WiNG Express Manager Version 5.7

USER GUIDE

Contents

Dashboard 5

System Dashboard 6
Site Dashboard 7
Heat Map 8

Monitor 9

Monitor AP Radios (System) 9
Radio Details (System) 11
Monitor AP Radios (Site) 12
Radio Details (Site) 14
Monitor WLANs (System) 15
WLAN Details (System) 19
Monitor WLANs (Site) 20
WLAN Details (Site) 23
Monitor Clients (System) 24
Clients Details (System) 25
Monitor Clients (Site) 27
Clients Details (Site) 28

Configuration 31

Configuration (System) 31
Basic Configuration (System) 31
Sites Details (System) 37
Sites Auto Provisioning (System) 38
LAN Configuration (System) 40
Wireless Configuration (System) 42
Security Firewall Configuration (System) 49
Security Certificate Configuration (System) 53
RADIUS Configuration (System) 55
Management Configuration (System) 58
Device Configuration (System) 61
Configuration (Site) 64
Basic Configuration (Site) 64
LAN Configuration (Site) 65
Wireless Configuration (Site) 67
Security Firewall Configuration (Site) 74
Security WIPS Configuration (Site) 77
DHCP Configuration (Site) 79
RADIUS Configuration (Site) 80
Device Configuration (Site) 83

Troubleshoot 87

Event History 87
Tools 89

Support Center 90

Customer Support Web Site 90
Manuals 90

Chapter 1
Dashboard

WiNG Express Manager is offered in both hardware and virtual appliance models to meet your deployment needs. If you have less than 26 access points in a single site, WiNG Express provides you the power of centralized management without the need to purchase and manage a controller. The result is a new level of simplicity and a new low cost-point for Enterprise-class wireless networking.

This controllerless management allows one of your Access Points to simply manage an entire network of up to 25 Access Points. If your 25 Access Points are spread out in multiple locations, or your business requires more than 25 Access Points in one or more locations, WiNG Express Manager can easily manage up to 1,024 Access Points in all of your sites.

In This Chapter

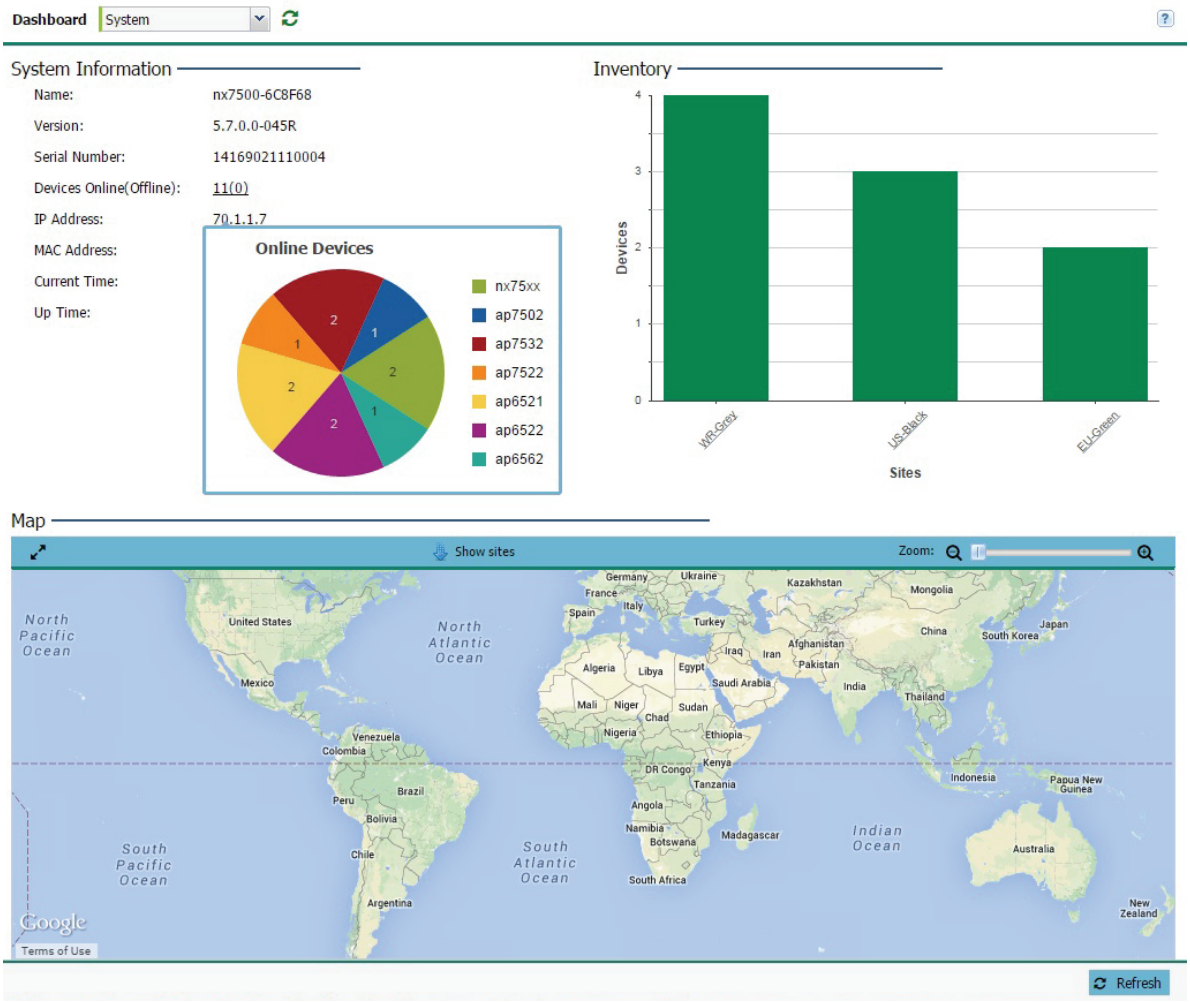
System Dashboard 6
Site Dashboard 7

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 dashboard information:

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



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

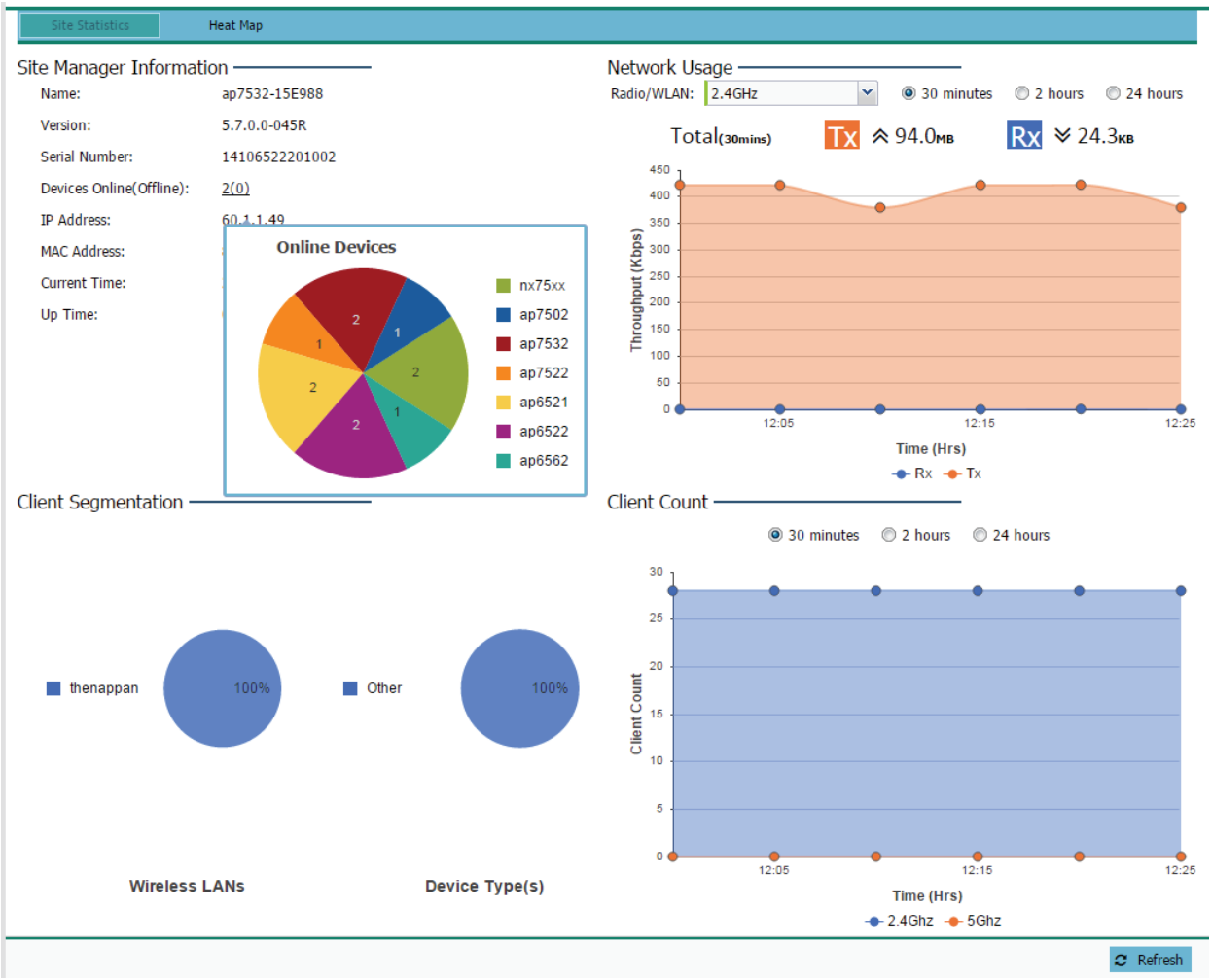
System Information	Displays the administrator assigned device *Name, Version, Serial Number*, the number of Online and Offline devices, the designated *IP* and *Device MAC* addresses, *Current Time* and *Up Time* listing when the Express Manager was last offline.
Inventory	Displays a graph showing device utilization amongst devices on the managed network. Use this information to help assess the device load of APs currently being deployed with 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:

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

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

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

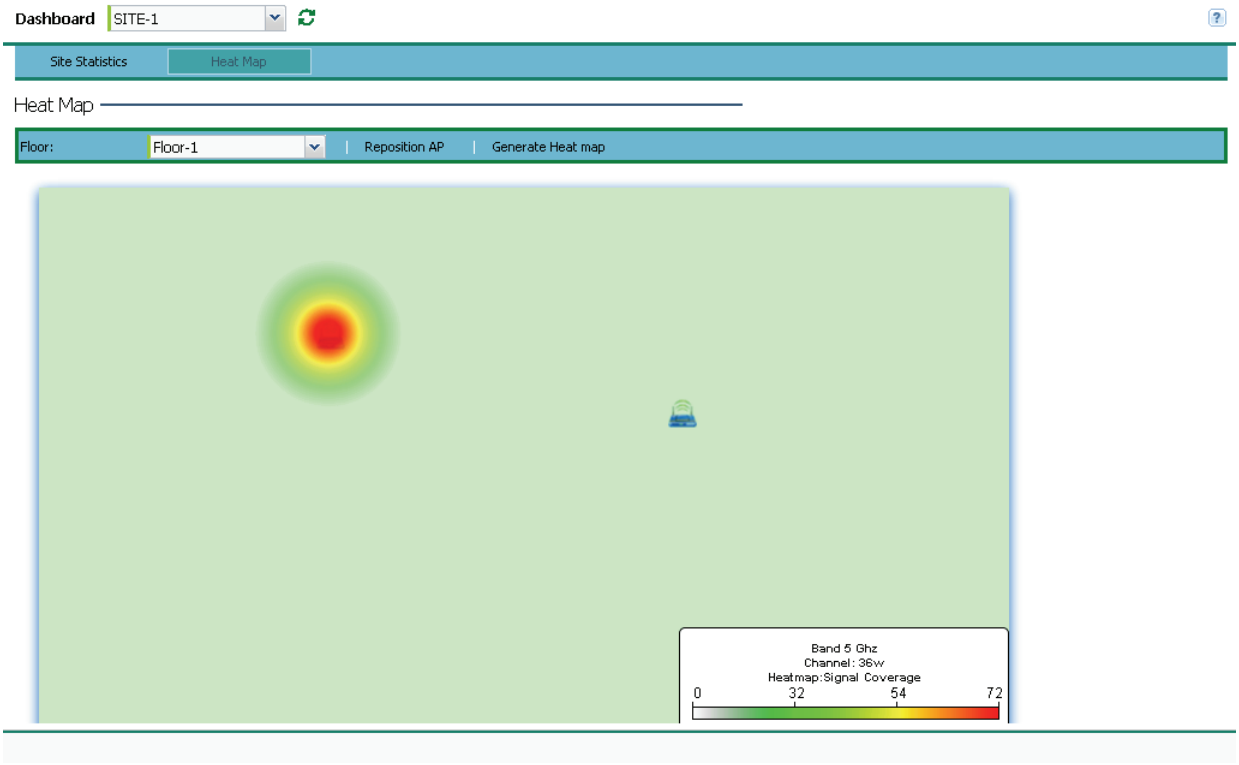
Heat Map

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 showing the signal coverage corresponding to the key in the bottom right of the screen.

Chapter 2
Monitor

This ongoing system and site level log tracks and maintains a complete WLAN event history, providing valuable trending information as well as details you need to address a specific incident and prevent a re-occurrence. You can inspect aggregated analytics at the system level, or drill-down to site-specific details for more granularity.

In This Chapter

Monitor AP Radios (System) 9
Monitor AP Radios (Site) 12
Monitor WLANs (System) 15
Monitor WLANs (Site) 20
Monitor Clients (System) 24
Monitor Clients (Site) 27

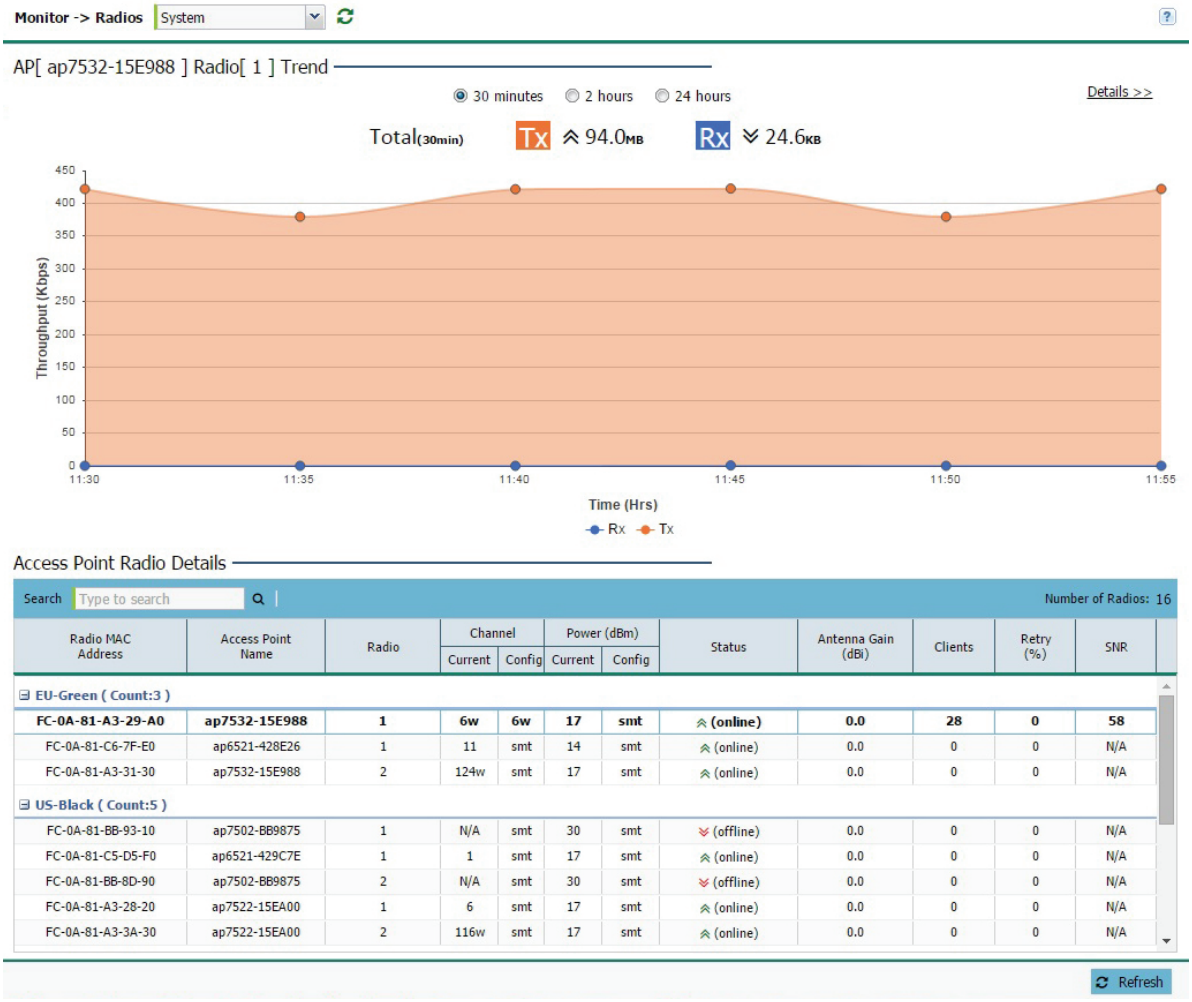
Monitor AP Radios (System)

Use the **Radios** screen to assess the quality of 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 select **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.



Radio MAC Address	Access Point Name	Radio	Channel		Power (dBm)		Status	Antenna Gain (dBi)	Clients	Retry (%)	SNR
			Current	Config	Current	Config					
EU-Green (Count:3)											
FC-0A-81-A3-29-A0	ap7532-15E988	1	6w	6w	17	smt	(online)	0.0	28	0	58
FC-0A-81-C6-7F-E0	ap6521-428E26	1	11	smt	14	smt	(online)	0.0	0	0	N/A
FC-0A-81-A3-31-30	ap7532-15E988	2	124w	smt	17	smt	(online)	0.0	0	0	N/A
US-Black (Count:5)											
FC-0A-81-BB-93-10	ap7502-BB9875	1	N/A	smt	30	smt	(offline)	0.0	0	0	N/A
FC-0A-81-C5-D5-F0	ap6521-429C7E	1	1	smt	17	smt	(online)	0.0	0	0	N/A
FC-0A-81-BB-8D-90	ap7502-BB9875	2	N/A	smt	30	smt	(offline)	0.0	0	0	N/A
FC-0A-81-A3-28-20	ap7522-15EA00	1	6	smt	17	smt	(online)	0.0	0	0	N/A
FC-0A-81-A3-3A-30	ap7522-15EA00	2	116w	smt	17	smt	(online)	0.0	0	0	N/A

3 Review the following **Access Point Radio Details**:

Radio MAC Address	Displays the *Media Access Control* (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 set to transmit and receive on, as well as its configured channel number. 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 **Smart** 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 in the WiNG Express Manager network. AP6511 and AP6521 single radio Access Points support 128 clients,other models support 128 clients per radio up to a total of 256 client connections.
Retry (%)	Displays the retry percentage for packets sent on each Access Point radio. The retry rate helps assess the overall effectiveness of the RF environment (as displayed as a percentage) and a function of the connection rate in both directions.
SNR	Displays the connected client's *signal to noise ratio* (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 assess details 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 a 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 period of time.

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

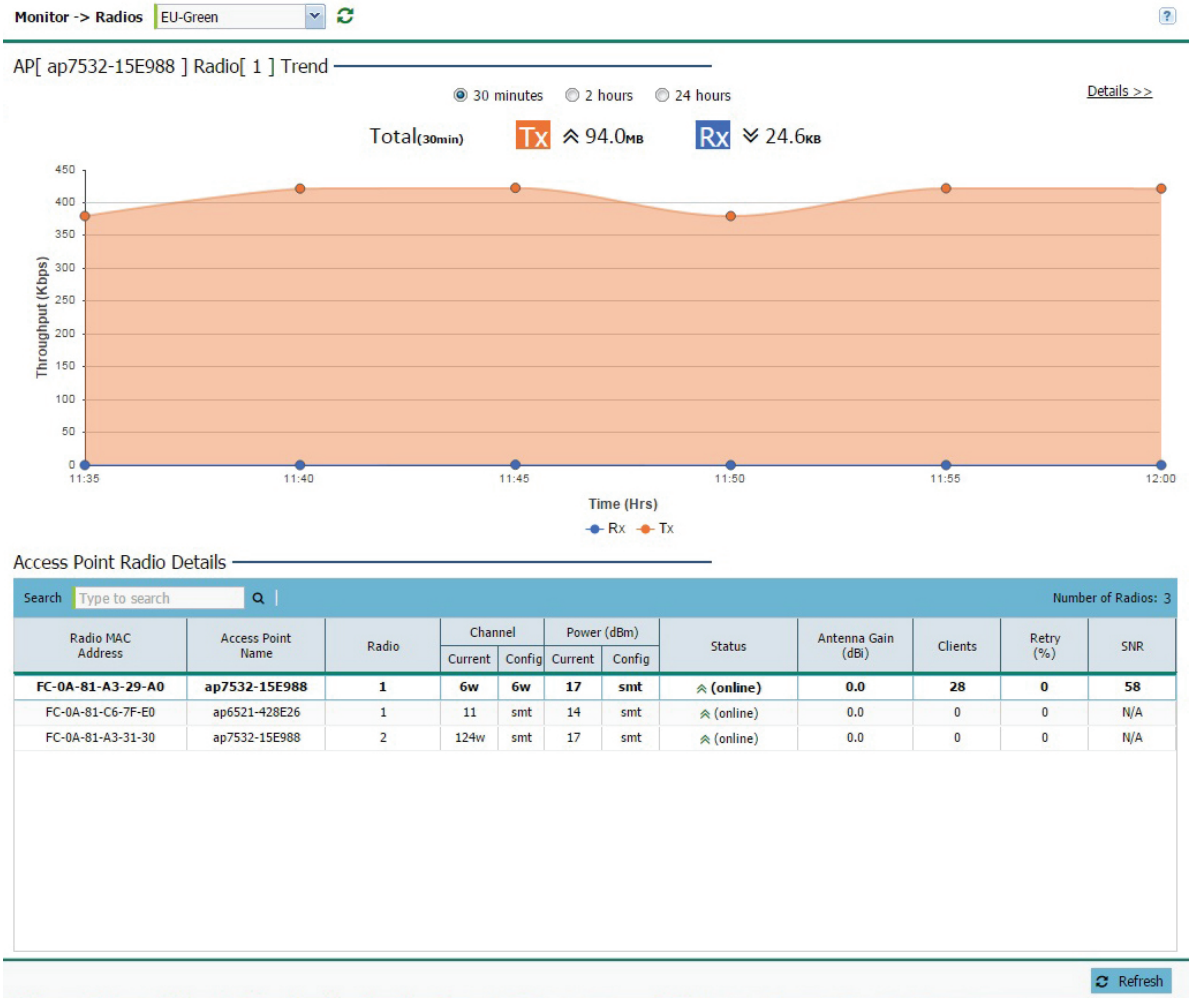
Monitor AP Radios (Site)

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**.

2 Select a data 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.



Radio MAC Address	Access Point Name	Radio	Channel		Power (dBm)		Status	Antenna Gain (dBi)	Clients	Retry (%)	SNR
			Current	Config	Current	Config					
FC-0A-81-A3-29-A0	**ap7532-15E988**	**1**	**6w**	**6w**	**17**	**smt**	**(online)**	**0.0**	**28**	**0**	**58**
FC-0A-81-C6-7F-E0	ap6521-428E26	1	11	smt	14	smt	(online)	0.0	0	0	N/A
FC-0A-81-A3-31-30	ap7532-15E988	2	124w	smt	17	smt	(online)	0.0	0	0	N/A

3 Review the following **Access Point Radio Details**:

Radio MAC Address	Displays the *Media Access Control* (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 is set to transmit and receive on, as well as its configured channel number. 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 **Smart** 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 on the network. AP6511 and AP6521 single radio Access Points support 128 clients, the remaining models support up to 256 client connections.
Retry (%)	Displays the retry percentage for packets sent on each Access Point radio. The retry rate helps assess the overall effectiveness of the RF environment (as displayed as a percentage) and a function of the connection rate in both directions.
SNR	Displays the connected client's *signal to noise ratio* (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)

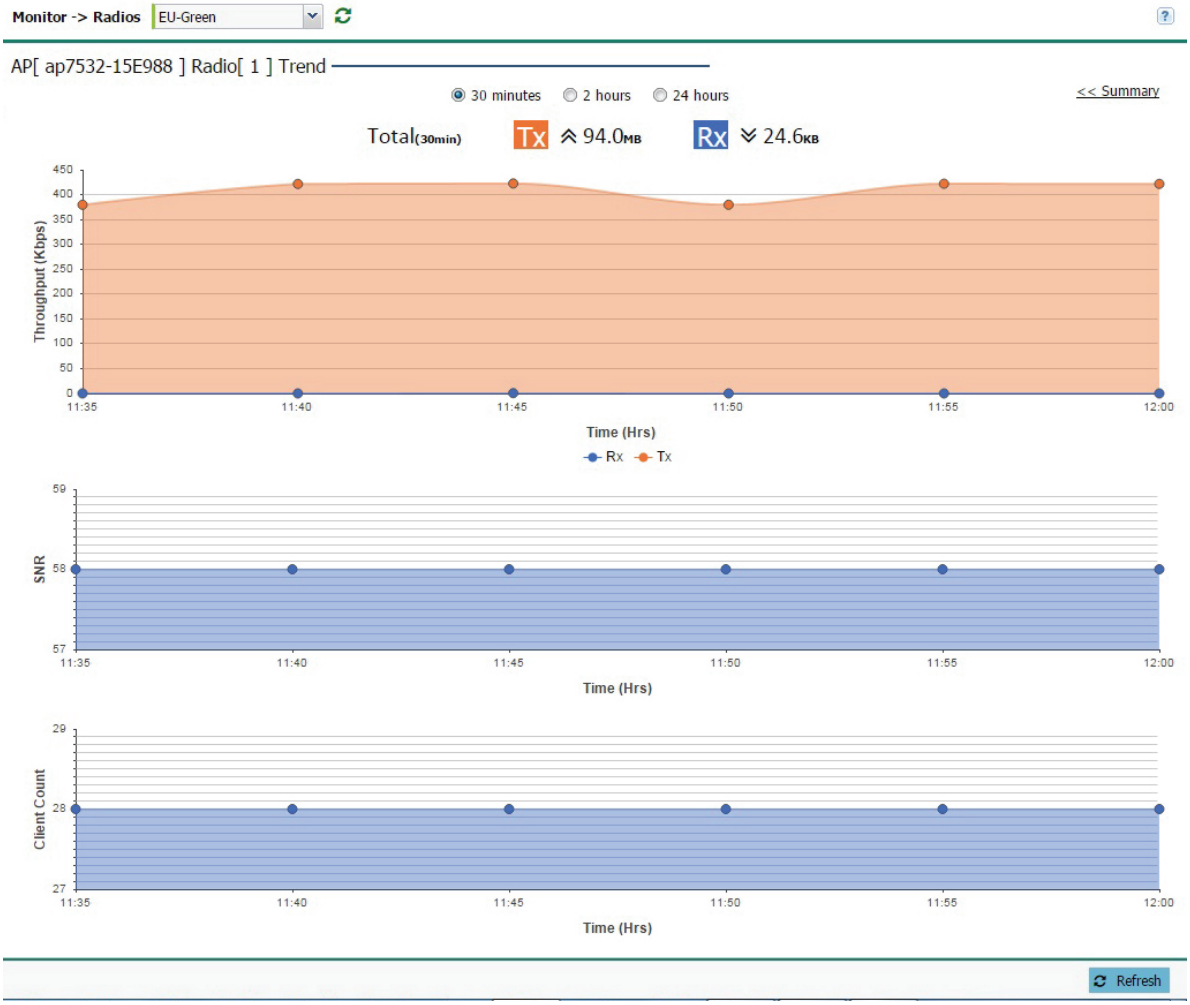
Use the **Radio Details** screen to assess details about the quality of the WiNG Express Manager connected radio utilization, power consumption, and client connections.

To monitor WiNG Express Manager connected Access Point radios:

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

2 Select 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 period of time.

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

Monitor WLANs (System)

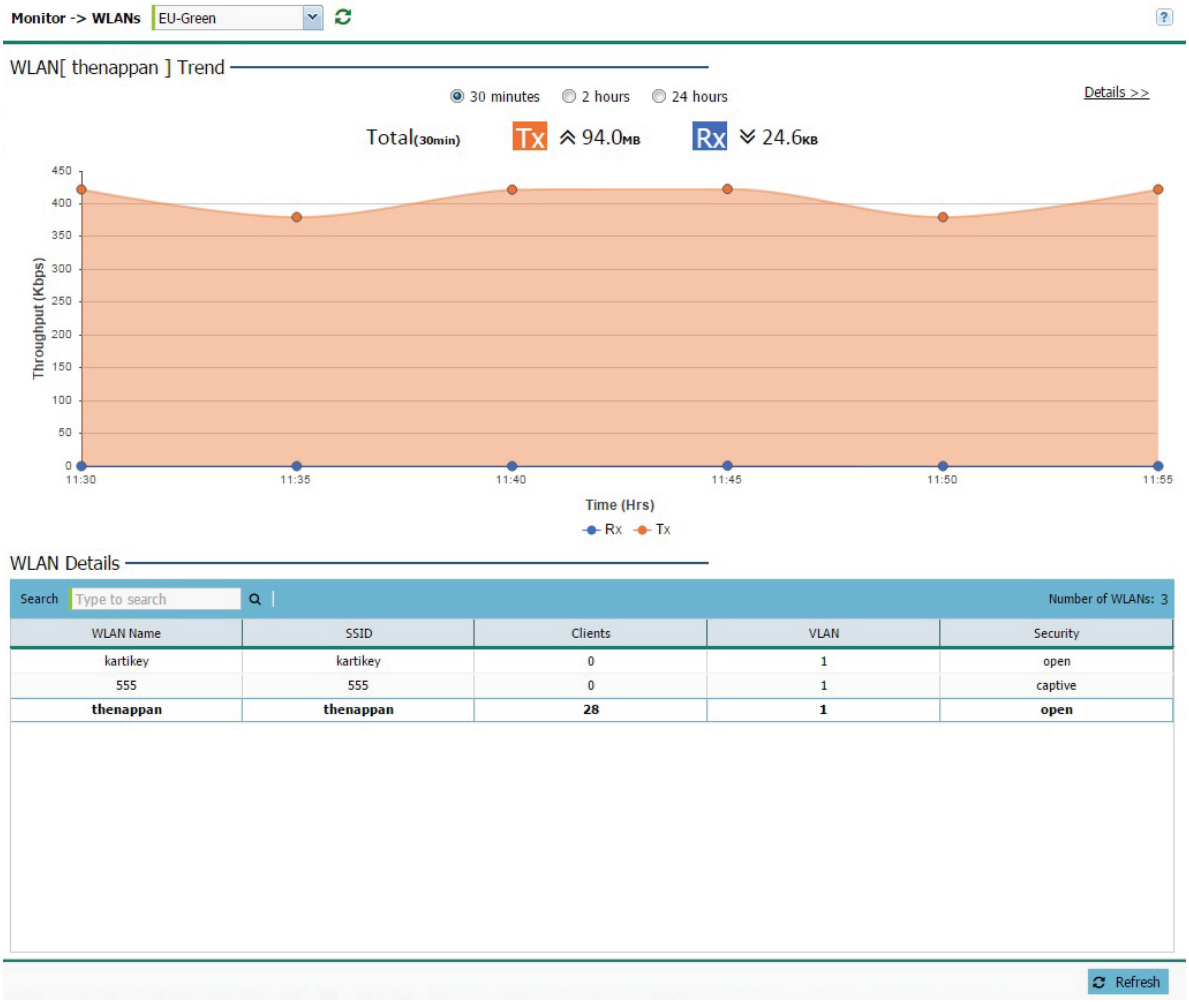
A WLAN can be advertised from a single Access Point radio or can span multiple Access Points and radios. WLAN configurations can be defined to only support to specific areas of a site. For example, a guest access WLAN may only be mapped to a 2.4GHz radio in a lobby or conference room providing limited 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**.

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 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 *Services Set Identification* (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	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. The screen displays with the Open option selected. Naming and saving such a policy (as is) would provide no security and might only make sense in a network wherein no sensitive data is either transmitted or received. This default setting is not recommended. If selecting Secure-PSK, select an encryption type for the WLAN. Define whether the key is entered in ASCII or HEX characters. Selecting Show to expose the key is not recommended. If selecting Secure-802.1x, 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. Selecting Guest displays fields for captive portal Web page creation, and is beyond the scope of this basic WiNG Express Access Point configuration.

Encryption (Secure-PSK only)	When Secure-PSK security is selected, use the drop-down menu to select an encryption type. Available encryption types are: *WEP-64* - Wired Equivalent Privacy (WEP) is a security protocol specified in the IEEE Wireless Fidelity (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 initialization vector (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. *WEP-128* - Wired Equivalent Privacy (WEP) is a security protocol specified in the IEEE Wireless Fidelity (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 128 uses a 104 bit key which is concatenated with a 24-bit initialization vector (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. *TKIP-CCMP* - CCMP is a security standard used by the Advanced Encryption Standard (AES). AES serves the same function TKIP does for WPA-TKIP. CCMP computes a Message Integrity Check (MIC) using the proven Cipher Block Chaining (CBC) technique. Changing just one bit in a message produces a totally different result. The encryption method is Temporal Key Integrity Protocol (TKIP). 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. *WPA2-CCMP* - WPA2 is a 802.11i standard that provides even stronger wireless security than Wi-Fi Protected Access (WPA) and WEP. CCMP is the security standard used by the Advanced Encryption Standard (AES). AES serves the same function TKIP does for WPA-TKIP. CCMP computes a Message Integrity Check (MIC) using the proven Cipher Block Chaining (CBC) technique. Changing just one bit in a message produces a totally different result. WPA2/CCMP is based on the concept of a Robust Security Network (RSN), 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.

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 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.

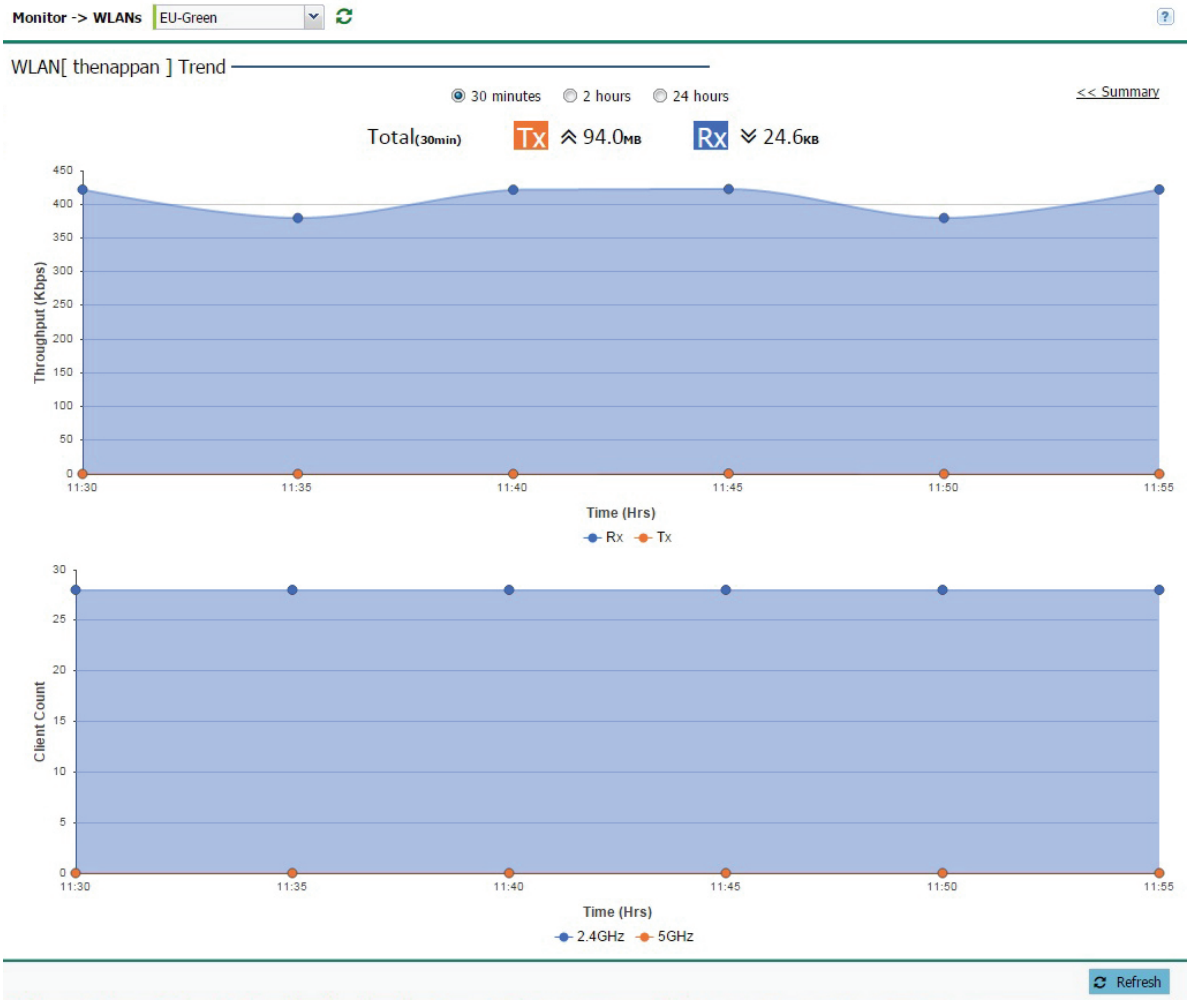
Periodically refer to the WLANs screen to monitor an Access Point's WLAN utilization and whether WLAN usage is consistent with an Access Point's deployment objective and the security needs of its connected clients.

To review WiNG Express Manager Access Point utilization:

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

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)

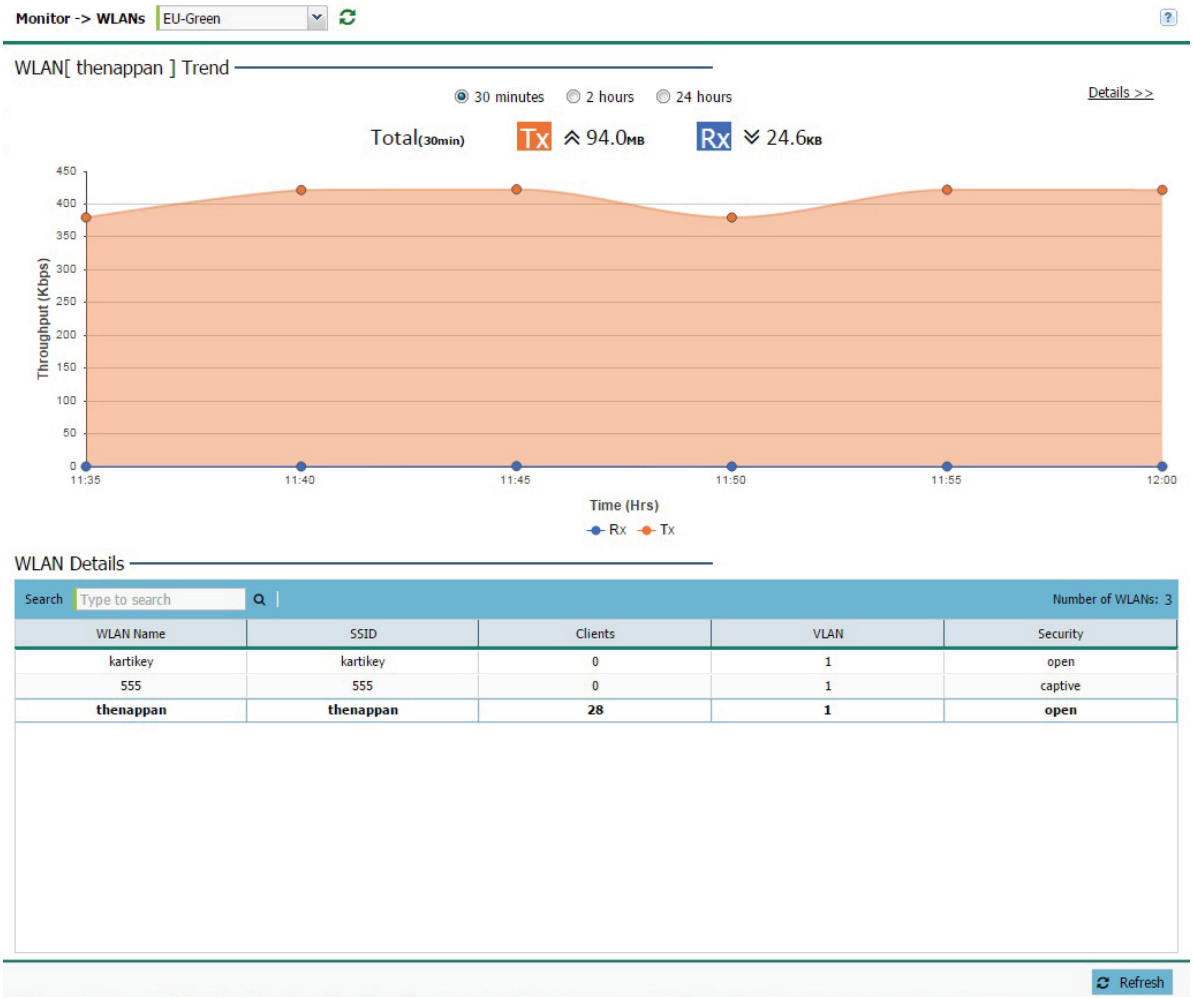
A WLAN can be advertised from a single Access Point radio or can span multiple Access Points and radios. WLAN configurations can be defined to only provide to specific areas of a site. For example, a guest access WLAN may only be mapped to a 2.4GHz radio in a lobby or conference room providing limited 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 WiNG Express Manager 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 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 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 *Services Set Identification* (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	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. The screen displays with the Open option selected. Naming and saving such a policy (as is) would provide no security and might only make sense in a network wherein no sensitive data is either transmitted or received. This default setting is not recommended. If selecting Secure-PSK, select an encryption type for the WLAN. Define whether the key is entered in ASCII or HEX characters. Selecting Show to expose the key is not recommended. If selecting Secure-802.1x, 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. Selecting Guest displays fields for captive portal Web page creation, and is beyond the scope of this basic WiNG Express Access Point configuration.

Encryption (Secure-PSK only)	When Secure-PSK security is selected, use the drop-down menu to select an encryption type. Available encryption types are: *WEP-64* - Wired Equivalent Privacy (WEP) is a security protocol specified in the IEEE Wireless Fidelity (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 initialization vector (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. *WEP-128* - Wired Equivalent Privacy (WEP) is a security protocol specified in the IEEE Wireless Fidelity (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 128 uses a 104 bit key which is concatenated with a 24-bit initialization vector (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. *TKIP-CCMP* - CCMP is a security standard used by the Advanced Encryption Standard (AES). AES serves the same function TKIP does for WPA-TKIP. CCMP computes a Message Integrity Check (MIC) using the proven Cipher Block Chaining (CBC) technique. Changing just one bit in a message produces a totally different result. The encryption method is Temporal Key Integrity Protocol (TKIP). 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. *WPA2-CCMP* - WPA2 is a 802.11i standard that provides even stronger wireless security than Wi-Fi Protected Access (WPA) and WEP. CCMP is the security standard used by the Advanced Encryption Standard (AES). AES serves the same function TKIP does for WPA-TKIP. CCMP computes a Message Integrity Check (MIC) using the proven Cipher Block Chaining (CBC) technique. Changing just one bit in a message produces a totally different result. WPA2/CCMP is based on the concept of a Robust Security Network (RSN), 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.

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 and radios. 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.

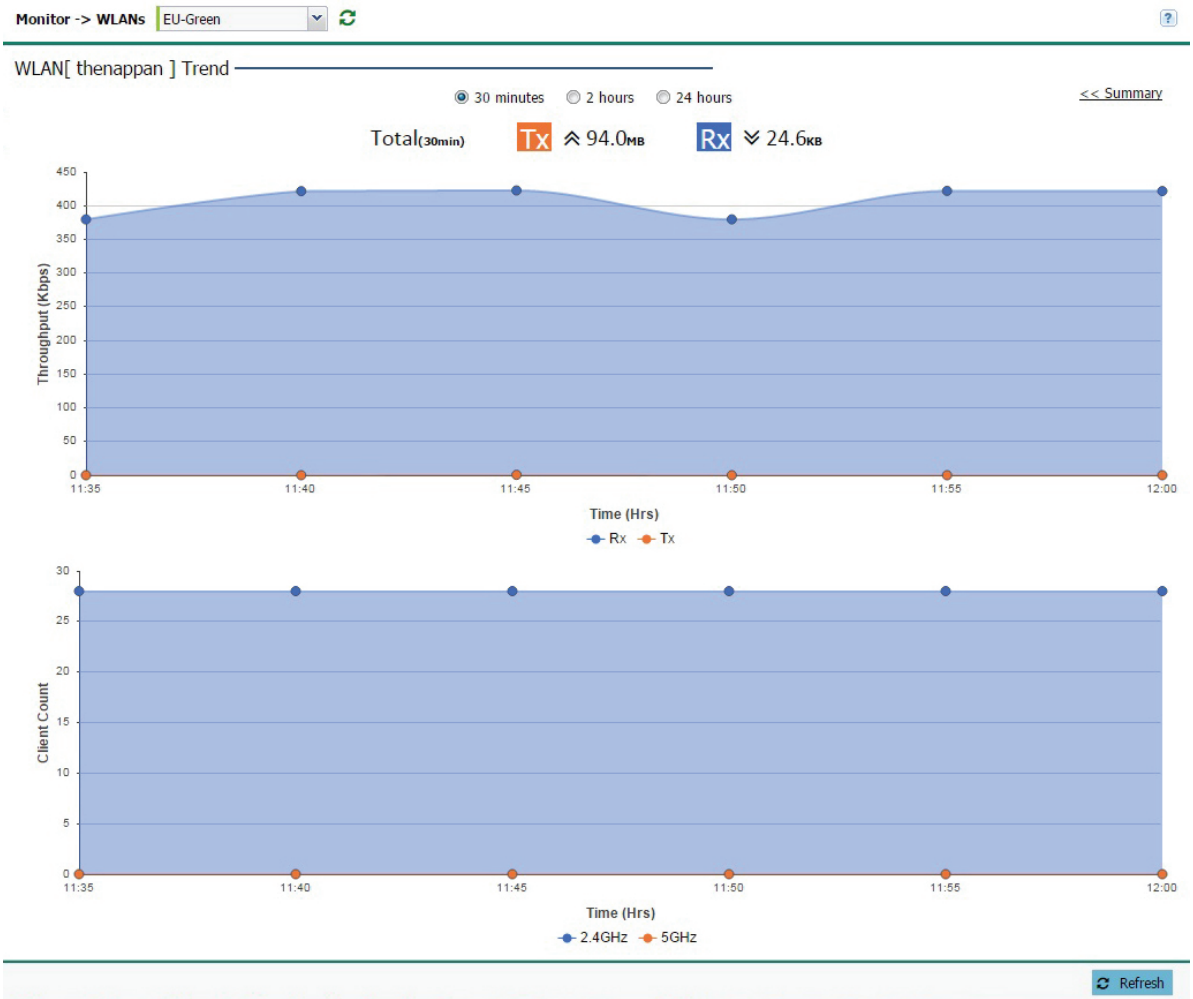
Periodically refer to the WLANs screen to monitor an Access Point's WLAN utilization and whether WLAN usage is consistent with an Access Point's deployment objective and the security needs of its connected clients.

To review WiNG Express Manager Access Point utilization:

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

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.

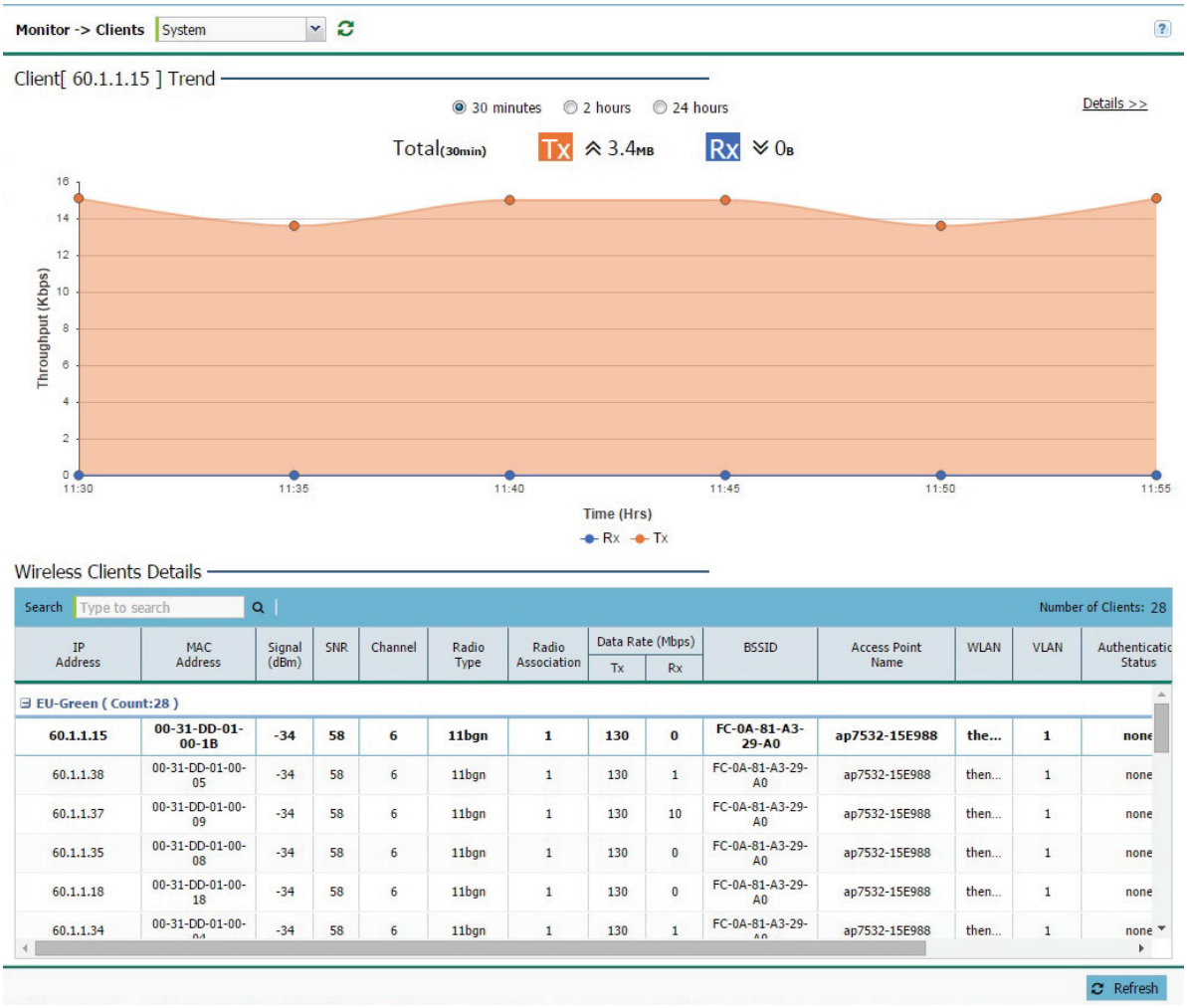
5 Select **<< Summary** to return to the main WLAN screen.

Monitor Clients (System)

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

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

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



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.

2 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 *Media Access Control* (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 *signal to noise ratio* (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. New 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 initiial 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 in use 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 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 wireless infrastructure.

Clients Details (System)

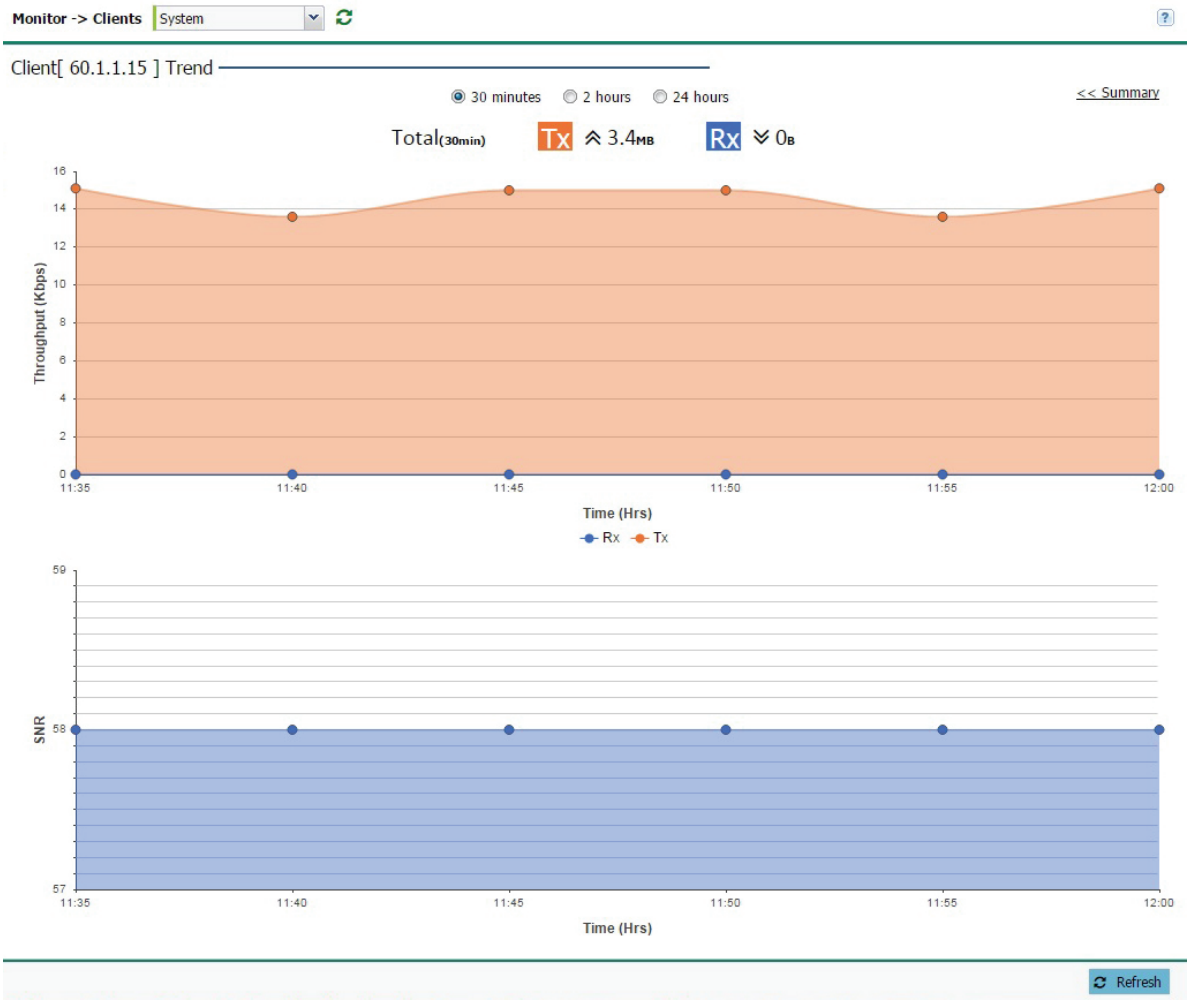
Refer to the **Clients** screen to assess system-wide performance on specific wireless client interfaces.

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) over the specified period of time.

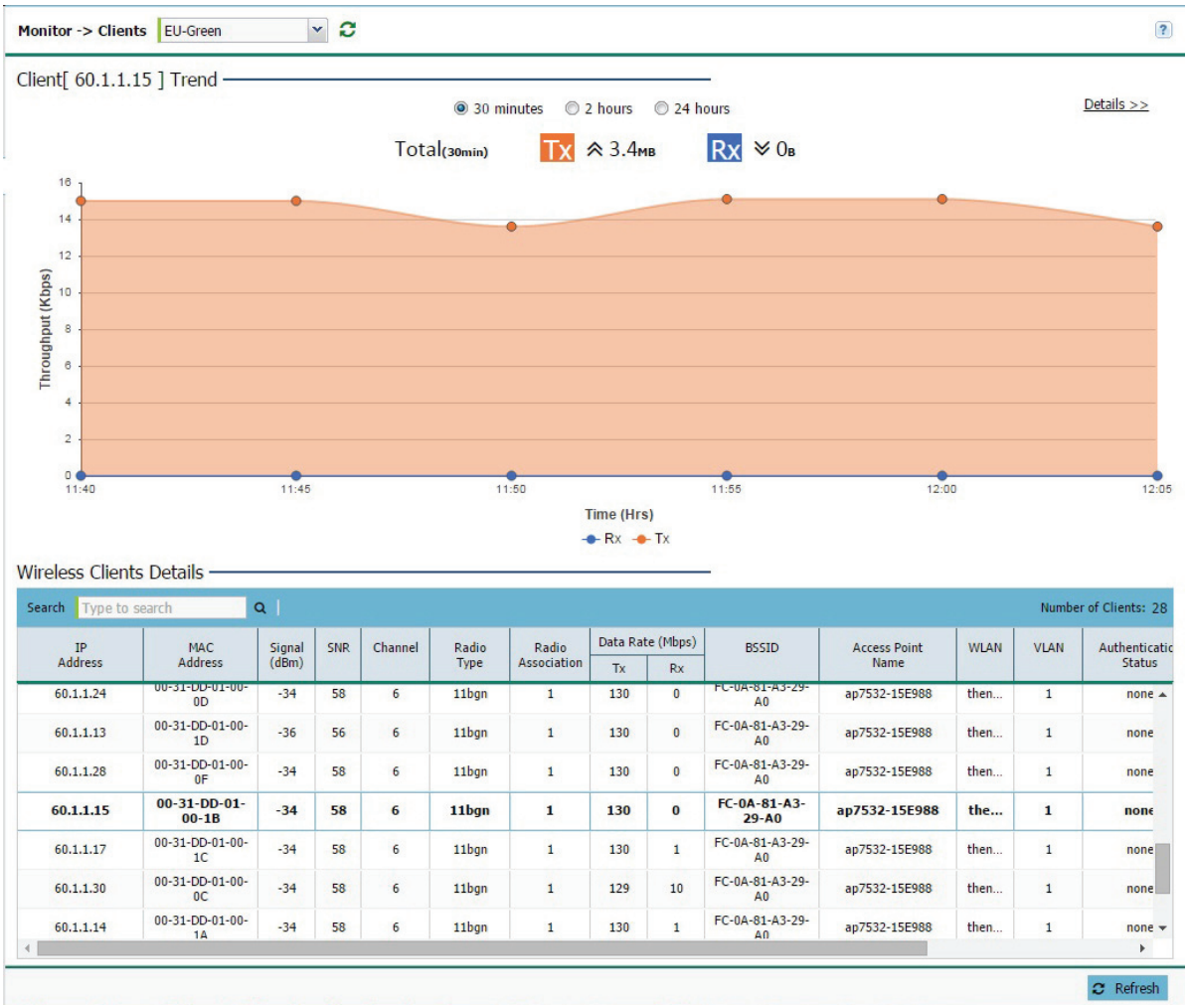
5 Select **<< Summary** to return to the main clients screen.

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 information for clients connected to 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 *Media Access Control* (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 *signal to noise ratio* (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. New 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 in use 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. 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 within the WiNG Express managed network.

Clients Details (Site)

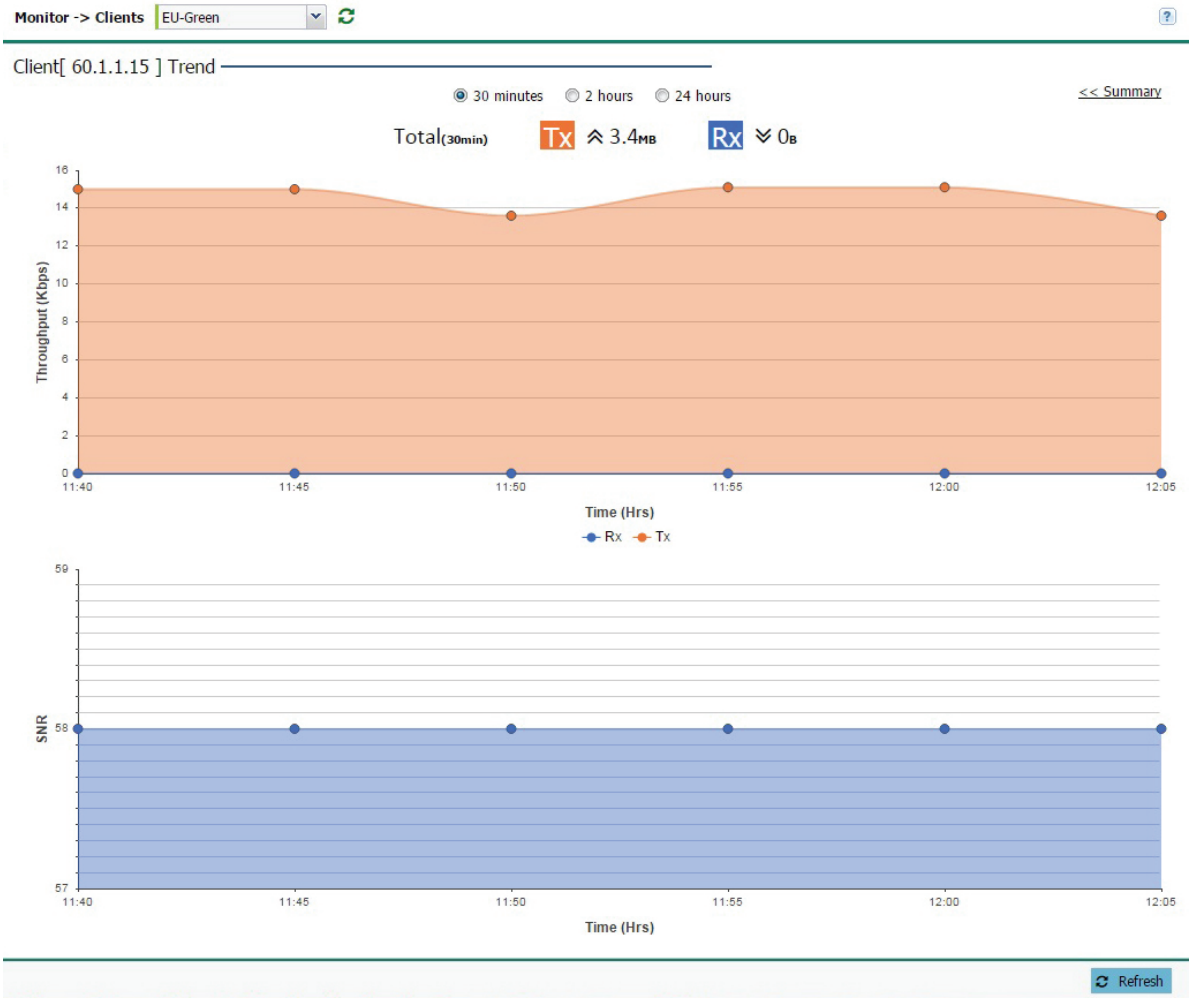
Refer to the **Clients** screen to assess performance on specific wireless client interfaces.

To review a client's wireless interface connection utilization:

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

2 Select **Clients**.

3 Select **Details**.



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

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

Chapter 3

Configuration

In This Chapter

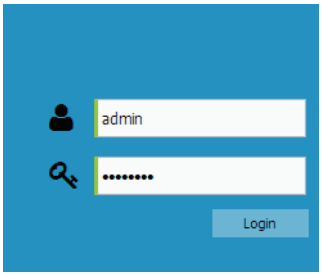
Configuration (System) 31
Configuration (Site) 64

Configuration (System)

Basic Configuration (System)

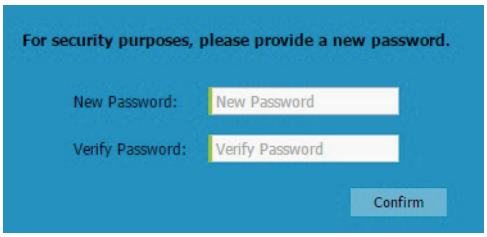
To provide the basic configuration and access WiNG Express Manager functions:

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 WiNG Express Manager interface has been accessed, a screen displays prompting to enter a new password.

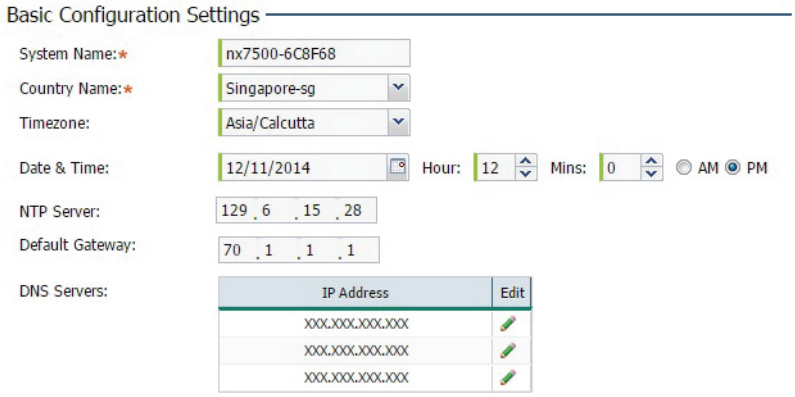


5 Enter a new password for the admin user.

6 The device automatically displays a Dashboard where administrator can assess network health and conduct a diagnostic review of network performance.

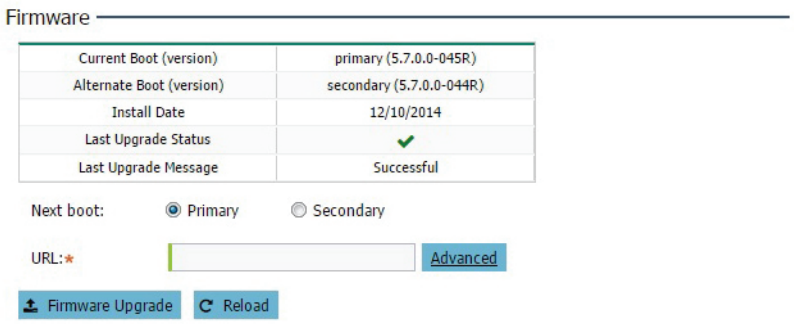
7 Expand the Configuration menu item and select **Basic**.

8 Set the following **Basic Configuration Settings** for this device:



- *System Name* - Provide a System Name used as WiNG 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) 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.

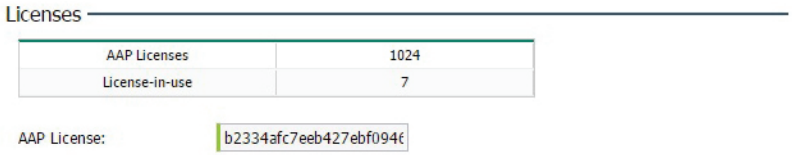
9 The **Firmware** section displays the current and alternate firmware versions for the device, the date which the most recent firmware was installed and the last upgrade status. In the URL field, enter the complete path to the firmware file for the target device.



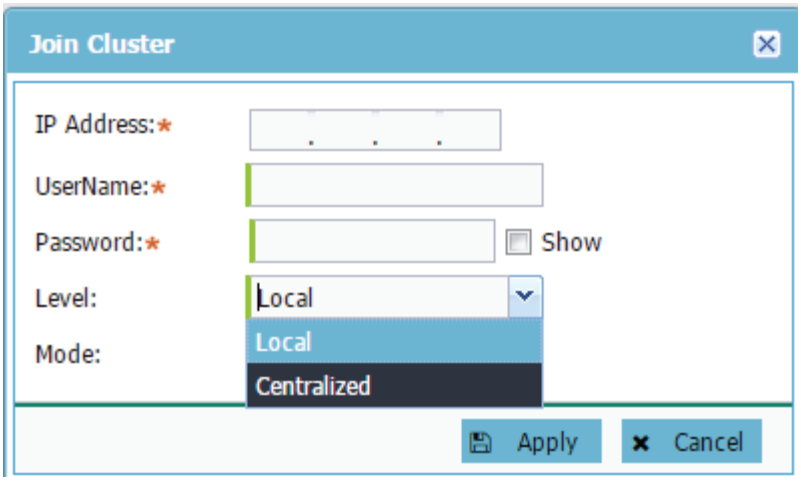
10 Alternately click **Advanced** and provide the following information to accurately define the location of the target firmware file:

Protocol	Select the connection protocol used for updating device firmware. Available options include: • *tftp* • *ftp* • *sftps* • *http* • *cf* • *usb1-4*
Port	Use the spinner control or manually enter the value to define the port used for firmware updates. This option is not valid for *cf* and *usb1-4*.
IP Address	Enter IP address of the server used to update the firmware. This option is not valid for *cf* and *usb1-4*.
Hostname	Provide the hostname of the server used to update the firmware. This option is not valid for *cf* and *usb1-4*.
User Name	Define the user name used to access either a *FTP* or *SFTP* server.
Password	Specify the password for the user account to access a *FTP* or a *SFTP* 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 which is number of APs available for adoption under the restrictions of the license. This number applies to dependent mode adaptive APs only, and not independent mode APs. The number of licenses currently in use is displayed below and the AP License key is displayed below that.



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



State	Displays a status indicating whether the cluster is running or disabled.
Mode	A cluster member can be in either an *Active* or *Standby* 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 Join Cluster 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.

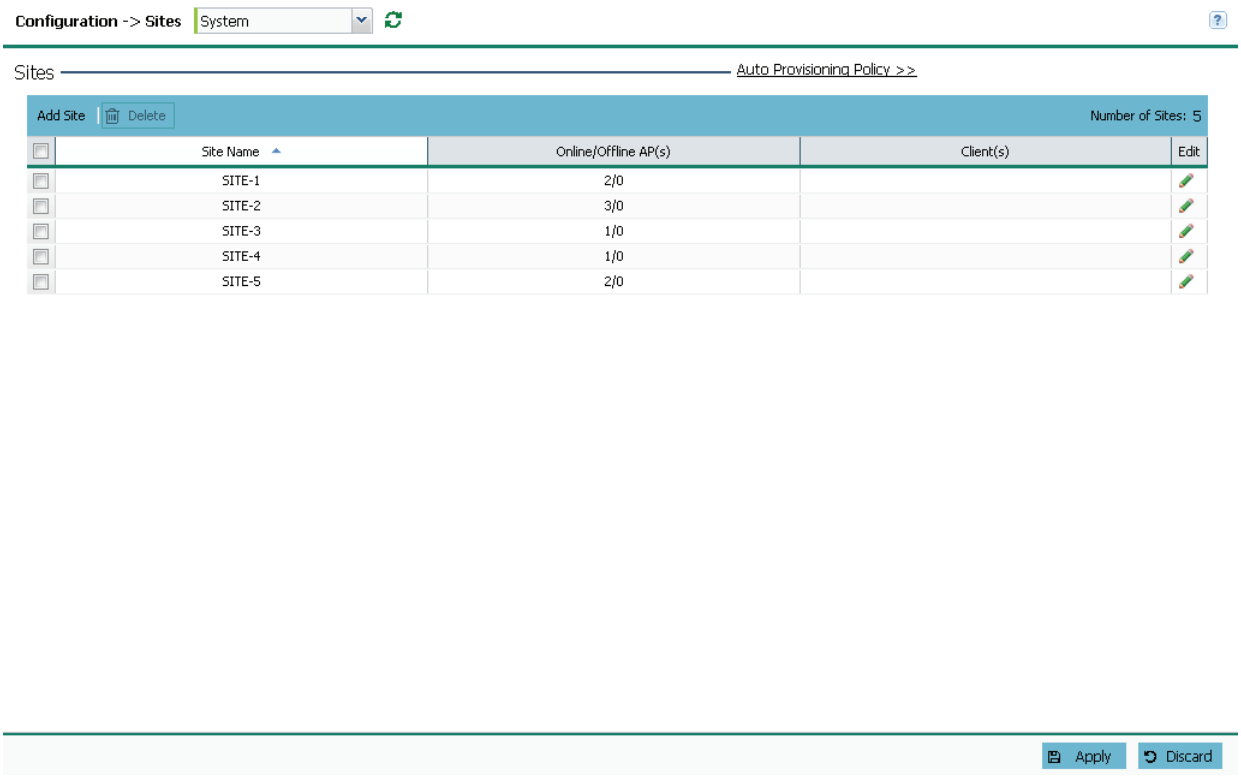
14 Click **Apply** to save the basic system configuration settings.

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.**



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

Site Name	Displays the user defined site name for each configured site.
Health	Displays the health of each configured site in a color coded block.
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.

Sites Auto Provisioning (System)

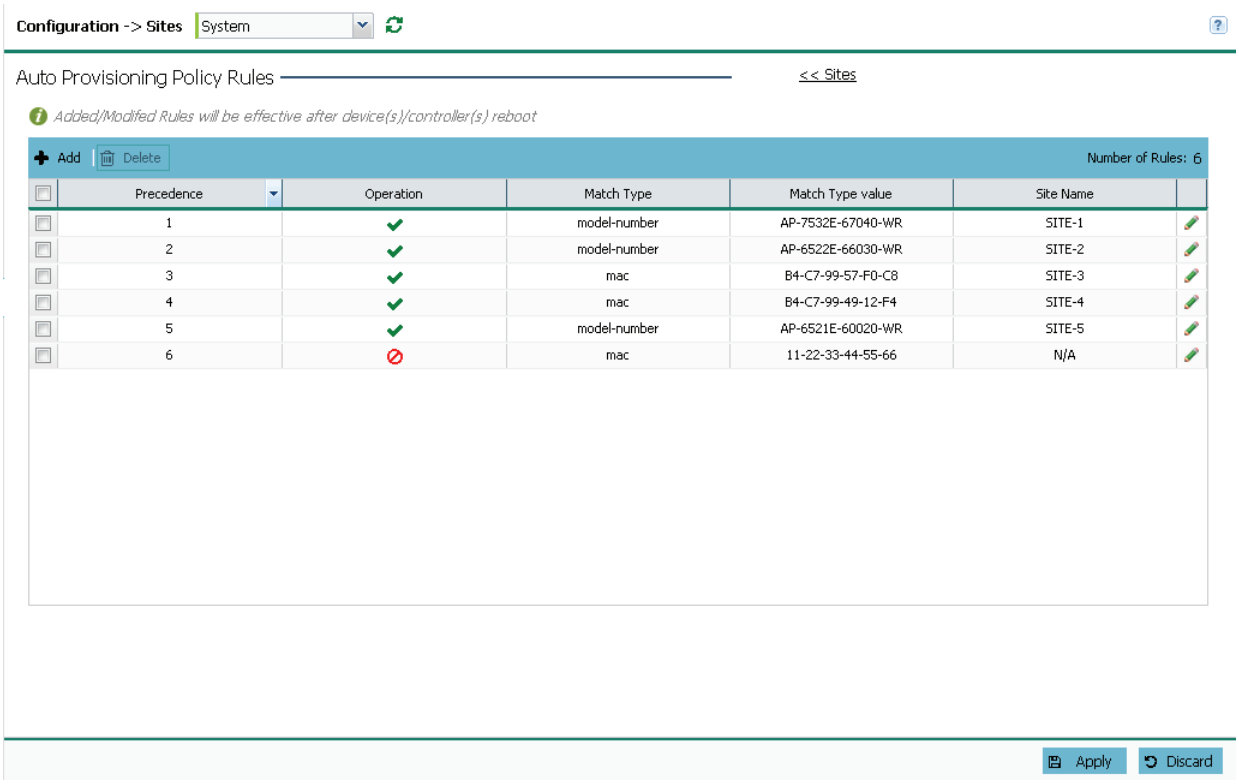
WiNG Express Manager's auto-provisioning feature allows you to deploy a multi-site WLAN network without any pre-staging. Policies can be defined for each site to match against parameters such as CDP/LLDP string, AP MAC and IP address to place APs in a specific site and apply the appropriate configuration.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

The system level dashboard presents a map view of all the sites with inventory details for immediate visualization of the entire network. The site-level dashboard allows you to see the status of your Access Points and their radios, the client devices connected to your access points, how much capacity is available and more. A drop-down box 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**.



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

Precedence	Define the precedence (sequence) the Adoption Policies 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	Define the operation taken upon receiving an adoption request from an Access Point. The following operations are available: *Allow* – Allows the normal provisioning of connected Access Points upon request. *Deny* – Denies (prohibits) the provisioning of connected Access Point upon request. *Redirect* – When selected, an Access Point seeks a steering controller (upon adoption request), will forward the network credentials of a designated controller resource that initiates the provisioning process. *Upgrade* – Conducts the provisioning of requesting Access Points from this controller resource.
Match Type	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: *MAC Address* – The filter type is a MAC Address of the selected Access Point model. *IP Address* – The filter type is the IP address of the selected Access Point model. *VLAN* – The filter type is a VLAN. *Serial Number* – The filter type is the serial number of the selected Access Point model. *Model Number* – The filter type is the Access Point model number. *DHCP Option* – The filter type is the DHCP option value of the selected Access Point model.
Match Type value	Displays the match type value based on the match type specified. The match type value will display the output for the selected match type of *MAC Address, IP Address, VLAN, Serial Number, Model Number and DHCP Option.*
Site Name	Displays the name of the site associated with each rule.

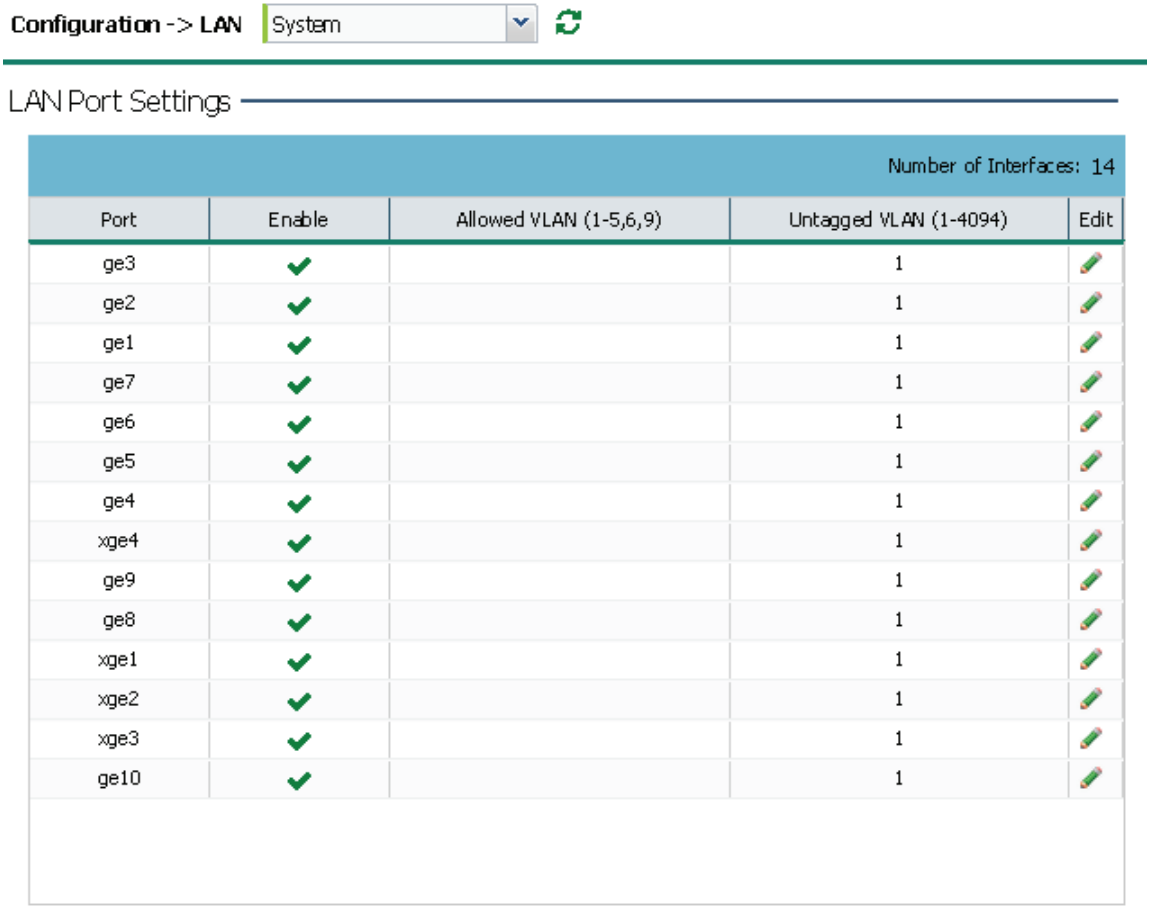
LAN Configuration (System)

Refer to the **LAN** screen to set specific WiNG Express Manager wired interfaces.

To configure wired interface settings:

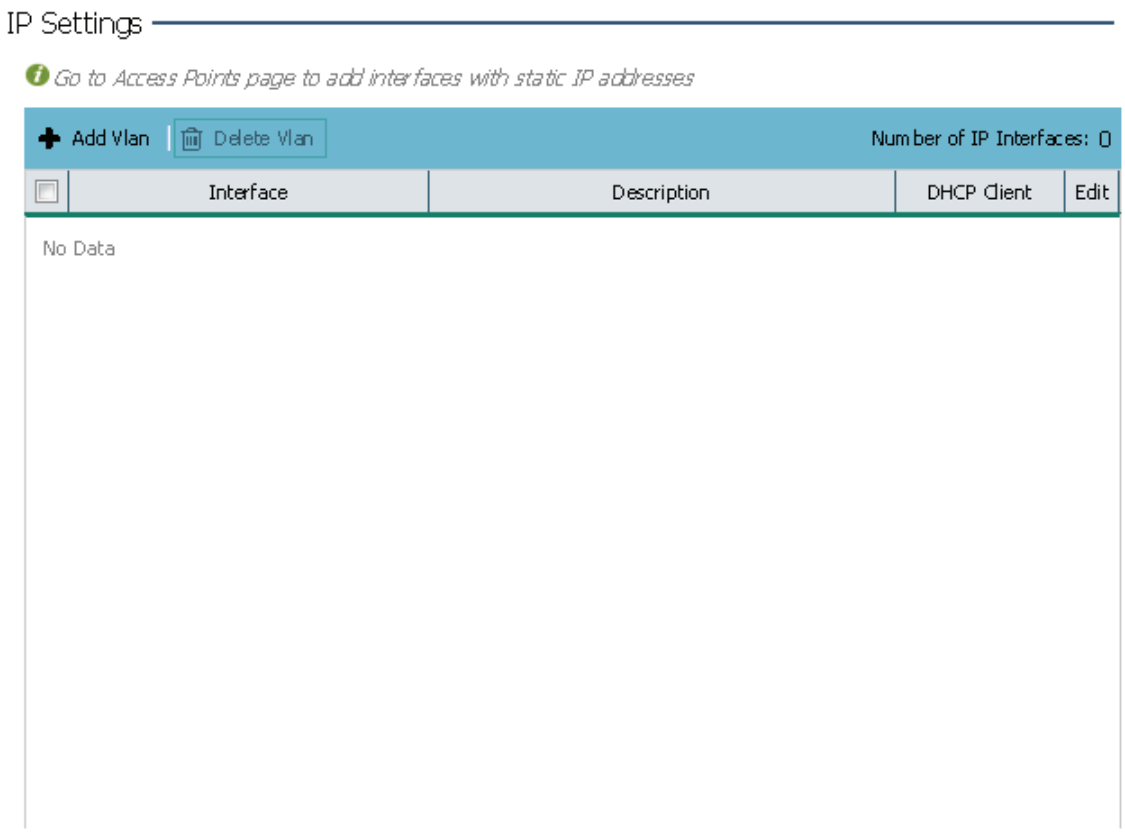
1 Select **Configuration** settings from the main menu then select **LAN**.

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



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 *Enable* 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) that traffic is allowed on as a virtual interface for each wired port.
Untagged VLAN	Displays the VLAN(s) that untagged traffic will be transmitted and received on.
Edit	Select *Edit* to make changes to the selected interface.

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



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 *Edit* to make changes to the selected interface.

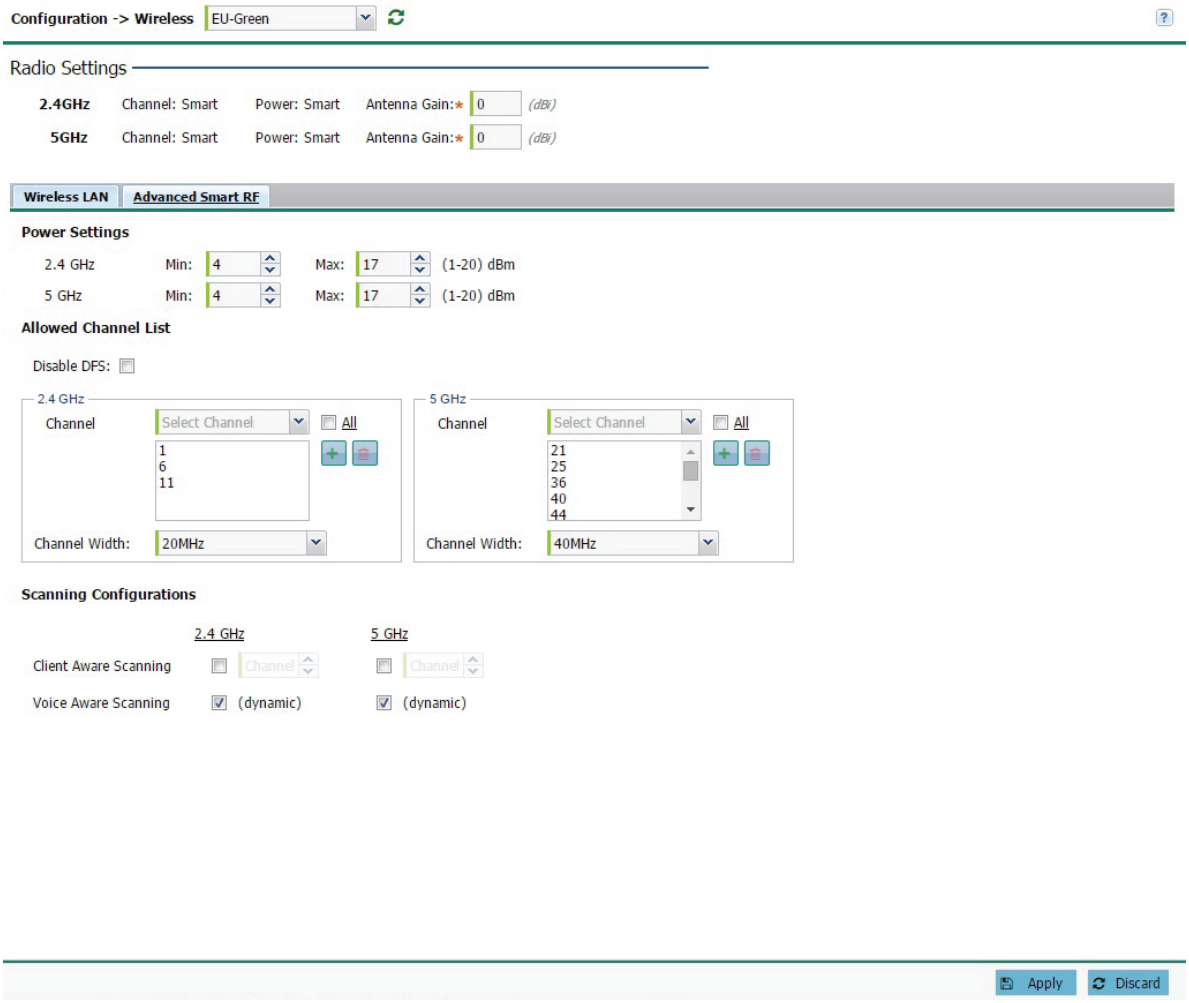
Wireless Configuration (System)

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 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 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 *Smart* 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 *Smart* as the Power setting automatically configures radio power to not exceed the maximum power allowed by the defined country. For static power settings, the professional installer must ensure the configured power levels are compliant with local and regional regulations. The county selected automatically limits the maximum output power that can be set.
Gain	Set the antenna gain between 0.00 - 15.00 dBi. The *Power Management Antenna Configuration File* (PMACF) automatically configures the radio transmit power based on antenna type, 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. The default value is 0.00. For external antenna model Access Points, configure the Antenna Gain based on the antenna used in the deployment. The set gain value should include the antenna gain, along with any additional components, such as extension cables used between the Access Point and the antenna.

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 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	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. The screen displays with the *Open* option selected. Naming and saving such a policy (as is) would provide no security and might only make sense in a network wherein no sensitive data is either transmitted or received. This default setting is not recommended. If selecting *Secure-PSK*, 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. If selecting *Secure-802.1x*, 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 WLAN resources.
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 *Edit* to change the settings of the selected WLAN.

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.

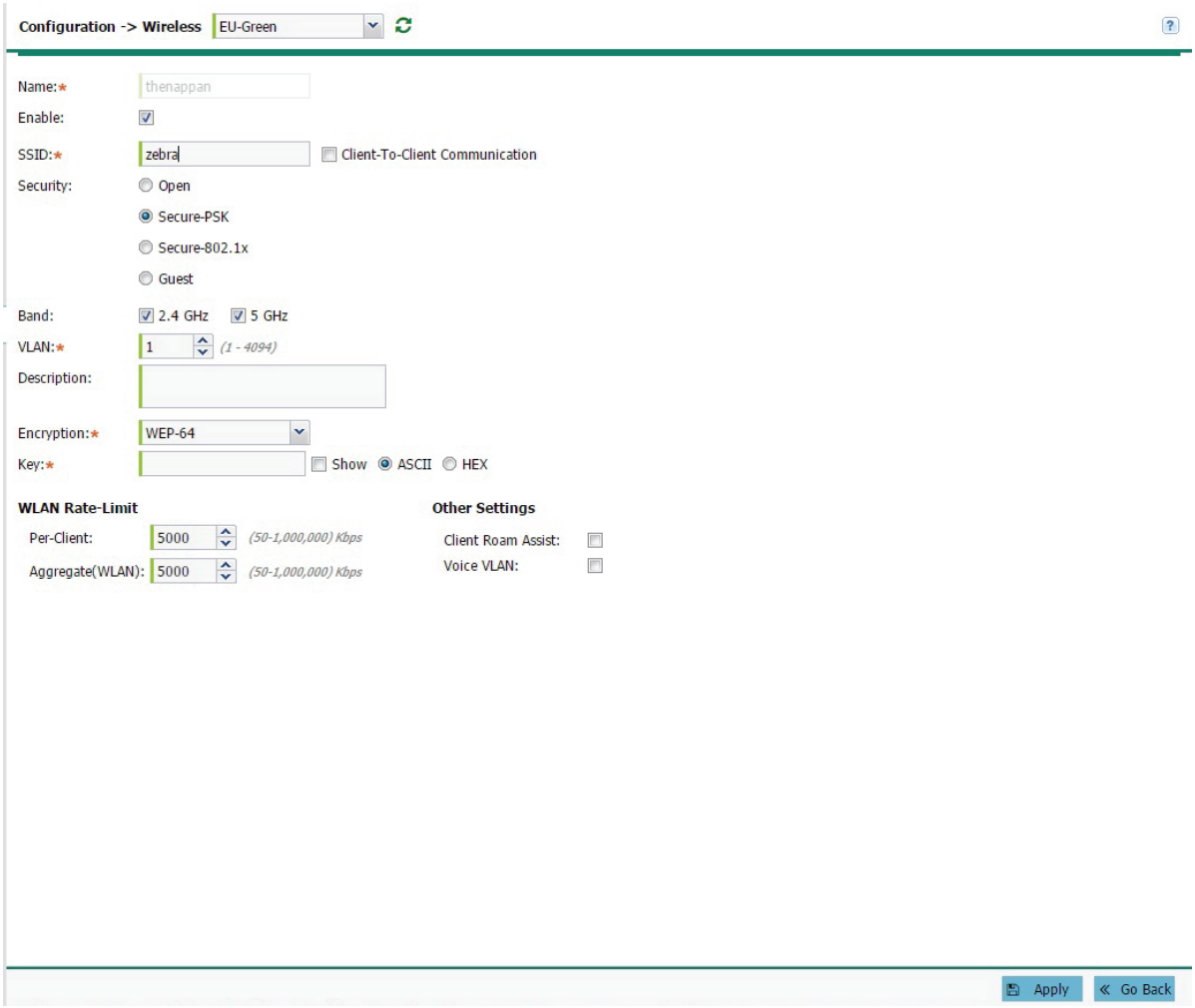
WLANs are mapped to radios on each connected Access Point. A WLAN can be advertised from a single Access Point radio or can span multiple Access Points and radios. WLAN configurations can be defined to only provided service to specific areas of a site. For example a guest access WLAN may only be mapped 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 support needs:

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

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



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 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	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. The screen displays with the Open option selected. Naming and saving such a policy (as is) would provide no security and might only make sense in a network wherein no sensitive data is either transmitted or received. This default setting is not recommended. If selecting Secure-PSK, select an encryption type for the WLAN. Define whether the key is entered in ASCII or HEX characters. Selecting Show to expose the key is not recommended. If selecting Secure-802.1x, 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. Selecting Guest displays fields for captive portal Web page creation, and is beyond the scope of this basic WiNG Express Access Point configuration.
Band	Select a band, *2.4Ghz or 5Ghz* (if supported), to enable specific client radio support on the WLAN.
VLAN	Use the spinner control to specify a VLAN from 1 - 4,094 for this WLAN. When a client associates with a WLAN, the client is assigned a VLAN by load balance distribution. Do not use VLAN 1 with the WLAN if the WAN port has been enabled.
Description	Optionally, enter descriptive text which can be used by administrators to help identify each WLAN.

Encryption (Secure-PSK only)	When *Secure-PSK* security is selected, use the drop-down menu to select an encryption type. Available encryption types are: *WEP-64 - Wired Equivalent Privacy* (WEP) is a security protocol specified in the IEEE *Wireless Fidelity* (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 *initialization vector* (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. *WEP-128 - Wired Equivalent Privacy* (WEP) is a security protocol specified in the IEEE *Wireless Fidelity* (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 128 uses a 104 bit key which is concatenated with a 24-bit *initialization vector* (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. *TKIP-CCMP* - CCMP is a security standard used by the *Advanced Encryption Standard* (AES). AES serves the same function TKIP does for WPA-TKIP. CCMP computes a Message Integrity Check (MIC) using the proven *Cipher Block Chaining* (CBC) technique. Changing just one bit in a message produces a totally different result. The encryption method is *Temporal Key Integrity Protocol* (TKIP). 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. *WPA2-CCMP* - WPA2 is a 802.11i standard that provides even stronger wireless security than *Wi-Fi Protected Access* (WPA) and WEP. CCMP is the security standard used by the *Advanced Encryption Standard* (AES). AES serves the same function TKIP does for WPA-TKIP. CCMP computes a *Message Integrity Check* (MIC) using the proven *Cipher Block Chaining* (CBC) technique. Changing just one bit in a message produces a totally different result. WPA2/CCMP is based on the concept of a *Robust Security Network* (RSN), 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.

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 *Generate* 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.

4 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. A client's maximum data speed will be 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 between 50 to 1,000,000 kbps. The collective data rate for all clients on the WLAN will be limited the configured rate.

5 In the **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 *received signal strength indicator* (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 will be tagged with with this VLAN.

Security Firewall Configuration (System)

When protecting wireless traffic to and from a WiNG Express Manager connected Access Point, an administrator should not lose sight of the security solution in it's entirety, since the chain is as weak as its weakest link. WiNG 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. 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.

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 WiNG 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 fireall, 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 WiNG Express Manager is processing, the firewall uses that rule's action to determine whether traffic is allowed or denied.

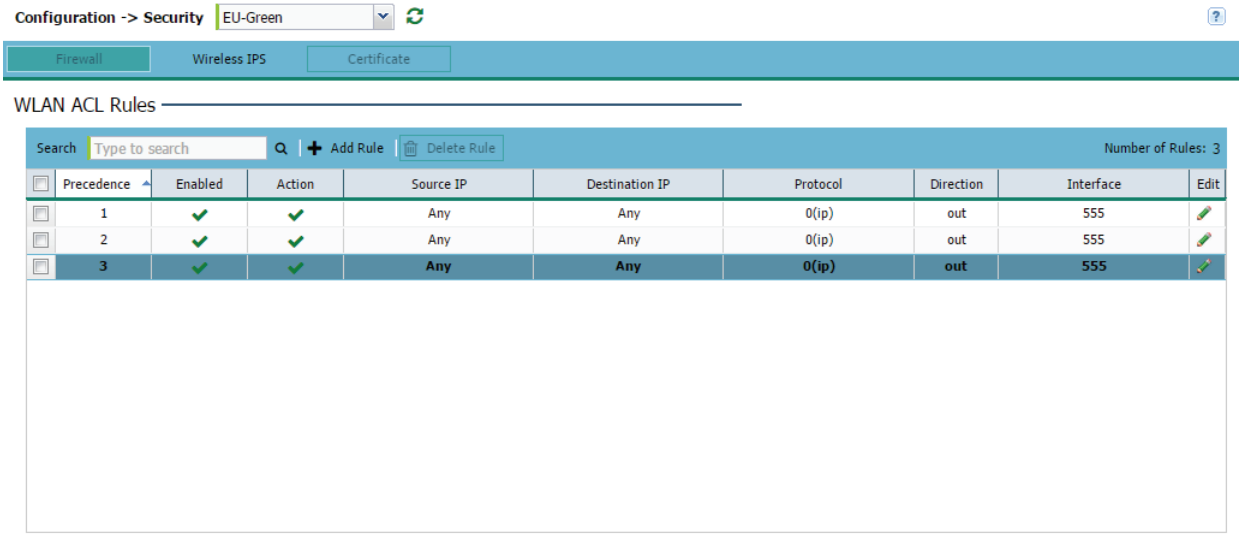
Rules comprise conditions and actions. A condition describes a traffic stream of packets. Define constraints on the source and destination device, the service (for example, protocols and ports), and the incoming interface. An action describes what should occur to packets matching the conditions set.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

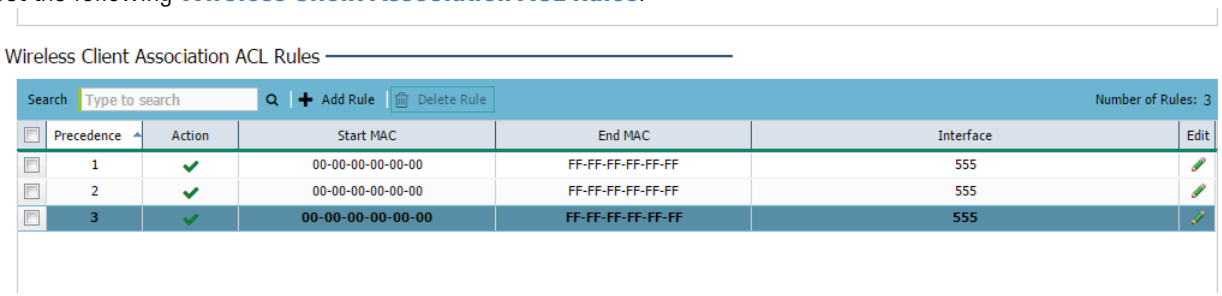
The firewall screen is divided into **WLAN ACL Rules** and **Wireless Client Association ACL Rules** fields.

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 will move down the table to reflect its lower priority.
Enabled	Select a firewall rule's *Enable* or *Disable* 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: *Deny* - Instructs the firewall stop a packet from its destination. *Permit* - 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	Define the access protocols impacted by the WLAN's ACL rule configuration.
Source Port	If using either *tcp* or *udp* 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 *Low* and *High* numeric range settings. A source port cannot be a destination port.
Destination Port	If using either *tcp* or *udp* 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 *Low* and *High* 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 will move down the table to reflect its lower priority.
Action	Every IP firewall rule is made up of matching criteria rules. The action defines what to do with the packet if it matches the specified criteria. The following actions are supported: *Deny* - Instructs the firewall stop a packet from its destination. *Permit* - 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.

WiNG 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 help protect the Access Point managed wireless network.
- *Rogue Detection and Segregation* - A WIPS supported Access Point distinguishes itself by both identifying and categorizing nearby Access Points. WIPS identifies threatening versus non-threatening Access Points by segregating Access Points attached to the network (unauthorized APs) from those not attached to the network (neighboring Access Points). The correct classification of potential threats is critical for administrators to act promptly against rogues and not invest in a manual search of neighboring Access Points to isolate the few attached to the network.
- *Locationing* - Administrators can define the location of wireless clients as they move throughout a site. This allows for the removal of potential rogues though the identification and removal of their connected Access Points.
- *WEP Cloaking* - WEP Cloaking protects organizations using the *Wired Equivalent Privacy* (WEP) security standard to protect networks from common attempts used to crack encryption keys. There are several freeware WEP cracking tools available and 23 known attacks against the original 802.11 encryption standard; even 128-bit WEP keys take only minutes to crack. WEP Cloaking module enables organizations to operate WEP encrypted networks securely and to preserve their existing investment in mobile devices.

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:

Event Name	Displays the rogue AP event type detected by the sensor. Several different event types can occur: An *Excessive Action Event* is an event where an action is performed repetitively and continuously. DoS attacks come under this category. *MU Anomaly Events* are suspicious events by wireless clients that can compromise the security and stability of the network. *AP Anomaly Events* are suspicious frames sent by neighboring APs.
Reporting AP	Displays the hardware encoded *Media Access Control* (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 network approved Access Point or if this Access Point is unauthorized and could jeopardize network security, and consequently warrants quarantine.
Detector Radio	Displays the radio number of the detecting Access Point reporting the event. AP6511 and AP6521 model Access Points are single radio devices, 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.

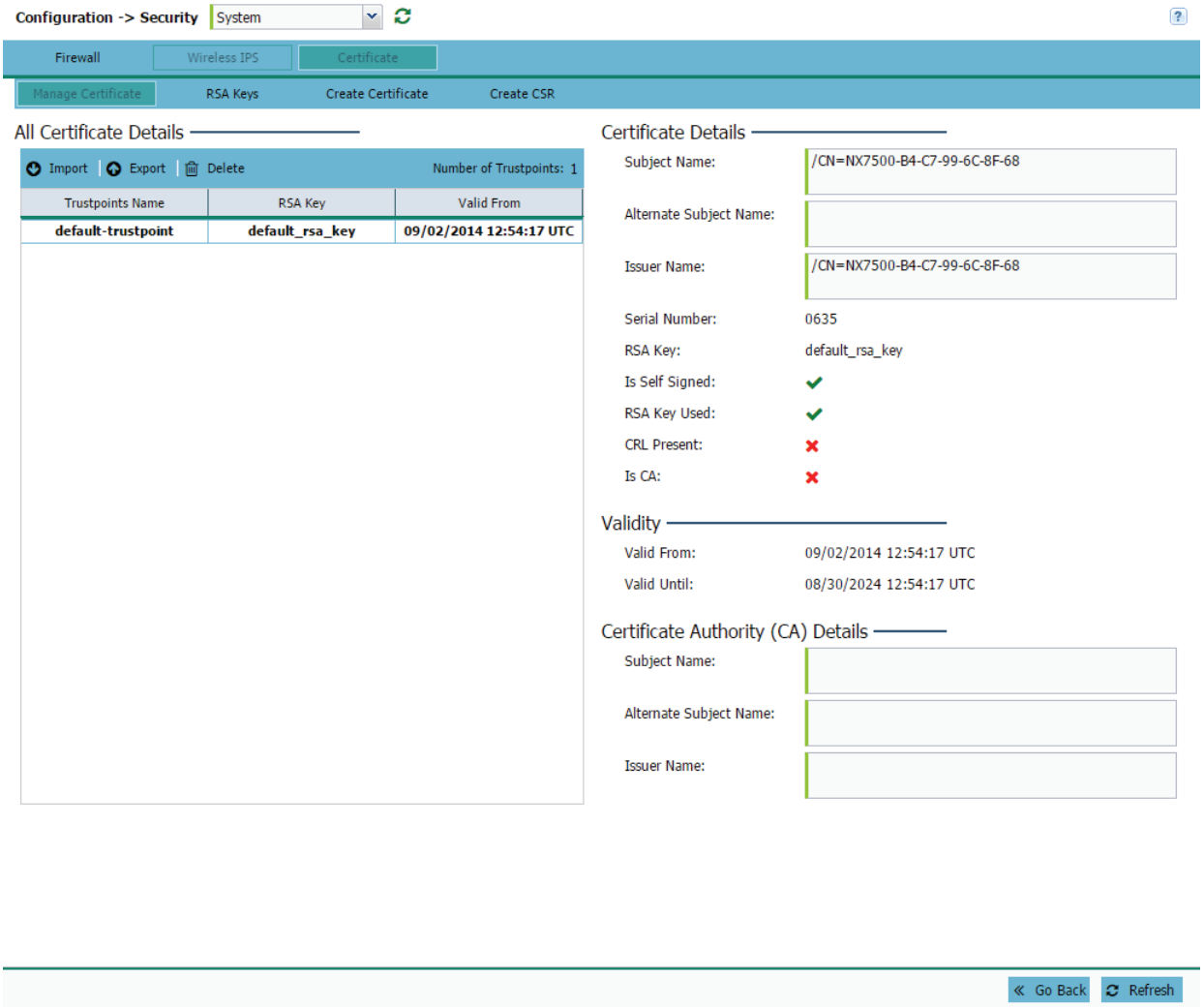
Depending on the public key infrastructure, the digital certificate includes the owner's public key, the certificate expiration date, the owner's name and other public key owner information.

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.



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

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

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

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

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

RADIUS Configuration (System)

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

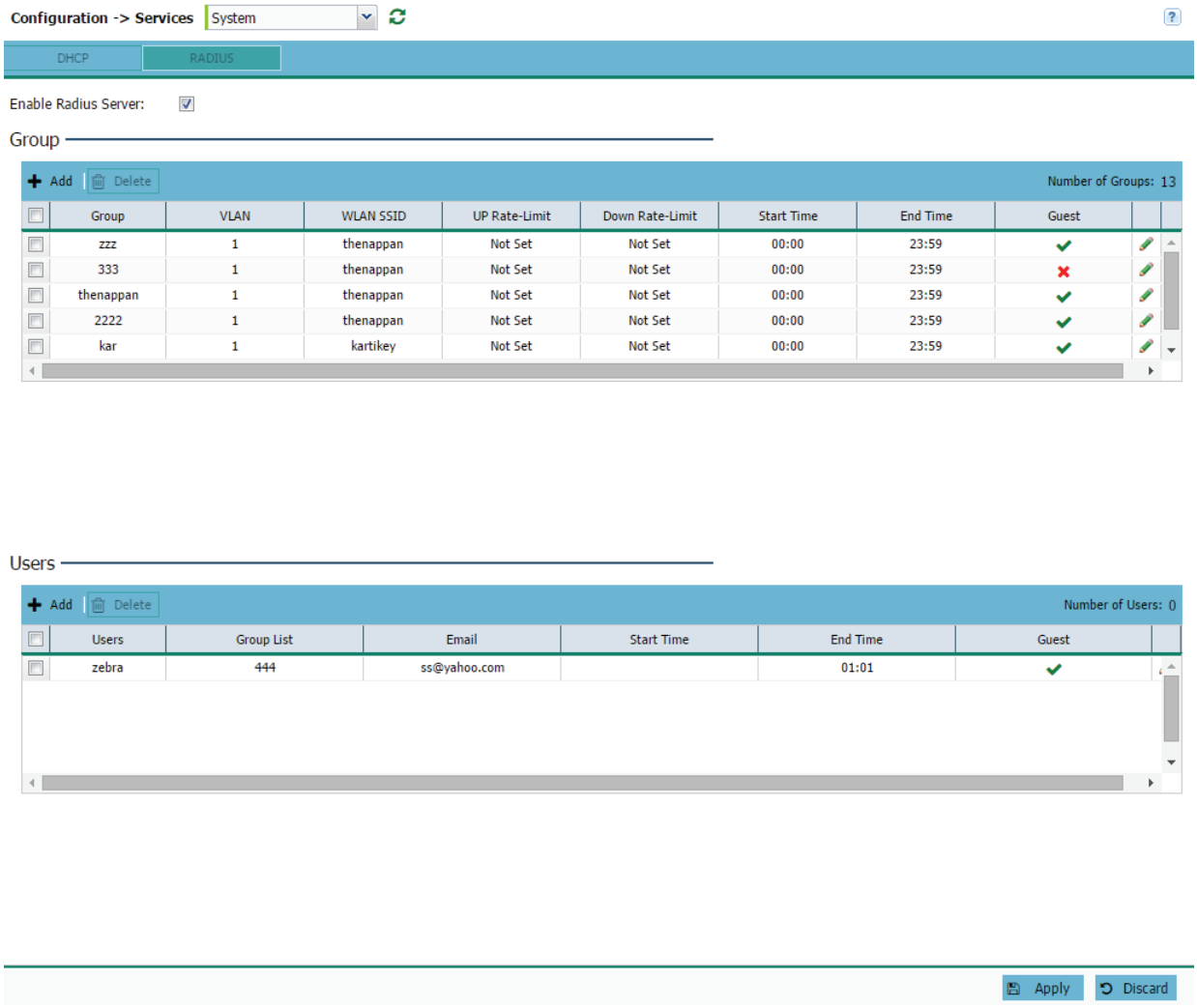
To view RADIUS configurations:

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).



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 network (once authenticated by the local RADIUS server).
WLAN SSID	Displays the *Service Set ID* (SSID) of the network to which the Access Point belongs to.
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 desitned 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 starting 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 pull-down menu to select which group to associate with the RADIUS user.
Email ID	Specify an e-mail address for the RADIUS user. This can be a local E-mail address or a fully qualified E-mail address.
Telephone	Specify the telephone number associated with the RADIUS user. This is an optional field.
Start Date / Start Time	Specify a 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 Til Expiry option. To specify a duration of time the account will be active, set the 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.

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.

Management Configuration (System)

WiNG 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.

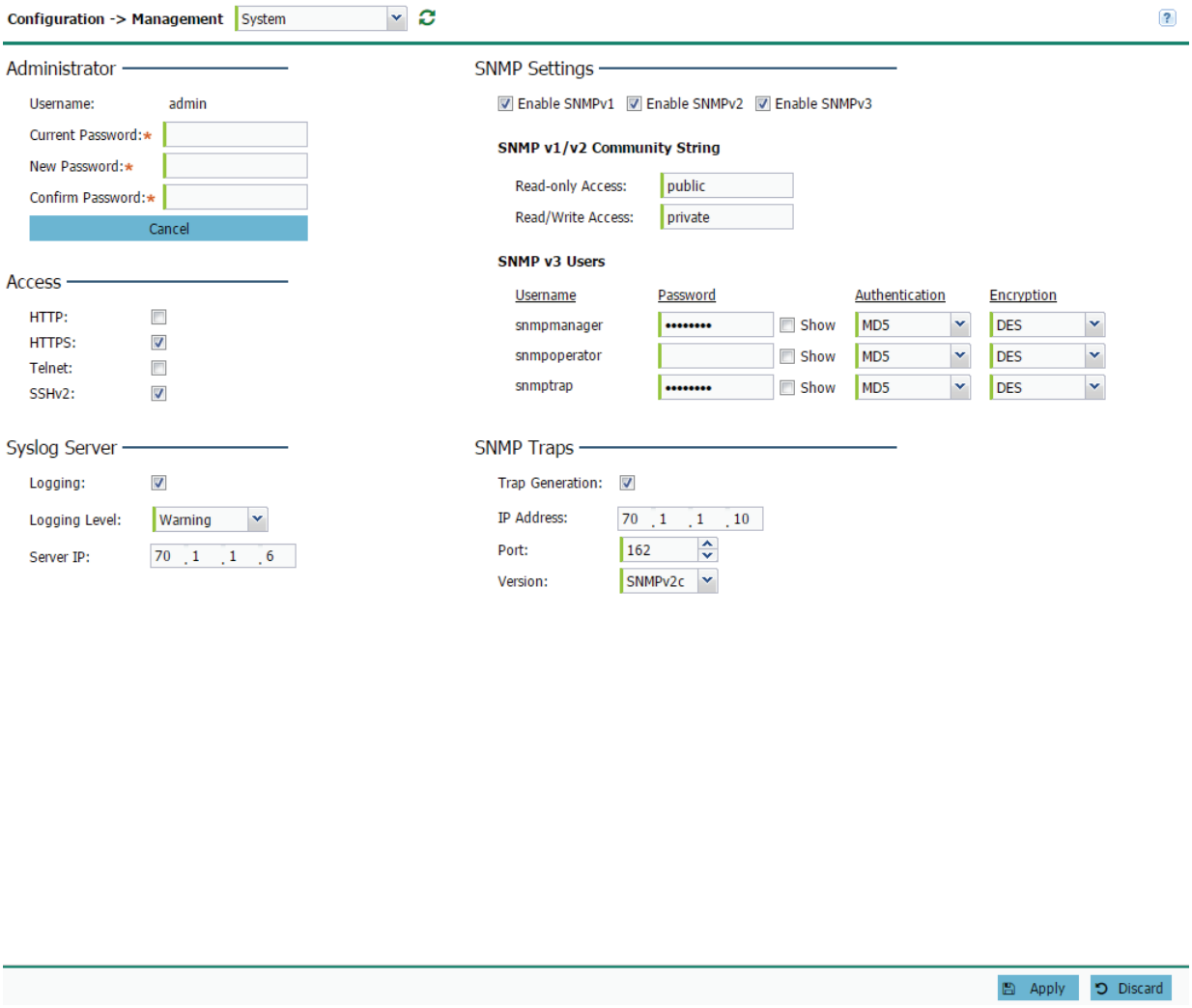
To enhance security, administrators can apply various restrictions as needed to:

- 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 **Wireless**.



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 WiNG Express Manager. Assign a numeric identifier to log events based on criticality. Severity levels include *0 - Emergency, 1 - Alert, 2 - Critical, 3 - Errors, 4 - Warning, 5 - Notice, 6 - Info and 7 - Debug*. 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 *user-based security model* (USM) for message security and the *view-based access control model* (VACM) for access control. The architecture supports the concurrent use of different security, access control and message processing techniques. SNMPv3 is enabled by default.

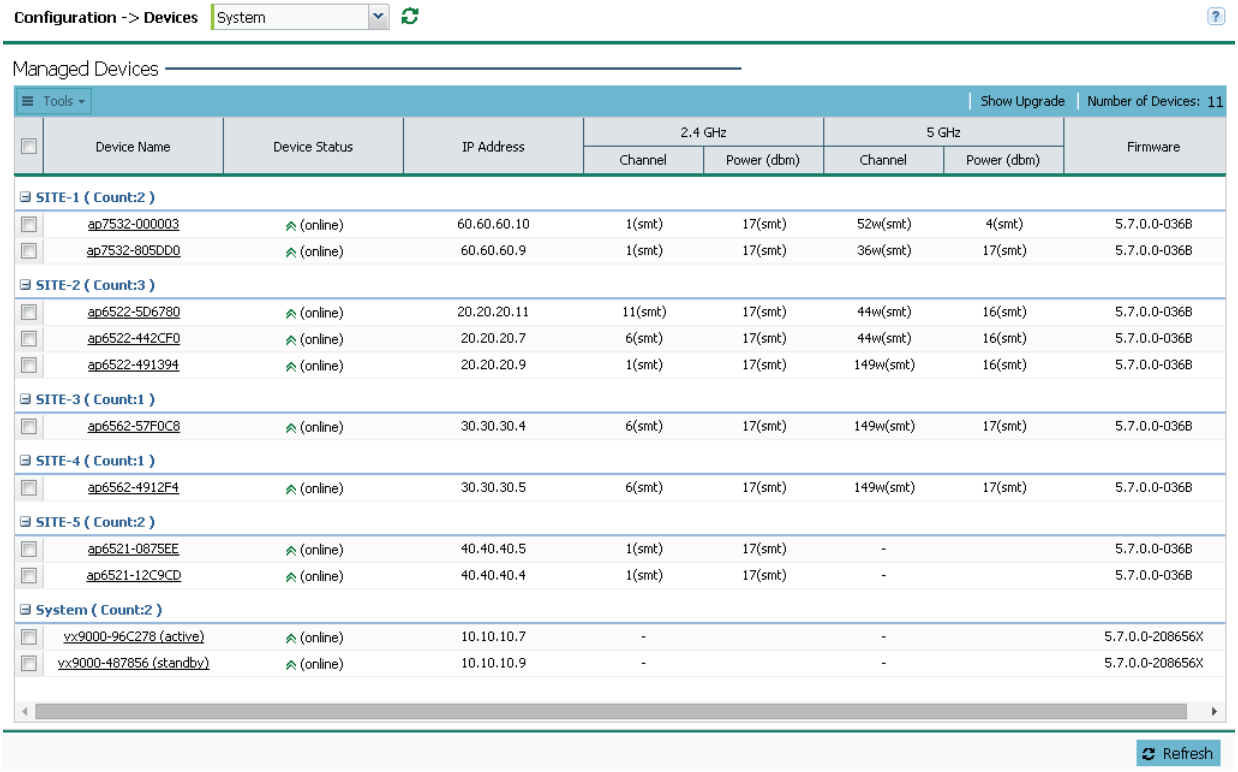
SNMP v1/v2 Community String: Access Control	Set the access permission for each community string used to retrieve or modify information. Available options include: *Read Only* - Allows a remote device to retrieve information. *Read-Write* - Allows a remote device to modify settings.
SNMPv3 Users: User 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 WiNG 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 WiNG Express Manager's network resources.

6 In the **SNMP Traps** section, configure the following:

Trap Generation	Select the *Trap Generation* 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 the WiNG Express Manager.
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.

Device Configuration (System)

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



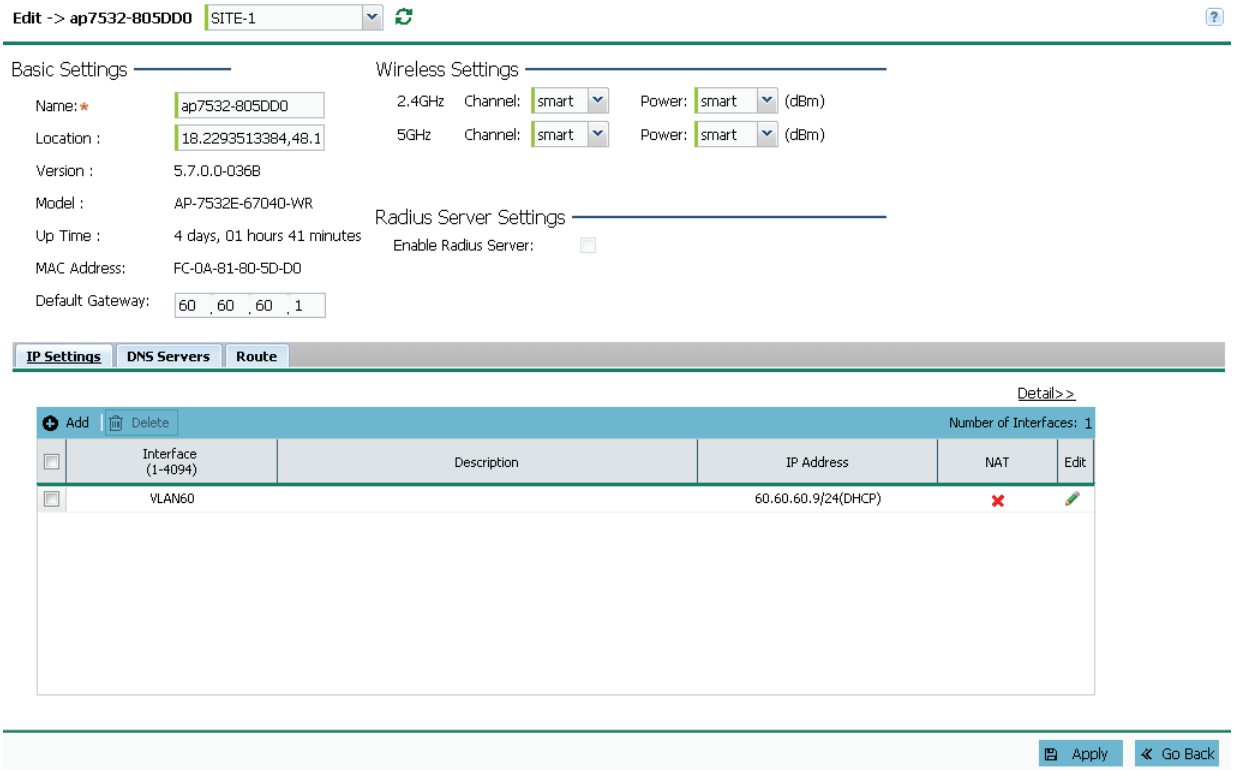
2 The **Managed Devices** table displays the following information about devices managed at both the system and the site level:

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 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* will appear instead of a channel number. If a device is using smart channel selection, *(smt)* will display 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)* will display after the power level.
5 GHz Channel	Displays the 5 GHz radio channel that each configured device is using. If a devices is not using a channel or status is unavailable, *N/A* will appear instead of a channel number. If a device is using smart channel selection, *(smt)* will display 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)* will display after the power level.

Editing Devices Configuration (System)

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

2 Select the **Device Name** to edit the device configuration.



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 gatway where all external network traffic is routed through.
2.4 GHz Channel	Displays the 2.4 GHz radio channel that each configured device is using. If a devices is not using a channel or status is unavailable, *N/A* will appear 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.

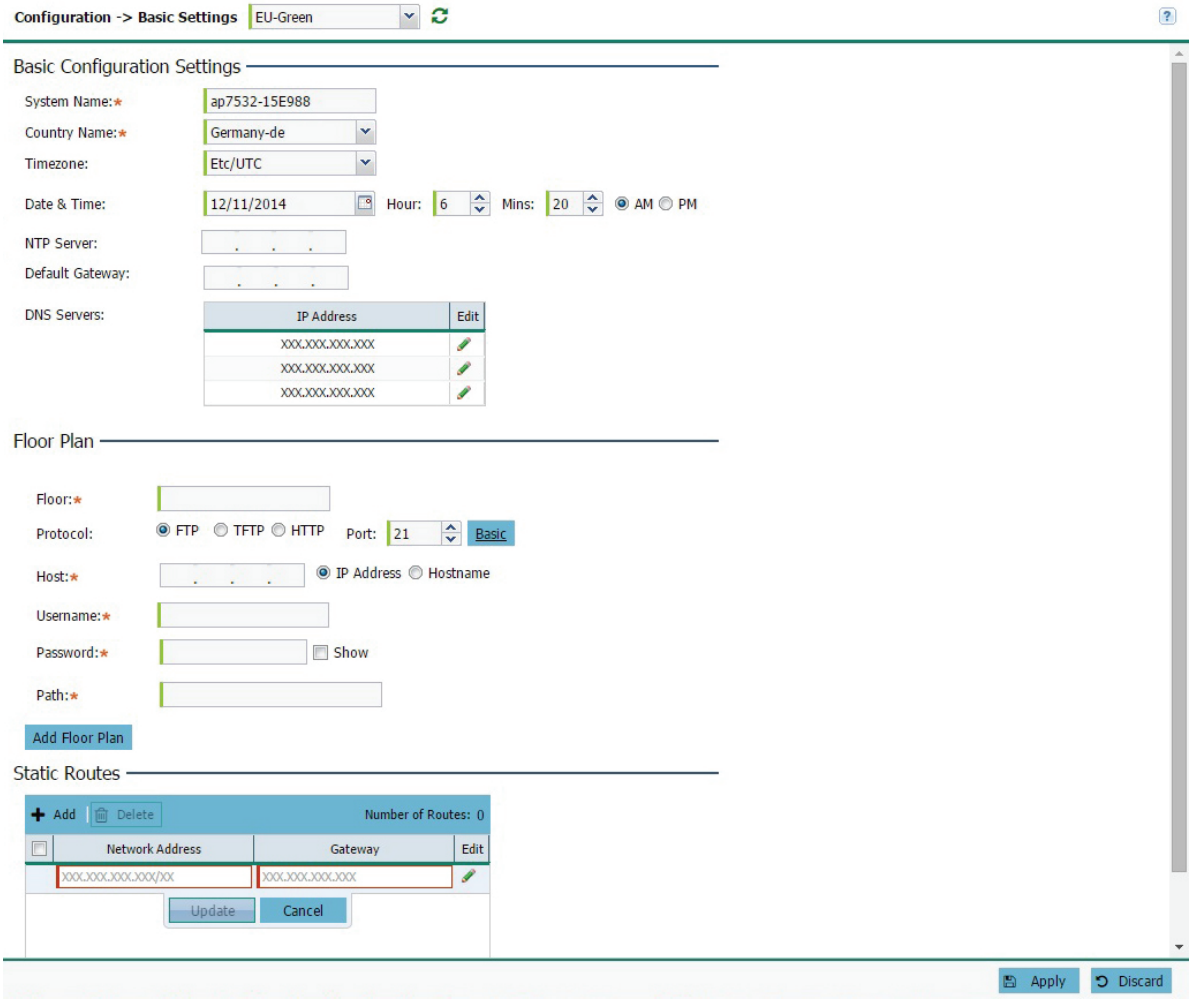
2.4 GHz Antenna Gain	Set the 2.4 GHz antenna between 0.00 - 15.00 dBm. The Access Point's Power *Management Antenna Configuration File* (PMACF) automatically configures the Access Point's radio transmit power based on the antenna type, its antenna gain (provided here) and the deployed country's regulatory 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, *N/A* will appear instead of a channel number. If a device is using smart channel selection, *(smt)* will display 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)* will display after the power level.
5 GHz Antenna Gain	Set the 5 GHz antenna between 0.00 - 15.00 dBm. The Access Point's Power *Management Antenna Configuration File* (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)

Basic Configuration (Site)

To configure the basic configuration for the site:

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



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

- *System Name* - Provide a System Name used as the WiNG 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. WiNG 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.

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.

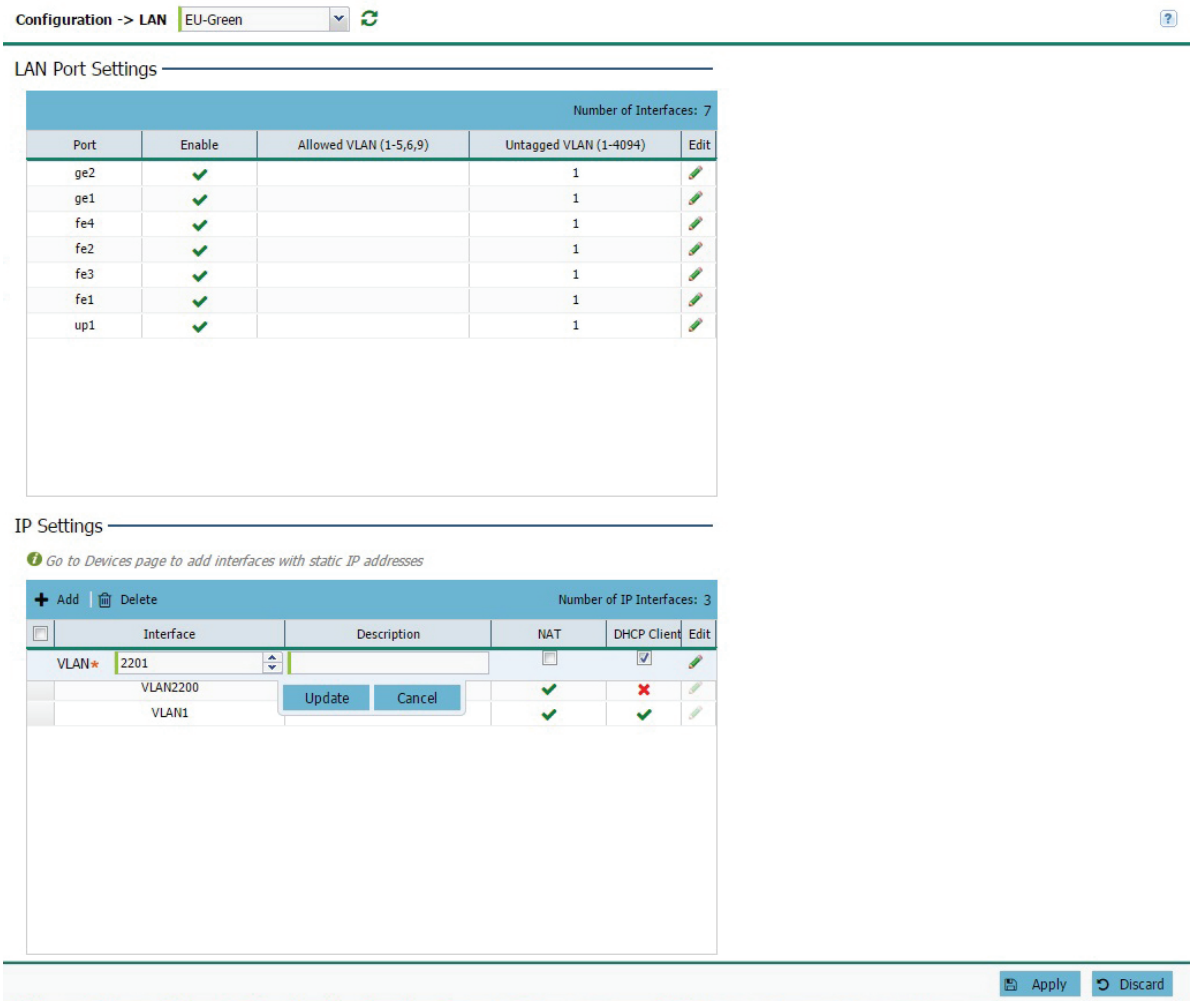
5 Click **Apply** to save the basic system configuration settings.

LAN Configuration (Site)

Refer to the **LAN** screen to set specific WiNG Express Manager wired interfaces.

To configure wired interface settings:

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



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 *Enable* 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 *Edit* 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 *Edit* to make changes to the selected interface.

Wireless Configuration (Site)

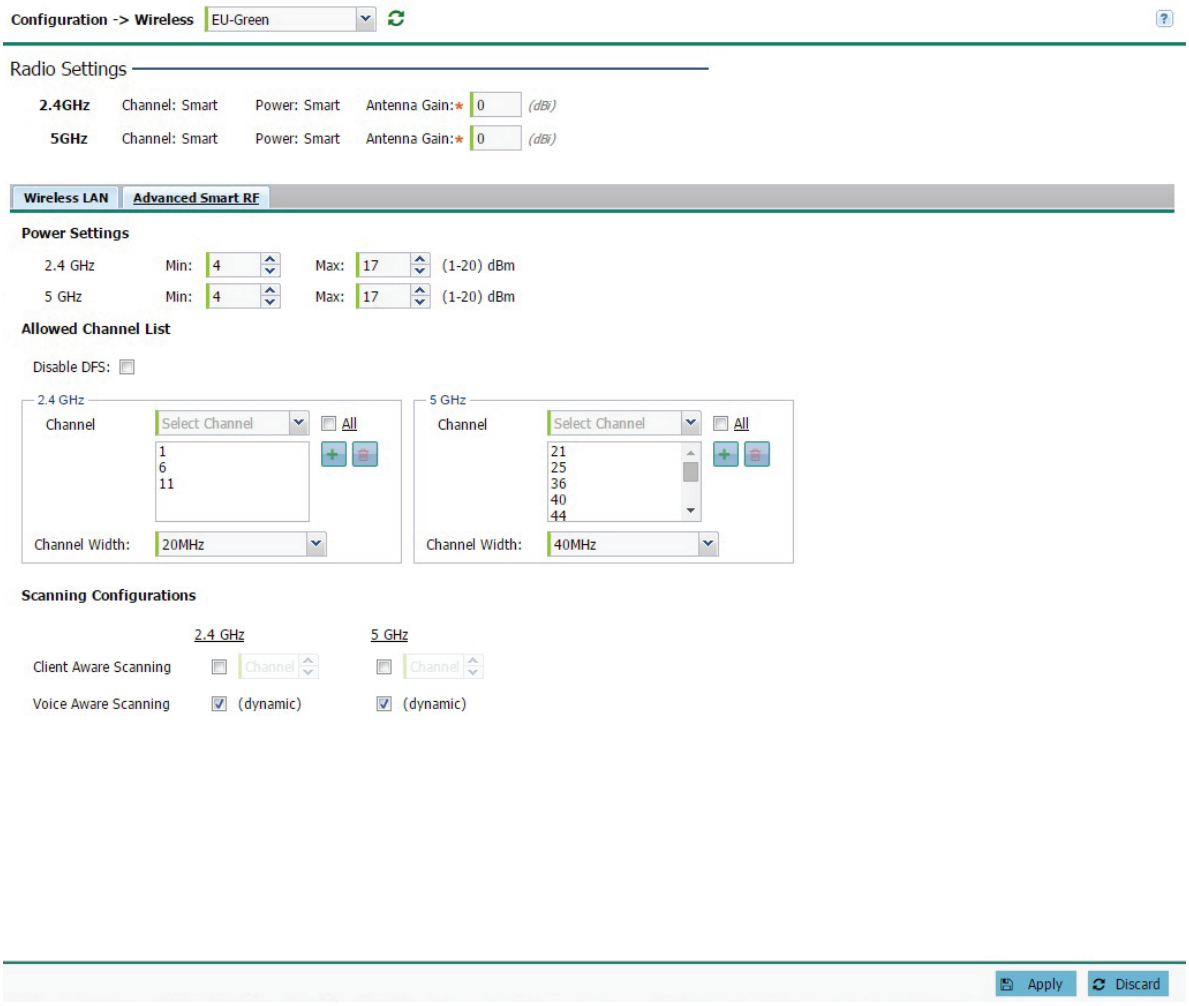
A *Wireless Local Area Network* (WLAN) is a data-communications system and wireless local area network that flexibly extends the functionalities of a wired LAN. A WLAN links two or more devices using spread-spectrum or OFDM modulation based technology. A WLAN does not require lining up devices for line-of-sight transmission, and are thus, desirable for wireless networking. Roaming users can be handed off from one WiNG 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 WiNG 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 WiNG Express Manager's connect Access Point's deployment objectives and the security needs of its connected clients.

To configure WLAN properties a WiNG 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 WiNG 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 **Smart** 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 *Smart* as the Power setting automatically configures radio power to not exceed the maximum power allowed by the defined country. For static power settings, the professional installer must ensure the configured power levels are compliant with local and regional regulations. The county selected automatically limits the maximum output power that can be set.
Gain	Set the antenna gain between 0.00 - 15.00 dBi. The Access Point's *Power Management Antenna Configuration File* (PMACF) automatically configures the radio transmit power based on antenna type, 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. The default value is 0.00. For external antenna model Access Points, configure the Antenna Gain based on the antenna used in the deployment. The set gain value should include the antenna gain, along with any additional components, such as extension cables used between the Access Point and the antenna.

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 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	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. The screen displays with the *Open* option selected. Naming and saving such a policy (as is) would provide no security and might only make sense in a network wherein no sensitive data is either transmitted or received. This default setting is not recommended. If selecting *Secure-PSK,* 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. If selecting *Secure-802.1x*, 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. Selecting *Guest* displays fields for captive portal Web page creation.
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 *Edit* to change the settings of the selected WLAN.

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 WiNG 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.

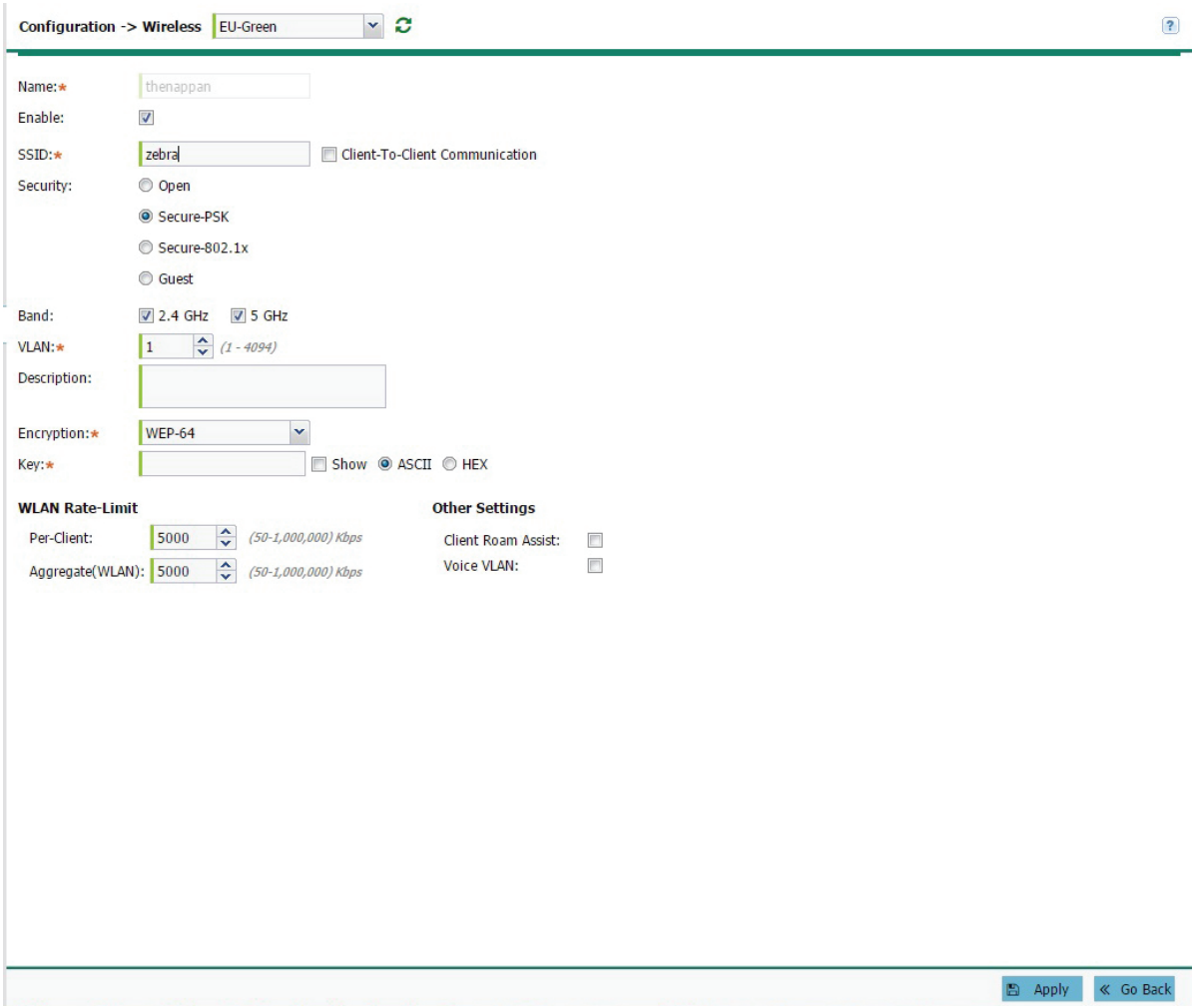
WLANs are mapped to radios on each connected Access Point. A WLAN can be advertised from a single Access Point radio or can span multiple Access Points and radios. WLAN configurations can be defined to only provided service to specific areas of a site. For example, a guest access WLAN may only be mapped 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 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	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. The screen displays with the *Open* option selected. Naming and saving such a policy (as is) would provide no security and might only make sense in a network wherein no sensitive data is either transmitted or received. This default setting is not recommended. If selecting *Secure-PSK,* select an encryption type for the WLAN. Define whether the key is entered in ASCII or HEX characters. Selecting *Show* to expose the key is not recommended. If selecting *Secure-802.1x*, 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. Selecting *Guest* displays fields for captive portal Web page creation, and is beyond the scope of this basic WiNG Express Access Point configuration.
Band	Select a band, *2.4Ghz or 5Ghz* (if supported), to enable operation of that band on the WLAN.
VLAN	Use the spinner control to specify a VLAN from 1 - 4,094 for this WLAN. When a client associates with a WLAN, the client is assigned a VLAN by load balance distribution. Do not use VLAN 1 with the WLAN if the WAN port has been enabled.
Description	Optionally, enter descriptive text which can be used by administrators to help identify each WLAN.

Encryption (Secure-PSK only)	When Secure-PSK security is selected, use the drop-down menu to select an encryption type. Available encryption types are: *WEP-64 - Wired Equivalent Privacy* (WEP) is a security protocol specified in the IEEE *Wireless Fidelity* (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 *initialization vector* (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. *WEP-128 - Wired Equivalent Privacy* (WEP) is a security protocol specified in the IEEE *Wireless Fidelity* (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 128 uses a 104 bit key which is concatenated with a 24-bit *initialization vector* (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. *TKIP-CCMP* - CCMP is a security standard used by the *Advanced Encryption Standard* (AES). AES serves the same function TKIP does for WPA-TKIP. CCMP computes a *Message Integrity Check* (MIC) using the proven *Cipher Block Chaining* (CBC) technique. Changing just one bit in a message produces a totally different result. The encryption method is *Temporal Key Integrity Protocol* (TKIP). 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. *WPA2-CCMP* - WPA2 is a 802.11i standard that provides even stronger wireless security than *Wi-Fi Protected Access* (WPA) and WEP. CCMP is the security standard used by the *Advanced Encryption Standard* (AES). AES serves the same function TKIP does for WPA-TKIP. CCMP computes a *Message Integrity Check* (MIC) using the proven *Cipher Block Chaining* (CBC) technique. Changing just one bit in a message produces a totally different result. WPA2/CCMP is based on the concept of a *Robust Security Network* (RSN), 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.

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 *Generate* 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.

4 In the **WLAN Rate Limit** section configure the following settings:

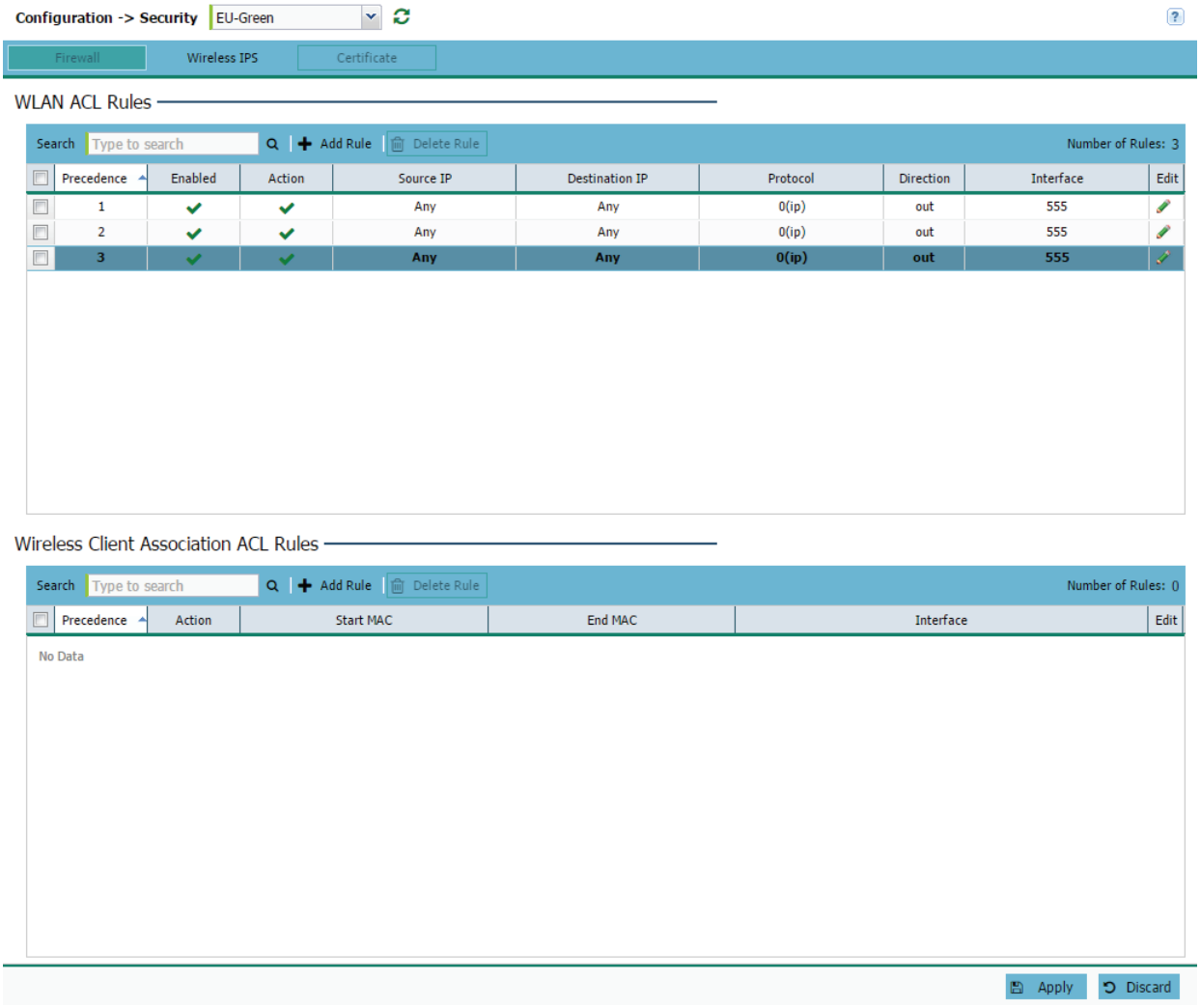
Enable (Per-Client)	Select this option to enable WLAN Rate limiting on a per client basis. Once enabled configure the value in the per-client field.
Per-Client	If per-client WLAN rate limiting is enabled use the spinner controls to configure the per-client data rate limit between 50 to 1,000,000 kbps. 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.

5 In the **Other Settings** section configure the following settings:

Client Roam Assist	Select this option to enable client roam assist. By monitoring a client's packets and the *received signal strength indicator* (RSSI) of a given client 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 a WiNG Express Manager connected Access Point, an administrator should not lose sight of the security solution in it's entirety, since the chain is as weak as its weakest link. WiNG Express Manager provides seamless data protection and user validation to protect and secure data at each vulnerable point in the network. WiNG 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.



A *firewall* is a mechanism enforcing network access control, and is considered a first line of defense in protecting proprietary information within the WiNG 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 WiNG 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 WiNG 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 will move down the table to reflect its lower priority.
Enabled	Select a firewall rule's *Enable* or *Disable* 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: *Deny* - Instructs the firewall stop a packet from its destination. *Permit* - 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 *tcp* or *udp* 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 *Low* and *High* numeric range settings. A source port cannot be a destination port.
Destination Port	If using either *tcp* or *udp* 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 *Low* and *High* 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 will move down the table to reflect its lower priority.
Action	Every IP firewall rule is made up of matching criteria rules. The action defines what to do with the packet if it matches the specified criteria. The following actions are supported: *Deny* - Instructs the firewall stop a packet from its destination. *Permit* - 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 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.

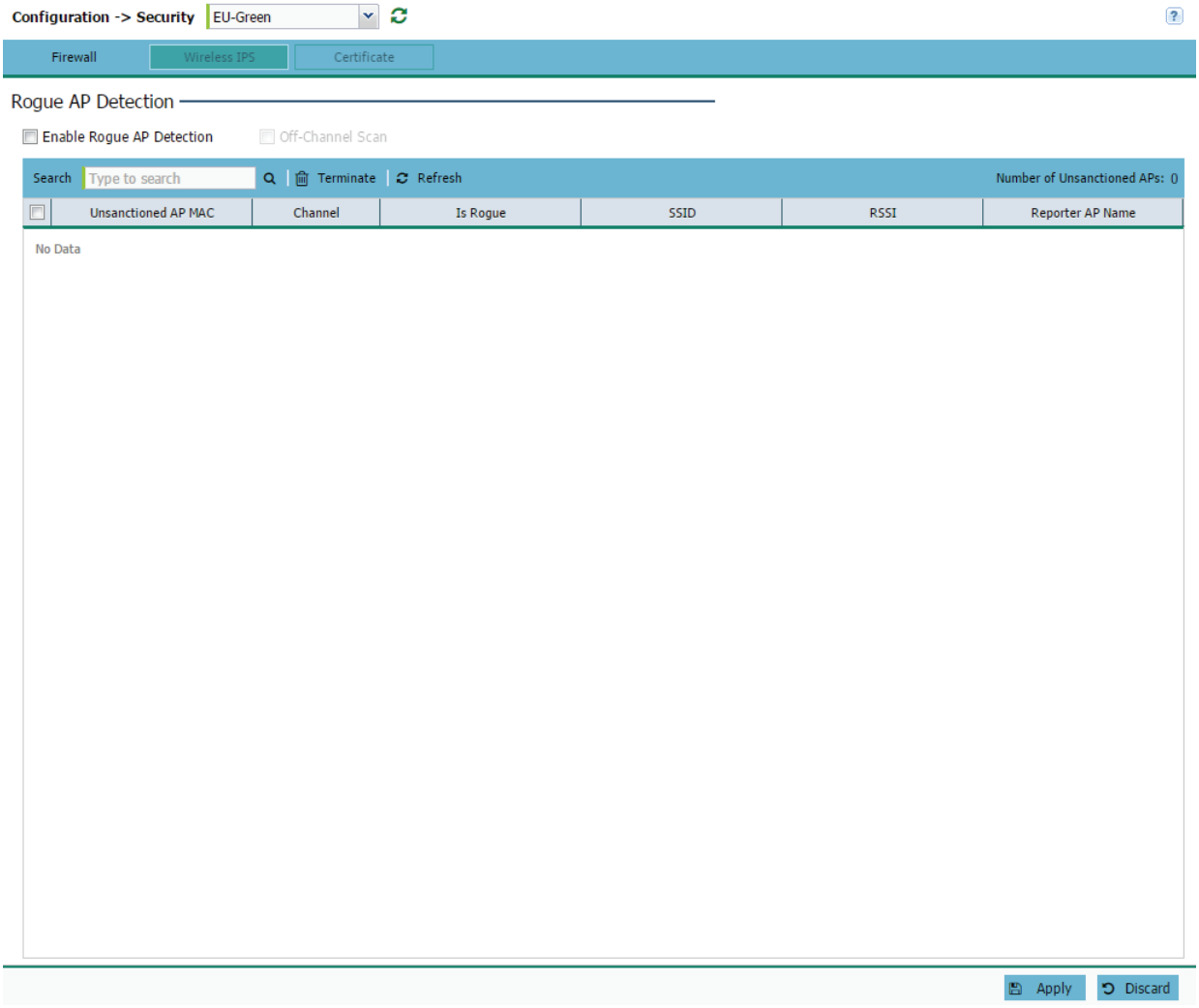
Unauthorized APs are untrusted Access Points connected to a LAN accepting client associations. They can be deployed for illegal wireless access to a corporate network, implanted with malicious intent by an attacker, or could just be misconfigured Access Points that do not adhere to corporate policies. 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 WiNG Express Manager) as a dedicated solution within a separate enclosure. When used within a WiNG 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.
- *Locationing* - Administrators can define the location of wireless clients as they move throughout a site. This allows for the removal of potential rogues though the identification and removal of their connected Access Points.
- *WEP Cloaking* - WEP Cloaking protects organizations using the *Wired Equivalent Privacy* (WEP) security standard to protect networks from common attempts used to crack encryption keys. There are several freeware WEP cracking tools available and 23 known attacks against the original 802.11 encryption standard; even 128-bit WEP keys take only minutes to crack. WEP Cloaking enables organizations to deploy WEP encrypted networks securely to preserve their existing investment in mobile devices.

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:

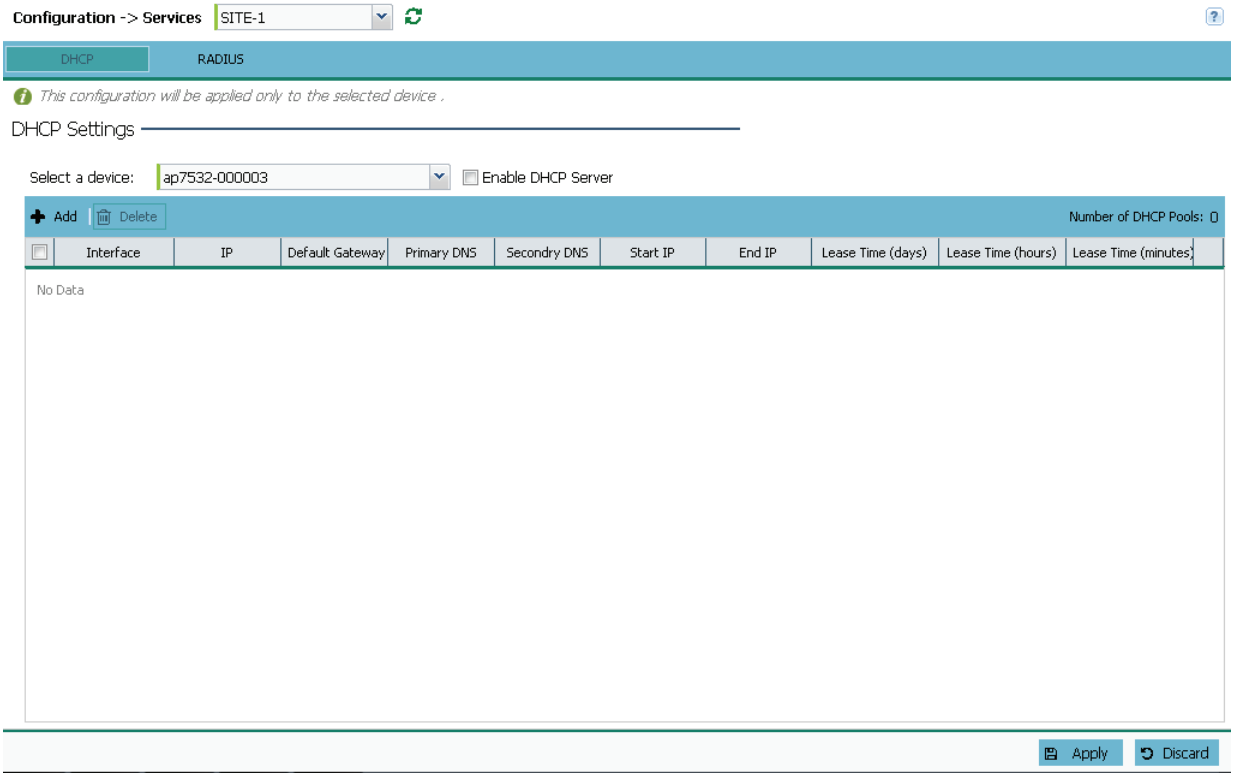
Unsanctioned AP MAC	Displays the hardware encoded MAC address of each listed Access Point. The MAC address is set at the factory and canot be modified via the management software.
Channel	Displays the channel where the unsanctioned AP was detected.
Is Rogue	Displays whether the detected device has been classified as a rogue device, whose detection threatens the interoperation of WiNG Express Manager connected devices.
SSID	Displays the *Service Set ID* (SSID) of the network to which the detected Access Point belongs.
RSSI	Displays the *Received Signal Strength Indicator* (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 *Media Access Control* (MAC) address of the Access Point reporting the listed WIPS event.

DHCP Configuration (Site)

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

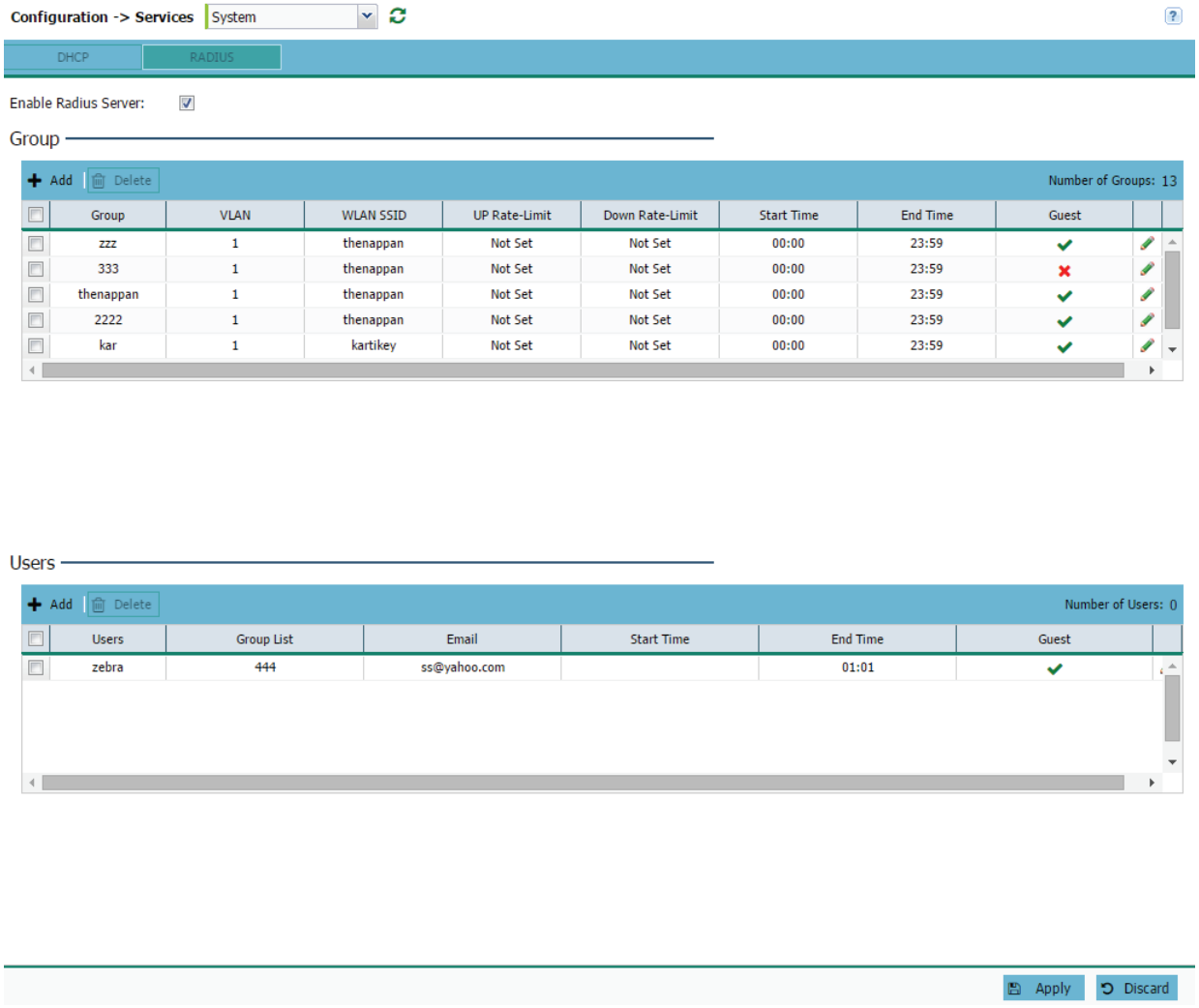
To view RADIUS configurations:

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).



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 WiNG Express Manager network (once authenticated by the local RADIUS server).
WLAN SSID	Displays the *Service Set ID* (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 desitned 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 starting 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.

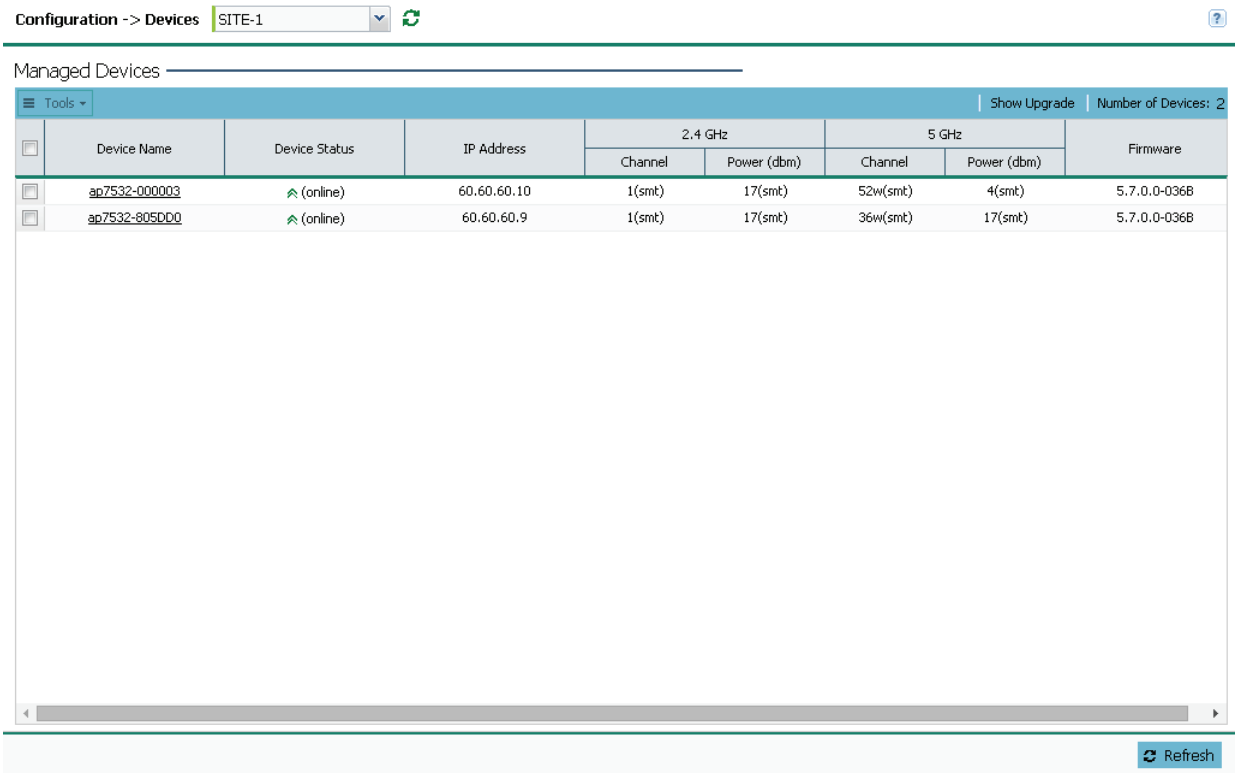
6 When adding or editing a RADIUS user, verify and configure the following:

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 pull-down menu to select which group to associate with the RADIUS user.
Email ID	Specify an E-mail address for the RADIUS user. This can be a local E-mail address or a fully qualified E-mail address.
Telephone	Specify the telephone number associated with the RADIUS user. This is an optional field.
Start Date / Start Time	Specify a 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 Til 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.**



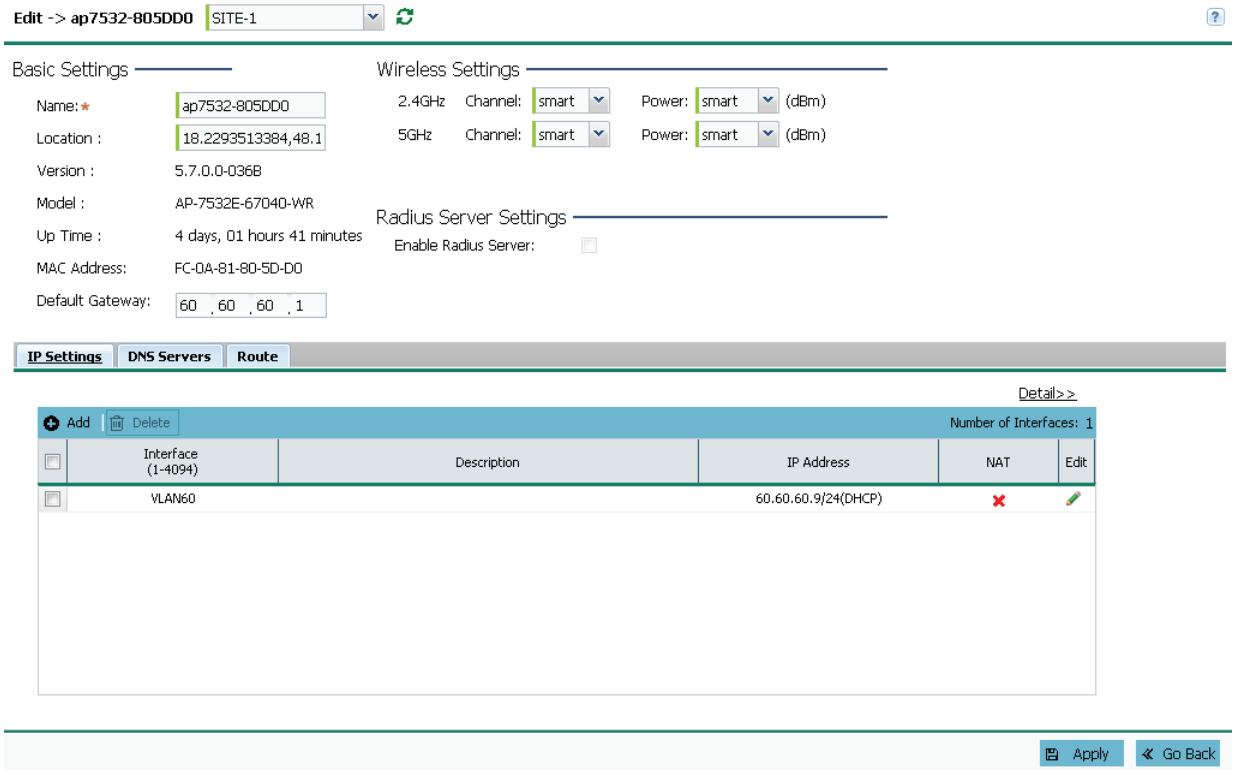
2 The **Managed Devices** table displays the following information about devices managed at the site level:

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 devices is not using a channel or status is unavailable, *N/A* will appear 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 devices is not using a channel or status is unavailable, *N/A* will appear instead of a channel number. If a device is using smart channel selection, *(smt)* will display 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)* will display after the power level.

Editing Devices Configuration (Site)

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

2 Select the **Device Name** to edit the device configuration.



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 will be used throughout the WiNG 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 *Days, Hours and Minutes* format.
Default Gateway	Specify the IP address of this default gatway 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 devices is not using a channel or status is unavailable, *N/A* will appear 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.

2.4 GHz Antenna Gain	Set the 2.4 GHz antenna between 0.00 - 15.00 dBm. The Access Point's Power *Management Antenna Configuration File* (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, *N/A* will appear instead of a channel number. If a device is using smart channel selection, *(smt)* will display 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)* will display after the power level.
5 GHz Antenna Gain	Set the 5 GHz antenna between 0.00 - 15.00 dBm. The Access Point's Power *Management Antenna Configuration File* (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.

Chapter 4

Troubleshoot

In This Chapter

Event History 87
Tools 89

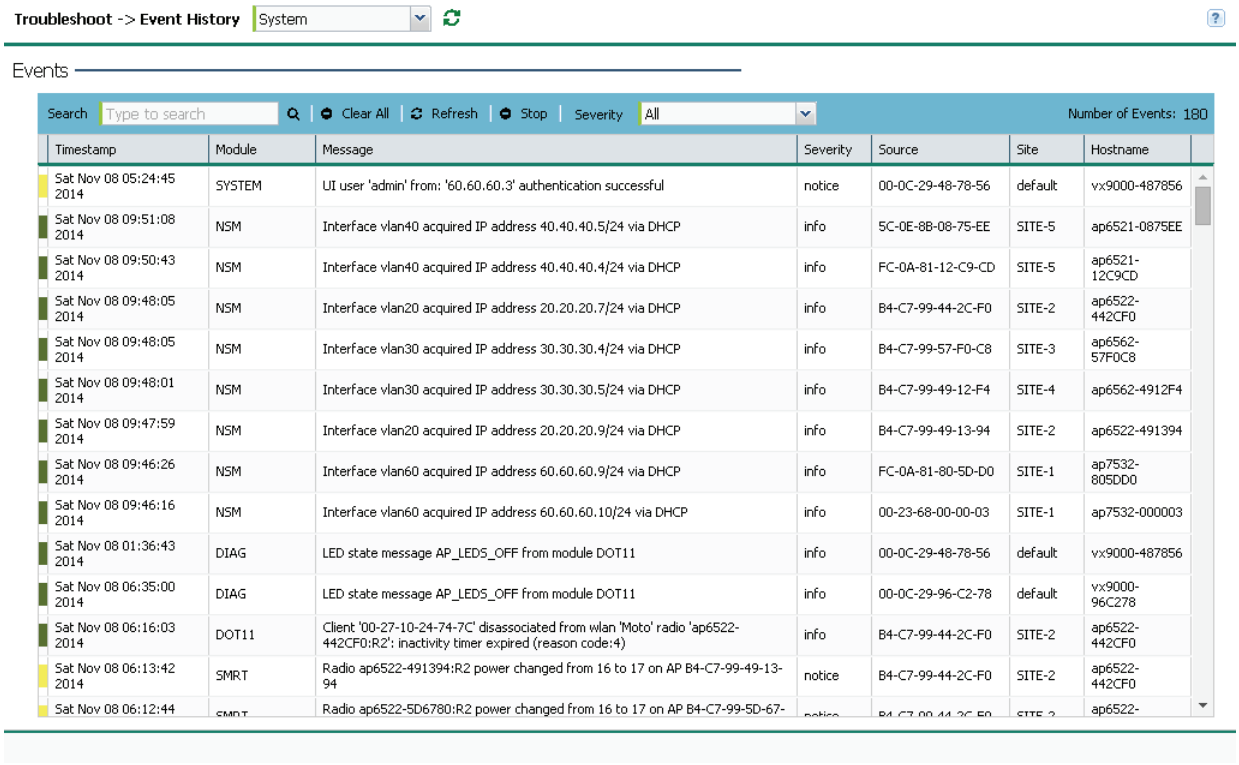
Event History

The **Event History** screen displays historical events for WiNG Express Manager connected devices. Events can be filtered by using criteria in the search field.

To review the WiNG Express event history:

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

2 Select **Event History**.



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	SMRT	Radio ap6522-5D6780:R2 power changed from 16 to 17 on AP B4-C7-99-5D-67-	notice	B4-C7-99-44-2C-F0	SITE-3	ap6522-

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	Displays the severity of the event as defined for tracking from the Configuration screen. Severity options include: *All Severities* – All events are displayed irrespective of their severity *Critical* – Only critical events are displayed *Error* – Only errors and above are displayed *Warning* – Only warnings and above are displayed *Informational* – Only informational and above events are displayed
Source	Displays the hardware encoded MAC address of the source device tracked by the selected module.

Hostname	Displays the administrator assigned name of the source device tracked by the listed module.

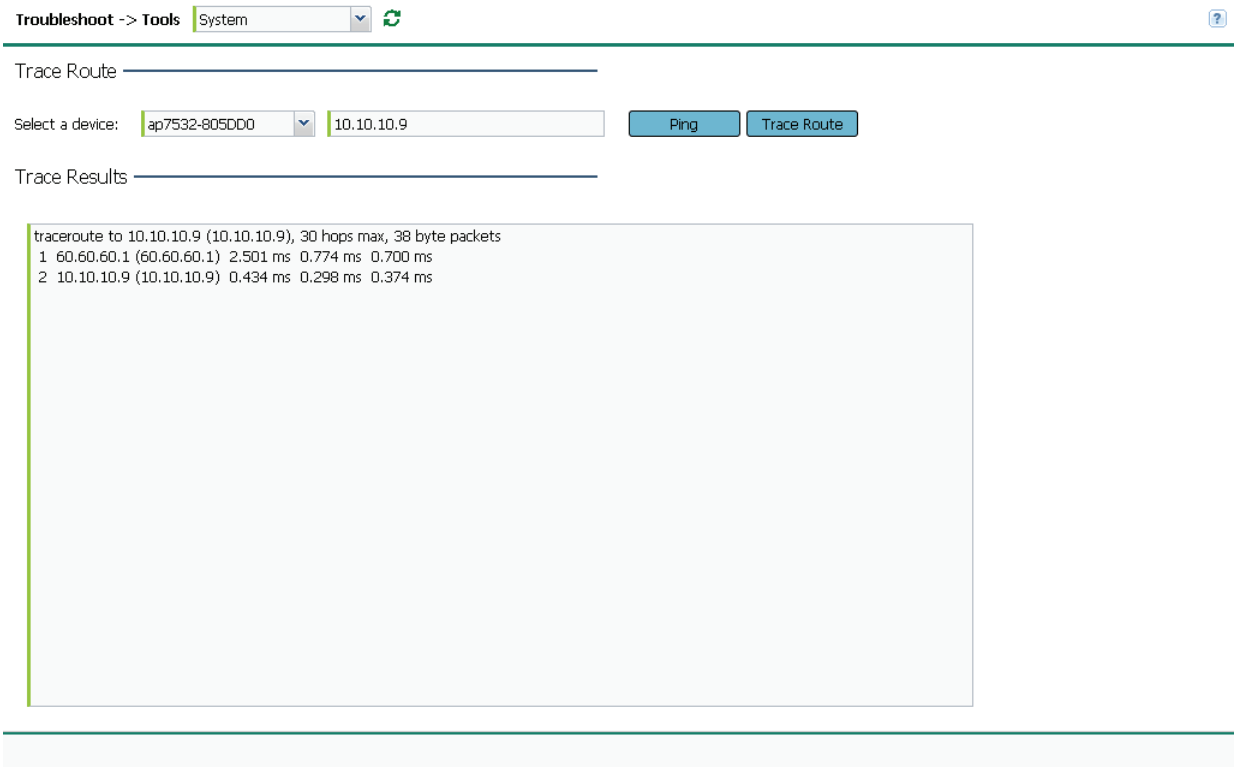
4 Use the **Search** field as necessary to refine event history to specific criteria.

Tools

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

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

2 Select **Tools**.



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.

Chapter 5
Support Center

If you have a problem with your equipment, contact support for your region.

Contact information is available at: http://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 e-mail, telephone, or fax 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

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

Manuals

http://www.zebra.com/support

MN001495A01 Revsion A

February 2015