal on association to the captive portal SSID. Users are displayed an internal (or) externally hosted registration page where the guest user must complete the registration process if not previously registered.

These fields are customizable to meet the needs of organizations providing guest access. The captive portal sends a message to the user (on the phone number or E-mail address provided at registration) containing an access code. The user inputs the access code and the captive portal verifies the code before returning the Welcome page and providing access. This allows the organization to verify the phone number or E-mail address is correct and can be traced back to a specific individual.

- 6 In the **WLAN Rate Limit** section configure the following settings:



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

- 7 Configure the following **Other Settings**:

Client Roam Assist	Select this option to enable client roam assist. By monitoring a client's packets and the <i>received signal strength indicator</i> (RSSI) of a given client by a group of Access Points, 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 this VLAN.




Security Firewall Configuration (Site)

When protecting wireless traffic to and from an Express Manager connected 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. Express Manager provides seamless data protection and user validation to protect and secure data at each vulnerable point in the network. Express Manager connected 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.

Configuration -> Security EU-Green  



Firewall Wireless IPS Certificate

WLAN ACL Rules

Search	Type to search	+	Add Rule	-	Delete Rule	Number of Rules: 3			
	Precedence	Enabled	Action	Source IP	Destination IP	Protocol	Direction	Interface	Edit
<input type="checkbox"/>	1	✓	✓	Any	Any	0(ip)	out	555	
<input type="checkbox"/>	2	✓	✓	Any	Any	0(ip)	out	555	
<input type="checkbox"/>	3	✓	✓	Any	Any	0(ip)	out	555	

Wireless Client Association ACL Rules

Search	Type to search	+	Add Rule	-	Delete Rule	Number of Rules: 0			
	Precedence	Action	Start MAC	End MAC	Interface	Edit			
No Data									

 Apply  Discard

A *firewall* is a mechanism enforcing network access control, and is considered a first line of defense in protecting proprietary information within the Express Manager 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 Express Manager connected 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 from first to last. When a rule matches the network traffic a Express Manager 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**.
The firewall screen is divided into **WLAN ACL Rules** and **Wireless Client Association ACL Rules** fields.
- 2 Set the following **WLAN ACL Rules**:

Precedence	Specify or modify a precedence for this IP policy between 1-5000. 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 stop a packet from reaching 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 requires 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 requires 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. 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.
Source Port	If using either <i>tcp</i> or <i>udp</i> as the protocol, define whether the source port for incoming ACL rule application is any, equals or an administrator defined range. If not using <i>tcp</i> or <i>udp</i> , this setting displays as N/A. This is the data local origination port designated by the administrator. Selecting equals invokes a spinner control for setting a single numeric port. Selecting range displays spinner controls for <i>Low</i> and <i>High</i> numeric range settings. A source port cannot be a destination port.
Destination Port	If using either <i>tcp</i> or <i>udp</i> as the protocol, define whether the destination port for outgoing IP ACL rule application is any, equals or an administrator defined range. If not using <i>tcp</i> or <i>udp</i> , this setting displays as N/A. This is the data destination port designated by the administrator. Selecting equals invokes a spinner control for setting a single numeric port. Selecting range displays spinner controls for <i>Low</i> and <i>High</i> numeric range settings.
Direction	Specify the direction for ACL rule to determine whether inbound or outbound traffic is filtered.
Interface	Specify the interface for the WLAN ACL rule to affect.

3 Set the following **Wireless Client Association ACL Rules**:

Precedence	Specify or modify a precedence for this IP policy between 1-5000. 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.
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 stop a packet from its destination. <i>Permit</i> - Instructs the firewall to allow a packet to proceed to its destination.
Source 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.
WLANs	Use the drop-down menu to specify the Express Manager WLAN configurations impacted by the ACL's rule configuration.

Security WIPS Configuration (Site)

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 the use of 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 lockdown.

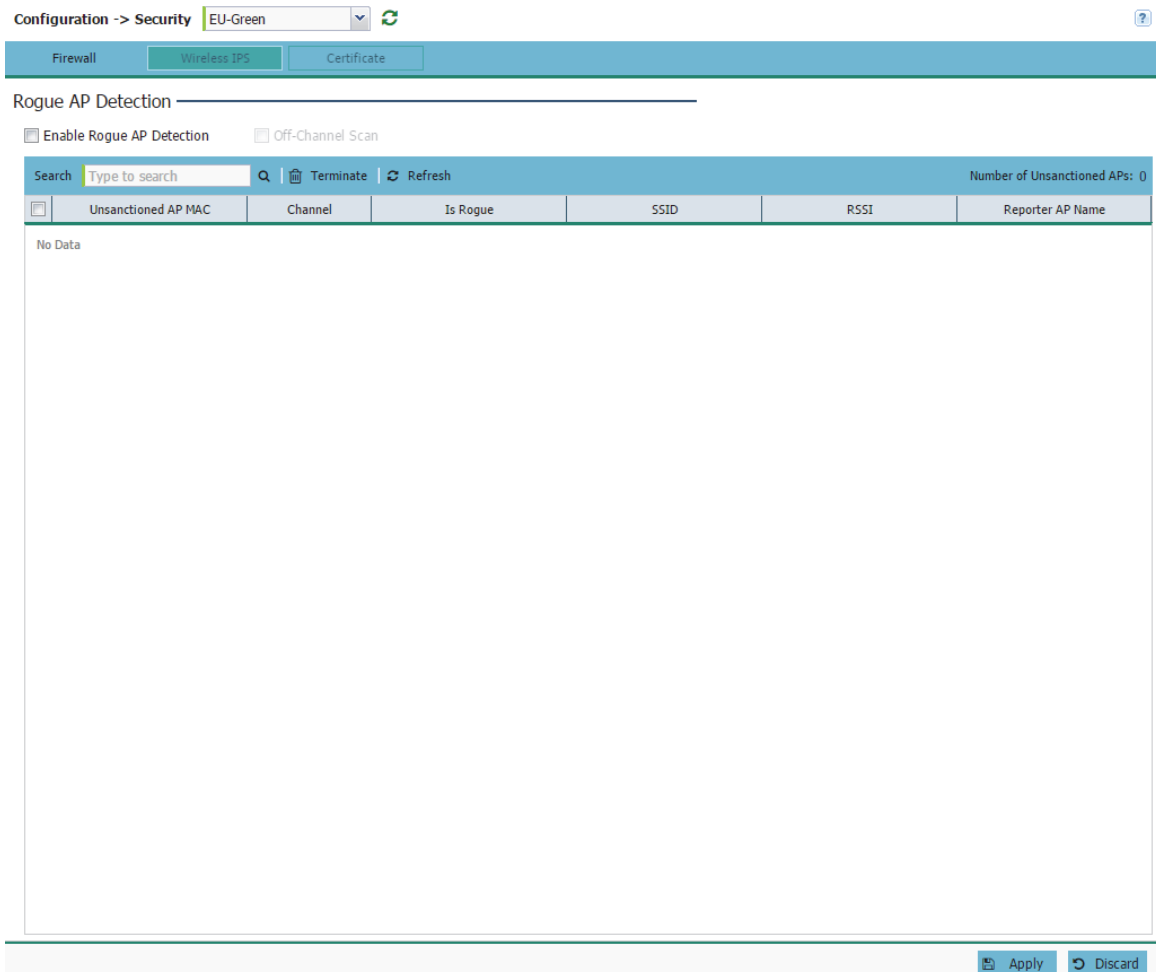
Unauthorized APs are untrusted Access Points connected to a LAN accepting client associations. They can be deployed for illegal wireless access to a corporate network, implanted with malicious intent by an attacker, or could just be misconfigured Access Points that do not adhere to corporate policies. 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 and its Express Manager) as a dedicated solution within a separate enclosure. When used within a Express Manager network and its associated Access Point radios, 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 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 WiNG Express managed Access Point:

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



- 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 your sure the radio can afford bandwidth be dedicated to the channel scan and does not negatively impact client support.
- 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 Express Manager 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 a device connection would improve network coverage or add noise.

Reporter AP Name	Displays the hardware encoded <i>Media Access Control (MAC)</i> address of the Access Point reporting the listed WIPS event.
-------------------------	--

DHCP Configuration (Site)

Dynamic Host Configuration Protocol (DHCP) allows hosts on an IP network to request and be assigned IP addresses and discover information about the network where they reside. Each subnet can be configured with its own address pool. Whenever a DHCP client requests an IP address, the DHCP server assigns an IP address from that subnet's address pool. When the onboard DHCP server allocates an address for a DHCP client, the client is assigned a lease, which expires after an predetermined interval. Before a lease expires, wireless clients (to which leases are assigned) are expected to renew them to continue to use the addresses. Once the lease expires, the client is no longer permitted to use the leased IP address. The DHCP server ensures all IP addresses are unique, and no IP address is assigned to a second client while the first client's assignment is valid (its lease has not yet expired). Therefore, IP address management is conducted by the internal DHCP server, not by an administrator.

To configure **Services**:

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

- 2 Select **Enable DHCP Server** to assign IP addresses to requesting wireless clients. Enabling DHCP allows the 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	Use the drop-down menu to select an interface for the DHCP server.
------------------	--

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)	If a lease time has been defined for a listed network pool, it displays in an interval in days. DHCP leases provide addresses for defined times to various clients. If a client does not use the leased address for the defined number of days, that IP address can be re-assigned to another requesting DHCP client.
Lease Time (hours)	If a lease time has been defined for a listed network pool, it displays in an interval in hours. DHCP leases provide addresses for defined times to various clients. If a client does not use the leased address for the defined number of hours, that IP address can be re-assigned to another requesting DHCP client.
Lease Time (minutes)	If a lease time has been defined for a listed network pool, it displays in an interval in minutes. DHCP leases provide addresses for defined times to various clients. If a client does not use the leased address for the defined number of minutes, that IP address can be re-assigned to another requesting DHCP client.

RADIUS Configuration (Site)



The RADIUS configuration allows the configuration of user groups with common user policies such as VLAN and access schedule and is mapped to WLAN for authentication. User names are created and associated with the user group. Names and associated users are stored in the controller, service platform or 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, left-hand side pane of the User interface displays the **RADIUS** option.






The **RADIUS Group** screen displays (by default).

Configuration -> Services System  


DHCP RADIUS


Enable Radius Server:

Group _____

+ Add		Delete									Number of Groups: 13
<input type="checkbox"/>	Group	VLAN	WLAN SSID	UP Rate-Limit	Down Rate-Limit	Start Time	End Time	Guest			
<input type="checkbox"/>	zzz	1	thenappan	Not Set	Not Set	00:00	23:59	<input checked="" type="checkbox"/>			
<input type="checkbox"/>	333	1	thenappan	Not Set	Not Set	00:00	23:59	<input checked="" type="checkbox"/>			
<input type="checkbox"/>	thenappan	1	thenappan	Not Set	Not Set	00:00	23:59	<input checked="" type="checkbox"/>			
<input type="checkbox"/>	2222	1	thenappan	Not Set	Not Set	00:00	23:59	<input checked="" type="checkbox"/>			
<input type="checkbox"/>	kar	1	kartikey	Not Set	Not Set	00:00	23:59	<input checked="" type="checkbox"/>			

Users _____

+ Add		Delete						Number of Users: 0
<input type="checkbox"/>	Users	Group List	Email	Start Time	End Time	Guest		
<input type="checkbox"/>	zebra	444	ss@yahoo.com		01:01	<input checked="" type="checkbox"/>		

 Apply  Discard

- 3 Select **Enable Radius Server** to activate the internal RADIUS server.
- 4 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 Express Manager network (once authenticated by the local RADIUS server).
WLAN SSID	Displays the <i>Service Set ID</i> (SSID) of the network to which the Access Point belongs.
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.

- 5 Review the following RADIUS schedule information and modify as needed:

Access by time	To enable 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 time users within each listed group can access local RADIUS resources.
End Time	When Access by Time is enabled, specify the time users within each listed group lose access to local RADIUS resources.
Access by Day of Week	To enable guest access to the RADIUS server by specific days of the week, select this option and select each of the days you wish to enable access.

- 6 When adding or editing a RADIUS user, verify and configure the following:

User ID	Displays the name or identifier assigned to each user when it was 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 drop-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 starting date and time when this RADIUS user will be activated.
Expiry Date / Expiry Time	Specify an end date and time when this RADIUS user will be deactivated.
Access Duration	Specify how long the RADIUS user will be active by selecting an access duration. To allow the use of the Expiry Date and Expiry Time fields select the Till Expiry option. Specify a duration in Days:Hours:Minutes format. The RADIUS user will be deactivated once the set duration has passed.

- 7 To add a new group click the **Add** button. To modify the settings of an existing group, select the group and click the **Edit** button. To delete an obsolete group, select the group and click the **Delete** button.

Device Configuration (Site)

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

Configuration -> Devices SITE-1 ↻ ?

Managed Devices Show Upgrade Number of Devices: 2

	Device Name	Device Status	IP Address	2.4 GHz		5 GHz		Firmware
				Channel	Power (dbm)	Channel	Power (dbm)	
<input type="checkbox"/>	ap7532-000003	↑ (online)	60.60.60.10	1(smt)	17(smt)	52w(smt)	4(smt)	5.7.0.0-0368
<input type="checkbox"/>	ap7532-805000	↑ (online)	60.60.60.9	1(smt)	17(smt)	36w(smt)	17(smt)	5.7.0.0-0368

↻ Refresh

- 2 The **Managed Devices** table displays the following information about devices managed at the site level:

Device Name	Displays the user specified device name for each configured device.
Device Status	Displays the online status of each device. If a device is online it shows two green arrows pointing up. If the device is offline it shows two red arrows pointing down.
IP Address	Displays the IPv4 IP Address associated with each configured device.
2.4 GHz Channel	Displays the 2.4 GHz radio channel that each configured device is using. If a device is not using a channel or status is unavailable, <i>N/A</i> appears instead of a channel number. If a device is using smart channel selection, <i>(smt)</i> displays after the channel number.
2.4 GHz Power	Displays the configured power level of the 2.4 GHz radio (in dbm) for each configured device. If a device is using smart channel selection, <i>(smt)</i> displays after the power level.
5 GHz Channel	Displays the 5 GHz radio channel that each configured device is using. If a device is not using a channel or status is unavailable, <i>N/A</i> appears instead of a channel number. If a device is using smart channel selection, <i>(smt)</i> displays after the channel number.
5 GHz Power	Displays the configured power level of the 5 GHz radio (in dbm) for each configured device. If a device is using smart channel selection, <i>(smt)</i> displays after the power level.

- 3 The **Tools** menu provides device specific actions that can be performed on one or more device selected from the **Managed Devices** table.



The following actions are available from the **Tools** drop-down menu:

Factory-Default	Selecting <i>Factory-Default</i> displays a prompt confirming you want to reset the selected device or devices to their factory defaults. Selecting Yes resets the selected device or devices to factory default settings and reboots the device. Choosing this option erases all information and settings stored on the device. Selecting No cancels the reset and return you to the Device screen.
Reboot	Selecting Reboot displays a prompt confirming you want to reboot the device. Selecting Yes reboots the device and the user interface is unavailable until the device has rebooted. You are required to log in to the user interface once the device has finished rebooting. Selecting No cancels the reboot and return you to the Devices screen.
Upgrade	Selecting <i>Upgrade</i> opens a dialogue window with firmware upgrade options. Firmware upgrades can be performed on a single selected device, or multiple selected devices of the same device model.
Tech-Support	Selecting <i>Tech-Support</i> 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 the path for the tech support server. Transfer of this information is supported via FTP, TFTP and HTTP protocols. The techsupport filename is auto generated by the device based on the device mac address, passing file name in path results in failure.
Packet Capture	Selecting <i>Packet Capture</i> allows you to capture client packet data based on the packet's address type or port on which received from each selected device or devices. Dropped client packets can also be trended to help assess network and client connectivity health.
IP Route	Selecting <i>IP Route</i> opens a window showing the current IP routes for the selected device or devices.
Export / Import Config	Selecting <i>Export / Import Config</i> displays a screen where configuration files can be imported to or exported from the selected device or devices. When <i>Local</i> is selected the current system configuration file is displayed as plain text in a window. To import a new configuration using this method, 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 and Local is selected, 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. To use this method select <i>Remote</i> and specify the Protocol, Port, Hostname or IP Address, Username, Password and the path for the remote server. Transfer of this information is supported via FTP, TFTP and HTTP protocols.
Locator ON	Selecting <i>Locator ON</i> flashes the LEDs of the selected device or devices to make them easier to find in large deployments.

Locator OFF	Selecting <i>Locator OFF</i> stops flashing the LEDs of the selected device or devices if they have been set to flash using the Locator ON option.
Delete Offline Device(s)	Selecting <i>Delete Offline Device(s)</i> removes any offline devices listed in the Managed Devices table from the network and from the Managed Devices table.

Editing Devices Configuration (Site)

- 1 Select **Configuration** from the main menu then select **Devices**.
- 2 Select the **Device Name** to edit the device configuration.

Edit -> ap7532-805DD0 [SITE-1]  

Basic Settings

Name: *

Location:

Version: 5.7.0.0-0368

Model: AP-7532E-67040-WR

Up Time: 4 days, 01 hours 41 minutes

MAC Address: FC-0A-81-80-5D-D0

Default Gateway:

Wireless Settings

2.4GHz Channel: Power: (dBm)

5GHz Channel: Power: (dBm)

Radius Server Settings


Enable Radius Server:



IP Settings

DNS Servers

Route

[Detail >>](#)

	Interface (1-4094)	Description	IP Address	NAT	Edit
<input type="checkbox"/>	VLAN60		60.60.60.9/24(DHCP)	✖	

 Apply  Go Back

- 3 The Managed Devices table displays the following information about devices managed at the site level:

Name	Enter a name for the device. This name is used throughout the Express Manager interface to refer to this device.
Location	Enter a location for the device. This can be a generic name, such as First Floor, or a specific latitude and longitude.
Version	Displays the software version number currently active on the device.
Model	Displays the device model number and SKU for the selected device.
Uptime	Displays the device uptime in a <i>Days, Hours and Minutes</i> format.
Default Gateway	Specify the IP address of this default gateway where all external network traffic is routed.

2.4 GHz Channel	Displays the 2.4 GHz radio channel each configured device is using. If a device is not using a channel or status is unavailable, <i>N/A</i> appears instead of a channel number. If a device is using smart channel selection, (<i>smt</i>) displays after the channel number.
2.4 GHz Power	Displays the configured power level of the 2.4 GHz radio (in dbm) for each configured device. If a device is using smart channel selection, (<i>smt</i>) displays after the power level.
2.4 GHz Antenna Gain	Set the 2.4 GHz antenna between 0.00 - 15.00 dBm. The Access Point's <i>Power Management Antenna Configuration File</i> (PMACF) automatically configures the Access Point's radio transmit power based on the antenna type, its antenna gain (provided here) and the deployed country's regulatory domain restrictions. Once provided, the Access Point calculates the power range. Antenna gain relates the intensity of an antenna in a given direction to the intensity that would be produced ideally by an antenna that radiates equally in all directions (isotropically), and has no losses. Although the gain of an antenna is directly related to its directivity, its gain is a measure that takes into account the efficiency of the antenna as well as its directional capabilities. Only a professional installer should set the antenna gain. The default value is 0.00.
5 GHz Channel	Displays the 5 GHz radio channel each configured device is using. If a device is not using a channel or status is unavailable, <i>N/A</i> appears instead of a channel number. If a device is using smart channel selection, (<i>smt</i>) displays after the channel number.
5 GHz Power	Displays the configured power level of the 5 GHz radio (in dbm) for each configured device. If a device is using smart channel selection, (<i>smt</i>) displays after the power level.
5 GHz Antenna Gain	Set the 5 GHz antenna between 0.00 - 15.00 dBm. The Access Point's <i>Power Management Antenna Configuration File</i> (PMACF) automatically configures the Access Point's radio transmit power based on the antenna type, its antenna gain (provided here) and the deployed country's regulatory domain restrictions. Once provided, the Access Point calculates the power range. Antenna gain relates the intensity of an antenna in a given direction to the intensity that would be produced ideally by an antenna that radiates equally in all directions (isotropically), and has no losses. Although the gain of an antenna is directly related to its directivity, its gain is a measure that takes into account the efficiency of the antenna as well as its directional capabilities. Only a professional installer should set the antenna gain. The default value is 0.00.
Enable RADIUS Server	Select this option to enable the onboard RADIUS server. RADIUS settings can be configured on the RADIUS screen.

TROUBLESHOOT

In This Chapter

Event History	123
Tools.....	124

Event History

The **Event History** screen displays historical events for Express Manager connected devices. The event history allows you to check for issues at various severity levels at each site or system. Events can be filtered by using criteria in the search field.

To review the Express Manager event history:

- 1 Select **Troubleshoot** from the main menu.
- 2 Select **Event History**.

Troubleshoot -> Event History

Events

Search	Type to search	Q	Clear All	Refresh	Stop	Severity	All	Number of Events: 180
Timestamp	Module	Message	Severity	Source	Site	Hostname		
Sat Nov 08 05:24:45 2014	SYSTEM	UI user 'admin' from: '60.60.60.3' authentication successful	notice	00-0C-29-48-78-56	default	vx9000-487856		
Sat Nov 08 09:51:08 2014	NSM	Interface vlan40 acquired IP address 40.40.40.5/24 via DHCP	info	5C-0E-8B-08-75-EE	SITE-5	ap6521-0875EE		
Sat Nov 08 09:50:43 2014	NSM	Interface vlan40 acquired IP address 40.40.40.4/24 via DHCP	info	FC-0A-81-12-C9-CD	SITE-5	ap6521-12C9CD		
Sat Nov 08 09:48:05 2014	NSM	Interface vlan20 acquired IP address 20.20.20.7/24 via DHCP	info	B4-C7-99-44-2C-F0	SITE-2	ap6522-442CF0		
Sat Nov 08 09:48:05 2014	NSM	Interface vlan30 acquired IP address 30.30.30.4/24 via DHCP	info	B4-C7-99-57-F0-C8	SITE-3	ap6562-57F0C8		
Sat Nov 08 09:48:01 2014	NSM	Interface vlan30 acquired IP address 30.30.30.5/24 via DHCP	info	B4-C7-99-49-12-F4	SITE-4	ap6562-4912F4		
Sat Nov 08 09:47:59 2014	NSM	Interface vlan20 acquired IP address 20.20.20.9/24 via DHCP	info	B4-C7-99-49-13-94	SITE-2	ap6522-491394		
Sat Nov 08 09:46:26 2014	NSM	Interface vlan60 acquired IP address 60.60.60.9/24 via DHCP	info	FC-0A-81-80-5D-D0	SITE-1	ap7532-805DD0		
Sat Nov 08 09:46:16 2014	NSM	Interface vlan60 acquired IP address 60.60.60.10/24 via DHCP	info	00-23-68-00-00-03	SITE-1	ap7532-000003		
Sat Nov 08 01:36:43 2014	DIAG	LED state message AP_LEDS_OFF from module DOT11	info	00-0C-29-48-78-56	default	vx9000-487856		
Sat Nov 08 06:35:00 2014	DIAG	LED state message AP_LEDS_OFF from module DOT11	info	00-0C-29-96-C2-78	default	vx9000-96C278		
Sat Nov 08 06:16:03 2014	DOT11	Client '00-27-10-24-74-7C' disassociated from wlan 'Moto' radio 'ap6522-442CF0:R2': inactivity timer expired (reason code:4)	info	B4-C7-99-44-2C-F0	SITE-2	ap6522-442CF0		
Sat Nov 08 06:13:42 2014	SMRT	Radio ap6522-491394:R2 power changed from 16 to 17 on AP B4-C7-99-49-13-94	notice	B4-C7-99-44-2C-F0	SITE-2	ap6522-442CF0		
Sat Nov 08 06:12:44 2014	SMRT	Radio ap6522-5D6780:R2 power changed from 16 to 17 on AP B4-C7-99-5D-67-80	notice	B4-C7-99-44-2C-F0	SITE-2	ap6522-5D6780		

- 3 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 WiNG Express Manager connected Access Point.
Severity	<p>Displays the severity of the event as defined for tracking from the Configuration screen. Severity options include:</p> <p><i>All Severities</i> – All events are displayed irrespective of their severity</p> <p><i>Critical</i> – Only critical events are displayed</p> <p><i>Error</i> – Only errors and above are displayed</p> <p><i>Warning</i> – Only warnings and above are displayed</p> <p><i>Informational</i> – Only informational and above events are displayed</p>
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.



- 4 Use the **Search** field as necessary to refine event history to specific criteria.

Tools

The **Tools** screen contains network troubleshooting tools for Express Manager connected devices. Tools allow you to ping or traceroute the path to other devices on the Express Manager network.

- 1 Select **Troubleshoot** from the main menu.

2 Select Tools.

Troubleshoot -> Tools System  

Trace Route

Select a device: ap7532-805000 10.10.10.9

Trace Results

```
traceroute to 10.10.10.9 (10.10.10.9), 30 hops max, 38 byte packets
1 60.60.60.1 (60.60.60.1) 2.501 ms 0.774 ms 0.700 ms
2 10.10.10.9 (10.10.10.9) 0.434 ms 0.298 ms 0.374 ms
```

- 3 Select **System** or a specific site from the drop-down menu.
- 4 Select a connected device from the drop-down menu and enter a corresponding IP address or hostname to **Ping** or **Trace Route** from the selected device to the specified IP.

The Ping and Trace Route results display in the window below. If a destination is unreachable this could indicate network problems or the target device being down.

CUSTOMER-SUPPORT

Support Center

If you have a problem with your equipment, contact support for your region. Support and issue resolution is provided for products under warranty or that are covered by a services agreement. Contact information and Web self-service is available by visiting www.zebra.com/support

When contacting support, please provide the following information:

- ◆ Serial number of the unit
- ◆ Model number or product name
- ◆ Software type and version number

Support responds to calls by email or telephone within the time limits set forth in support agreements. If you purchased your product from a business partner, contact that business partner for support.

Customer Support Web Site

The Support Web site, located at www.zebra.com/support provides information and online assistance including developer tools, software downloads, product manuals, support contact information and online repair requests.

Manuals

www.zebra.com/support



Zebra Technologies Corporation
Lincolnshire, IL 60069 USA

Zebra and the Zebra head graphic are registered trademarks of ZIH Corp. The Symbol logo is a registered trademark of Symbol Technologies, Inc. a Zebra Technologies company.

© 2015 Symbol Technologies, Inc.

MN-002678-01 December 2015